

TABLE OF CONTENTS

EDITORIAL

ARTICLES

Use of Artificial Intelligence by Public Authorities for the Detection and Prevention of Cyberterrorism

Carlos Ramírez Castañeda

Convergence between transnational organized crime and contemporary terrorism in Latin America: the Ecuadorian case between pragmatism and utopia

Luis Miguel Hernández Flores, Cristian Fernando Hernández Flores, Carlos Eduardo Ortega Tapia and Miguel Iván Pazmiño Sotomayor

From Crime-Terror Convergence to Hybrid Violence: Drone Attacks in Latin America

Mauricio Heise and Cristian Rodríguez

Radicalization Through Images: Extremist Propaganda in IS's Dabiq Magazine

Jocelyn Vega Vargas and Dulce Sarai González González

BIBLIOGRAPHIC REVIEW

Islamic State, Media, and Propaganda: Performances of the 'Visual Caliphate'

Aarón Ferrando-Mkarbel

HISTORY OF TERRORISM

Terrorist organization: Provisional Irish Republican Army (PIRA)

The event: The Marrakech Attack, 24 August 1994

Ephemeris

DID YOU KNOW THAT...?

IN MEMORY OF THE VICTIMS

EDITORIAL POLICY

EDITORIAL BOARD

CARLOS IGUALADA

Director

JAVIER YAGÜE

Chief Editor

ANA AGUILERA

Deputy Editor

SCIENTIFIC COMMITTEE

Carmen Aguilera

Centre for Analysis of the Radical Right

Sergio Altuna

Real Instituto Elcano

Ignacio Álvarez-Ossorio

Complutense University

Rubén Arcos

Rey Juan Carlos University

Carlos Ardila

Escuela de Guerra de Colombia

Cristina Ariza

Tony Blair Institute of Global Change

Miguel Ángel Ballesteros

Departamento de Seguridad Nacional

Tamir Bar-On

Tec de Monterrey

Jose María Blanco

Autonoma University of Madrid

Alessandro Boncio

European Foundation for Democracy

Moussa Bourekba

Barcelona Centre for International Affairs

Alberto Bueno

Pablo Olavide University

Pilar Cebrián

Freelance Journalist

Álvaro Cremades

Complutense University

Luis de la Corte

Autonoma University of Madrid

Gustavo Díaz

Complutense University

Jesús Díez

Departamento de Seguridad Nacional

Gaizka Fernández

Centro Memorial de las Víctimas del Terrorismo

Carola García-Calvo

Real Instituto Elcano

Alexandra Gil

State Secretariat Government of Spain

Tore Hamming

International Centre for the Study of
Radicalisation

Thomas Hegghammer

Norwegian Defence Research Establishment

María Jiménez

Navarra University

Raúl López Romo

Centro Memorial de las Víctimas del Terrorismo

María Lozano

UNOCT

Francesco Marone

George Washington University

Manuel Moyano

Cordoba University

Diego Muro

St. Andrews University

Petter Nesser

Norwegian Defence Research Establishment

Matteo Re

Rey Juan Carlos University

Jerónimo Ríos

Complutense University

Agata Serranò

Complutense University

Louie Dean Valencia

Texas University

Aaron Zelin

Washington Institute for Near East Policy

REVISTA INTERNACIONAL DE ESTUDIOS SOBRE TERRORISMO

Online academic journal published three times yearly.
International Observatory for Terrorism Studies (OIET).
Collective of Victims of Terrorism, San Sebastian, Spain

ISSN 2660-9673

<https://rietjournal.org/>

@RIET_revista



This work is licensed under Creative Commons International Attribution 4.0 License



INDEX

5	EDITORIAL
	ARTICLES
7	Use of Artificial Intelligence by Public Authorities for the Detection and Prevention of Cyberterrorism Carlos Ramírez Castañeda
30	Convergence between transnational organized crime and contemporary terrorism in Latin America: the Ecuadorian case between pragmatism and utopia Luis Miguel Hernández Flores, Cristian Fernando Hernández Flores, Carlos Eduardo Ortega Tapia and Miguel Iván Pazmiño Sotomayor
50	From Crime-Terror Convergence to Hybrid Violence: Drone Attacks in Latin America Mauricio Heise and Cristian Rodríguez
69	Radicalization Through Images: Extremist Propaganda in IS's Dabiq Magazine Jocelyn Vega Vargas and Dulce Sarai González González
	BIBLIOGRAPHIC REVIEW
88	<i>Islamic State, Media, and Propaganda: Performances of the 'Visual Caliphate'</i> Aarón Ferrando-Mkarbel
	HISTORY OF TERRORISM
92	Terrorist Organization: Provisional Irish Republican Army (PIRA)
93	The event: The Marrakech Attack, 24 August 1994
100	Ephemeris
101	DID YOU KNOW THAT...?
102	IN MEMORY OF THE VICTIMS
109	EDITORIAL POLICY

EDITORIAL

On 11 September the twenty-fifth anniversary was marked of the attacks that irreversibly transformed contemporary international security. On that fateful morning in 2001, nineteen terrorists linked to Al-Qaeda hijacked four commercial airliners: two were flown into the Twin Towers of the World Trade Center, a third into the Pentagon, and the fourth crashed in Pennsylvania after passengers and crew confronted the hijackers. The attacks caused 2.977 fatalities and placed jihadist terrorism at the center of the international agenda. A quarter of a century later, 9/11 continues to constitute a turning point for understanding the evolution of terrorism, the response of states, and the transformation of security policies. Its legacy projects onto the intervention in Afghanistan, the expansion of counter-terrorist cooperation, the strengthening of intelligence services and border controls, as well as onto debates that remain current concerning the balance between security and liberties. The commemoration of this anniversary also acquires a generational dimension: a growing portion of the world's population now knows 9/11 solely as a historical event, which reinforces the importance of preserving its memory and explaining its consequences.

In this context, the present issue of the *Revista Internacional de Estudios sobre Terrorismo* once again approaches the terrorist phenomenon from diverse perspectives, combining academic research, historical analysis, the study of new threats, and the memory of victims. The plurality of approaches brought together by the publication makes it possible to observe both the evolution of terrorist organizations and their repertoires of action, and the changes experienced by prevention and response policies over recent decades.

As regards the academic content, in the first of the articles Carlos Ramírez analyses the use of artificial intelligence by public authorities for the detection and prevention of cyberterrorism, paying special attention to the balance between the effectiveness of these tools and the legal guarantees necessary to protect fundamental rights. Next, four Ecuadorian authors with extensive experience in the security forces examine the functional convergence between transnational organized crime and the instrumental use of terror in Latin America, taking Ecuador as an especially illustrative case of the transformation of criminal violence, coercive governance, and the limits of state responses. For their part, Mauricio Heise and Cristian Rodríguez study the employment of unmanned aerial systems by non-state actors in Colombia, Mexico, and Brazil, showing how drones are incorporated into

repertoires of surveillance, attack, and territorial control within scenarios of hybrid violence. Jocelyn Vega and Dulce Sarai González analyze, through a qualitative analysis of visual frames, the role of images in Islamic State propaganda on the basis of a study of the fifteen issues of the magazine *Dabiq*. The academic section is completed by the review prepared by Aarón Ferrando-Mkarbel of Islamic State, Media, and Propaganda: Performances of the ‘Visual Caliphate’, a work by Moign Khawaja and Christian Kaunert that analyses how Islamic State used especially its audiovisual production to project before different audiences an image of statehood, governing capacity, territorial control, and power.

With respect to the sections of a more popularizing character, the selected historical event is the attack committed on 24 August 1994 against the Atlas Asni hotel in Marrakech. The attack, in which two Spanish tourists, Salvador Torras and Antonia Cuevas, were murdered, became an especially significant episode in the evolution of jihadist terrorism in the Maghreb and anticipated the growing transnational dimension of radical networks connected with the Algerian context of those years. The terrorist organization addressed in this issue is the Provisional Irish Republican Army (PIRA), protagonist for decades of an armed campaign linked to the Northern Ireland conflict and an indispensable actor for understanding both the evolution of European ethno-nationalist terrorism and the complex process that culminated in the peace agreements of the late 1990s. For its part, the section “Did you know...?” once again gathers various episodes that make it possible to approach the history of terrorism and counter-terrorism through concrete facts. Among them is recalled Richard Reid’s attempt in December 2001 to detonate explosives concealed in his footwear during a flight between Paris and Miami, an episode that would end up influencing airport-control procedures.

Following the habitual closing of RIET, the section dedicated to the victims of terrorism, prepared by Inés Gaviria and under the sponsorship of the Centro Memorial para las Víctimas del Terrorismo, is entitled “The ‘Traitors’ of ETA”. The text recovers the stories of María Dolores González Katarain, Yoyes; Miguel Francisco Solaun Angulo, Mikel; Eduardo Moreno Bergaretxe, Pertur; and Juan María Jáuregui Apalategui, different trajectories united by having known ETA from within and having represented, in distinct ways, rupture, disagreement, or the rejection of violence. Their remembrance makes it possible to show an especially revealing dimension of the organisation’s totalitarian logic: the conversion of former members or dissidents into enemies to be punished, while at the same time recalling that recognising their status as victims does not require erasing or simplifying their prior responsibilities or biographies.

Having briefly presented the content of this new issue of RIET, we invite the reader to continue with its reading. Twenty-five years after 9/11, studying terrorism continues to require the combination of memory, rigorous research, and the capacity to interpret its transformations. We thank, as always, the contribution of authors, reviewers, and collaborators who make possible the publication of a new issue of the Revista Internacional de Estudios sobre Terrorismo.

Carlos Ramírez Castañeda

Use of Artificial Intelligence by Public Authorities for the Detection and Prevention of Cyberterrorism

Abstract

The use of artificial intelligence by public authorities to detect and prevent risks associated with cyberterrorism raises a central tension between institutional effectiveness and constitutional limits. These tools make it possible to process large volumes of information, identify anomalies, and protect critical infrastructure, yet their legitimacy cannot be measured solely by their operational usefulness. In a democratic state governed by the rule of law, algorithmic prevention requires a sufficient legal basis, a legitimate aim, proportionality, personal data protection, non-discrimination, meaningful human oversight, traceability, and judicial control. This article develops a legal-documentary and comparative analysis of the use of artificial intelligence systems in early detection, risk assessment, and cyberterrorism prevention. It examines the Budapest Convention, the UNESCO and OECD recommendations, the NIST AI Risk Management Framework and Regulation (EU) 2024/1689, together with the experience of ENISA and CISA, the United Nations frameworks on artificial intelligence and counter-terrorism, and three judicial decisions that have subjected algorithmic risk systems to review. It concludes that artificial intelligence can only be legitimately employed when it is embedded in a guarantee-based architecture of legality, auditing, accountability, and effective review.

Keywords: artificial intelligence; cyberterrorism; public authorities; fundamental rights; cybersecurity; algorithmic governance; critical infrastructure

Carlos Ramírez Castañeda, PhD in Public Administration and Public Policy, Postdoctoral Fellow in Law. National Open and Distance University of Mexico (UnADM).

Received
05/18/2026

To cite this article: Ramírez, C. (2026), Use of Artificial Intelligence by Public Authorities for the Detection and Prevention of Cyberterrorism, *Revista Internacional de Estudios sobre Terrorismo*, issue 18:7-29.

Accepted
08/24/2026

1. Introduction

Artificial intelligence has become one of the most relevant tools in the digital transformation of the public sector. Its incorporation into state functions has generated expectations of efficiency, anticipation, and optimization in areas as diverse as health, administration, justice, security, and the management of critical infrastructures. In the field of cybersecurity, these expectations intensify, since AI offers capacities for mass processing, anomaly detection, incident classification, and decision-support in scenarios characterized by speed, complexity, and uncertainty.

When these capacities are oriented toward the detection and prevention of cyberterrorism, the debate acquires a singular legal density. The question is no longer solely whether the technology can improve the State's response, but whether its use by public authorities is compatible with the principle of legality, fundamental rights, and the material limits of preventive power. In this context, AI stands at the intersection of two constitutional requirements: on the one hand, the State's obligation to protect the population and ensure the continuity of essential services; on the other, the necessity that every public intervention remain subject to democratic control and to the guarantees proper to the rule of law.

The difficulty increases owing to the conceptual instability of cyberterrorism itself. It is a category frequently employed in an expansive manner, mixing attacks on critical infrastructure, sabotage, online extremist propaganda, coordinated campaigns of digital intimidation, and other manifestations of technological criminality. As Macdonald et al. (2022) note, the academic community has not reached a definitive consensus on the constitutive elements of cyberterrorism, which hinders its normative treatment and its distinction from related figures such as hacktivism, digital espionage, or cyberwarfare. This conceptual breadth is legally problematic, for it may lead both to the banalization of the term and to excessive state responses. For this reason, a serious analysis of the use of AI by authorities must begin with a careful delimitation of the preventive object.

The study is situated within a doctrinal debate that has gained density in recent years. The literature on algorithmic governance has shown that automated risk-management systems are not mere auxiliary instruments but devices that reconfigure the very manner in which public power defines, measures, and anticipates danger (Yeung, 2018). In parallel, European and Ibero-American public law has begun to discuss the legal nature of the algorithms employed by the administration and the standard of legal authorization that their use requires (Boix Palop, 2020; Cotino Hueso, 2023). To this is added specific institutional production on artificial intelligence and counter-terrorism, driven by the United Nations, which warns of the risks of opacity, bias, and over-surveillance associated with these applications (UNOCT and UNICRI, 2021; OHCHR, 2025). The present work dialogues with that literature and seeks to contribute a reading situated in the Mexican legal order.

The purpose of the present article is to examine under what conditions the use of artificial intelligence by authorities to detect and prevent cyberterrorism may be considered legally legitimate.

The thesis advanced is that the validity of these tools does not derive from their technical utility alone. Their legitimacy depends on a rights-protective architecture based on legality, legitimate purpose, proportionality, data protection, meaningful human oversight, traceability, independent audit, and the existence of effective mechanisms of review and accountability.

2. Methodology

The research is qualitative, legal-documentary, and analytical-comparative. It is based on the review of specialized academic literature on cyberterrorism, artificial intelligence, public function, algorithmic governance, fundamental rights, and technological risk management. Likewise, relevant legal instruments and international frameworks of reference are examined in order to assess the use of AI in sensitive contexts of state prevention.

At the national level, the Political Constitution of the United Mexican States and the Federal Penal Code are taken as referents, with the aim of situating the discussion within the framework of the principles of legality, due process, human rights, and the prosecution of serious threats. At the international and comparative level, the following are reviewed: the United Nations Convention against Transnational Organized Crime, the Council of Europe Convention on Cybercrime, the UNESCO Recommendation on the Ethics of Artificial Intelligence, the OECD Council Recommendation on Artificial Intelligence, the NIST AI Risk Management Framework, and Regulation (EU) 2024/1689 of the European Parliament and of the Council.

The comparative approach does not seek to transfer foreign solutions mechanically to the Mexican context. Rather, it aims to identify functional principles and normative standards that make it possible to evaluate the lawfulness of the state use of algorithmic systems in preventive tasks. To this end, the analysis is organized around five variables: legitimate purpose, sufficient normative basis, intensity of impact on fundamental rights, level of autonomy of the system, and existence of ex ante, concurrent, and ex post controls.

Alongside the normative analysis, the work incorporates three judicial decisions that have subjected to review algorithmic risk-assessment systems deployed by public authorities. Their selection responds to three criteria: that the system examined had been operated by a public power for preventive or security purposes; that the decision had expressly addressed the sufficiency of the legal authorization or the guarantees against automated processing; and that the pronouncement had come from a judicial body whose doctrine is transferable, as an argumentative standard, to the constitutional examination proper to the Mexican legal order. These decisions do not operate as binding precedents, but as cases that make it possible to observe how the five indicated variables are applied in real litigation scenarios.

From an epistemological standpoint, the research adopts a critical legal approach that recognizes that law is not neutral in the face of technology. As Danaher et al. (2017) point out, legal institutions

tend to lag behind technological development, and that gap may generate normative voids with direct consequences for the protection of rights. For this reason, the analysis is not limited to describing the current state of regulation but evaluates its sufficiency and formulates proposals for improvement oriented toward guaranteeing the legitimate exercise of the State's preventive power.

3. Cyberterrorism and Algorithmic Prevention: Necessary Clarifications

3.1. *Definition and Delimitation of Cyberterrorism*

The category of cyberterrorism requires careful delimitation. Not every high-impact computer incident can be classified as such, nor does every criminal activity in cyberspace entail the purpose of collective intimidation or institutional destabilization proper to terrorism. The decisive criterion is found not in the digital medium employed, but in the purpose pursued and in the nature of the interests affected.

Specialized literature has insisted that cyberterrorism involves the use of digital means with the objective of instilling fear, coercing authorities, or altering essential functions of the State or of social life (Denning, 2000; Conway, 2017; Mayer Lux, 2018). Denning (2000) defined cyberterrorism as unlawful attacks and threats of attack against computers, networks, and the information stored therein when carried out to intimidate or coerce a government or its population in the pursuit of political or social objectives. This definition, pioneering in the field, continues to be an obligatory reference in the specialized literature, although it has been the object of subsequent refinements.

Macdonald et al. (2022) conducted a survey of specialist terrorism researchers and found that there is broad consensus on the need to distinguish cyberterrorism from ordinary cybercrime and from hacktivism on the basis of the intentional element: while the first seeks to generate terror or political destabilization, the second pursues economic gains or the temporary interruption of services, and the third has protest motivations without necessarily producing damage of the magnitude proper to terrorism. This distinction has first-order legal implications, for it determines the applicable regime, the procedural guarantees required, and the proportionality of preventive measures.

For their part, Venkatachary et al. (2024) analyze the specific challenges that cyberterrorism poses for critical infrastructures in the energy sector, identifying differentiated attack vectors, applicable cybersecurity frameworks, and economic dimensions of the problem. Their analysis confirms that attacks on essential infrastructures may produce cascading effects with consequences for public security, health, and the continuity of the State, which justifies a high-intensity preventive response, albeit subject to strict legal conditions.

The UNODC, in its educational module on cybercrime (n.d.), distinguishes among hacktivism, terrorism, espionage, disinformation, and cyberwarfare as analytically separate categories, each with its own characteristics regarding actors, motivations, targets, and legal consequences. This taxonomy

is useful because it demonstrates that algorithmic prevention cannot operate with undifferentiated categories: the system must be designed to detect legally typified conduct, not to track generically “suspicious activities” without precise normative contours.

3.2. Algorithmic Prevention: Technical and Legal Characterization

In parallel, algorithmic prevention may be understood as the use of computational systems capable of identifying patterns, inferring risks, classifying events, or prioritizing alerts in order to orient institutional response. In public cybersecurity contexts, such prevention may manifest itself in anomaly-detection systems in networks, incident-correlation tools, automated analysis of indicators of compromise, or natural-language processing of open sources. From a technical perspective, AI systems applied to cybersecurity may be classified into various categories according to their function: machine-learning-based intrusion-detection systems (ML-IDS), threat-intelligence platforms (TIP), user-and-entity-behavior-analytics tools (UEBA), AI-enhanced security-information-and-event-management systems (SIEM), and natural-language models for the analysis of content in open sources (OSINT). Each type of system raises distinct legal constraints in terms of the data processed, the level of autonomy, and the potential impact on rights (European Union Agency for Cybersecurity, 2023; National Institute of Standards and Technology, 2023). It is also necessary to specify what type of algorithmic regulation is at stake. Yeung (2018) proposes distinguishing between reactive systems, which respond to already verified behaviors, and preventive or anticipatory systems, which act upon inferences about future conduct, and warns that the latter concentrate the most serious problems of legitimacy, since they intervene before a legally relevant fact exists. The detection of cyberterrorism is situated precisely within this second group. Hence the examination cannot be limited to the statistical reliability of the model: what is under discussion is the lawfulness of anticipating legal consequences on the basis of a calculated probability. The legal complexity increases, however, when these systems cease to be simple technical supports and begin to influence institutional decisions concerning surveillance, risk prioritization, or the opening of lines of investigation. The difference between operational support and the structuring of preventive judgment is central. In the first case, the system may serve to strengthen the resilience of networks or infrastructures. In the second, AI begins to affect rights, privacy expectations, monitoring patterns, or administrative and criminal processes directly. Regulation (EU) 2024/1689, known as the Artificial Intelligence Act, establishes precisely this distinction as a criterion for risk classification. AI systems used by authorities for law enforcement, risk assessment, or the identification of suspects are considered high-risk and are subject to reinforced obligations of transparency, documentation, human oversight, and conformity assessment prior to deployment. This normative categorization confirms that European law already recognizes that not all uses of AI in the public sphere are equivalent and that regulatory intensity must be graduated according to the potential impact on fundamental rights. Consequently, the legal discussion should not focus solely on the technical sophistication of the model, but on the institutional place it occupies within state action.

4. Legal Risks of the Use of AI by Public Authorities

4.1. *Insufficient Normative Basis*

The first legal risk is the insufficiency of the normative basis. No public authority can justify the intensive use of AI in preventive functions on the basis of generic clauses of security or administrative modernization. The principle of legality requires a clear authorization regarding purposes, competent authorities, categories of data, temporal limits, activation scenarios, and oversight mechanisms. Without a sufficient normative basis, the technological tool ends up substituting for the norm and blurring the guarantee of foreseeability.

Administrative-law doctrine has offered a path for specifying this requirement. Boix Palop (2020) maintains that the algorithms employed by the administration to adopt decisions fulfill a function materially equivalent to that of a regulation, insofar as they regulate and predetermine the action of public power and should therefore be subject to the guarantees of publicity, participation, and control already provided for regulatory norms. Cotino Hueso (2023), examining biometric-identification systems, emphasizes that the overlap between artificial-intelligence regulation and data-protection regulation does not dispense with a specific and high-quality legal authorization, and that the standards demanded by various European constitutional courts are rarely satisfied in administrative practice. Both approaches converge on a point relevant to this work: the reservation of law is not exhausted by the existence of a norm that mentions the technology; rather, it demands normative density concerning its design, its limits, and its controls.

The European Court of Human Rights has developed in its case-law the doctrine of the “quality of the law” as a condition for interferences with fundamental rights to be compatible with the European Convention. According to this doctrine, the enabling law must not only exist but be accessible, foreseeable, and endowed with adequate safeguards against abuse. Although this case-law is not directly binding on Mexico, it offers a useful standard for evaluating the sufficiency of normative authorizations in matters of surveillance and algorithmic prevention.

In the Latin American context, the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights has alerted to the risks of digital surveillance without clear legal authorization, noting that the interception of communications and the mass processing of data by the State require specific normative frameworks that establish with precision the scenarios, the competent authorities, and the control mechanisms. Although its pronouncements refer primarily to the surveillance of communications, the principles they develop are fully applicable to algorithmic systems for the detection of cyberterrorism.

4.2. *Protection of Personal Data*

A second risk lies in the protection of personal data. The preventive logic tends to favor the accumulation of information under the premise that more data improve detection capacity. That assumption, however, must be subjected to the principles of minimization, specific purpose, proportionality, accuracy, and security. Mass and indiscriminate collection is not only legally problematic but also technically questionable, for it may increase informational noise and produce erroneous or excessive inferences.

In Mexico, the General Law on the Protection of Personal Data Held by Obligated Subjects establishes guiding principles applicable to the processing of data by public authorities, including lawfulness, purpose, loyalty, proportionality, and accountability. Nevertheless, the law contains no specific provisions on the processing of data in algorithmic systems of public security, thereby maintaining a zone of normative insufficiency that future regulation will have to address.

UNESCO (2021), in its Recommendation on the Ethics of AI, pays special attention to the protection of privacy and personal data as a necessary condition for the ethical development and deployment of AI systems. The Recommendation establishes that AI systems must not be used to infringe the right to privacy, which includes control over personal data and protection against arbitrary or unlawful surveillance. These principles are directly applicable to the design of algorithmic systems for the detection of cyberterrorism by public authorities.

4.3. *Bias, Discrimination, and Epistemic Validity*

In the third place, the problem of bias and discrimination must be considered. Algorithmic systems learn from data, design decisions, and institutional contexts. If those elements are marked by asymmetries, errors, or logics of over-surveillance, the tool may reproduce or amplify such distortions. In the field of cyberterrorism prevention this is especially serious, since an erroneous classification may activate enhanced surveillance, affect reputations, or generate disproportionate treatments before effective judicial control exists.

Specialized literature has extensively documented the risks of bias in AI systems used in security contexts. Studies such as those of Obermeyer et al. (2019) have demonstrated that algorithms employed in public decision-making may encode and amplify racial, socioeconomic, or gender biases present in training data. In the specific domain of security, biases may translate into the over-surveillance of particular communities, generating a disproportionate impact on persons and groups already in situations of vulnerability. This dynamic is incompatible with the principle of equality and non-discrimination, enshrined in Article 1 of the Political Constitution of the United Mexican States and Article 24 of the American Convention on Human Rights.

The NIST AI Risk Management Framework (2023) addresses the problem of bias as a systemic risk that must be managed at all stages of the system life-cycle: design, development, validation, deployment, and continuous monitoring. The framework proposes mechanisms for fairness evaluation, adversarial testing, and feedback mechanisms to detect and correct biases, underscoring that bias management is not a one-time event but a permanent process. This perspective is especially relevant for cyberterrorism-detection systems, where the dynamics of threats change constantly and training data may rapidly become obsolete or biased.

4.4. Opacity and the Demand for Explainability

A fourth risk is opacity. When the authority cannot sufficiently explain how the system operated, which data were relevant, or how the algorithmic recommendation was integrated into the final decision, the requirement of reasoned motivation is weakened and judicial control becomes precarious. For this reason, traceability and explainability are not desirable attributes in the abstract, but conditions of lawfulness.

The OECD (2023), in its revised Recommendation on AI, establishes that AI systems must be transparent and that operators must be able to explain their decisions and predictions to the extent reasonably possible. It further notes that AI agents should be able to provide sufficient information to help stakeholders understand the capabilities and limitations of the systems and to respond to the outcomes they produce. These explainability requirements are especially relevant in the context of the state use of AI, where decisions taken on the basis of algorithmic systems may affect fundamental rights and must be capable of effective judicial review.

Regulation (EU) 2024/1689 operationalizes these requirements through concrete obligations for high-risk systems, including the keeping of automatic logs, detailed technical documentation, the provision of instructions for use, and the obligation to design the system so that its outputs are interpretable by the natural persons responsible for its oversight. These obligations not only have instrumental value for judicial control but also contribute to building the institutional trust necessary for the legitimate deployment of AI in sensitive contexts.

Doctrine has nevertheless pointed to the limits of this model. Veale and Zuiderveen Borgesius (2021) warn that a substantial part of the transparency obligations of the European regime rests on mechanisms of self-assessment of conformity, so that compliance remains in the hands of the provider itself or of the deploying organization, with limited external oversight. This observation is especially pertinent in the security domain, where requirements of secrecy may be invoked to restrict access to technical documentation. If the explanation is reduced to an internal file inaccessible to the affected person and to the judge, the guarantee becomes nominal.

4.5. Public Responsibility and the Risk of Technocracy

Finally, there exists the risk of a weakening of public responsibility. The administration cannot shield itself behind the technical complexity of the system or the prestige of the provider in order to dilute its responsibility. If the technology influences a state action, legal imputation continues to correspond to the authority. Meaningful human oversight, in this sense, is also a requirement of democratic responsibility.

The risk of technocracy manifests itself when the technical complexity of algorithmic systems generates an informational asymmetry between technological operators and political and judicial decision-makers. This asymmetry may produce what doctrine terms “algorithmic deference”: the tendency of officials to accept without questioning the recommendations of automated systems, effectively delegating the decision to the algorithm. In contexts of cybersecurity and terrorism prevention, where operational urgency is high, this risk intensifies.

The OECD Recommendation on AI (2023) addresses this problem by requiring that AI systems be designed in such a way as to permit oversight, replacement, or reversal by human operators. UNESCO (2021) goes further by establishing that decisions that significantly affect the rights and freedoms of persons must be capable of being reviewed and, if necessary, corrected by human beings.

5. International and Comparative Referents

5.1. United Nations Convention against Transnational Organized Crime

The United Nations Convention against Transnational Organized Crime does not directly regulate artificial intelligence or cyberterrorism, yet it provides a valuable architecture for international cooperation against complex and cross-border phenomena. Its principal teaching is that the state response to organized risks cannot rest solely on technical tools, but on institutional coordination, information exchange, and capacity strengthening. The Convention establishes, in its Article 29, the obligation of States Parties to adopt, develop, or improve training programmes for their personnel, including training in investigative techniques compatible with human rights. This provision is relevant to the use of AI in the prevention of cyberterrorism, since it implies that any technological tool must be accompanied by adequate training that guarantees its use within the parameters of the rule of law.

5.2. Budapest Convention on Cybercrime

The Budapest Convention, for its part, offers an essential framework in matters of criminal cooperation and the preservation of digital evidence. Its relevance in this study lies in recalling that technological detection does not replace the lawfulness of the investigation. AI may contribute to identifying early signals or threat patterns, but any subsequent action must remain integrated into

procedures compatible with due process and with the rules governing the obtaining and preservation of evidence. The Budapest Convention, in its Chapter II, establishes specific provisions on procedural measures that States must adopt for the investigation of computer-related offences, including the expedited preservation of stored computer data, the expedited disclosure of preserved traffic data, and the interception of content data. These provisions must be understood as a minimum floor of guarantees that AI systems used in the detection of cyberterrorism cannot ignore.

5.3. UNESCO and OECD Ethical Frameworks

The UNESCO Recommendation on the Ethics of Artificial Intelligence and the OECD Recommendation on Artificial Intelligence provide principles directly useful for evaluating the state use of AI: respect for human rights, privacy, transparency, explainability, accountability, security, robustness, and human oversight. Both instruments show that the public sector, especially in sensitive domains such as security and justice, must operate with more demanding standards than purely private or experimental contexts.

UNESCO (2021) introduces the concept of “ethical impact assessment” as a prospective tool for identifying the possible effects of AI systems on human rights prior to their deployment. This tool is especially relevant for cyberterrorism-detection systems, given that the anticipation of effects on privacy, equality, and due process may contribute to designing systems more respectful of rights from the outset, incorporating what doctrine terms “privacy by design”.

The OECD (2023), for its part, has updated its Recommendation on AI to reinforce the principles of accountability and responsibility, noting that AI actors should be accountable for the proper implementation of AI-related principles. In the public-sector domain, this responsibility acquires a constitutional dimension, since the State does not act as merely another private agent, but as the holder of public power whose action is subject to the principles of legality, effectiveness, and service to the general interest.

5.4. NIST AI Risk Management Framework

The NIST AI Risk Management Framework adds an especially valuable operational approach: the continuous management of risk. The governance of AI should not be conceived as a one-time authorization, but as a permanent process of identification, assessment, mitigation, monitoring, and review. In preventive contexts, where risk and uncertainty change constantly, this logic is indispensable.

The NIST AI RMF 1.0 (2023) structures risk management into four principal functions: Govern, Map, Measure, and Manage. The Govern function establishes the policies, processes, procedures, and practices for the governance of AI risk. The Map function contextualizes the identified risks according to purpose and stakeholders. The Measure function analyzes, assesses, and monitors risks.

And the Manage function prioritizes risk responses and applies appropriate measures. This framework is directly applicable to the design of cyberterrorism-detection systems by authorities.

5.5. Regulation (EU) 2024/1689 and the Experience of ENISA

Regulation (EU) 2024/1689 confirms that the greater the sensitivity of the use environment and the greater the possibility of impact on fundamental rights, the denser the regulatory obligations must be. Its comparative value for the Mexican case does not lie in the automatic transposition of its content, but in the rationality that inspires it: public innovation is legitimate only when accompanied by reinforced obligations of documentation, oversight, evaluation, and accountability.

Regulation (EU) 2024/1689 classifies as high-risk systems, among others, AI systems used by competent authorities to perform individual assessments of the risk of crime and terrorism (Annex III). For these systems, the Regulation requires: the establishment of risk-management systems, data governance and management of training data, technical documentation, automatic event logging, transparency and information to users, human oversight, and levels of accuracy, robustness, and cybersecurity. This set of obligations constitutes the most advanced standard currently available for the legitimate use of AI in preventive public-security contexts.

The European Union Agency for Cybersecurity (ENISA) has published specific guidelines on the use of AI in cybersecurity, underscoring both the opportunities these technologies offer for incident detection and response and the risks inherent in AI itself, including specific vulnerabilities such as adversarial attacks, data poisoning, and model evasion. These technical risks have a direct legal dimension: a compromised or manipulated detection system may produce false negatives, allowing real threats to pass, or false positives, generating unjustified state interventions against innocent persons.

5.6. The Experience of CISA in the United States

The Cybersecurity and Infrastructure Security Agency (CISA) of the United States has developed an integral approach to the use of AI in the protection of critical infrastructures that offers relevant lessons from a comparative perspective. CISA has published guidelines on the responsible use of AI in the cybersecurity domain that establish principles of transparency, human oversight, privacy, and accountability.

CISA's experience illustrates the importance of distinguishing between defensive uses of AI (protection of one's own systems, intrusion detection, incident response) and offensive or surveillance uses (identification of actors, tracking of individuals, analysis of communications). While the former are less controversial from the standpoint of fundamental rights, the latter require additional legal guarantees and more robust oversight mechanisms.

5.7. United Nations Frameworks on Artificial Intelligence and Counter-Terrorism

The United Nations system has produced in recent years a body of work specifically oriented toward the relationship between artificial intelligence and terrorism prevention, which is directly applicable to the object of this study. The United Nations Office of Counter-Terrorism and UNICRI (2021) documented both the malicious use of these technologies by terrorist actors and their employment by state agencies for content detection and network analysis and concluded that technical capacity advances more rapidly than the frameworks of guarantees that should accompany it.

With greater legal density, the position paper of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (OHCHR, 2025) examines the risks these systems project onto equality and non-discrimination, privacy, freedom of expression, due process, and the right to an effective remedy. The document underscores that international human-rights obligations bind States independently of the degree of automation of the decision, and that the delegation of functions to private providers does not displace that responsibility. It constitutes a relevant referent for Mexico, insofar as it originates from a mechanism of the universal system itself whose interpretive doctrine bears upon the fulfilment of the conventional obligations assumed by the State.

6. Case Studies: Judicial Control of Algorithmic Prevention

The normative frameworks reviewed enunciate principles, but it is in the judicial forum that one observes how those principles operate in the face of concrete systems. The three cases examined below share a common feature: in each of them a public authority deployed an algorithmic risk-assessment system and a court verified whether the normative authorization and the associated guarantees proved sufficient. Their interest for the object of this work does not reside in the identity of the regulated phenomenon, but in the structure of the judicial reasoning applied.

6.1. The SyRI Case (Netherlands, 2020)

The District Court of The Hague decided, on 5 February 2020, the challenge to the *Systeem Risico Indicatie* (SyRI), a state tool that cross-referenced databases from different administrations to generate risk reports on persons allegedly linked to social-security fraud. The court declared that the enabling legislation was incompatible with Article 8(2) of the European Convention on Human Rights, as it failed to satisfy the test of necessity in a democratic society and the required balance between the purpose pursued and the interference with private life (Rechtbank Den Haag, 2020).

Three elements of the reasoning are transferable. The first is that the legitimacy of the aim—the fight against fraud—did not suffice to validate the means. The second is that the opacity of the risk model, whose indicators were not disclosed, prevented both public scrutiny and individual defense,

which the court assessed as an insufficiency of guarantees and not as a discretionary technical decision. The third is that persons included in the risk registers were not notified, so that they could neither know nor challenge their classification. Transposed to the domain of cyberterrorism, where requirements of secrecy are even more intense, this last point anticipates the central problem: if the affectation remains invisible to the affected person, the right to a remedy is emptied of content.

6.2. *The Ligue des droits humains Case (Court of Justice of the European Union, 2022)*

This pronouncement is the most directly pertinent, as it examines an automated processing system designed precisely to prevent terrorist offences. In its judgment of 21 June 2022, the Grand Chamber of the Court of Justice analyzed the validity of Directive (EU) 2016/681 on the use of passenger name record data and admitted its compatibility with the Charter of Fundamental Rights only under a strict interpretation, recognizing that the regime entails serious interferences with the rights to private life and to the protection of personal data (Court of Justice of the European Union, 2022). Two precisions of the ruling have the value of a standard. The first is the exclusion of machine-learning systems capable of modifying the evaluation criteria without human intervention or review: the Court reasoned that such a capacity for self-adaptation prevents both the human reviewer and the affected person from knowing the reasons for a positive match, thereby emptying supervision and judicial control of content. The second is the requirement that the pre-established evaluation criteria be specific, reliable and non-discriminatory, and that every match be the object of individual review by non-automated means before producing any effect. For the object of this work, the teaching is twofold. On the one hand, it confirms that the counter-terrorism purpose, even when it constitutes an objective of general interest of the first order, does not function as an open authorization for mass processing or for the technical autonomy of the system. On the other hand, it offers an operational criterion infrequently found in soft-law instruments: the opacity derived from self-learning is not an inconvenience that must be mitigated, but a reason to exclude that architecture from the domain of state prevention.

6.3. *The Bridges Case (United Kingdom, 2020)*

The Court of Appeal of England and Wales declared unlawful the use of live automated facial recognition by South Wales Police on three convergent grounds: the absence of a sufficient legal basis delimiting who could be included in the watchlists and where the system could be deployed; the insufficiency of the data-protection impact assessment; and the failure to fulfil the duty to assess whether the software presented biases on grounds of sex or ethnic origin (Court of Appeal of England and Wales, 2020). The ruling is useful because it shows that the deficit of normative authorization is not located in the absence of a norm, but in its indeterminacy: codes of practice and internal procedures existed, yet none resolved the questions of the who and the where. That requirement of

precision coincides with what is sustained in section 4.1 and reinforces the conclusion that generic security clauses do not satisfy the principle of legality. The third ground adds a relevant procedural element: the evaluation of bias was not treated as a technical best practice, but as a legal obligation whose non-fulfilment vitiated the deployment.

6.4. Cross-Cutting Lessons for the Design of Algorithmic Prevention

Read together, the three cases reveal a stable argumentative pattern. The courts do not question the legitimacy of the preventive aim or the utility of the tool; what they examine is the density of the legal authorization, the effective possibility of reconstructing the functioning of the system in a concrete case, the existence of human review with a real capacity for contradiction, and the availability of a remedy for the classified person. When any of these elements is lacking, unlawfulness is declared independently of the technical performance of the system.

This pattern permits the formulation of a warning for the Mexican debate. Public discussion of artificial intelligence in security tends to be framed in terms of installed capacity, budget and technological acquisition. The cases examined show that the critical point is situated earlier: without a norm that determines purposes, subjects, data and controls, and without accessible avenues of challenge, the deployment remains exposed to a declaration of invalidity that may render the investment made useless. Rights-protective regulation does not operate here as a brake on innovation, but as a condition of its legal sustainability.

7. The Mexican Case and the Need for Rights-Protective Regulation

7.1. Existing Constitutional and Normative Framework

Mexico faces a complex reality in which technological vulnerabilities, growing dependence on digital services, risks to critical infrastructure and the presence of criminal dynamics with adaptive capacity converge. In that context, the idea of strengthening state capacities for detection and prevention through AI is understandable. Nevertheless, institutional necessity does not equate to automatic legal authorization.

The Mexican legal order possesses constitutional bases for affirming the state obligation of protection, yet still lacks a specific and sufficiently developed regulation on public algorithmic governance in highly sensitive preventive tasks. Essential questions persist: which authorities could use these systems, under what exact purposes, with what activation parameters, what type of data could be processed, what external controls should intervene, and what rights the persons eventually affected by AI-assisted decisions or classifications would have.

The Political Constitution of the United Mexican States establishes in its Article 6 the right of access to public information and the protection of personal data as fundamental rights. Article 16 of the Constitution enshrines the right to privacy and establishes that private communications are inviolable, except by resolution of a judicial authority and with the formalities provided by law. These constitutional provisions constitute the minimum floor of protection that any algorithmic system for the detection of cyberterrorism must respect. For its part, the Federal Penal Code does not contain an autonomous definition of cyberterrorism as a criminal offence, which obliges recourse to the general figure of terrorism (Article 139 FPC) and to computer-related offences (Article 211 bis FPC), with the difficulties this entails in terms of normative determination and foreseeability.

7.2. Competent Institutions and Current State of Capacities

In the cybersecurity domain, Mexico has various institutions with relevant competences, although their coordination is not always clear. The Secretariat of Security and Citizen Protection (SSPC) and the Federal Ministerial Police have competences in the investigation of cyber offences. The National Guard has a Scientific Division with capacities in cybersecurity and digital investigation. The Secretariat of National Defense (SEDENA) and the Secretariat of the Navy (SEMAR) have cyber-defense capacities within their respective spheres. The National Intelligence Centre (CNI) has strategic-intelligence functions that include cyberspace as a domain of attention.

This institutional distribution generates the risk of duplication of efforts, lack of coordination and gaps in the chain of command, especially in the response to incidents that simultaneously have dimensions of public security and national security. The National Cybersecurity Strategy published in 2017 established a general governance framework in the matter but was not accompanied by the specific legislation necessary for its effective implementation, nor did it expressly contemplate the use of AI systems in detection and prevention functions.

It is necessary to mention that the latter has been entirely neglected and needs updating, being the first and only public policy for the Mexican State in the matter (to date). The foregoing is mentioned solely in order to provide an understanding of the Mexican context.

7.3. The Normative Gap and Its Consequences

This absence of normative definition generates a double risk. On the one hand, it may provoke institutional paralysis or underutilization of potentially valuable tools. On the other, it may encourage improvised, technocratic or opaque implementations based more on technological availability than on constitutional legitimacy. Between both extremes, the only juridically sustainable way out is a rights-protective regulation that integrates from the outset requirements of legality, documentation, impact assessment, audit, human oversight and avenues of review.

In the Latin American context, Mexico is not the only country that faces this gap. A review of regional normative frameworks shows that, unlike the European Union or the United States, Latin America lacks specific regulations on the use of AI in public security and terrorism prevention. In Latin America there exist heterogeneous normative and public-policy developments in the fields of data protection and artificial intelligence; nevertheless, a consolidated regional regulation on the state use of AI in public security and terrorism prevention is still not observed.

This regional situation contrasts with the persistence of cyber incidents against governmental infrastructures and essential services, which evidences the need to strengthen institutional capacities and normative frameworks. Thus, the gap between the escalation of threats and the normative lag is one of the principal challenges faced by the legal systems of the region.

8. Minimum Criteria for a Legitimate Use of AI in This Matter

On the basis of the analysis developed, it is possible to sustain that the use of AI by public authorities for the detection and prevention of cyberterrorism would be juridically defensible only if certain minimum criteria are fulfilled in a cumulative manner.

8.1. *Legitimate, Specific and Delimited Purpose*

In the first place, there must exist a legitimate, specific and delimited purpose. The tool cannot be authorized for open formulas of security or general surveillance. It must be clearly defined whether its objective is to protect critical infrastructures, to strengthen incident response or to detect concrete threats against strategic systems. The principle of purpose limitation, enshrined both in the LGPDPPSO and in the international frameworks reviewed, requires that data may not be processed for purposes distinct from those originally declared. In the context of AI systems, this implies that the system must be designed for a specific function and must not be used to identify, monitor or classify persons for reasons other than the prevention of cyberterrorism.

8.2. *Sufficient Normative Basis*

In the second place, a sufficient normative basis is required. The regulation must specify competent authorities, categories of data, temporal limits, activation scenarios, documentation mechanisms and institutional controls. Without this, the use of AI becomes an administrative practice without clear legal contours. Following the standard of “quality of the law” developed by the ECtHR, the enabling norm must be accessible to the public, formulated with sufficient precision so that citizens can foresee, to the extent reasonably possible, the circumstances in which the authorities may have recourse to such measures, and contain adequate safeguards against abuse.

8.3. *Suitability, Necessity and Proportionality*

In the third place, it is indispensable to overcome an analysis of suitability, necessity and proportionality. The adoption of the system must be justified as adequate to the purpose pursued, necessary in the face of the absence of less intrusive means, and proportional in relation to the intensity of impact on fundamental rights. The proportionality test, widely developed by constitutional doctrine and applied by constitutional courts in the Ibero-American sphere, requires a reasoning that demonstrates:

1. that the system is apt to contribute to the preventive purpose pursued;
2. that there do not exist alternative means equally effective yet less restrictive of rights and;
3. that the benefits in terms of security are superior to the costs in terms of restriction of rights. This analysis must be carried out *ex ante*, before the deployment of the system, and reviewed periodically in order to evaluate whether the conditions that justified it remain valid.

8.4. *Meaningful Human Oversight*

In the fourth place, meaningful human oversight is indispensable. No system should by itself generate decisions that affect rights, activate investigations or produce relevant legal consequences without qualified and documented human review. UNESCO (2021) and the OECD (2023) coincide in underscoring that human oversight cannot be merely formal. It is not enough that a responsible official exists in the organizational chart; the oversight must be effective, which implies that the official must have the information, the training and the authority necessary to understand the recommendations of the system, to question them when necessary and to assume responsibility for the final decision. Regulation (EU) 2024/1689 operationalizes this requirement by establishing that high-risk AI systems must be designed in such a way that human operators can ignore, interrupt or revoke the outputs of the system in real time.

8.5. *Data Quality, Audit and Independent Validation*

In the fifth place, data quality, audit and independent validation must be guaranteed. This includes bias assessment, robustness testing, continuous review and protocols for suspension or correction in the face of structural errors. The NIST AI RMF (2023) establishes that the management of data quality is an essential component of the governance of AI systems. Training, validation and testing data must be representative of the domain of application, must be documented and must be subjected to periodic quality evaluations. In the context of cyberterrorism-detection systems, this implies that the data used must adequately reflect the current threat landscape and must not be biased toward particular types of actors, techniques or attack vectors.

8.6. Traceability and Explainability

In the sixth place, sufficient traceability and explainability must be assured. The authority must be able to reconstruct the functioning of the system in a concrete case and to justify how its output was incorporated into the institutional decision.

8.7. Regime of Challenge and Responsibility

In the seventh place, there must exist a clear regime of challenge and responsibility. The person affected by an AI-assisted action must have effective means of review and reparation. The administration cannot dilute its responsibility in the algorithm or in the technological provider. This principle of non-delegable responsibility of public authorities is recognized both by the OECD (2023) and by Regulation (EU) 2024/1689, which expressly establishes that the use of high-risk AI systems by public entities does not exempt those entities from their legal responsibility under applicable law. In the Mexican legal order, this principle finds support in the regime of state patrimonial liability provided for in Article 113 of the Political Constitution of the United Mexican States and in the Federal Law on the Patrimonial Liability of the State.

9. Toward Rights-Protective Regulation: Proposals for the Mexican Context

The analysis developed in the preceding sections makes it possible to formulate certain concrete proposals for advancing toward a rights-protective regulation of the use of AI by public authorities in the detection and prevention of cyberterrorism in Mexico. These proposals do not purport to be exhaustive; rather, they seek to orient the legislative and normative debate toward the minimum elements that a regulation of this type should incorporate.

A prior condition for any regulation of the use of AI in the prevention of cyberterrorism is the existence of a clear and precise legal definition of the conduct sought to be prevented. The absence of a specific criminal offence of cyberterrorism in the Federal Penal Code generates a normative indeterminacy that is incompatible with the principle of legality and hinders the delimitation of the preventive object of algorithmic systems. The Mexican legislature should consider the autonomous criminalization of cyberterrorism, following the standards of United Nations Security Council Resolution 1373 (United Nations Security Council, 2001).

The Mexican legal order requires a law or a specific normative framework that regulates the use of AI systems by public authorities in security and prevention functions. This norm should:

1. delimit with precision the competent authorities and their respective spheres of action;
2. establish a closed catalogue of purposes for which the use of AI is authorized;
3. define the types of data that may be processed by the systems, with express prohibitions regarding especially sensitive categories;
4. establish maximum periods of data retention and mechanisms of depuration;
5. create a regime of impact assessment and independent audit prior to the deployment of any system; and
6. establish mechanisms of effective judicial review of AI-assisted actions.

The governance of the use of AI in public security requires an independent supervisory body, endowed with the technical and legal competences necessary to evaluate compliance with normative requirements, conduct audits, receive complaints, and impose sanctions.

Given the cross-border nature of cyberterrorism, Mexico should advance in its accession to the Budapest Convention and in the negotiation of bilateral and multilateral cooperation agreements that permit information exchange, technical assistance, and the harmonization of standards for the use of AI in the prevention of cyberterrorism. Cooperation should not be limited to intelligence exchange but should extend to the joint development of technical standards, risk-assessment frameworks, and best practices in the design and deployment of algorithmic systems.

10. Conclusions

The use of artificial intelligence by public authorities to detect and prevent cyberterrorism cannot be presented as a legally neutral solution, nor as an instrument whose technical efficacy alone legitimates its deployment. It constitutes, on the contrary, one of the most delicate areas of technological public law, precisely because it places innovation at the very core of the State's preventive power.

The prevention of cyberterrorism requires real institutional capacities. The State needs tools to identify anomalies, protect critical infrastructures, and respond in a timely manner to complex threats. That necessity, however, does not authorize the substitution of legal rationality by a logic of opaque automation. Prevention remains legitimate only when it continues to be subject to legality, proportionality, oversight, and responsibility.

The review of international and comparative frameworks reveals a clear convergence: public uses of AI in sensitive contexts may be admitted only under reinforced conditions of governance and control. This convergence is visible in the UNESCO Recommendation (2021), the OECD

Recommendation (2023), the NIST AI RMF (2023), and Regulation (EU) 2024/1689, which share a common core of principles: legality, legitimate purpose, proportionality, human oversight, traceability, explainability, and responsibility.

That lesson is fully applicable to the Mexican case. If the country opts to advance in the state use of AI for the detection and prevention of cyberterrorism, it must do so by means of a specific, rights-protective, and technically serious regulation capable of preventing the promise of technological anticipation from becoming a sophisticated form of erosion of fundamental rights.

Comparative judicial experience reinforces this conclusion with a practical datum. In the three cases analyzed, the courts invalidated the deployment not because of deficiencies in the performance of the systems, but because of the insufficiency of the normative authorization, the opacity of the risk model, or the absence of avenues of challenge for the classified persons. The lesson for the Mexican legislature is that prior normative design does not constitute an obstacle to technological adoption, but the condition that makes it possible to sustain it over time.

The analysis of the Mexican case reveals three normative deficits that must be addressed as a matter of priority: the absence of a specific criminal offence of cyberterrorism, the lack of a specific regulation for the use of AI in public security, and the non-existence of an independent supervisory body with sufficient technical and legal capacities for the control of algorithmic systems. Overcoming these deficits is not merely a requirement of normative modernization, but a condition for the State to be able to exercise its preventive functions legitimately in the digital environment.

In the final analysis, the correct question is not whether the State should use artificial intelligence to confront complex digital risks, but under what constitutional conditions it may do so without disfiguring the democratic order it purports to protect. The sustainable answer is clear: only within an architecture of legality, audit, transparency, human oversight, and effective review.

11. References

- Boix Palop, A. (2020). Los algoritmos son reglamentos: La necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones. *Revista de Derecho Público: Teoría y Método*, 1, 223–270.
- Código Penal Federal. Cámara de Diputados.
- Constitución Política de los Estados Unidos Mexicanos. Cámara de Diputados.
- Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, 40(1), 77–98.

Cotino Hueso, L. (2023). Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos. In F. Balaguer Callejón & L. Cotino Hueso (Eds.), *Derecho público de la inteligencia artificial* (pp. 347–402). Fundación Manuel Giménez Abad.

Council of Europe. (2001). *Convention on Cybercrime* (Budapest Convention, ETS No. 185).

Court of Appeal of England and Wales. (2020). *R (on the application of Bridges) v. Chief Constable of South Wales Police*, [2020] EWCA Civ 1058.

Court of Justice of the European Union. (2022). *Ligue des droits humains ASBL v. Conseil des ministres* (Case C-817/19), ECLI:EU:C:2022:491.

Cybersecurity and Infrastructure Security Agency. (2023). *2023–2024 CISA roadmap for artificial intelligence*. U.S. Department of Homeland Security.

Danaher, J., Hogan, M. J., Noone, C., Kennedy, R., Behan, A., De Paor, A., Felzmann, H., Haklay, M., Khoo, S.-M., Mingoia, J., & Shankar, R. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big Data & Society*, 4(2), 1–21.

Denning, D. E. (2000). *Cyberterrorism* [Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives].

European Court of Human Rights. (1978). *Klass and Others v. Germany* (Application no. 5029/71).

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.

European Union Agency for Cybersecurity. (2023). *Artificial intelligence and cybersecurity research*. ENISA.

Inter-American Commission on Human Rights, Special Rapporteur for Freedom of Expression. (2013). *Freedom of expression and the internet* (OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13).

Ley Federal de Responsabilidad Patrimonial del Estado. (2004). *Diario Oficial de la Federación*.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. (2017). *Diario Oficial de la Federación*.

Macdonald, S., Jarvis, L., & Lavis, S. (2022). Cyberterrorism today? Findings from a follow-on survey of researchers. *Studies in Conflict & Terrorism*, 45(8), 727–752.

Mayer Lux, L. (2018). Una definición de ciberterrorismo. *Revista Chilena de Derecho y Tecnología*, 7(2), 5–25.

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce.

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464), 447–453.

Organization for Economic Co-operation and Development. (2023). *Recommendation of the Council on Artificial Intelligence*.

Office of the United Nations High Commissioner for Human Rights. (2025). *Protecting human rights while using artificial intelligence to counter terrorism* (PP/AI/CT). Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

Organization of American States. (1969). *American Convention on Human Rights*.

Rechtbank Den Haag. (2020). *NJCM et al. v. The State of the Netherlands* (SyRI), ECLI:NL:RBDHA:2020:1878.

Secretaría de la Presidencia. (2017). *Estrategia Nacional de Ciberseguridad*. Gobierno de México.

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*.

United Nations. (2000). *United Nations Convention against Transnational Organized Crime*. United Nations Office on Drugs and Crime.

United Nations Office of Counter-Terrorism & United Nations Interregional Crime and Justice Research Institute. (2021). *Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes*.

United Nations Office on Drugs and Crime. (n.d.). *Module 14: Hacktivism, terrorism, espionage, disinformation campaigns and cyber warfare*. Education for Justice Initiative.

United Nations Security Council. (2001). *Resolution 1373 (2001)* (S/RES/1373).

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112.

Venkatachary, S. K., Prasad, J., Alagappan, A., Andrews, L. J. B., Raj, R. A., & Duraisamy, S. (2024). Cybersecurity and cyber-terrorism challenges to energy-related infrastructures: Cybersecurity frameworks and economics. Comprehensive review. *International Journal of Critical Infrastructure Protection*, 45, Article 100677.

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523.

Author's Note on the Use of Artificial Intelligence: *It is hereby clarified that the use of Generative Artificial Intelligence tools was strictly auxiliary, instrumental, and non-substantive in nature within the process of preparing the manuscript. Their use was limited to tasks involving the formal revision of the text, such as spelling correction, punctuation, accentuation, grammatical agreement, removal of repetition, improvement of syntactic fluency, stylistic consistency, and adaptation to an appropriate academic register. In this regard, the tool served as editorial support comparable to linguistic or stylistic proofreading, aimed at improving the clarity, readability, and formal accuracy of the manuscript, without replacing the author's intellectual work.*

More specifically, Generative Artificial Intelligence was not used to produce substantive content for the article, formulate the research problem, develop the theoretical framework, define the methodology, conduct the analysis, interpret findings, generate arguments, draft complete sections, introduce new ideas, produce conclusions, select bibliographic sources, or create references. All academic, conceptual, methodological, and argumentative decisions remained under the sole responsibility of the author, who reviewed and validated every formal modification made to the text and retained full control over such changes.

Furthermore, it should be emphasized that the use of the tool was not intended to fill gaps in content, develop sections that had not previously been drafted, or replace any part of the research, reading, critical analysis, or academic writing processes. The manuscript was conceived, structured, and developed by the author; technological assistance was employed solely at a subsequent stage of linguistic revision and formal standardization, with the purpose of strengthening the academic presentation of the text without altering its authorship, originality, scientific content, or intellectual responsibility.

*Luis Miguel Hernández Flores, Cristian Fernando Hernández Flores,
Carlos Eduardo Ortega Tapia and Miguel Iván Pazmiño Sotomayor*

Convergence between transnational organized crime and contemporary terrorism in Latin America: the Ecuadorian case between pragmatism and utopia

Abstract

This study examines the convergence between transnational organized crime and the instrumental use of terror in Latin America, with particular emphasis on the Ecuadorian case. Through a qualitative documentary approach with an analytical-interpretive scope, the study integrates academic literature, reports from international organizations, official statistics, and verifiable documentary sources. The analysis suggests that Ecuador constitutes a particularly illustrative case of this convergence, visible in the rise of lethal violence, the use of explosives, the expansion of illicit economies, and the activity of non-state armed actors with criminal governance capacity. This study argues that predominantly reactive state responses show structural limitations when confronted with hybrid threats of an adaptive and transnational nature. Consequently, it concludes that the effectiveness of state responses to this hybrid threat depends on the sustained articulation of an understanding of the international context, territorial control, financial intelligence, specialized criminal investigation, international cooperation, and structural violence prevention, rather than on episodic coercive measures.

Keywords: organized crime, criminal governance, terrorism, regional security

Luis Miguel Hernández Flores, Police Captain (Ecuador). Foresight specialist. Specialist in Strategic Intelligence Analysis, Cyberintelligence, and Counterterrorism.

Cristian Fernando Hernández Flores, Police Lieutenant (Ecuador). Criminologist. Specialist in Organized Crime Analysis, Criminal Investigation, and Terrorism.

Carlos Eduardo Ortega Tapia, Colonel of the State General Staff Police (Ecuador). Former National Director of Anti-Drug Investigation, National Chief of the Anti-Crime Investigation Unit, and Police Attaché of Ecuador in Spain.

Miguel Iván Pazmiño Sotomayor, Colonel of the State General Staff Police (Ecuador). Former Police Attaché of Ecuador in the United States of America and National Chief of the Unit for the Fight Against Organized Crime.

To cite this article: Hernández Flores, L. et al. (2026), Convergence between transnational organized crime and contemporary terrorism in Latin America: the Ecuadorian case between pragmatism and utopia, *Revista Internacional de Estudios sobre Terrorismo*, issue 18:30-49.

Received

04/23/2026

Accepted

08/13/2026

1. Introduction

Ecuador is undergoing a structural transformation of its security landscape, marked by the convergence of transnational organized crime, extreme violence, and cross-border dynamics. This process does not constitute an isolated or exclusively conjunctural phenomenon; rather, it is embedded in a broader Latin American regional trend in which criminal organizations have evolved into configurations capable of influencing social and political life. This transformation is facilitated by neopatrimonial schemes, in which the private use of public office fosters a functional interdependence that enables criminal structures to establish local orders in the face of the limited institutional presence of the State (Alda-Mejías, 2021).

Specialized literature in security, criminology, and criminal governance has conceptualized this mutation through categories such as transnational organized crime, criminal governance, and, in recent works, neo-organized crime¹ (Hernández & Hernández, 2024). In this article, the term is employed in a heuristic sense, without any claim to consolidate it as an established theoretical category, with the purpose of apprehending the complexity of contemporary criminal structures beyond classical drug trafficking or local gangs. Neo-crime is characterized by its entrepreneurial logic, its diversification of illicit portfolios (drug trafficking, extortion, illegal mining, arms trafficking, contract killings, and money laundering), its articulation in transnational networks, and its capacity to operate simultaneously in urban, port, prison, and border spaces (Feldmann & Luna, 2022; Shelley, 2014). Unlike criminal organizations of the past, these structures do not rely exclusively on rigid hierarchical leaderships but combine hierarchy with flexible networks, thereby increasing their resilience to state action.

In this context, one of the most relevant features of neo-organized crime is the instrumental use of repertoires of violence associated with contemporary terrorism as a mechanism of social control, strategic communication, and territorial discipline. Far from responding to a classical ideological motivation, extreme violence—including the use of explosives, car bombs, selective attacks, and indiscriminate threats—is integrated into the criminal repertoire as a functional tactic aimed at generating collective fear, inhibiting citizen cooperation with the State, and pressuring institutional decisions in matters of security and justice (Farber, 2025; Makarenko, 2004; Phillips, 2018). This functional convergence between organized crime and terrorism has been recognized even in the realm of international law and global security, which has noted that both phenomena share methods, resources, and destabilizing effects on democratic governability (United Nations Security Council [UNSC], 2019).

¹ Organized neo-crime employs extreme violence and terror tactics to obtain criminal, economic, and territorial power. It does not pursue ideological aims and generates severe social consequences, such as the increase in homicides and insecurity.

The Ecuadorian case is particularly illustrative of this convergence. In recent years, the country has experienced an accelerated deterioration of internal security, manifested in the rise of lethal violence, the partial collapse of the prison system, the proliferation of firearms and explosives, and its strategic positioning as a logistical platform for transnational drug trafficking, especially toward European and North American markets (United Nations Office on Drugs and Crime [UNODC], 2024; National Police of Ecuador, 2024). These dynamics have been aggravated by the fragmentation of internal criminal organizations that operate with open visibility and by the growing influence of transnational actors that remain in the shadows, generating violent territorial disputes and a scenario of structural insecurity.

Likewise, in Amazonian border spaces, the convergence of illicit economies, state absence, and armed violence has fostered the presence and expansion of non-state armed actors of predominantly criminal orientation, such as the Comandos de la Frontera. These groups not only control strategic routes and illegal economies but also regulate the everyday life of entire communities through coercive norms, exemplary punishments, and mechanisms of social control, thereby configuring local orders parallel to state authority (García-Pinzón & Mantilla, 2021; Williams et al., 2025).

Within this framework, the present article proposes to analyze the impact of the convergence between transnational organized crime and contemporary terrorism in Latin America, with particular emphasis on the Ecuadorian case. The research problem examines whether the State's strategic architecture in response to this phenomenon evidences a pragmatic and proportional adaptation to the complexity of neo-crime, or whether it remains anchored in utopian, reactive, and fragmented responses. To this end, a qualitative-documentary approach of analytical-interpretive scope is adopted, integrating specialized academic literature, reports from international organizations, official statistics, and verifiable documentary sources, with the purpose of contributing to the debate on security, criminal governance, and the limits of the state response to hybrid threats in contexts of high organized criminality.

2. Methodology

The present study adopts a qualitative-documentary approach of analytical-interpretive scope, oriented toward examining the functional convergence between transnational organized crime and the instrumental use of terror in Latin America, with emphasis on the Ecuadorian case. The methodological strategy combined structured bibliographic review, documentary analysis, and interpretive examination of recent cases of high public and institutional relevance, with the purpose of strengthening the conceptual framework and the empirical base of the manuscript through pertinent academic and documentary sources.

The bibliographic corpus was constructed through structured searches in Scopus, Web of Science, and EBSCO. A total of 681 records were identified (Scopus, $n = 321$; Web of Science, $n = 185$; EBSCO, $n = 175$). After a conservative screening of exact duplicates by DOI and title, the corpus consisted of 488 unique records. Given that the study does not correspond to a systematic literature review, a PRISMA protocol was not applied; instead, an intentional selection by theoretical-empirical relevance was employed. From this universe, a core sample of 29 works of direct utility for the four analytical axes of the manuscript was prioritized: (i) convergence between transnational organized crime and contemporary terrorism; (ii) empirical indicators of the deterioration of security in Ecuador; (iii) criminal governance and the actions of non-state armed actors; and (iv) critical evaluation of state responses.

Complementarily, the study incorporated reports from international organizations, official statistics, and relevant institutional documents for the analysis of the Ecuadorian case, particularly regarding homicides, seizures, armed violence, non-state armed actors, and state responses. Likewise, for the analysis of recent events of high public visibility, verifiable journalistic sources and concurrent institutional documents were incorporated, employing them with a contextual and contrastive function, without assigning them autonomous evidentiary status when they lacked additional documentary support. This criterion sought to safeguard the traceability of the empirical information and to avoid unsupported inferences drawn from isolated secondary sources.

Analytically, the review was organized around the four axes previously described. The treatment of the material was interpretive in character, oriented toward identifying recurrent patterns, conceptual convergences, and tensions among specialized literature, available empirical evidence, and institutional discourse.

Finally, it should be noted that the study relies on secondary sources of varying empirical density, that the bibliographic screening prioritized thematic relevance over exhaustiveness, and that some recent events of the Ecuadorian case depend on public information still subject to updating. These limitations are discussed in greater detail in the corresponding section.

3. Convergence between Transnational Organized Crime and Contemporary Terrorism: Conceptual Clarifications

The convergence between transnational organized crime and contemporary terrorism² can be understood as a process of functional approximation and strategic adaptation between phenomena that, although analytically distinguishable, may share repertoires of violence, logistical resources, financial mechanisms, and forms of territorial control. In this sense, the classical literature has emphasized

² Contemporary terrorism is manifested through the use of terror as a means, instrument, and tactic. It employs violence, intimidation, and new technologies such as drones to generate fear, destabilize institutions, and achieve objectives. Intelligence sources indicate that in Ecuador and the region it is manifested primarily through convergence with organized crime, involving attacks with improvised explosive devices (IEDs), threats, and extreme violence aimed at controlling territories and illicit economies.

that the relationship between the two should not be reduced to an organic fusion or to an automatic conceptual equivalence, but rather to a continuum of interaction ranging from limited instrumental linkages to more complex forms of cooperation, transformation, or operational overlap (Makarenko, 2004; Paoli & Fijnaut, 2022; Kleinschmidt & Palma, 2020). This distinction is important because it makes it possible to avoid excessively broad classifications while simultaneously recognizing that certain criminal actors adopt tactics, languages, and practices of intimidation that exceed conventional criminality.

From this perspective, convergence does not imply that criminal organizations necessarily pursue ideological aims comparable to those of classical terrorism. What the evidence suggests, rather, is that certain criminal groups incorporate repertoires of high-visibility violence with strong psychological impact when these prove functional for disciplining territories, inhibiting cooperation with the State, intimidating competitors, or influencing political, judicial, and police decisions. In Latin America, this pattern has been observed in cases where public violence, open threats, attacks with explosives, and other forms of coercive communication fulfill a function of criminal ordering rather than of ideological mobilization (Bevilacqua et al., 2024; Johnson & Gillooly, 2023; Johnson, 2019; Phillips, 2018). The threat, in these contexts, operates not only as physical violence but also as a message of authority and social regulation.

More recent discussion has shifted the focus from violence alone toward criminal governance. This literature shows that numerous criminal structures do not limit themselves to exploiting illicit rents but establish rules, administer disputes, delimit acceptable behaviors, and produce local orders that may coexist with, compete with, or become intertwined with state authority. In the Latin American case, this type of arrangement has been described as one of the most relevant transformations in the relationship among crime, politics, and violence, insofar as it compromises state legitimacy, fundamental rights, and the effective force of the rule of law (Badillo-Sarmiento & Trejos-Rosero, 2025; Blattman et al., 2025; Feldmann & Luna, 2022). From this angle, the crime–terror convergence acquires a broader dimension: it is not limited to the use of violent tactics but is inserted into processes of social, territorial, and symbolic control with direct effects on governability.

In Latin America, the literature also warns that these dynamics are not uniform. Patterns of convergence vary according to the density of illicit economies, the strength or fragmentation of the state apparatus, the relationship between armed actors and public authorities, and the type of territoriality in dispute. Comparative studies of non-state violent actors in the region have questioned the more expansive versions of the convergence hypothesis, noting that not every combination of profit, violence, and territorial control should be interpreted as full hybridization between crime and insurgency or between crime and terrorism (Kleinschmidt & Palma, 2020). Along the same lines, recent research on Tren de Aragua and other regional structures shows that criminal transnationalization can be sustained through franchises, territorial nodes, co-optation, and coercion, without necessarily implying a mutation toward classical insurgent forms (Sampó & Troncoso, 2024). In addition, recent

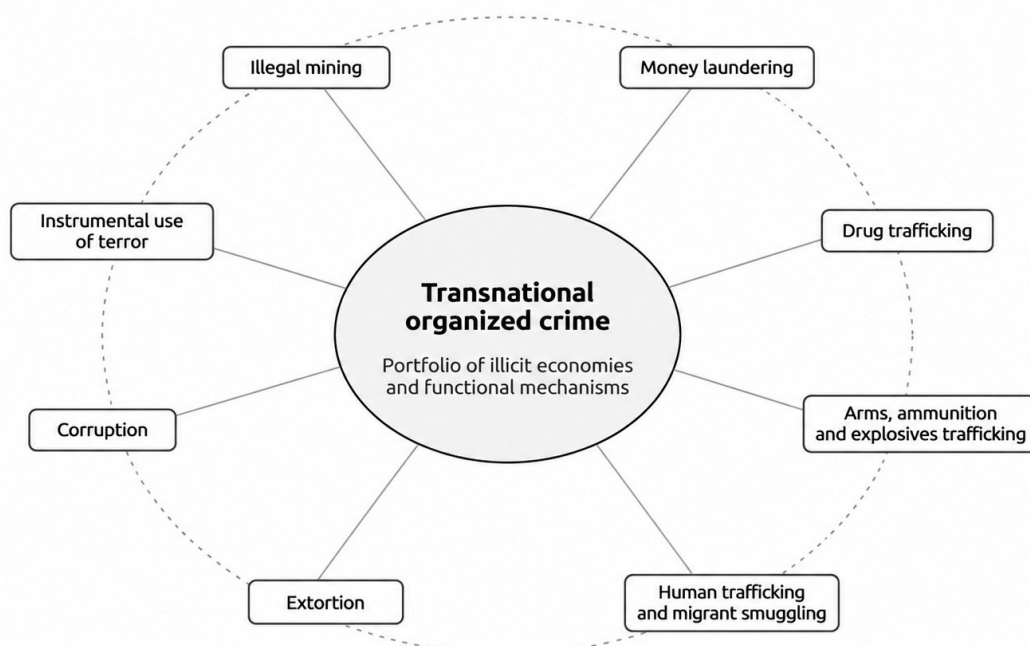
regional reports document that money laundering, migrant trafficking, and other illicit economies may operate as mechanisms of articulation between transnational organized crime and terrorist or hybrid actors in Latin America (United Nations Interregional Crime and Justice Research Institute [UNICRI], 2024). Consequently, the use of the concept must be analytically careful and empirically graduated.

The expansion of these arrangements is favored by broader processes of illicit globalization, diversification of criminal markets, and sophistication of financing mechanisms. Recent literature on the crime–terror nexus has underscored that convergence does not depend solely on repertoires of violence but also on the transnational circulation of capital, technologies, arms, routes, and tactical knowledge. In particular, illicit financial mechanisms, informal systems of value transfer, and the exploitation of regulatory gaps strengthen the adaptive capacity of organizations that combine criminal economies with high-impact intimidation practices (Farber, 2025; Jupp, 2025; Shelley, 2014). Likewise, cross-border corridors and peripheral areas with weak state presence facilitate the consolidation of criminal nodes capable of operating across multiple jurisdictions and, on occasion, of surpassing the level of inter-state coordination available in the region (Penagos, 2024; Global Initiative Against Transnational Organized Crime, 2025).

Within this framework, the porosity of borders, institutional fragmentation, and the unequal capacity of states to produce security contribute to criminal violence adopting increasingly expressive, public, and disciplinary forms. Regional evidence shows that criminal organizations with territorial vocation may resort both to lethal violence and to extra-lethal violence, public threats, and reputational control in order to consolidate obedience, resolve disputes, and fix hierarchies. Such practices have been documented, for example, in studies of criminal governance in Colombian cities and of reputational violence in Mexico, where the open threat constitutes part of the exercise of criminal power rather than a mere externality of the illicit market (Badillo-Sarmiento & Trejos-Rosero, 2025; Johnson & Gillooly, 2023). This finding is especially useful for the present article because it makes it possible to understand extreme violence not only as a problem of public security but as a technology of criminal governance.

From a strategic perspective, these processes pose relevant challenges for security policies. If the convergence between organized crime and terrorism is variable, functional, and territorially situated, responses based exclusively on rigid penal categories or on traditional counter-terrorism schemes prove insufficient. The literature concurs on the need for more comprehensive approaches capable of articulating financial intelligence, territorial control, institutional strengthening, international cooperation, and an understanding of local forms of criminal governance (Farber, 2025; Feldmann & Luna, 2022). In sum, rather than assuming a full identity between organized crime and terrorism, contemporary analysis tends to recognize a functional, selective, and empirically gradable convergence whose expression in Latin America requires flexible, comparative conceptual frameworks attentive to the relationship among violence, territory, and authority.

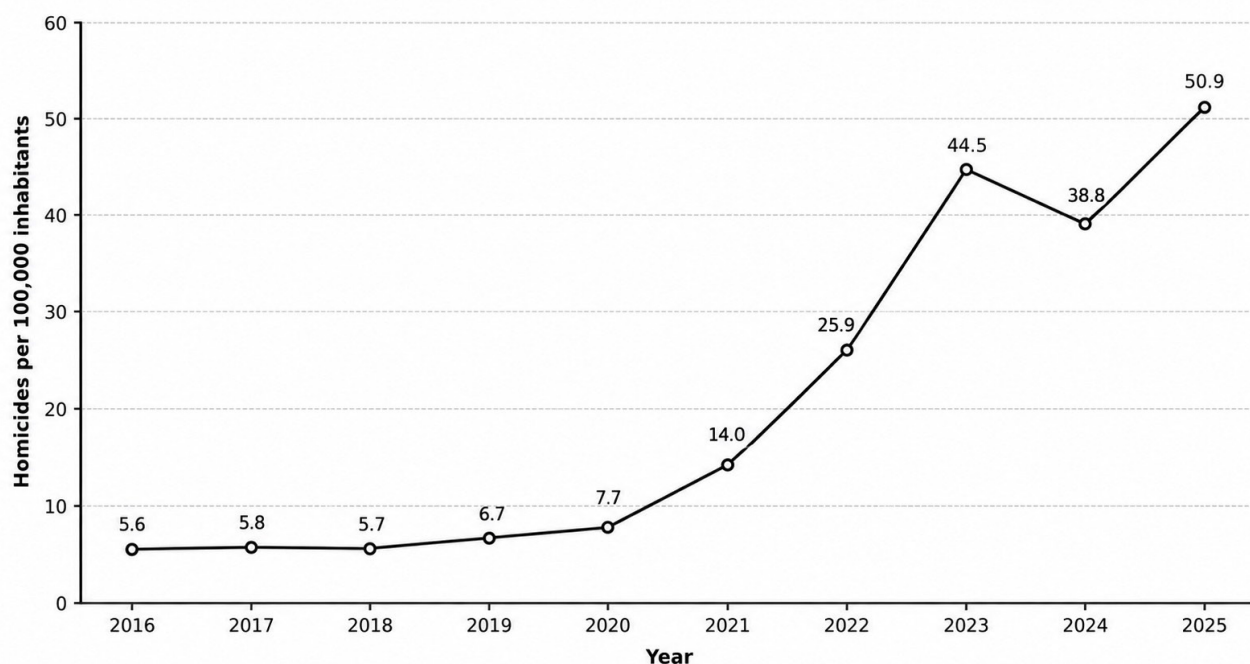
Figure 1. Portfolio of illicit economies and functional mechanisms of transnational organized crime



Note. Own elaboration based on Shelley (2014), Feldmann and Luna (2022) and Farber (2025).

4. The Ecuadorian Case: Indicators and Manifestations of Convergence

Available evidence situates Ecuador as a particularly relevant case for observing the functional convergence among transnational organized criminality, extreme violence, and the weakening of state capacity. The recent series of intentional homicides shows an abrupt deterioration of internal security: the national rate rose from 6.7 per 100,000 inhabitants in 2019 to 46.5 in 2023, declined to 38.8 in 2024, and recorded a new increase in 2025, reaching 50.91 per 100,000 inhabitants, according to official records and journalistic series compiled from state sources (Ministry of the Interior of Ecuador, 2024; González, 2026; UNODC, 2024). More than a linear progression, this trajectory suggests a pattern of escalation, partial containment, and reactivation, consistent with adaptive criminal disputes in contexts of intermittent state intervention.

Figure 2. Homicide rate in Ecuador (2016–2025)

Note. Own elaboration based on data from Statista (2026).

This deterioration cannot be read in isolation from the place Ecuador has acquired in regional drug-trafficking routes. Seizures exceeding 220 tons of controlled substances recorded in 2024 confirm the country's logistical centrality within illicit circuits that articulate production, storage, transit, and export toward extra-regional markets. The coexistence of growing interdiction and the persistence of elevated levels of violence indicates that state operational pressure has not dismantled the underlying structures but coexists with processes of criminal recomposition and territorial dispute (National Police of Ecuador, 2024; UNODC, 2024). This phenomenon generates a quantifiable economic impact; according to the Inter-American Development Bank (Perez-Vincent et al., 2024), the direct costs of criminality represented 3.44 percent of regional Gross Domestic Product (GDP) in 2022, constituting a macroeconomic constraint on growth and poverty reduction. Within this framework, violence fulfills not only a function of eliminating competitors but also of territorial regulation and public signaling of criminal power. A second relevant empirical feature is the adoption of forms of violence with high symbolic impact. In Ecuador, attacks with explosives, episodes of extreme prison violence, and the public dissemination of armed actions have amplified the intimidatory effect of criminal coercion beyond confrontation between rival organizations. The armed incursion into the TC Televisión channel on 9 January 2024 illustrates how a criminal act can be transformed into a mediatized terror event capable of producing collective fear, a perception of state vulnerability, and broad public resonance (Tusa et al., 2025). In analytical terms, these episodes do not justify an automatic equation between organized crime and terrorism, yet they are consistent with the instrumental use of repertoires of violence intended to communicate power, discipline audiences, and condition institutional responses (Bevilacqua et al., 2024; Makarenko, 2004; Tusa et al., 2025).

To this must be added the organizational and financial dimension of the phenomenon. Reports on the Euro 2024 case and the recent captures of Ecuadorian leaders or individuals linked to the Ecuadorian criminal scene in Spain, Colombia, and other countries suggest three convergent features: financial sophistication, externalization of command, and capacity for recomposition following the neutralization of leaderships. Considered here with an illustrative and contrastive function, and not as autonomous conclusive proof, these cases show that illicit economies do not depend solely on immediate territorial control but also on money-laundering networks, transnational operators, and schemes of extraterritorial coordination. Likewise, the violent reactions that follow high-profile captures reinforce the hypothesis that criminal coercion operates as a mechanism for preserving the illicit market and for exerting pressure on the state system (Shelley, 2014; Felbab-Brown, 2010; Primicias, 2024; National Police of Ecuador, 2025).

Table 1. Illustrative cases of convergence among organized criminality, transnational projection, and strategic coercion

Case / Proceeding	Structure	Vector of Convergence	Relevant Finding	Source Document
Euro 2024 case	Money-laundering network linked to Jezdimir Srdan	Transnational financial sophistication	The case documents capital movements, corporate structures, and coordination between Ecuador and Europe, showing that criminal capacity does not depend solely on territorial control.	Primicias (12 June 2025)
Recapture of José Adolfo Macías Villamar (“Fito”)	Los Choneros	Centrality of leadership and state pressure on high-value commanders	The recapture evidences the symbolic and operational weight of leaderships in security policy and in the public communication of state control.	Primicias (25 June 2025)
Capture of William Joffre Alcívar Bautista (“Comandante Willy”)	Los Tiguerones	Extraterritorial command	The detention in Spain, involving the use of false documentation, supports the hypothesis of externalization of command and operational refuge outside Ecuador.	Primicias (23 October 2024)
Capture of Wilmer Geovanny Chavarría Barré (“Pipo”)	Los Lobos	Organizational resilience and documentary fraud	The simulation of death and the capture in Málaga make it possible to observe strategies of international evasion, identity substitution, and continuity of criminal command.	Primicias (17 November 2025)

Note. Only cases with direct analytical utility for examining financial sophistication, externalization of command, organizational resilience, and strategic coercion in the Ecuadorian case are included. The links refer to the principal source document used in each row.

Taken together, these indicators make it possible to sustain that the Ecuadorian case presents features consistent with a functional convergence between transnational organized crime and the instrumental use of terror. The combination of elevated lethal violence, intensification of anti-drug

interdiction, public visibility of high-impact attacks, prison crisis, and transnational projection of criminal actors suggests a transformation of the security problem: from a scheme centered on conventional organized criminality toward another in which violence also fulfills functions of governance, social intimidation, and dispute over territorial authority. In this sense, the Ecuadorian case does not demonstrate a full identity between crime and terrorism, yet it does provide relevant evidence of the ways in which contemporary criminal violence can acquire political and social effects comparable to those analyzed by the literature on criminal governance and hybrid threats (Badillo-Sarmiento & Trejos-Rosero, 2025; Feldmann & Luna, 2022).

5. Comandos de la Frontera as a Non-State Armed Actor of Criminal Orientation

The Comandos de la Frontera may be understood, for analytical purposes, as a non-state armed actor of predominantly criminal orientation, arising in a post-insurgent environment³ and linked to the reconfiguration of the Colombian conflict following the peace agreements. Its trajectory does not fully conform to the model of classical insurgency, insofar as its actions appear oriented primarily toward the control of illicit economies, strategic corridors, and mechanisms of territorial regulation rather than toward open dispute of state power through a defined ideological program. This characterization is consistent with recent literature on hybrid armed actors in Latin America, which warns of the need to distinguish among organizational continuity, criminal functionality, and the persistence of armed repertoires without automatically assuming a full insurgent identity or uncritically transferring categories of armed conflict to territorially situated criminal configurations (Badrán, 2024; Durán-Martínez, 2023; Kleinschmidt & Palma, 2020; Global Initiative Against Transnational Organized Crime, 2025).

Its relevance for the Ecuadorian case derives from its insertion in Amazonian border spaces where low institutional density, transnational circulation of illicit rents, and high dependence on riverine and terrestrial corridors converge. In these environments, diverse sources have described forms of control that combine armed coercion, regulation of economic activities, and instrumental linkages with local structures—features that the literature associates with schemes of criminal governance rather than with mere occasional armed presence. In this sense, the analytical interest of the group resides not only in its capacity for violence but in its aptitude to operate as a *de facto* authority in peripheral territories, administering access, disciplining conduct, and protecting illicit activities (Blattman et al., 2025; Feldmann & Luna, 2022; García-Pinzón & Mantilla, 2021; Penagos, 2024; Williams et al., 2025).

3 Post-insurgency, primarily in Colombia, describes the transformation and persistence of armed structures following demobilization processes and peace agreements. It is manifested mainly in guerrilla dissident groups and residual formations that maintain territorial control, armed violence, and linkages with illicit economies.

Available evidence further suggests that the expansion of the Comandos de la Frontera in Ecuador should not be interpreted solely as a mechanical prolongation of the Colombian conflict but as part of a process of cross-border adaptation to logistical opportunities, control vacuums, and local alliances. Reports on detentions and operations in 2024 indicate a structured presence of the group in Ecuadorian territory, supported by logistical operators, intermediate commanders, and support networks functional to the transport of drugs, arms, and financial resources. Considered with the caution proper to public documentary sources, these antecedents are consistent with a pattern of territorial deepening and with an organizational logic that combines limited armed visibility and sustained capacity for criminal coordination (García-Pinzón & Mantilla, 2020; Penagos, 2024; Primicias, 2024; Global Initiative Against Transnational Organized Crime, 2025).

A particularly significant element is that the coercion attributed to the group does not appear oriented exclusively toward permanent confrontation with the State but toward the preservation of illicit corridors, extractive enclaves, and zones of influence. Under this logic, violence functions as a mechanism for the protection of markets and as a technology of territorial government. The ambush in which eleven Ecuadorian soldiers died in Alto Punino, attributed by national authorities to structures linked to the Comandos de la Frontera—despite the group's denial of authorship—constituted a turning point by evidencing the capacity of a non-state armed actor to inflict high-intensity lethal damage on state forces in an environment of difficult control. More than an isolated event, the episode suggests the existence of tactical capacities, knowledge of the terrain, and a disposition to employ high-impact violence in order to defend strategic positions and deter state intervention (Primicias, 2025; Global Initiative Against Transnational Organized Crime, 2025).

Table 2. Empirical indicators of territorial insertion and cross-border projection of the Comandos de la Frontera in Ecuador

Empirical Indicator	Documented Manifestation	Analytical Variable	Relevance for the Ecuadorian Case	Source Document
Structured presence in Ecuador	Indictment of 17 alleged members in 2025 for organized crime, drug trafficking, arms trafficking, and money laundering.	Operational insertion in national territory	Suggests a non-episodic presence compatible with local support, financing, and criminal logistics networks.	Primicias (16 April 2025)
Logistics network of alias “Chavalo”	Judicial and journalistic coverage links the network to the movement of drugs from Sucumbios toward Central America and Europe.	Local–cross-border articulation	Makes it possible to observe the role of intermediate operators and Amazonian corridors in the connection among border, ports, and external markets.	Primicias (13 September 2024)
Alto Punino	Ambush against a military patrol with 11 fatalities; authorities attributed it to the Comandos de la Frontera, although the group denied responsibility.	Capacity for high-intensity armed violence	Indicates capacity for lethal confrontation against state forces in a corridor linked to illegal mining and border illicit economies.	Primicias (9 May 2025)
Capture and transfer of Roberto Carlos Álvarez Vera, alias Gerente	Detention in Abu Dhabi and subsequent transfer to Ecuador; authorities identify him as the group’s leader in the country.	Extra-regional projection and separation between nodes of coercion and nodes of protection/management	Reinforces the hypothesis of articulation among Amazonian anchorage, extraterritorial coordination, and protection of leadership.	Primicias (29 December 2025)

Note. The table summarizes verifiable indicators of territorial insertion, cross-border articulation, and extra-regional projection of the Comandos de la Frontera in Ecuador. The attribution of Alto Punino is formulated prudently and in accordance with available public evidence.

To this is added a relevant organizational feature: the extraterritorial projection of part of its leadership and of its coordination circuits. Reports on captures outside the Andean region suggest that, like other contemporary criminal structures, the group can spatially separate spaces of direct violence from spaces of financial and logistical management. This pattern does not by itself convert the Comandos de la Frontera into a globally integrated organization, yet it does reinforce the hypothesis that it operates under a transnational rationality, with the capacity to articulate local nodes of coercion and external nodes of protection, coordination, or money laundering (UNODC, 2019; Shelley, 2014). Taken together, these elements make it possible to sustain that its importance for the Ecuadorian case resides less in a supposed “guerrilla reappearance” than in the consolidation of a form of cross-border armed criminality that is adaptable and territorially situated, whose analysis is central to understanding the limits of conventional security responses.

6. State Strategies in the Face of the Hybrid Threat: Between Pragmatism and Utopia

The disjunction between pragmatism and utopia should not be understood here as an abstract opposition, but as a criterion for evaluating the adequacy between the design of state responses and the effective nature of the threat. In the Ecuadorian case, that adequacy depends less on the discursive

intensity of the measures than on their capacity to interrupt illicit financial circuits, reduce the autonomy of prison centers, sustain transnational cooperation, and diminish the social conditions that facilitate criminal recruitment. Regional literature suggests that responses centered exclusively on coercion, exceptionality, and punitive expansion may produce immediate effects of visibility, yet tend to be insufficient and even counterproductive when they fail to alter the institutional and territorial bases of criminal governance (Badrán, 2024; Feldmann & Luna, 2022; Magaloni et al., 2020).

*Financial intelligence*⁴. Among the available tools, financial intelligence constitutes probably the most clearly pragmatic strategy, insofar as it acts upon the material support of criminal organizations: their money flows, mechanisms of asset concealment, and capacity for reinvestment. Its efficacy, however, depends not only on the formal existence of anti-money-laundering norms but on the articulation among financial intelligence units, prosecutors' offices, registration systems, banking supervision, and international cooperation. In a scenario such as the Ecuadorian one, where criminal structures display externalization of command, use of covert identities, and transnational economic circuits, the gap between normative design and sustained implementation may convert an operatively rational tool into a policy of low practical effectiveness. At that point, the problem is not the lack of pertinence of the strategy but its weak institutionalization (Financial Action Task Force [FATF], 2025; Shelley, 2014).

*Specialized criminal investigation*⁵. Ortiz Luzuriaga, Flores Sánchez, Caicedo Leones, and Ordóñez Guartazaca (2021) maintain that the prevention of money laundering requires an integral system of risk management in which state institutions, the financial system, and obligated subjects participate in a coordinated manner. The authors emphasize that the early identification of suspicious operations, effective supervision, and inter-institutional cooperation are essential elements for preventing resources of illicit origin from entering the formal economy, thereby strengthening the transparency of the financial system and the security of the State.

Consequently, specialized criminal investigation of money laundering transcends the prosecution of an economic crime and becomes a strategic tool for protecting the integral security of Ecuador. It permits an approach that differentiates the pragmatic from the utopian because, unlike traditional investigations, specialized investigation of money laundering requires a multidisciplinary approach that combines several techniques and is not limited to identifying those responsible for the predicate offense; rather, it seeks to dismantle the economic structure that sustains criminal organizations, depriving them of their financial capacity and reducing their influence over public and private institutions, thereby rendering visible the end of the criminal business.

4 Financial intelligence. Strategy oriented toward identifying and disrupting the economic and patrimonial flows of organized crime, whose efficacy depends on solid institutional coordination and international cooperation (FATF, 2025; Shelley, 2014).

5 Specialized criminal investigation. Multidisciplinary approach that seeks to identify and dismantle the economic structures of organized crime through the detection of money laundering, thereby reducing their financial capacity and institutional influence (Ortiz Luzuriaga et al., 2021).

*Prison control*⁶. A second decisive domain is the prison system. As the available evidence for Ecuador and other regional cases shows, prisons have functioned not only as spaces of confinement but as nodes of command, internal discipline, and reproduction of illicit economies (Fondevila & Vilalta-Perdomo, 2024; Sozzo, 2022). Recent research on Latin American prisons suggests that carceral violence and the capacity of organizations for control are not explained solely by overcrowding or material precariousness, but also by the existence of schemes of self-government or criminal government inside the establishments (Sozzo, 2025). This phenomenon is analyzed with greater precision under the category of nodal governance, in which the exercise of power does not originate in an exclusive sovereign center but in a network of interconnected actors that integrates both state officials and criminal structures operating through operational clandestinity (Ferreira, 2025).

*International cooperation*⁷. International cooperation constitutes another central component, given that the structures examined in this work operate in networks that readily overflow national jurisdiction. Exchange of information, judicial assistance, asset tracing, migratory alerts, and operational coordination are indispensable mechanisms against organizations capable of moving persons, capital, and goods among several countries. Nevertheless, regional experience shows that these tools are often limited by institutional asymmetries, divergent national priorities and, in certain cases, by an insufficient reading of hybrid threats. The consequence is cooperation that is usually normatively adequate but operatively fragmentary. In this sense, cooperation does not constitute a utopian strategy by definition; it becomes utopian when it fails to translate into continuity, interoperability, and shared recognition of the problem (FATF, 2025; Pont, 2025).

*Prevention of vulnerabilities and recruitment*⁸. The structural prevention of recruitment and of the social base of organized crime is often presented as an idealistic strategy in the face of the urgency of violence. That opposition is, however, misleading. Available evidence suggests that youth vulnerability, educational exclusion, territorial precariousness, and the absence of legitimate trajectories of social insertion form part of the environment that facilitates the expansion of criminal organizations in contexts of high violence. In the Ecuadorian case, recent studies have explicitly linked the discussion of public violence and mediatized terror with the need to strengthen durable social responses, especially in education and the inclusion of young people exposed to recruitment by criminal groups. Regional literature on social responses to violence under criminal governance further suggests that this type of strategy produces consistent effects only when it possesses community

6 Prison control. Strategy oriented toward recovering state control of prisons and neutralizing their use as command centers and sites of criminal reproduction, thereby limiting self-government and the governance exercised by criminal organizations (Sozzo, 2025; Ferreira, 2025).

7 International cooperation. Strategy for confronting transnational criminal networks through information exchange, judicial assistance, and operational coordination, whose efficacy depends on continuity and interoperability among states (FATF, 2025; Pont, 2025).

8 Prevention of vulnerabilities and recruitment. Strategy oriented toward reducing social factors that favor criminal recruitment, through education, youth inclusion, and sustained community strengthening (Arias, 2019; Escotto Quesada, 2015; Tusa et al., 2025).

anchorage, institutional continuity, and the capacity to sustain itself in territories of high conflictivity (Arias, 2019; Escotto Quesada, 2015; Tusa et al., 2025). For this reason, rather than a “utopian” policy, social prevention constitutes a dimension of medium-term pragmatism that rarely receives the political time, financing, or institutional continuity required to produce cumulative effects.

Taken together, the Ecuadorian case suggests that the opposition between pragmatism and utopia is not resolved by choosing a single strategy, but by evaluating the capacity of the State to articulate them in a sustained manner. Financial intelligence, specialized criminal investigation, prison reform, international cooperation, and the prevention of recruitment prove pragmatic only when they are integrated into a continuous institutional response that is territorially differentiated and capable of adapting to a changing threat. When these dimensions operate with systemic asymmetry, episodically, or subordinated to conjunctural crises, the instrumental efficacy of the strategies is nullified, reducing them to an inoperative formalism (Badrán, 2024; Feldmann & Luna, 2022).

7. Discussion

The findings of the present study dialogue with the recent literature on convergence between organized crime and terrorism on at least four planes. In the first place, the Ecuadorian case reinforces yet also nuances the thesis of the continuum between crime and terrorism: the evidence examined does not permit sustaining a structural or ideological fusion between the two phenomena, but it does show a functional and selective convergence in which repertoires of high-impact violence are incorporated by criminal organizations when they prove useful for protecting illicit markets, disciplining territories, intimidating audiences, and conditioning state responses. In this sense, the case confirms that the analytical key does not reside in labeling these actors as “terrorists” in the strict sense, but in understanding under what conditions certain tactics, effects, and rationalities proper to terror are instrumentalized by criminal structures without abandoning their primary orientation toward illicit accumulation (Farber, 2025; Kleinschmidt & Palma, 2020; Phillips, 2018; Makarenko, 2004).

In the second place, the Ecuadorian case expands the literature on criminal governance by showing that violence acts not only as a destructive resource but also as a technology of social and territorial regulation. The combination of elevated lethal violence, disputed prison control, transnational illicit corridors, extractive enclaves, and non-state armed actors with capacity for localized coercion suggests that part of contemporary organized criminality in Ecuador is not limited to exploiting illegal rents but produces situated orders, imposes rules, defines hierarchies, and models behaviors in spaces where state authority is fragmentary, disputed, or intermittent. From this perspective, the principal analytical displacement of the manuscript consists in showing that the problem is not solely one of public security but also of authority, governance, and the production of obedience in contexts of the factual pluralization of power (Badillo-Sarmiento & Trejos-Rosero, 2025; Blattman et al., 2025; Feldmann & Luna, 2022).

In the third place, the results permit proposing an interpretive hypothesis that, while exploratory, offers relevant explanatory yield and departs from more conventional readings. The most dangerous organized neo-criminality does not appear to be necessarily that which attempts to substitute the State frontally in an insurgent key, but rather that which learns to operate in strategic relation with a fragmented, reactive, or selectively coercive statehood. In this reading, the threat is expressed not only in the capacity to challenge the State but also in the capacity to adapt to it, exploit its discontinuities, reorder illicit markets after cycles of intervention, and convert institutional crises into opportunities for organizational recomposition. This hypothesis is consistent with works that show, on the one hand, that convergence tends to be less intense and more graduated than maximalist versions of the debate suggest and, on the other, that state presence does not always displace criminal governance but, under certain conditions, may coexist with it or even reconfigure its incentives (Blattman et al., 2025; Feldmann & Luna, 2022; Kleinschmidt & Palma, 2020; Magaloni et al., 2020).

In the fourth place, the analysis of state responses permits a critical discussion of the apparent opposition between pragmatism and utopia. The Ecuadorian case suggests that this dichotomy is not resolved by the simple choice between coercion and prevention, nor between militarization and social policies, but by the capacity of the State to articulate heterogeneous instruments in a sustained institutional sequence. Regional literature supports the idea that fragmented, episodic, or exclusively punitive interventions may produce immediate effects of visibility yet do not necessarily alter the structures of criminal governance; on occasion they even intensify violence or reinforce the adaptability of the groups. For this reason, the contribution of the article does not consist in mechanically opposing security and rights, nor prevention and control, but in sustaining that state efficacy in the face of hybrid threats depends on coordination among financial intelligence, specialized criminal investigation, prison control, transnational cooperation, effective territorial presence, and durable social strategies for the reduction of vulnerabilities (Arias, 2019; Badrán, 2024; FATF, 2025; Pont, 2025; Tusa et al., 2025).

From that base, the article contributes a broader implication for the Latin American debate: the necessity of shifting the focus from the question of the “nature” of the actors toward the question of their effective capacities to produce order, fear, transnational coordination, and political conditioning. In other words, the category of organized neo-criminality acquires value not as a closed label but as a heuristic tool for examining criminal configurations that combine entrepreneurial rationality, organizational flexibility, communicative coercion, and a vocation for territorial regulation.

This rereading avoids both conceptual inflation—which confuses all criminal violence with terrorism—and classical penal reductionism, which underestimates the political and social dimension of contemporary forms of organized criminality. At that point, the Ecuadorian case should not be read as an isolated anomaly but as a particularly visible regional laboratory of transformations that will probably continue to expand in environments marked by porous borders, transnational illicit circuits, and differentiated state weakness (Farber, 2025; Johnson & Gillooly, 2023; UNICRI, 2024; Global Initiative Against Transnational Organized Crime, 2025).

As limitations, the study must be read in an analytical and interpretive key. It relies on secondary sources of varying empirical density, incorporates recent events still subject to documentary updating, and employs the notion of “organized neo-crime” in a heuristic sense, not as a closed theoretical category. Consequently, the inferences proposed do not pretend to establish definitive causal equivalences between organized criminality and terrorism, but to offer a conceptually graduated interpretation of an observable functional convergence. With a view to future research, it would be especially valuable to contrast this hypothesis through mixed designs, primary territorial data, subnational comparative analyses, and longitudinal studies of the relationship among state intervention, criminal recomposition, and coercive governance.

8. Conclusion

The Ecuadorian case shows that contemporary criminal violence does not fully conform either to the classical categories of organized delinquency or to those of terrorism in the strict sense, but expresses a functional convergence in which criminal actors instrumentalize repertoires of terror in order to secure territorial control, protect illicit economies, and condition the state response. Within this framework, the principal analytical and political challenge does not reside in the nominal classification of the phenomenon, but in understanding its effective capacity to erode state authority, produce coercive governance, and destabilize democratic environments. From this perspective, Ecuador should be understood less as an anomaly than as a particularly visible manifestation of broader regional transformations, which reinforces the need for conceptually precise and institutionally integrated approaches in the face of increasingly hybrid, adaptive, and transnational forms of organized criminality.

9. References

- Alda-Mejías, S. (2021). La cultura del privilegio y la privatización de las funciones públicas, elementos esenciales para la gobernanza criminal. En S. Alda Mejías (Coord.), *Los actores implicados en la gobernanza criminal en América Latina* (pp. 11-44). Real Instituto Elcano.
- Arias, E. D. (2019). Social responses to criminal governance in Rio de Janeiro, Belo Horizonte, Kingston, and Medellín. *Latin American Research Review*, 54(1), 165–180.
- Badillo-Sarmiento, R., & Trejos-Rosero, L. F. (2025). Governing the underworld: How organized crime governs other criminals in Colombian cities. *Trends in Organized Crime*, 28(3), 359–385.
- Badrán, F. (2024). The signing of the peace agreement in Colombia. Old wine in new skins: Implications for national security and organized crime. *Trends in Organized Crime*, 27(2), 173–196.
- Bevilacqua, S., Cukla, A. R., & Tello Gamarra, D. F. (2024). Terrorism and police countermeasures in the fight against the “Novo Cangaço”. *Revista Criminalidad*, 66(3), 97–110.

- Blattman, C., Duncan, G., Lessing, B., & Tobón, S. (2025). Gang rule: Understanding and countering criminal governance. *The Review of Economic Studies*, 92(3), 1497–1531.
- Durán-Martínez, A. (2023). Large-scale criminal violence in the 21st century. In A. Gruszczak & S. Kaempf (Eds.), *Routledge handbook of the future of warfare* (pp. 421–431). Routledge.
- Escotto Quesada, T. (2015). *Las juventudes centroamericanas en contextos de inseguridad y violencia: Realidades y retos para su inclusión social (LC/W.666)*. Comisión Económica para América Latina y el Caribe.
- Farber, S. (2025). The globalization of threat: A systematic review of crime-terror convergence. *Journal of Money Laundering Control*, 28(3), 533–549.
- Felbab-Brown, V. (2010). *Shooting up: Counterinsurgency and the war on drugs*. Brookings Institution Press.
- Feldmann, A. E., & Luna, J. P. (2022). Criminal governance and the crisis of contemporary Latin American states. *Annual Review of Sociology*, 48, 441–461.
- Ferreira, M.A. (2025): Organizaciones criminales y gobernanza criminal. Análisis Carolina, nº 11, Madrid, Fundación Carolina.
- Financial Action Task Force. (FATF). (2025). *International standards on combating money laundering and the financing of terrorism and proliferation: The FATF recommendations*.
- Fondevila, G., & Vilalta-Perdomo, C. (2024). Prison violence in Latin America: Criminal governance and an absent state. *International Criminology*, 4, 149–165.
- García-Pinzón, V., Mantilla, J. (2021). Contested borders: organized crime, governance, and bordering practices in Colombia-Venezuela borderlands. *Trends in Organized Crime*, 24, 265–281.
- Global Initiative Against Transnational Organized Crime. (2025). *Índice global de crimen organizado 2025: La criminalidad en una encrucijada*.
- González, M. A. (2026, March 11). *Ecuador es el tercer país más violento de América Latina y el Caribe, según Insight Crime*. Primicias.
- Johnson, P. L. (2019). The crime and state terrorism nexus: How organized crime appropriates counterinsurgency violence. *Perspectives on Terrorism*, 13(6), 16–26.
- Johnson, P. L., & Gillooly, S. N. (2023). Grammar of threat: Governance and order in public threats by criminal actors. *Comparative Political Studies*, 56(10), 1567–1596.
- Jupp, J. (2025). *The crime-terror nexus and the illicit trade in drugs*. *Studies in Conflict & Terrorism*. Advance online publication.
- Kleinschmidt, J., & Palma, O. (2020). The conceptual puzzle of violent non-state actors in Latin America: A critique of the convergence hypothesis. *Small Wars & Insurgencies*, 31(6), 1323–1348.
- Magaloni, B., Franco-Vivanco, E., & Melo, V. (2020). Killing in the slums: Social order, criminal governance, and police violence in Rio de Janeiro. *American Political Science Review*, 114(2), 552–572.
- Makarenko, T. (2004). The crime-terror continuum: Tracing the interplay between transnational organised crime and terrorism. *Global Crime*, 6(1), 129–145.

- Ministry of the Interior of Ecuador. (2024). *Informe estadístico de seguridad ciudadana y homicidios*.
- National Police of Ecuador. (2024). *Reporte estadístico de incautaciones y operaciones contra el crimen organizado*.
- National Police of Ecuador. (2025). *Boletines operativos de capturas de objetivos de alto valor 2024–2025*.
- Ortiz Luzuriaga, M. T., Flores Sánchez, J., Caicedo Leones, W., & Ordoñez Guartazaca, M. (2021). Prevención del riesgo de lavado de activos. Caso Colombia y Ecuador. *Revista Universidad de Guayaquil*, 133(2).
- Paoli, L., & Fijnaut, C. (2022). Conceptualizing the nexus between organized crime and terrorism. En L. Paoli, J. Wouters, & C. Fijnaut (Eds.), *The nexus between organized crime and terrorism: Types and responses* (pp. 48–84). Edward Elgar Publishing.
- Penagos, L. (2024). *Reconfigurations institutionnelles sur la frontière colombo-vénézuélienne, frontière de tous les trafics* [Institutional reconfigurations on the Colombian-Venezuelan border, border of all organized crimes]. *Caravelle*, 122, 49–63.
- Perez-Vincent, S. M., Puebla, D., Alvarado, N., Mejía, L. F., Cadena, X., Higuera, S., & Niño, J. D. (2024). *Los costos del crimen y la violencia: ampliación y actualización de las estimaciones para América Latina y el Caribe*. Banco Interamericano de Desarrollo.
- Phillips, B. J. (2018). Terrorist tactics by criminal organizations: The Mexican case in context. *Perspectives on Terrorism*, 12(1), 46–63.
- Pont, A. S. (2025). Strengthening transatlantic ties: Latin America-Europe cooperation against organized crime. In J. A. Sanahuja & R. Domínguez (Eds.), *The Palgrave handbook of EU-Latin American relations* (pp. 473–488). Palgrave Macmillan.
- Primicias. (2024, August 29). *Golpe a Comandos de la Frontera en Ecuador: 17 detenidos y USD 200 millones intervenidos*.
- Primicias. (2024, November 20). *Caso Euro 2024: Cae red de lavado de activos vinculada al narcotráfico que operaba en Ecuador y Europa*.
- Primicias. (2025, May 13). *En la zona del alto Punino, donde asesinaron a 11 militares, está en auge el negocio millonario de la minería ilegal*.
- Sampó, C., & Troncoso, V. (2024). El Tren de Aragua: La transnacionalización del crimen organizado a través del tráfico de migrantes. *Análisis Político*, 37(108), 147–176.
- Shelley, L. I. (2014). *Dirty entanglements: Corruption, crime, and terrorism*. Cambridge University Press.
- Sozzo, M. (2022). Introduction: Inmate governance in Latin America. Context, trends and conditions. En M. Sozzo (Ed.), *Prisons, inmates and governance in Latin America* (pp. 1–32). Palgrave Macmillan.
- Sozzo, M. (2025). El auge de los esquemas de gobierno de los presos en las prisiones latinoamericanas. Condiciones, estrategias y luchas. *Latin American Law Review*, (14). 1–26.
- Tusa, F., Aguaded, I., Tejedor, S., & Rivera, C. (2025). Ecuador: A state of violence—Live broadcast of terror. *Journalism and Media*, 6(2), Artículo 56.

- United Nations Interregional Crime and Justice Research Institute. (2024, June). *The nexus between transnational organized crime and terrorism in Latin America*.
- United Nations Office on Drugs and Crime. (2019). *World drug report 2019*.
- United Nations Office on Drugs and Crime. (2024). *World drug report 2024*.
- United Nations Security Council. (2019, March 28). *Resolution 2462 (2019) on the prevention and suppression of the financing of terrorism (S/RES/2462)*.
- Williams, M., Melendez, M., & Morales, R. (2025). Crimen Organizado y Violencia en América Latina y el Caribe. Informe Económico América Latina y el Caribe (Abril). Banco Mundial.

Author's Note on the Use of Artificial Intelligence: *It is hereby clarified that the use of Generative Artificial Intelligence tools was strictly auxiliary, instrumental, and non-substantive in nature within the process of preparing the manuscript. Their use was limited to tasks involving the formal revision of the text, such as spelling correction, punctuation, accentuation, grammatical agreement, removal of repetition, improvement of syntactic fluency, stylistic consistency, and adaptation to an appropriate academic register. In this regard, the tool served as editorial support comparable to linguistic or stylistic proofreading, aimed at improving the clarity, readability, and formal accuracy of the manuscript, without replacing the author's intellectual work.*

Mauricio Heise y Cristian Rodríguez

From Crime–Terror Convergence to Hybrid Violence: Drone Attacks in Latin America

Abstract

This article analyzes the use of Unmanned Aerial Systems (UAS) as instruments of “hybrid violence” due to their employment by non-state actors in Latin America, particularly in Colombia, Mexico, and Brazil. Between 2020 and 2026, criminal organizations with economic or politico-economic motivations have used these systems for the delivery of explosive devices, surveillance, and territorial control, challenging state authority and affecting public security conditions in these countries.

Drawing on Makarenko’s *Crime-Terror Continuum* model, the article examines empirical cases through academic literature, intelligence reports, and media sources to identify patterns of tactical adaptation, key characteristics, and the current state of the phenomenon. In this regard, the study suggests the emergence of a threat capable of reducing traditional state tactical advantages, including through the use of fiber-optic-guided drones that are resistant to electronic jamming, as well as the potential deployment of chemical agents.

Keywords: drones, security, Latin America, crime-terror continuum, hybrid threat, territorial control, criminal innovation

Mauricio Heise, PhD in Political Science (UB). Master’s in Terrorism Studies (UNIR). Analyst of terrorism and violent extremism.

Cristian Rodríguez, Graduate in Criminology and Security Sciences (VIU). Master’s in Advanced Studies in Terrorism (UNIR). PhD candidate in International Security (UNED).

To cite this article: Heise, M. and Rodríguez, C. (2026), From Crime-Terror Convergence to Hybrid Violence: Drone Attacks in Latin America, *Revista Internacional de Estudios sobre Terrorismo*, issue 18:50-68.

Received

08/15/2026

Accepted

09/12/2026

1. Introduction

For decades the use of drones was confined almost exclusively to the state military domain, as means of reconnaissance and attack. In recent years, however, this technology has been progressively incorporated by non-state actors into their repertoires of violence. This phenomenon constitutes a criminal innovation, in that it combines the use of readily accessible technologies, artisanal modifications, and the projection of violence from aerial space, thereby representing a security challenge for Latin America.

Diverse non-state armed actors, such as the drug-trafficking cartels in Mexico and the dissident factions of the Revolutionary Armed Forces of Colombia (FARC), have integrated drones into their operational tactics, primarily for the launching of improvised explosive devices against law enforcement and security forces, rival groups, and even the civilian population. These incidents, frequently documented since 2020, evidence a significant risk to public security, as they imply the adaptation of these armed actors through the use of devices that are accessible and low-cost.

Far from completely replacing other modalities of violence such as the use of car bombs, armed ambushes, or attacks with firearms, the employment of drones is added to an expanded tactical repertoire, offering operational advantages: the possibility of executing attacks at a distance, reduced direct exposure of the operators, and a high psychological impact upon security forces and affected communities. In this sense, the drone must not be understood solely as a technical instrument, but as symbolic coercion, intended to exhibit power, exercise territorial control, and demonstrate the capacity to challenge the state.

From a theoretical perspective, these dynamics fit precisely within the crime–terror continuum model¹ proposed by Makarenko (2005), which describes the progressive convergence between organized crime and terrorism. The use of drones by criminal organizations and armed dissidents illustrates how these actors adopt tactics that are traditionally proper to political violence and terrorism, yet with economic motivations, giving rise to hybrid configurations of violence. Cases such as the drone attacks of the Jalisco New Generation Cartel (CJNG) against police forces in Mexico, or those of the FARC dissidents against military and police units in Colombia, reflect this operational and symbolic convergence, in which terror and criminality intertwine to exercise territorial control and erode state authority.

The employment of drones by armed actors in Latin America constitutes the manifestation of a deep structural convergence. In this phenomenon material capacities converge, derived from the easy acquisition of commercial technology, together with a strategic rationality that seeks to maximize tactical damage with the minimum personal risk, which is made possible by remote attacks. Nevertheless, the technological dimension is insufficient to explain the phenomenon without

1 The Crime-Terrorism Continuum Model describes a dynamic relationship in which organized crime and terrorism are not separate phenomena, but coexist on a continuous spectrum based on their methods and motivations; they can therefore converge through tactical alliances, mutual appropriation of techniques, or even transform into one another.

considering the recourse to violence as the articulating axis and instrument of psychological coercion. This evolution is especially relevant in contexts of low state capacity, where technological innovation combines with governance voids and high levels of structural violence.

To examine this dynamic, the present work focuses on the temporal framework spanning 2020 to 2026 –the period in which an exponential and documented increase in explosive drone attacks would be recorded in the region– analyzing the situation of Colombia, Mexico, and Brazil, as constituting the most representative scenarios of this phenomenon.

2. Development

2.1 Makarenko's Crime–Terror Continuum: Hybrid Violence

One of the central contributions of Makarenko's crime–terror continuum (2005) is the idea that organized crime and terrorism should not be understood as rigid normative categories, but as forms of non-state violence susceptible of converging under certain structural conditions. Within this framework, non-state actors adopt tactics, structures, and narratives traditionally associated with the other spectrum when this proves functional to their strategic objectives. This logic makes it possible to explain why contemporary criminal organizations, even in the absence of a concrete ideological project, resort to forms of high-impact symbolic violence, such as reiterated attacks against security forces, that have historically been associated with terrorism, as a rational adaptation in contexts of territorial dispute, state fragmentation, and armed competition (Makarenko, 2005; InSight Crime, 2023).

Without limiting the foregoing, it must be clarified that not every high-impact attack should be considered terrorist, since the psychological effect or intimidation alone do not suffice to classify it as terrorism; therefore, the employment of drones is understood as a tool of coercion that enriches a broader tactical repertoire.

In Mexico, the method of action of the Jalisco New Generation Cartel (CJNG) constitutes one of the most evident examples of displacement along the continuum described by Makarenko. Although its central motivation is economic, multiple journalistic investigations and specialized observatories have documented how the CJNG has systematically incorporated tactics proper to armed political violence: attacks against police and military personnel, use of improvised explosives and drones, coordinated blockades of infrastructures, and deployments of violence with a strong communicative charge (InSight Crime, 2022; Villegas, 2025). Following the death of one of its regional leaders, far from an organizational withdrawal being observed, coordinated violent actions occurred in order to reaffirm territorial control and demonstrate its capacity for coercion, thereby reinforcing a logic of instrumental terror oriented toward state deterrence and political messaging, and not solely toward criminal retaliation (InSight Crime, 2021).

Meanwhile, Colombia represents a paradigmatic case of the inverse trajectory envisaged in Makarenko's model, in which an organization of insurgent origin progressively transitions toward criminal structures without completely abandoning political violence. As Makarenko herself anticipated (2005) in her original analysis of the FARC, growing dependence on illicit economies does not necessarily imply renunciation of terrorist tactics when these continue to offer strategic advantages.

The FARC dissidents have consolidated their insertion into networks of drug trafficking, illegal mining, and extortion, yet simultaneously have executed systematic attacks against the public force, including the use of explosive-laden drones, a practice documented by national media and specialized reports since 2021 (BBC Mundo, 2022; InSight Crime, 2024). This combination of criminality and symbolic violence reflects a permanent hybrid configuration, rather than a transitory phase.

Regarding the foregoing, a difference between the dissidents and their predecessor is that “both organizations seek territorial control; however, the former FARC-EP intended to fulfil its strategic plan by expanding into fronts and generating a social base in order to achieve its objective, which was the seizure of power, whereas the dissidents seek to conquer territories for the existence of illicit economies or strategic corridors” (García & Hernández, 2024).

In this sense, the armed forces and the police of Colombia currently confront a complex strategic scenario, characterized by the persistence of residual insurgency, the intensification of illicit economies, and the consolidation of hybrid threats, with armed groupings such as the FARC, the ELN, and the Clan del Golfo (Ríos, 2025).

These armed groups could be understood under the categorization of “hybrid threat”, considering that “the hybrid has undergone a long conceptual journey from its origins to the present day. Heir to the concept of complex-irregular warfare, this idea became popular after the clash between Israel and Hezbollah in 2006 to describe the integration of conventional and irregular tactics, techniques, and procedures, mixed with terrorist acts, propaganda, and connections with organized crime” (Colom, 2019). From this perspective, concepts such as “hybrid threat” or “terrorist tactics” are descriptive categories for examining the functional adoption of intimidatory dynamics by criminal organizations.

Meanwhile, the Brazilian case further reinforces the validity of the continuum by showing how “strictly criminal” actors can adopt quasi-political practices, without the need to articulate a formal political or ideological agenda. Organizations such as the Comando Vermelho and the Primeiro Comando da Capital have consolidated enclaves of territorial control in favelas, where they regulate illicit economic activities, impose social norms, and exercise armed coercion in the face of state presence (InSight Crime, 2022; The Guardian, 2021). From the perspective of the crime–terror continuum, these groups do not transform into terrorist organizations with respect to their motivations, yet they assimilate repertoires of collective intimidation and social disciplining that fulfil functions analogous to those of terrorism, especially when attacks are directed against police forces as visible symbols of the state and of its formal authority.

Taken together, these Latin American examples confirm the empirical validity of the proposed analytical framework and suggest the need to employ it in order to interpret contemporary forms of hybrid violence, characterized by the superposition of economic, political, and symbolic rationalities. The use of drones by criminal organizations and armed dissidents must not be understood solely as a technological innovation, but as an indicator of position within the crime–terror continuum, in which the adoption of terrorist tactics responds both to operational incentives and to objectives of territorial control, violent legitimization, and open challenge to state authority (Makarenko, 2005; InSight Crime, 2023).

In this sense, to the operational and technological aspects is added a less visible yet equally relevant dimension: the social, cultural, and symbolic context in which these attacks occur. As Crespo (2018) notes, violence against security forces cannot be explained solely as a tactical or reactive decision, but as the result of prior processes of social radicalization and consolidation of subcultures of violence that legitimize aggression against the state agent. In territories where police or military presence is perceived as a form of occupation, provocation, or oppression, a symbolic framework is configured that facilitates the dehumanization of the “state other” and its conversion into a legitimate target of violence. This sociocultural environment is key to understanding why sophisticated attacks—such as the use of explosive drones—can be deployed repeatedly without necessarily generating a social rejection proportional to the impact they produce.

2.2. *Use of Explosive-Laden Drones by Armed Groups in Latin America*

In territories where illicit economies (drug trafficking or illegal mining) generate financing for armed groups, drones function as a tool of “criminal sovereignty”, representing a challenge to state security in the three countries analyzed.

The tactic of executing attacks by means of improvised explosive devices (IEDs) employing drones has intensified in Latin America as part of the adaptation of non-state actors to a technological environment of high availability and low cost. In Colombia and Mexico –and increasingly in other countries– the drone consolidates itself as an offensive and harassment platform, with the capacity to project violence at a distance and to alter the operational routines of state forces and rival groups (De Lorenzo de Guindos, 2026; Ginn & Goodwin, 2025). In comparative terms, the pattern is not uniform: in Colombia the incentives combine political and economic components (with predominance of the latter), whereas in Mexico the rationality is linked predominantly to the control of criminal markets and strategic territories (Heise, 2025; Institute for Economics & Peace, 2026).

Beyond motivations, a key convergent element exists: the drone attack functions as an instrument of intimidation that generates psychological effects disproportionate to the immediate physical damage, eroding the adversary’s morale through the persistent threat from the air. In Mexico,

the deployment of “droneros” (drone operators) and the use of droppers (drones that release payloads) has contributed to installing a perception of constant vulnerability in disputed territories, affecting both opponents and civilian communities (De Lorenzo de Guindos, 2026; Heise, 2025). In Colombia, the diffusion of the buzzing of drones in conflict zones and the expansion of attacks documented by the press and strategic reports reinforce their function as a tool of symbolic coercion and territorial control (Heise, 2025; Institute for Economics & Peace, 2026).

At the operational level, drones enable these actors to access and attack objectives situated in areas where terrestrial approach would be slower, riskier, or more easily interceptable. Their utility lies in reducing the direct exposure of operators, expanding tactical reach, and facilitating opportunity attacks against patrols, convoys, and infrastructure, while maintaining the initiative at relatively low costs (Heise, 2025; Ginn & Goodwin, 2025). Although limitations exist –flight autonomy, payload, vulnerability to inhibitors or layered defense– the cost-impact balance favors their adoption, especially when commercial devices are combined with artisanal adaptations, cumulative learning, and logistical networks for the supply of components (De Lorenzo de Guindos, 2026; Ginn & Goodwin, 2025).

Meanwhile, in Brazil indications are observed of the incorporation of the drone as a resource of violence in urban conflict environments, associated with the armed escalation of criminal organizations with territorial control in favelas. For example, the use of drones by the Comando Vermelho is reported during² Operation *Contenção* in Rio de Janeiro in October 2025, which left 122 dead (Folha de S.Paulo, 2025), suggesting the regional diffusion of this innovation toward scenarios of organized criminality with high firepower and local criminal governance (De Lorenzo de Guindos, 2026).³ This case is analytically relevant because it transfers the problem from the rural dispute (drug-trafficking corridors and peripheral control) toward the dense urban space, where the psychological impact and the risk of collateral damage may be amplified.

Likewise, outside the three countries mentioned the drone also begins to appear as a resource in contexts of state crisis and gang violence, as in Haiti, where drone operations are recorded within the framework of governmental actions against gangs, together with explicit threats of response by gang leaders by means of their own drones, within scenarios of extremely fragile governability (De Lorenzo de Guindos, 2026; Ginn & Goodwin, 2025). Taken together, these cases show that the adoption of drones is not an isolated phenomenon, but part of a regional transformation of non-state repertoires of violence, with impact upon public security and the protection of security forces and critical infrastructure (Institute for Economics & Peace, 2026; Ginn & Goodwin, 2025).

2 The operation was named “*Contenção*”.

2.3 Tactical Adaptation as a Hybrid Threat

The principal motivation of the groups operating in Mexico and Colombia would be to exercise territorial control, in terms of the deployment of power in specific zones in order to develop their illicit operations, preventing the state from imposing its authority in those territories; therefore, drone attacks are also a demonstration of power, intended to generate influence through intimidation. From this perspective, the tactical innovation of drone use is framed within a phenomenon of non-state actors that possess a high level of hierarchical organization, with capacities that can impact the condition of governability and exercise territorial control in order to carry out their criminal operations, so that these actors come to represent criminal insurgencies (Bustamante, 2020).

On the basis of the foregoing, drone attacks generate effects comparable to those of terrorist tactics, inasmuch as their offensive use transcends punctual attacks and direct victims, producing a climate of fear and psychological impact. In this sense, “what distinguishes acts of terrorism from other types of violent action is their capacity to provoke an intense psychological and social impact (anxiety or fear) disproportionate to the physical damage inflicted upon the persons or objects chosen as the target of the aggression” (De la Corte, 2013).

These criminal insurgencies employ this method of attack, of a terrorist type, within the framework of a broader range of actions, configuring a hybrid threat, whose concept, although it has different interpretations, implies the employment of conventional and irregular means, together with the perpetration of terrorist attacks, the deployment of propaganda, and the exploitation of the adversary’s weaknesses in order to exercise power and coercion (Colom, 2019).

Hybrid threats imply the use of different tactics, including military ones, a situation that is applicable to the cases analyzed. In Colombia, despite the 2016 peace agreement, the armed conflict persists with actors that employ guerrilla and terrorist tactics; meanwhile, the Mexican cartels are organized-crime groups that possess specific capacities, even proto-insurgent ones, through the use of guerrilla tactics. Likewise, in both cases there is use of cyberspace and disinformation, whose application as a whole generates destabilization and the possibility of eroding social cohesion, weakening institutions, terrifying populations, and exercising territorial control (Ortiz, 2015). Although it is not a conventional “military invasion”, one is unequivocally in the presence of a multidimensional phenomenon with impact upon political systems.

Criminal groupings employ drones for purposes that range from the propagandistic to the tactical-offensive, the latter dimension corresponding to attacks against personnel and infrastructure of security forces, rival groups, and the civilian population. In addition, they can conduct aerial reconnaissance for surveillance and attack planning, transport small quantities of drugs into penitentiary centers, but above all exercise fear, for example, by recording videos of attacks for subsequent dissemination on the internet.

2.4 Drone Attacks in Colombia

Drone attacks present a direct symmetry with the cartography of illicit economies, specifically those related to the routes of production, processing, and trafficking of drugs, as well as illegal mining. The departments in which the deployment of this technique has been concentrated include Cauca, Norte de Santander, Arauca, Guaviare, Tolima, Cesar, Valle del Cauca, and Putumayo (Torrado, 2025; Cifuentes, 2025b). In the north-east of the country, the department of Norte de Santander—particularly the Catatumbo sub-region—has established itself as an epicenter of confrontation. In this zone, the “33rd Front” of the FARC dissidents and the ELN have waged a violent territorial dispute for control of the trans-border routes toward Venezuela (Bonilla, 2025a; Torrado, 2025).

In the south-west, departments such as Cauca and Valle del Cauca have suffered attacks by the “Estado Mayor Central”. In Cauca, structures such as the Bloque Occidental Jacobo Arenas and the Frente Carlos Patiño have used drones to secure control over the Micay Canyon, a fundamental enclave for cocaine processing (Torrado, 2025). For their part, Arauca, Guaviare, and Putumayo function as zones of strategic rearguard and export corridors, where denial of airspace hinders eradication efforts and state control.

The use of these devices in the Colombian conflict has transitioned from an experimental phase to a state of “technical-military maturity”. Initially, the armed groups adapted commercial and recreational drones to drop rudimentary explosive devices, such as PVC cylinders loaded with ammonium nitrate and shrapnel (Bonilla, 2025a). However, the ELN and the FARC dissidents have drastically increased investment in technology in order to achieve greater precision and lethality (Cifuentes, 2025b). The search for greater certainty has led criminal organizations to recruit specialists in programming and remote piloting, forming “drone-operator schools” in zones such as the Pacific and Cauca (Bonilla, 2025a).

Likewise, in response to the implementation of radio-frequency inhibition systems (jammers) by the state, the armed actors have initiated a phase of technological adaptation through the importation of fiber-optic-guided drones. This innovation, which Cifuentes (2025b) links to transnational technological flows originating from Iran via Venezuela, ensures a command, control, and real-time video link that is absolutely immune to electromagnetic countermeasures, so that the criminal groups “remain one step ahead”. Additionally, another critical aspect is the reconversion of high-capacity agricultural drones for the dissemination of chemical agents (Torrado, 2025). This tactic not only possesses a dimension of “small-scale chemical warfare”, but eventually saturates emergency-response capacities and, moreover, violates the fundamental principles of International Humanitarian Law, maximizing psychological terror through the invisibility of the attack.

To dimension the current asymmetric threat, it is imperative to analyze events that evidence the technical sophistication and capacities of the National Liberation Army (ELN) with the use of drones. A critical milestone occurred on 20 July 2025 in the municipality of El Carmen, Norte de

Santander, where troops of the Vulcano Task Force of the National Army were attacked at a military base by means of explosive-laden drones. The toll of this attack, three professional soldiers killed and eight military personnel seriously wounded, not only represents a human tragedy, but marks a turning point in the capacity of non-state actors to breach protected military enclaves (Cifuentes, 2025b).

From this incident it is necessary to note that it constituted a coordinated operation involving “airspace saturation”, which implies the existence of a command that coordinates and that planning would have occurred, considering furthermore that this technique allows that if one or two drones are intercepted another may still strike the target.

Regarding the foregoing, this event, attributed to the ELN, evidenced the vulnerability of the state’s security forces and the capacity of the armed groups to conduct “saturation operations”. The precision and operational success of the attack suggest a process of training and knowledge transfer that surpasses empirical learning and even opens the possibility that Latin American insurgent groups are adopting combat manuals from conflicts such as those of the Middle East.

Subsequently, another incident occurred on 21 August 2025 in the rural zone of the municipality of Amalfi, in the department of Antioquia, where a National Police helicopter was shot down by a drone attack in which 13 police officers died. The aircraft was heading to support a group of personnel engaged in manual eradication of illicit crops in the area (Ávila and Cueto, 2025b). The attack exposed shortcomings of anticipation, since intelligence reports had allegedly warned of the intention of criminal groups to attack aircraft in the zone. Although initially the authorship generated confusion, the Frente de Guerra Darío Ramírez Castro of the ELN claimed responsibility for the attack by means of a video on social networks on 4 September 2025 (Bernal, 2025a). This event stands out in the Colombian conflict, confirming that the armed actors now possess a real capacity for “anti-aircraft defense”, drastically limiting the state’s traditional superiority in low-altitude airspace.

As Cifuentes (2025a) sets out, in order to confront this threat, the authorities have invested in military anti-drone technology originating from Canada and Spain. The institutional response has been articulated mainly around two major fronts: the acquisition of massive defensive systems and the development of own offensive platforms. In the defensive sphere, the National Government implemented the “National Anti-Drone Shield Project”. With an investment exceeding 1.680 million dollars, this strategy seeks to deploy early-warning radars and inhibition systems in strategic garrisons, refineries, and the Casa de Nariño (Bonilla, 2025b). In the offensive sphere, the Colombian Aeronautical Industry Corporation (CIAC) developed the DRAGOM drone (Guided Reconnaissance and Attack Drone for Military Operations). This device possesses more than 90 minutes of autonomy, capacity to transport payloads of up to 10 kilograms, high-definition cameras, and a dual encrypted and satellite communication channel, permitting tactical intelligence and the execution of precise attacks with explosives (Cifuentes, 2025a).

Nevertheless, the efficacy of these measures has been severely questioned. As Bonilla (2025b) rightly argues, the response of the Colombian state has been late and fragmented. Technical and strategic analysis expose a fundamental disconnection between the capacities acquired and the operational reality of the conflict, because, in the first place, the static inhibition systems of the National Shield are designed principally to protect critical infrastructures in urban or semi-urban environments, leaving unprotected the jungle areas where the conflict is actually fought, since the state argues that it lacks the capacity to equip with inhibitors the more than 3.000 platoons deployed (Bonilla, 2025b; Torrado, 2025); in the second place, state bureaucracy presents a temporal lag vis-à-vis insurgent innovation, given that while the state requires lengthy procurement processes, the armed groups succeed in overcoming these defenses rapidly by changing frequencies, flying autonomously, and adopting fiber-optic-controlled drones.

The Colombian conflict has entered the era of unmanned aerial warfare. The capacity of these organizations to shoot down state aircraft and penetrate military bases demonstrates a level of sophistication that nullifies the traditional logistical advantages of the military forces. Likewise, the dissemination of chemical agents, the use of fiber optics to evade inhibitors, and surgical precision configure a panorama of highly complex asymmetric threat.

2.5 Drone Attacks in Mexico

In Mexico, the struggles among drug cartels have led them to seek new forms of deploying violence in order to exercise territorial control and predominate in the illicit business; consequently, they have incorporated “Claymore mines, rocket-propelled grenades, mortars fabricated from petrol-tank tubes, and armored trucks equipped with heavy machine guns. They are burying improvised explosive devices to kill their rivals and modifying drones purchased online to convert them into attack drones loaded with toxic chemical substances and bombs” (Villegas, 2025).

In this context, the tactic of explosive attacks using drones is employed by the drug cartels against other cartels, but also against the police and the army. Indeed, these attacks have left military personnel dead. This tactic is used principally by the Jalisco New Generation Cartel (CJNG), Sinaloa, and La Familia Michoacana cartels in Michoacán, Chihuahua, and Guanajuato (Jaramillo, 2025).

The explosive devices are of homemade manufacture. In fact, “the casings are usually made from plastic bottles, cut drainpipes, and even fire extinguishers. Steel, glass, and plastic fins are fitted to the devices to stabilize them during flight. Inside they contain homemade gunpowder and ammonium nitrate mixed with fuel, an explosive frequently used in mining and construction” (Villegas, 2025).

The CJNG is regarded as the precursor in Mexico of this modality; it currently even possesses a cell dedicated to this task, under the designation of “drone operators”, with a military style and the use of tactical attire. However, “security analysts and Mexican officials note that the cartels began

to militarize in the mid-2000s, when Los Zetas, a group formed by former members of the army, introduced battlefield discipline, encrypted communications, and heavy weaponry into organized crime” (Villegas, 2025). “The CJNG began to employ explosive-laden drones in Michoacán around 2020, using them in attacks against rival groups and local communities. Over time, this tactic was replicated in Guerrero by La Familia Michoacana, which has resorted to these devices to strengthen its territorial dominion and expand its influence” (Jaramillo, 2025).

These groups are reported to have acquired knowledge from military experience: “additionally, Mexican criminal groups have turned to the experience of former Colombian military personnel in order to improve and professionalize the adaptation of explosives on drones” (Jaramillo, 2025).

Regarding the origin of the drones, these are acquired commercially but adapted to carry and release explosive devices; nevertheless, more sophisticated explosive drones may also have been acquired abroad.

In April 2024, in Michoacán, the CJNG used drones to launch explosive devices containing chemical substances whose gases are reported to have produced effects on the respiratory tracts of the inhabitants of the zone, similar to the incidents that have been reported in Colombia (Jaramillo, 2025).

2.6 Drone Attacks in Brazil

The proliferation of Unmanned Aerial Vehicles (UAVs) in the Brazilian organized-crime ecosystem has radically transformed the dynamics of urban violence and public security (Pyatakov, 2025), owing to the appropriation and modification of commercial drones by groups such as the Comando Vermelho (CV), the Primeiro Comando da Capital (PCC), and the Terceiro Comando Puro (TCP) (Portal CIP, 2025).

Although the first documentations of weaponized “narco-drones” emerged on the Mexico-United States border at the hands of cartels such as the Jalisco New Generation Cartel (Diálogo Américas, 2023), the threat has expanded geographically, and Brazil has consolidated itself as a critical epicenter of this escalation (Pyatakov, 2025). In a context marked by the historical militarization of urban space and the metaphor of war in the management of the favelas (Leite, 2012), Brazilian criminal organizations have incorporated aerial dominion in order to evade the traditional terrestrial perimeters of the security forces and to project three-dimensional territorial control (Portal CIP, 2025).

Current operability can be classified into three categories: in the first place, Intelligence, Surveillance, and Reconnaissance (ISR) tasks stand out, carried out by actors such as the PCC, the CV, and the TCP to map police deployments, monitor authorities of the justice system, and identify vulnerabilities through the incorporation of thermal and infrared cameras and autonomous-flight

software (Portal CIP, 2025; Pyatakov, 2025). In the second place stands logistics and infiltration, operated principally by prison factions and port networks for the smuggling of narcotics, weapons, and communication devices by means of cargo drones equipped with release mechanisms (Pyatakov, 2025; Portal CIP, 2025). In the third place is narcoterrorism, led by the CV and the TCP, focused on “aerial bombing” with improvised explosive devices and grenades against rivals, civilians, and police, availing themselves of adapted electromechanical claws and first-person-view systems (InfoMoney, 2024; Pyatakov, 2025).

The transition of drones to platforms of lethal attack has altered the balance of the urban conflict in Brazil, given that, for example, it is possible to release grenades without the safety pin directly onto terrestrial targets (InfoMoney, 2024). Territorial fragmentation among the Comando Vermelho, the Terceiro Comando Puro, and paramilitary groups has precipitated an “aerial arms race” (The Dialogue, 2024). Police records indicate that systematic weaponization began during territorial disputes when the TCP, under the leadership of traffickers, started to use drones to bomb areas dominated by the CV (InfoMoney, 2024). In a documented incident that illustrates the indiscriminate nature of these attacks, a grenade was launched from a drone onto a public square in which children were playing, generating mass panic and profound psychological terror in the community (Band Jornalismo, 2024).

Attacks have also been directed frontally against the state. On 28 October 2025, within the framework of “Operation Contenção”, executed in the complexes of Penha and Alemão, the CV used drones to launch explosive devices onto agents of the Special Resources Coordination of the Civil Police (G1 Rio, 2025), an incident that the governor classified as “narcoterrorism” (G1 Rio, 2025).

Investigations further reveal a dangerous overflow of tactical knowledge from military institutions toward organized crime. In September 2024, the Federal Police’s “Operation Buzz Bomb” dismantled a network in Gardênia Azul that operated grenade-launching drones (Policia Federal do Brasil, 2024). It was discovered that a corporal of the Brazilian Navy was directly involved in the piloting and military adaptation of these devices for the criminal factions (G1 Rio, 2024).

In contrast to the open belligerence in Rio, the PCC in São Paulo employs drones under a corporate and mafia logic oriented toward high-precision tactical intelligence (Pyatakov, 2025). At the end of 2025, investigations by the Public Prosecutor’s Office revealed the plans of the Sintonia Restrita, a PCC cell dedicated to perpetrating attacks against state authorities (Record News, 2025). The criminals used drones to monitor meticulously the residences and routines of Lincoln Gakiya, a historic prosecutor in the fight against the PCC, and of Roberto Medina, coordinator of the penitentiary system (G1 São Paulo, 2025); for this purpose members of the faction rented adjacent properties in order to operate the drones with a direct line of sight, evaluating the height of the walls, the location of cameras, and the security vulnerabilities of the officials’ families, with the objective of planning selective assassinations (G1 São Paulo, 2025).

This technology of armed UAVs has surpassed the barriers of the large urban centers. In Itaberaí, State of Goiás, a criminal group operated a drone with explosives to extort and attempt against the life of a local businessman (Ôguen, 2026); however, the attack failed owing to a piloting error that caused the device to collide with a tree, yet it demonstrated that the technical barrier to executing acts of aerial terror is currently minimal and accessible to these groups (InfoMoney, 2024).

To counteract this asymmetry, the security forces are adopting counter-unmanned aerial vehicle systems. Current countermeasures operate mainly in detection and tracking through the use of passive radio-frequency (RF) systems and 3D digital-beam radars powered by artificial intelligence to discriminate autonomous drones (Ôguen, 2026). They likewise operate in neutralization, for which the government of the State of Rio de Janeiro has begun the acquisition of portable anti-drone rifles that interfere with the GPS signal at distances of up to 2 kilometers (Portal Nacional de Contratações Públicas, 2024). Nevertheless, adaptive criminality generates immediate countermeasures, so that in the face of the use of jammers the criminal incorporation of fiber-optic-guided drones occurs (Jovem Pan News, 2024). These devices, connected by micro-cables of up to 50 km in length, emit no radio signals and are completely immune to electronic interference (Jovem Pan News, 2024).

In definitive terms, the adoption of armed and surveillance drones by Brazilian criminal organizations is not a simple technological anomaly, but a systemic evolution in criminal governance and asymmetric conflict. Groups such as the CV, the TCP, and the PCC have demonstrated the capacity to apply “adaptive criminality”, transforming commercial devices into weapons of psychological terror and directed lethality. Confronting this threat requires a multidimensional response that integrates advanced countermeasures, forceful legal reforms, and policies oriented toward eradicating the transfer of military doctrine toward drug-trafficking networks.

2.7 Observed Convergences and Particularities in the Three Countries

The employment of drones by non-state criminal actors, with economic and/or political motivations, presents similarities across the three countries, yet also nuances and differences, owing to their own contexts and to the objectives pursued by the groupings that resort to this tactic, as well as to the spatial realities in which they operate.

In the case of Colombia, unlike the other two countries, it occurs within the framework of an internal armed conflict, in which these devices were incorporated as an extension of the armed capacities of the groupings involved, as a means of compensating for the asymmetry with respect to state capacities, in addition to the need to operate in zones of difficult access. At the tactical level, the incorporation of fiber-optic technology has been observed in order to evade inhibition systems, as well as the dissemination of chemical agents from drones, a situation that generates a high psychological impact. It must be specified that in this country the actors pursue objectives that combine political

and economic motivations, with pre-eminence of the latter, whereas in the other two countries the motivations are exclusively economic.

In Mexico, the preponderant feature of this phenomenon is that its purpose is the control of criminal markets, with its territorial implications regarding strategic zones for developing illicit businesses; therefore, drone attacks are a form of intimidating security forces and rival groups, through their psychological impact, in order to operate without difficulties: that is, this method is oriented toward the control of criminal markets. A distinctive element is the CJNG's "drone-operator units", with tactical attire and an implicit "professionalization".

On the other hand, in Brazil the principal particularity is that, unlike the preceding cases, it is exercised in densely populated urban environments, in the favelas, which are places of confined constructions and large numbers of inhabitants, dedicating its use to countering police action and thereby increasing the possibility of producing collateral damage owing to population concentration. Likewise, the use of drones for the surveillance of authorities has been evidenced, within the framework of assassination plans.

Table 1: Comparison of Drone Use in the Three Countries

Variable	Colombia	Mexico	Brasil
Actors	FARC dissidents and the ELN	Jalisco New Generation, Sinaloa, and Familia Michoacana cartels	Comando Vermelho and Primeiro Comando da Capital
Operational environment	Jungle and rural areas	Rural and semi-urban	Urban, densely populated
Objective of use	Confrontation with the armed forces, seeking to wear them down; territorial control for drug cultivation and other illicit activities	Territorial control, intimidation of rival cartels and security forces	Offensive against police operations in favelas, attacks on rival groups
Differentiating characteristic	Fiber optics to evade jammers, use of agricultural drones, dissemination of chemical agents	High-precision explosive-release mechanism, "swarm" attacks, artisanal drone construction, professionalization of "drone operators"	Attacks in urban areas, aerial surveillance, and plans for selective assassinations

Source: Authors' own elaboration.

This phenomenon shows that strategic convergence occurs in which this technology consolidates itself as a tool for the protection and strengthening of illicit economies through territorial control. In the three contexts, the use of these devices seeks to compensate for tactical asymmetry vis-à-vis the security forces, functioning as a force multiplier that enables guerrillas, cartels, and criminal groups to wear down the security forces and to subjugate, or at least intimidate, rival groups.

This adoption of readily accessible technology responds not only to an operational necessity but also, as has already been explained, pursues a psychological and coercive impact, employing aerial surveillance and attack to intimidate both the authorities and the civilian population and thereby “operate with relative impunity”. The most critical similarity lies in the capacity of these groups to evade countermeasures, succeeding in saturating or circumventing state responses through technical innovation and the exploitation of complex geographical environments, such as the jungle or the favelas, which poses a public-security challenge.

On the basis of the foregoing, specific challenges are shown for each country with regard to the neutralization of drones by law enforcement and security forces: for example, the theatre of operations of the Brazilian favelas, where high urban density hinders the deployment of countermeasures by the police; while in Colombia the use of fiber-optic technology represents a limitation for countermeasures such as jammers, in addition to the context in which it occurs, which, being an armed conflict, increases the temporality and intensity of its use; whereas in Mexico the complexity of confronting this threat is the tactical escalation determined by “swarm attacks” and high-precision explosive-release devices that limit or saturate police response capacity.

3. Conclusion

The reality of security in Latin America shows that the proliferation of unmanned aerial systems (UAS) has ceased to be a tactical innovation and has become the axis of a hybrid threat that redefines territorial control. This method has passed from being an emerging threat to becoming a present threat.

This phenomenon represents the materialization of the crime–terror continuum, in which criminal organizations in Mexico, Colombia, and Brazil adopt tactics of “asymmetric warfare” in order to dispute the monopoly of force. The integration of emerging technological capacities, illicit economies, and symbolic frameworks that legitimize violence consolidates the fact that these criminal actors reinforce hybrid forms of coercion and reinforces the relevance of Makarenko’s model for analyzing the contemporary transformation of non-state violence in Latin America. In this sense, the use of drones to execute attacks, conduct surveillance, and transport narcotics has eroded the traditional aerial superiority of states, compelling them to undertake a profound re-engineering of national-defense doctrines.

In Colombia, the shooting down of the helicopter in Amalfi on 21 August 2025, which resulted in the death of 13 police officers and was claimed by the ELN, marked a milestone in the capacity of the armed groups to deny airspace to the state. This sophistication is also manifested in the use of fiber-optic-guided drones, which are immune to conventional electronic-interference systems.

Despite institutional efforts to develop technological sovereignty and to install anti-drone systems, the absence of an integral strategy has generated ineffective containment. The state's response requires a profound re-engineering that prioritizes tactical mobility, preventive intelligence, and the capacity for technological adaptation in real time.

In Mexico, cartels such as the CJNG and La Familia Michoacana have militarized their actions through units of "drone operators" that employ improvised explosives to besiege communities and attack federal forces. Likewise, the use of drones for the dissemination of chemical agents in Michoacán and Guerrero implies a dimension of terrorism that occasions forced displacement and psychological impact upon the civilian population.

In Brazil, "Operation Contenção" of 2025 showed how the Comando Vermelho employs explosive-laden drones to harass elite units in dense urban environments. Meanwhile, in São Paulo the PCC uses this technology for precision surveillance of high judicial officials, demonstrating that the drone is a versatile tool both for direct offensive action and for advanced criminal intelligence.

In Colombia the armed forces are incorporating anti-drone systems and a bill to regulate their possession and use is also under consideration; nevertheless, it would be complex to guarantee the security of all personnel deployed on the ground. Together with the acquisition of technology and legal modifications, it is fundamental to establish civil-protection plans and to strengthen coordination among the state institutions with competence in the matter.

Toward 2030 the development of this threat is headed toward the deployment of autonomous swarms coordinated by artificial intelligence and the use of fiber-optic technologies to evade electronic warfare. The transition toward autonomous attacks and the possible dispersion of biological agents in urban centers represent risks for regional stability.

Regarding the foregoing, institutional success will not depend on isolated technological acquisitions, but on integral aerial governance that includes hemispheric legal harmonization and transnational cooperation.

It must be specified that, were this an exclusively political-violence phenomenon, the state response would fundamentally require attacking the narrative that sustains the struggle of the armed actors in order to diminish their social base of support, delegitimize their message, and generate demobilization. However, given that the motivations of these armed groups are not political or ideological, the strategy must not focus on the political dimension of the phenomenon, but mainly on addressing illicit activities such as drug trafficking and illegal mining, which constitute the sources of financing and motivation of these groupings – a situation that requires a police–military response, including the intelligence function, in addition to legal reforms and the intensification of state presence in specific territories.

4. References

- Ávila-Claudio, R. & Cueto, J. (2025a). Ataque aéreo en Amalfi: El derribo de helicóptero de la Policía y sus repercusiones. *Análisis de Conflicto y Seguridad*.
- Ávila-Claudio, R. & Cueto, J. (2025b, 24 August). Qué se sabe del ataque contra una base militar y el derribo de un helicóptero de la policía que dejaron al menos 19 muertos y decenas de heridos en Colombia. *BBC News Mundo*.
- Band Jornalismo. (2024). *Traficantes usam drone para lançar granada em praça no Rio de Janeiro* [Video]. YouTube.
- BBC Mundo. (2022). *Cómo los grupos armados en Colombia usan drones con explosivos*.
- Bernal, J. (2025a, 4 September). Atentado terrorista contra un helicóptero que dejó 13 policías muertos en Amalfi, Antioquia fue realizado por el ELN: El mismo grupo terrorista confirmó el ataque. *Infobae*.
- Bernal, J. (2025b). El Frente de Guerra Darío Ramírez Castro se atribuye ataque en Antioquia. *Reportes de Seguridad en Redes Sociales*.
- Bonilla, L. (2025a, 24 April). Drones de guerra: Así operan los grupos colombianos la nueva arma que siembra terror. *El Espectador*.
- Bonilla, L. (2025b). El ambicioso escudo antidrones con el que Colombia quiere combatir las ofensivas aéreas de los grupos armados. *BBC News Mundo*.
- Bustamante, A. (2020). Insurgencias criminales y guerra urbana en Latinoamérica: Una aproximación al proceso de urbanización regional y su impacto en la evolución táctica y operativa de las organizaciones criminales transnacionales. *Entretextos*, 12(35), 1-17.
- Cifuentes, I. (2025a). Desarrollo de tecnología militar y sistemas antidrones en el conflicto colombiano. *Ciencia y Poder Aéreo*, 18(2).
- Cifuentes, S. (2025b, 26 July). ELN y las disidencias de las Farc podrían estar usando drones con fibra óptica y visión nocturna para ataques y vigilancia precisa. *Infobae*.
- Colom, G. (2019). *La amenaza híbrida: Mitos, leyendas y realidades* (Documento de Opinión IEEE No. 24/2019). Instituto Español de Estudios Estratégicos.
- Crespo Alcázar, A. (2018). Radicalización social y subcultura de la violencia como legado de ETA: La agresión a la Guardia Civil en Alsasua como caso de estudio. *SCIO. Revista de Filosofía*, (14), 53-82.
- De la Corte, L. (2013). ¿Hasta qué punto convergen el terrorismo global y la criminalidad organizada? Parámetros generales y escenarios críticos. *Revista del Instituto Español de Estudios Estratégicos*, (1), 149-176.
- De Lorenzo de Guindos, D. (2026). La muerte desde arriba: Empleo de drones de ataque por organizaciones terroristas. *Logos Guardia Civil: Revista Científica del Centro Universitario de la Guardia Civil*, 4(1), 53-82.
- Diálogo Américas. (2023). *Organized crime and its use of drones to sow terror*.

- Folha de S.Paulo. (2025, 29 October). *El gobernador de Río de Janeiro califica de éxito la operación con al menos 121 muertos; familiares hablan de masacre*.
- G1 Rio. (2024). Cabo da Marinha é preso em operação da PF contra drones lança-granadas do tráfico. *Globo*.
- G1 Rio. (2025). Em retaliação à ação policial, criminosos lançam bombas com drones no Complexo da Penha. *Globo*.
- G1 São Paulo. (2025). PCC alugou casa vizinha e usou drones para monitorar promotor jurado de morte. *Globo*.
- García, J., & Hernández, A. (2024). Las disidencias de las FARC-EP: ¿Continuación de esta guerrilla o nuevos grupos criminales? *Política y Sociedad*, 61(2), 1-16.
- Ginn, P. & Goodwin, A. (2025, 30 October). *Crime by drone: A new paradigm for organized crime*. Global Initiative Against Transnational Organized Crime.
- Heise, M. (2025). Ataques con drones en Colombia y México como amenaza híbrida. *Al-Ghurabá*, (98), 12-19.
- InfoMoney. (2024). *Como funcionam os drones usados pelo tráfico para jogar explosivos em policiais*.
- InSight Crime. (2021). *How the CJNG responds to the death of its leaders*.
- InSight Crime. (2022). *Brazil's criminal groups and the challenge to state authority*.
- InSight Crime. (2023). *Drone warfare and criminal innovation in Latin America*.
- InSight Crime. (2024). *Colombia's FARC dissidents and the return of armed attacks*.
- Institute for Economics & Peace. (2026). *Global terrorism index 2026*. Institute for Economics & Peace.
- Jaramillo, J. (2025, 6 March). *Los drones refuerzan el arsenal criminal en América Latina y el Caribe*. InSight Crime.
- Jovem Pan News. (2024). *Especialistas alertam para uso de drones guiados por fibra óptica pelo crime organizado* [Vídeo]. YouTube.
- Leite, M. (2012). The metaphor of war extends across various urban domains. *SciELO Brasil*.
- Makarenko, T. (2005). *The crime-terror continuum: Modelling 21st century security dynamics*. University of Wales.
- Ôgüen. (2026). *Drones armados no Brasil: O caso de Itaberai e o novo risco à segurança*. Ôgüen Segurança Perimetral.
- Ortiz, R. (2015). El concepto de guerra híbrida y su relevancia para América Latina. *Revista Ensayos Militares*, 1(2), 131-148.
- Polícia Federal do Brasil. (2024). *PF reprime uso de drones lança-granadas utilizados por organização criminosa*. Ministério da Justiça e Segurança Pública.
- Portal CIP. (2025). *Unmanned aerial vehicles and organized crime in ports*.
- Portal Nacional de Contratações Públicas. (2024). *Facções criminosas do RJ usam drones carregados para "bombardear" inimigos*. PNCP.
- Pyatakov, A. N. (2025). The criminal use of drones in Latin America. *Aurora Journals*.

- Record News. (2025). *Veja detalhes do plano do PCC para matar autoridades em São Paulo* [Vídeo en programa Fala Brasil]. YouTube.
- Rios, H. (2025). Desarrollo estratégico del Ejército Nacional de Colombia, 75 años: Historia, modernización y desafíos del siglo XXI. *Escenarios Actuales*, (2), 203–225. Centro de Estudios e Investigaciones Militares.
- The Dialogue. (2024). *Is Brazil's security strategy making the country safer?* [Análisis].
- The Guardian. (2021). *Brazil's favelas and the rise of armed criminal governance*.
- Torrado, S. (2025, 30 August). Las disidencias multiplican los ataques con drones y encienden las alarmas en Colombia. *El País*.
- Villegas, P. (2025, 1 September). Drones y explosivos improvisados: Los cárteles de México adoptan armas de guerra moderna. *The New York Times*.

Author's Note on the Use of Artificial Intelligence: During the preparation of this article, the generative Artificial Intelligence tools Gemini and ChatGPT were used to assist with the preliminary search for bibliographic sources and with the stylistic review and proofreading of the text. Following the use of these tools, the authors thoroughly reviewed and verified the cited literature and edited the final content, assuming sole and full responsibility for the originality, analytical rigor, and accuracy of the manuscript.

Jocelyn Vega Vargas and Dulce Sarai González González

Radicalization Through Images: Extremist Propaganda in IS's Dabiq Magazine

Abstract

This article analyzes the images used in the fifteen issues of the English-language edition of Dabiq as a propaganda tool of the Islamic State (IS) between 2014 and 2016. To this end, a proprietary methodology was developed to facilitate the analysis of the images as constructions of narratives of collective identity, victimization, the organization's power, and its legitimacy as a state—all of which contribute to ideological radicalization and the symbolic legitimization of violence. Using ATLAS.ti software, a qualitative exploratory study was conducted with original manual coding of each photograph featured in the magazine, systematically categorizing the visual frames according to Entman's (1993) framing approach that predominated throughout its publications. Unlike previous studies that primarily emphasized utopian representations of the caliphate, the findings suggest a more pronounced predominance of images associated with its military capabilities.

This indicates that the photographic propaganda used in Dabiq largely focuses on glorifying the organization's military power and portraying its enemies through ridicule and dehumanization, thereby contributing to the normalization and legitimization of violence and potentially reinforcing narratives conducive to radicalization.

Keywords: IS, Dabiq, propaganda, ideological radicalization, visual frames.

Jocelyn Vega Vargas, Double degree in Law and International Relations from the Monterrey Institute of Technology and Higher Education.

Dulce Sarai González González, Double degree in Law and International Relations from the Monterrey Institute of Technology and Higher Education.

To cite this article: Vega, J. and González, D. (2026), Radicalization Through Images: Extremist Propaganda in IS's Dabiq Magazine, *Revista Internacional de Estudios sobre Terrorismo*, issue 18:69-87.

Received

06/23/2026

Accepted

07/30/2026

1. Introduction

As Cottee (2023, pp. 12–14) explains, just like terrorism, the term “radicalization” has multiple meanings; however, through an analysis of 50 studies on the subject, he explains that while anyone can be radicalized, he understands it to be a complex, multifaceted process and describes it as the accumulation of choices over time, involving both states and the individual’s “vulnerability.”

As Entman (1993, p. 2) points out, contemporary propaganda involves selecting certain aspects of perceived reality and making them more prominent in a text so that a causal, moral, and/or treatment-oriented interpretation is facilitated. Similarly, Bunzel (2015) notes that Islamic State (IS) was “founded by al-Qaeda in Iraq at a time when Iraq’s Sunni insurgency was rapidly losing momentum.” However, IS benefited from the political instability that arose following the Arab Spring, using it to expand regionally and establish a jihadist state in Iraq, where its radical rhetoric intensified and which would later expand, especially after the war in Syria in 2011 (Hoffman & Zeidel, 2021).

However, to achieve its expansion in the region, it was important to develop a media strategy. As part of this, IS expanded its target audience and began publishing English-language editions aimed at Western audiences, through magazines such as Dabiq (later Rumiya) (Milton, 2020, as cited in Qi, 2024).

Adapting to Western culture, IS selected images for Dabiq that projected narratives of victimization, heroism, and governance, using contemporary marketing tools as a soft power strategy to build a positive and idealized image of the “caliphate” and strengthen its legitimacy (Fahmy, 2020; Venkatesh et al., 2020; Kruglova, 2020; Archambault and Veilleux-Lepage, 2020, as cited in Qi, 2024).

According to Entman (2004, as cited in Winkler et al., 2021), photography is not neutral; it is possible to shape public perception through politics, emotions, and ideology (Goffman, 1974; Iyengar & Kinder, 1987; Scheufele, 1999, as cited in Winkler et al., 2021). In the case of IS, the magazine Dabiq served as a propaganda tool aimed at projecting an image of community, power, victimization, and legitimacy.

Therefore, this article analyzes how visual propaganda contributes to processes of ideological radicalization toward violent extremism through the images published in the fifteen issues of the Islamic State’s magazine Dabiq, published from 2014 to 2016 (Fahmy, 2020, pp. 264–265).

Rather than focusing on textual narratives, the study examines how visual elements construct meanings, reinforce ideological messages, and legitimize violence. The main theoretical framework is Robert Entman’s framing theory, which allows for the analysis of how images select, emphasize, and organize reality to shape audience interpretation.

From this perspective, the images published in Dabiq may contribute to ideological radicalization by visually framing collective identity, victimization, heroism, and existential threat, thereby creating symbolic narratives that normalize violence and strengthen extremist legitimacy.

2. Theoretical Framework

This research uses Robert M. Entman's framing theory to analyze propaganda. Entman notes that "framing essentially involves selection and salience" (1993, p. 53). Framing consists of selecting certain aspects of a perceived reality and making them more salient in communication. Frames can perform four principal functions: defining problems, diagnosing causes, making moral judgments, and suggesting remedies or treatments (Entman, 1993, p. 52).

Framing works by highlighting certain facts and giving them greater prominence. This is achieved through techniques such as repetition, strategic placement, or association with familiar symbols, which makes some elements more memorable while others fall outside the recipient's field of attention. In this way, framing directly influences the interpretation and processing of information (Entman, 1993, pp. 53–54). It possesses great persuasive power, as it is less intrusive than text; for this reason, it functions as a propaganda tool that allows for the construction of dominant narratives (Fahmy, 2020, p. 268).

Images are more effective than text at conveying messages, as they capture attention more effectively, amplify emotions, and reinforce narratives in a more visceral and memorable way, thereby influencing political attitudes (Baele et al., 2019, pp. 1–3). Furthermore, they help process complex realities and influence what is perceived as real (El Damanhoury & Winkler, 2018, p. 4). This persuasive power is rooted in the "betrayal of photography," where images construct a seemingly authentic representation of reality and legitimize war and conflict (Anfinson, 2021, p. 722).

IS propaganda relies heavily on visual framing to attract and maintain audience attention, reinforce its narratives, and preserve its credibility even in the face of leadership losses (Winkler et al., 2021, pp. 3, 9). According to Ellul, propaganda becomes more effective when it normalizes its ideology to the point where individuals obey impulses external to themselves (1962, as cited in Winter, 2020, p. 669). Thus, IS propaganda becomes a comprehensive strategy of radicalization.

Moreover, a study on IS videos notes that its visual propaganda was constructed using techniques of "abjection, shock, and horror," displaying violent and explicit scenes to generate adrenaline, erode empathy, and normalize suffering, thereby driving processes of radicalization (Venkatesh et al., 2020, pp. 1754, 1768). Another research paper asserts that these videos sought to intimidate adversaries, recruit sympathizers, and reinforce the group's narrative, revealing a new dimension of digital terrorism based on psychological, rhetorical, and theological strategies (2024:3; Fahmy, 2020:260).

3. Methodology

For the qualitative analysis of the images from the 15 issues of Dabiq, ATLAS.ti software was used. The analysis was divided into three groups: Dabiq 1–5, Dabiq 6–10, and Dabiq 11–15. In addition, a custom methodology was developed to analyze visual framing, involving the creation of specific codes.

The codes were based on five themes: utopia, images that portray the Caliphate as an ideal and prosperous society; governance and the state, images that project IS as a legitimate state with military capabilities, territorial control, and the ability to enforce order and coercion; martyrdom and heroism, images in which children and fighters are martyred, and leaders or fighters are glorified as heroes; enemy, images that expose or show the enemy as defeated; and victimization, where the consequences of the enemy's actions are presented.

Although the analysis focused on images and visual framing, the texts and captions were also analyzed to better understand and code them.

The theme of “Utopia” includes the following tags: `UTOPIAN_CHILDHOOD`, which portrays happy children at the center of the Caliphate; `COLLECTIVE_IDENTITY`, which projects an image of community and camaraderie; and `CALIPHATE_UTOPIA`, which depicts an idealized Caliphate with abundant markets, a happy society, and even doctors.

Under “Governance and State” are: `CALIPHATE_GOVERNANCE`, related to the exercise of control, the monopoly on violence, and military capability; `RELIGIOUS_AUTHORITY` and `RELIGIOUS_SYMBOLS`, linked to ideological imposition and religious imagery accompanied by narratives rooted in religion; `STATE_SYMBOLS`, such as IS emblems, flags, uniforms, and images of the coins created by IS; and `EXPLOITED_CHILDREN`, which reflects the use of minors within propaganda narratives, for example, to expose the enemy, construct a utopian image of the Caliphate, and portray children as the future of IS by showing them carrying weapons, wearing uniforms, and/or being trained as combatants.

The “Martyrdom and Heroism” category includes: `MARTYRDOM_CHILDREN` and `MARTYRDOM_ADULTS`, which refer to images of the martyrdom of civilians; `MARTYRDOM_HERO` and `HEROIC_FIGURE`, images intended to show martyred fighters in order to glorify them, portray a heroic image of a significant figure in IS history, or present dramatized scenes such as men on horseback with curved swords; and `FIGHTER_GLORIFICATION`, focused on the idealization of fighters.

The “Enemy” theme includes: `DEFEAT_THE_ENEMY`, which features images of the adversary being destroyed or weakened; `DEHUMANIZATION_OF_THE_ENEMY`, in which the enemy is depicted in a violent manner and stripped of individuality, whether dead or about to be executed;

and EXPOSURE_OF_THE_ENEMY, images that give a face to the enemy to identify or reveal their location.

Finally, under “Victimization,” there is the code VICTIMIZATION, which is used to identify depictions in which IS shows casualties or destruction resulting from enemy attacks.

The decision to create the codes in capital letters was made in order to facilitate the coding process in the software and to make the codes easier to identify.

4. Dabiq as a Visual Propaganda Device

Through Dabiq, IS expanded the international reach of its propaganda by publishing content in multiple languages, promoting a narrative aimed at influencing potential Western sympathizers and guiding them toward radicalization, while also dehumanizing and identifying its enemies (Fahmy, 2020, pp. 264–265). Likewise, Dabiq functions as a competitive system of meanings that shapes perceptions, fosters polarization, and seeks to mobilize its supporters (Ingram, 2017, p. 358).

On the other hand, gore content, characterized by the depiction of extreme violence and explicit suffering, was used by IS to amplify its propaganda and exploit fascination with the macabre, horror, and evil. Prolonged exposure to grotesque imagery can produce desensitization and encourage aggressive behavior. In this regard, a study on the visual content of Dabiq noted that its use of gore differed from most IS audiovisual productions, as it was primarily directed toward “Anglophone Muslims, especially those with Wahhabi and Salafi inclinations,” with the purpose of persuading them to join IS. Therefore, brutal images were employed in a calculated and strategic manner to generate impact on the target audience (Lakomy, 2019, pp. 146, 149, 157, 158).

5. Visual Framing of Collective Identity and Otherness

Propaganda contributes to the binary construction of otherness, framed as “us versus them,” in which IS presents itself as the legitimate defender of Islam, while anyone opposing the organization is portrayed as evil, unbelieving, and destined to fail (Qi, 2024:54).

This narrative is further legitimized through historical and contemporary experiences of Muslim communities, fostering a collective identity among IS followers and justifying the organization's hostile actions (Qi, 2024, Discussion section:1).

In fact, Milton (2020, cited in Qi, 2024:12) analyzed IS propaganda through 1,700 images, noting that the organization deliberately selected visuals representing both itself and its enemies, portraying the latter through violent imagery designed to capture the reader's attention.

IS's propaganda strategy is also embedded within the broader debate regarding the relationship between Islam and terrorism. In this regard, Qi (2024:4) refers to the essay by Graeme Wood (2015), who argues that IS's position on what it portrays as the "true Islam" generated extensive debate between those who agree with this interpretation and those who completely reject it. This discussion is particularly relevant because IS employed religious narratives as a mechanism for ideological legitimation and identity construction among its followers.

According to Qi (Makdisi & John, 1985; Mutahhari, 2014, as cited in Qi, 2024, Discussion section:6), the frequent emphasis on themes such as Islamic law and violent jihad contributed to IS's theological justification, which became one of the ideological foundations of the organization.

Although the central message remained consistent, the intensity with which certain themes were emphasized varied, particularly regarding religious narratives and the identification of the enemy, especially in Dabiq, the group's official English-language magazine (Colas, 2016a, as cited in Qi, 2024, Discussion section:9).

However, over time IS propaganda evolved from broad, generalized messages to propaganda content directed at specific audiences. In other words, the organization developed an understanding of its Western audience, allowing English-language videos to become an effective recruitment tool through the exploitation of frustrations and ideological inclinations (Cotte & Cunliffe, 2020, as cited in Qi, 2024, Literature Review section:13).

Indeed, by using English-language videos that appealed to identity, religion, and injustice, the group managed to reach a broader audience and generate a much greater impact (Qi, 2024, Literature Review section:11). This enabled IS to connect with individuals experiencing feelings of exclusion, identity crisis, or alienation, thereby reinforcing a collective identity grounded in religious and political belonging (Coolsaet, 2016; Roy, 2016, as cited in Qi, 2024, Discussion section: 22).

In other words, IS's religious foundation facilitated the construction of a narrative that projected and legitimized what the organization portrayed as the "true and correct" interpretation of Islam. At the same time, this narrative was reinforced through historical references to conflicts involving Muslims. Furthermore, by employing discursive strategies and propaganda techniques designed to evoke feelings of resentment, injustice, otherness, and identity, IS was able to expand regionally through its radical discourse. However, another technique that contributed to the organization's rapid growth was the use of imagery alluding to victimization and existential threat.

6. Visual Framing of Victimization and Existential Threat

Likewise, IS used the magazine Dabiq as a propaganda tool to disseminate its political and ideological strategy, challenge other jihadist groups, and threaten its Western enemies (Gambhir, 2014, p. 2). In

its early editions, the magazine reinforced a binary vision of the world divided between believers and unbelievers, projecting a sense of threat toward its adversaries while conveying legitimacy and belonging to its sympathizers (Gambhir, 2014, p. 4).

This duality between images of horror directed at enemies and utopian promises offered to supporters functioned as a mechanism for legitimizing violence, which the organization portrayed as a necessary means to achieve a sacred purpose (Venkatesh et al., 2020, as cited in Qi, 2024, IS Propaganda's Thematic and Tactical Development section: 1).

Themes such as "victimization, cruelty, utopianism, martyrdom, and apocalypse" also appeared prominently (Johnston, 2022; Lakomy, 2020; Price & Mooney, 2022; Winter, 2015, as cited in Qi, 2024, IS Propaganda's Thematic and Tactical Development section:2). These elements sought to construct a constant perception of threat and conflict, reinforcing emotional narratives capable of justifying extremist violence.

This can be observed in discursive examples in which, instead of referring to "Christians," the magazine employs language such as "cross worshippers" or "barbarians" (Rasoulkolamaki et al., 2025, "Sameness and Negative Diversity" section).

According to Rasoulkolamaki et al. (2025, p. 379), the magazine employs a discursive framework in which Muslims are portrayed as "victims" of oppression, while IS presents itself as the protector of the Islamic community. In this way, the violent actions carried out by the organization are interpreted as a justified response to the systematic victimization imposed by the "others."

Beyond the victimization depicted in its imagery, the organization also sought to generate emotional identification among individuals experiencing feelings of exclusion, alienation, or displacement, potentially facilitating recruitment processes.

Likewise, according to Cottee (2023, p. 13), radicalization does not necessarily stem from pathological differences, but also from factors such as anger, alienation, isolation, and the search for community. In this sense, IS propaganda exploited feelings of exclusion and displacement in order to attract individuals vulnerable to violent extremism.

Similarly, Cottee (2023, p. 15) discusses the vulnerability and impressionability of some Western IS recruits, underscoring the potential role of propaganda within broader processes of radicalization.

In other words, IS employed not only language that enabled readers to easily identify who the "alienated" groups were and who the "protectors" of Islam were, but also narratives of victimization and existential threat. In this way, the organization legitimized violence while simultaneously generating a sense of belonging among individuals susceptible to radicalization processes.

7. Visual Framing of Heroism and Martyrdom

A study on Dabiq indicated that IS identity was centered on projecting confidence and a divine path, in which hijrah (migration) and jihad (holy war or military self-sacrifice) were presented as obligations of the true Muslim and the only path toward salvation and eternal happiness. Themes such as “Virtues of Martyrdom,” “Obligatory Jihad,” and “Fear of God” reinforced the idea of sacrifice as something urgent and necessary (Hooker, 2015, pp. 58, 75, 86).

Herbers describes IS propaganda as a cult of death that glorifies both the deaths of its enemies and the martyrdom of its own members. Through images of death, IS transformed martyrs into propaganda tools and reinforced a narrative in which dying under the will of God acquired symbolic value. The abundance of martyr images in Dabiq demonstrates the organization's need to make them visible and publicly recognized (pp. 34, 38, 41).

In Dabiq, martyrs were portrayed through imagery distanced from gore and explicitly violent scenes. Bodies were shown intact, with wounds covered and peaceful facial expressions. Some altered images even included a glow resembling a Christian saint's aureole, symbolizing the mujahidin regarded as shahids by Allah. Thus, rather than shocking the reader, these images sought to familiarize audiences with martyrdom, transform it into a source of inspiration, and reinforce the idealization of the martyr figure (Lakomy, 2019, p. 159).

Regarding heroism, IS employed strategies of nomination and individualization in Dabiq, highlighting fighters through their names and personal stories in order to generate recognition, closeness, and empathy, as illustrated by the case of a soldier who died while helping another fighter (Rasoulkolamaki et al., 2025, pp. 883–884). This contrasts with the representation of its adversaries as collective, passive, and inferior actors (Rasoulkolamaki et al., 2025, p. 382; Rasoulkolamaki & Kaur, 2021, p. 656).

Likewise, Dabiq is filled with images of warriors dressed in black, carrying IS flags, riding horses, and wielding swords, accompanied by texts portraying them as brave knights. This medieval Islamic aesthetic associates jihadists with an ancient and pure form of warfare, evoking courage and commitment. The visual framing communicates the heroism of martyrdom and projects a powerful image of courageous fighters in order to attract more followers (Toguslu, 2019, p. 116).

IS also tends to frame the responsibility for resolving crises as belonging to men, promoting the idea that they must mobilize to protect their sisters, thereby constructing the figure of the hero as a necessary defender and associating mobilization with masculinity (Ingram, 2023, pp. 345–346). Furthermore, the organization instrumentalizes the image of children by portraying them as future warriors through depictions of military training and soldiers acting as paternal figures (Kaczowski, 2019, pp. 31–32).

In this way, IS employs visual and textual framing devices to reinforce its image of heroism. The organization presents itself as the ingroup capable of providing solutions and as the sole defender of Sunni Muslims, while the enemy outgroup is represented as responsible for both the crisis and its continuation (Ingram, 2023, p. 340; Kaczkowski, 2019, p. 26).

8. Visual Framing of Governance and the Caliphate Utopia

Through visual framing, IS portrayed the Caliphate in Dabiq as a utopian and ideal state-society in which Islam was practiced perfectly. Through images of well-supplied markets, united communities, clean streets, aid to those in need, and medical services, the group constructed the image of the Caliphate as a stable, prosperous, and fully religious state. Likewise, the representation of farmers and zakat collectors reinforced the idea of a devout and supportive Muslim community (Baele et al., 2019, p. 11; Toguslu, 2019, p. 109).

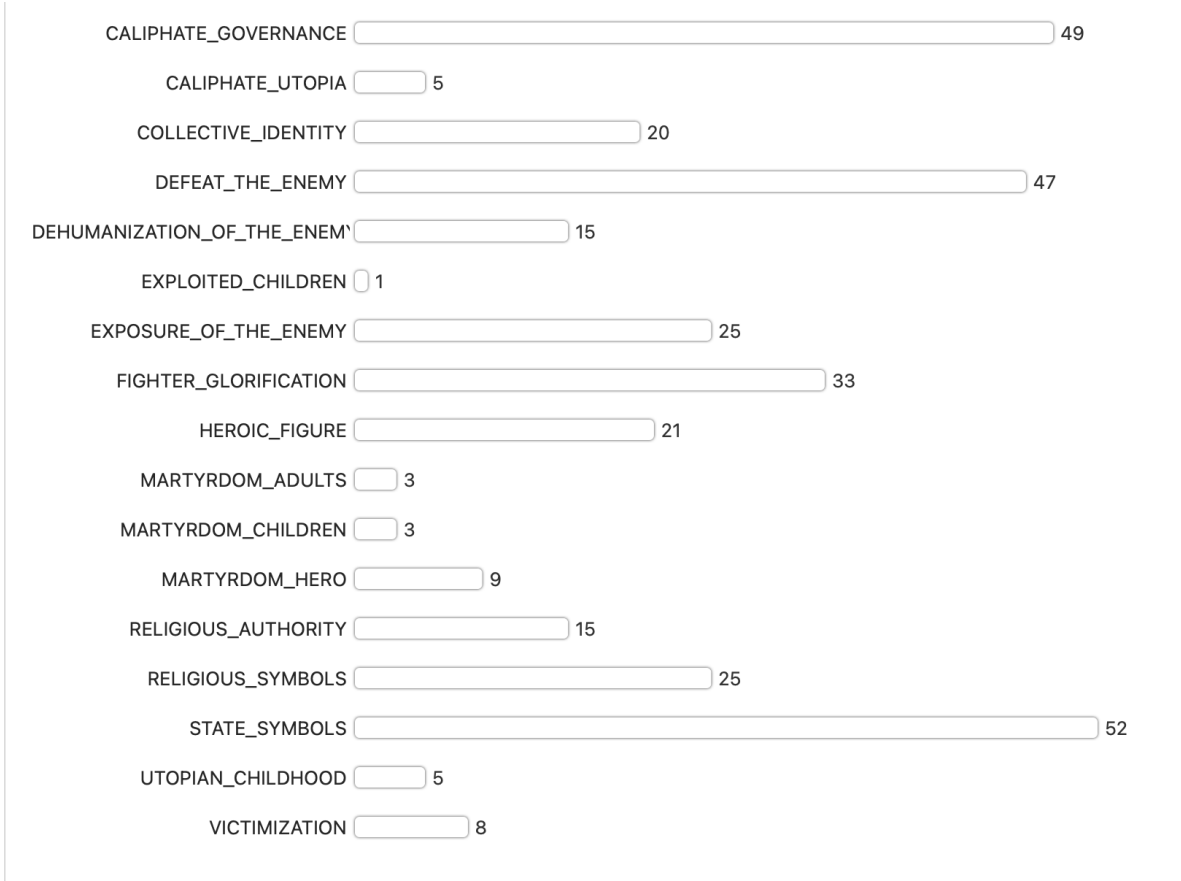
The appeal of the Islamic State's utopian propaganda also stemmed from the fact that it offered an ideological alternative to the status quo, grounded in millenarian foundations and associated with redemption and empowerment (Anfinson, 2021, p. 722). This governance framing was central to IS's global appeal, as Dabiq depicted the Islamic State as a functional, stable, and legitimate state with institutions, order, and control over the population, even though in practice its governance was far from effective (Anfinson, 2021, p. 732).

The images published in Dabiq were used to portray IS as a legitimate state possessing territory, population, governance, and international support. This visual framing sought to attract foreign recruits and reinforce the idea of the Caliphate as a sovereign project and a global Muslim community (Anfinson, 2021, pp. 720, 725–727).

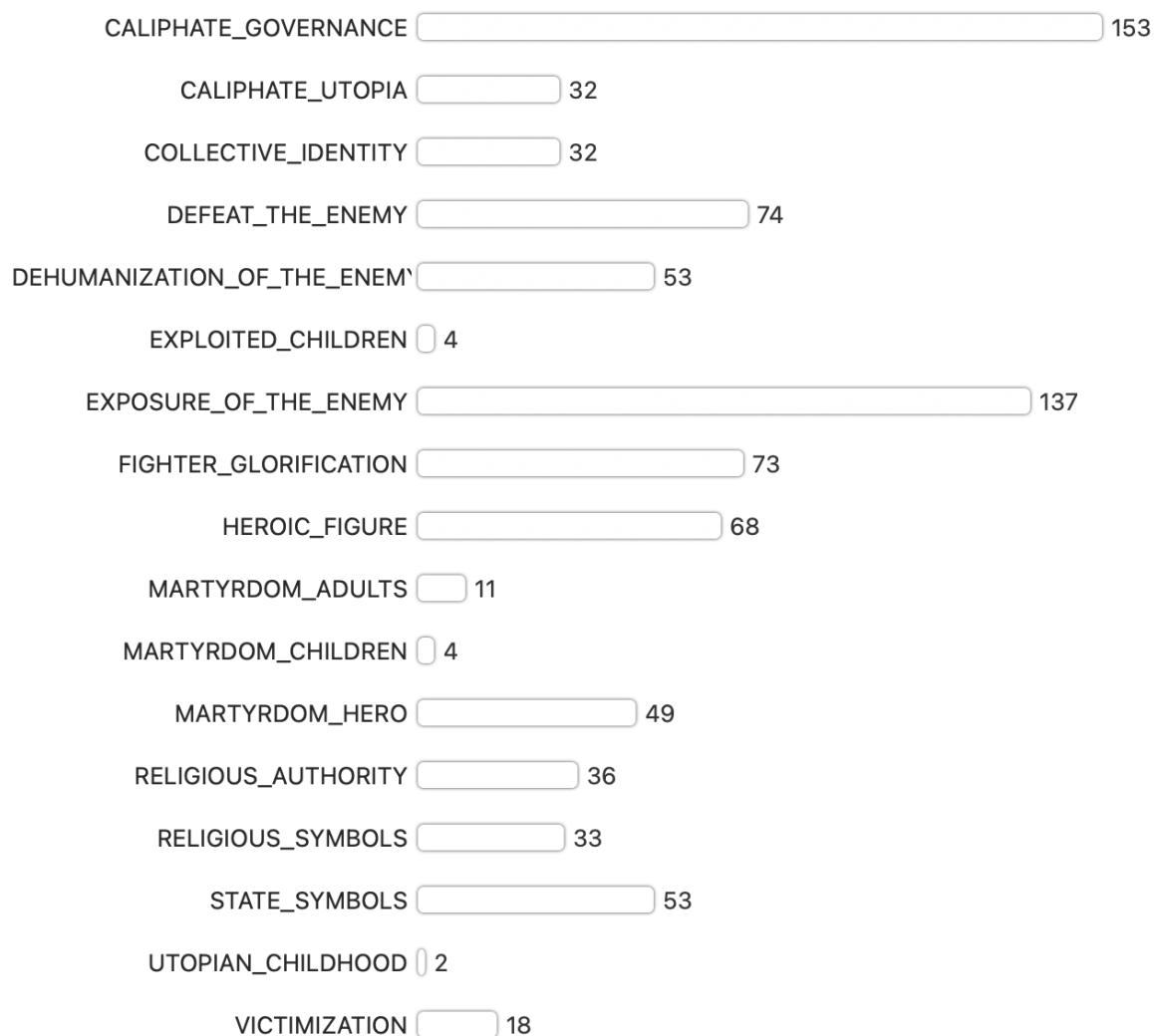
Likewise, Dabiq functioned as a strategy for constructing the idea of a total Muslim society by drawing upon religious and political concepts of Islam to legitimize IS and the Caliphate as an ideal society. Based on the idea that “There is no Islam except with jama’ah (community), and no jama’ah except with imarah (leadership), and no imarah except ta’ah (obedience),” IS argued that Islam could only fully exist within a unified community. Consequently, Muslims were portrayed as having a religious obligation to join the Caliphate and accept its leadership (Anfinson, 2021, p. 120; Toguslu, 2019, p. 109).

9. Results

Figure 1. Analysis with Atlas.ti Dabiq 1-5



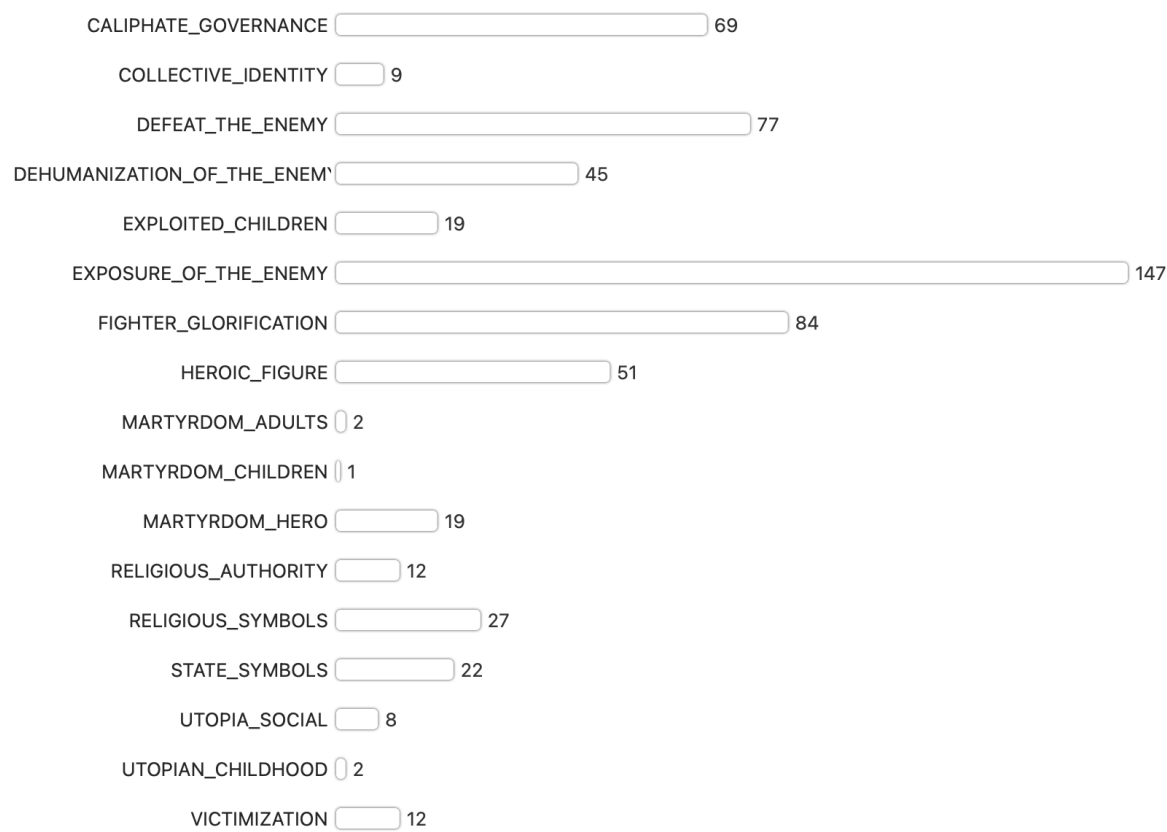
Within this group, the most predominant codes were STATE_SYMBOLS, followed by CALIPHATE_GOVERNANCE and DEFEAT_THE_ENEMY. In contrast, the least recurrent codes were EXPLOITED_CHILDREN, MARTYRDOM_CHILDREN, and MARTYRDOM_ADULTS.

Figure 2. Analysis with Atlas.ti Dabiq 6-10

Source: Own elaboration

Across volumes 6–10, the most prominent codes were CALIPHATE_GOVERNANCE, EXPOSURE_OF_THE_ENEMY, and DEFEAT_THE_ENEMY. The least frequent codes were UTOPIAN_CHILDHOOD, MARTYRDOM_CHILDREN, and EXPLOITED_CHILDREN.

Figure 3. Analysis with Atlas.ti Dabiq 11-15



Source: Own elaboration

The most predominant code across volumes 11–15 was EXPOSURE_OF_THE_ENEMY, followed by FIGHTER_GLORIFICATION and DEFEAT_THE_ENEMY. The least predominant codes were MARTYRDOM_ADULTS, UTOPIAN_CHILDHOOD, and MARTYRDOM_CHILDREN.

10. Discussion

In the Dabiq 1–5 group, unlike the other two groups, a large number of images were coded as STATE_SYMBOLS, with a high prominence of flags bearing the IS emblem. In addition, more images related to CALIPHATE_GOVERNANCE were identified, depicting tanks, weapons, and aircraft in order to emphasize the group’s military capability. This suggests that, during its early stages, IS sought to project an image of state legitimacy.

Another observation across all 15 volumes of Dabiq is that the weapons most frequently displayed were AK-47 rifles, turning this weapon into part of IS propaganda and the aesthetic identity of the mujahid.

Regarding the utopia of the Caliphate, unlike what was argued by Toguslu (2019, p. 109), only a very limited number of images related to services or welfare were identified, such as doctors, abundant markets, the restoration of electricity, or aid to those in need. Instead, symbolic and natural landscapes predominated, including mountains, trees, eagles, and temples, often accompanied by narratives or verses from the Quran in order to construct an idealized vision of the Caliphate. Likewise, within the utopian image of community, representations of camaraderie among mujahidin were more recurrent than depictions of crowds or broader communal populations.

With regard to images denoting religious authority, there was a high prominence of leaders considered important by IS accompanied by texts glorifying them. Particularly in Dabiq 11–15, there was an increase in images portraying IS members destroying temples or enemy religious symbols. Moreover, these later volumes included representations of leaders of the Catholic religion; in fact, the cover of the final volume depicts a man destroying a cross.

One highly recurrent religious symbol was the Quran, with numerous images showing people reading it, especially mujahidin. Likewise, in most volumes, individuals, leaders, mujahidin, and even children are depicted raising their index finger, a symbol meaning “There is no god but Allah,” which was appropriated by IS as part of its propaganda (Skoler, 2014).

Regarding images of instrumentalized children, these were more frequent in Dabiq 6–10 and 11–15, where children appeared carrying weapons, wearing IS uniforms, undergoing military training, or accompanied by a mujahid acting as a parental figure. These images were accompanied by texts presenting the training of children and the path of the mujahid as a divine duty, while also portraying children as the future of IS and the Caliphate.

In contrast, in Dabiq 1–5 the instrumentalization of children primarily occurred through martyrdom imagery, depicting deceased minors in order to appeal to the emotions of the viewer; this type of image disappeared in later volumes. The accompanying texts referred to them as *shahid* (martyrs) and framed their deaths as the result of enemy attacks. Regarding the martyrdom of adult civilians, the images were scarce and depicted bodies with peaceful expressions and clean wounds, reducing the grotesque impact.

Most martyrdom-related images portrayed mujahidin killed in combat or suicide operations. Although some included blood, the majority consisted of photographs showing them alive and smiling, accompanied by texts glorifying their sacrifice and idealizing their fate before God. These images functioned as a strategy of individualization by giving the martyr a face, name, and personal story in order to generate empathy and encourage recruitment.

Regarding heroic figures, dramatized scenes of medieval warriors on horseback carrying curved swords were identified, as noted by Toguslu (2019, p. 116). This heroic construction also included prominent IS leaders and idealized martyrs.

Regarding fighter glorification, representations of armed mujahidin posing or firing weapons were extremely frequent. Across all issues, images of heroic martyrdom, heroic jihad, and fighter glorification were consistently present. Both the images and accompanying texts included repeated calls for hijrah (migration) and jihad (holy war or military self-sacrifice), urging foreigners to join IS and participate in jihad as mujahidin (Hooker, 2015, pp. 58, 75, 86).

As for images portraying the defeat of the enemy, the most common scenes depicted temples or spaces destroyed following IS attacks, corpses of enemy fighters or civilians, and images displayed to “subjugated” populations in territories under IS control.

Regarding the dehumanization of the enemy, many images portrayed the bodies of killed fighters without visible faces, placed inside bags or surrounded by large amounts of blood, accompanied by texts expressing ridicule and hatred. Generally, their names were not mentioned, thereby stripping them of individuality.

Regarding dehumanization, this was particularly evident in the representation of hostages, mainly journalists and public figures, who were depicted wearing orange prisoner-style clothing, with shaved heads, beaten, and restrained by hooded individuals holding knives to their necks. Subsequently, some images portrayed them with signs reading “prisoner for sale” in order to demand ransom payments, and later they appeared either about to be executed or in the process of execution through shootings or beheadings.

It was observed that in each analyzed Dabiq group (1–5, 6–10, and 11–15) there was at least one image depicting a beheading. Nevertheless, the level of visual violence progressively increased in each issue, with the later images being the most graphic and grotesque.

Regarding the exposure of the enemy, two main categories were identified: Westerners, such as government leaders, journalists, and military forces, and traitors, represented by leaders of countries such as Saudi Arabia or members of groups such as Al-Qaeda. Although they belonged to Islam, they were portrayed as apostates or traitors. These images increased considerably over time, with a strong presence in Dabiq 6–10 and an even greater presence in Dabiq 11–15.

Finally, victimization predominated in Dabiq 1–5, where children, civilians, and destruction attributed to enemies were frequently depicted. In later volumes, IS focused more on projecting power and emphasizing the weakness of its enemies; therefore, Dabiq 11–15 presented a marked absence of these elements.

11. Conclusion

This study examined the visual propaganda published across the fifteen issues of *Dabiq* through Robert M. Entman's framing theory and a qualitative visual analysis conducted with ATLAS.ti. By systematically examining the visual frames associated with utopia, governance and statehood, martyrdom and heroism, the representation of the enemy, and victimization, the research provides a comprehensive account of how IS used photographic imagery to construct and reinforce its ideological narratives. The findings indicate that visual propaganda in *Dabiq* should not be understood merely as an aesthetic complement to textual discourse, but as an integral component of the organization's broader communication strategy, through which political legitimacy, collective identity, military strength, victimhood, and the moral justification of violence were visually constructed.

One of the main contributions of this study lies in identifying the evolution of these visual frames throughout the publication of *Dabiq*. The analysis reveals that the magazine did not maintain a static visual strategy between 2014 and 2016. In the earlier issues, images associated with state symbols, governance, victimization, and the construction of the Caliphate as a political and territorial entity were particularly prominent. These representations contributed to portraying IS not only as an armed organization, but also as a governing actor capable of exercising territorial control, enforcing authority, and providing the symbolic attributes associated with statehood. As the publication evolved, however, the visual emphasis increasingly shifted toward military capability, the exposure and defeat of enemies, and the glorification of fighters. This transformation suggests that *Dabiq*'s visual communication adapted to the changing political and military circumstances faced by IS.

A particularly relevant finding concerns the representation of the Caliphate as a utopian project. While previous research has emphasized images of prosperity, social welfare, community, public services, and everyday life as important components of IS propaganda, the present analysis found these representations to be comparatively limited. Instead, the visual construction of the Caliphate relied more heavily on symbols of authority, military power, territorial control, religious legitimacy, and collective identity. Consequently, the findings qualify the idea that *Dabiq* predominantly projected an idealized image of everyday life under the Caliphate. The visual legitimacy of IS appears to have been constructed not only through promises of a prosperous Islamic society, but also, and more prominently, through demonstrations of coercive capacity, religious authority, military strength, and the ability to defeat its adversaries. This constitutes one of the principal empirical contributions of the study.

The analysis also reveals an important asymmetry in the visual construction of the in-group and the out-group. IS fighters, leaders, and martyrs were frequently individualized through photographs, names, personal stories, and narratives of sacrifice, courage, and religious commitment. Such

representations provided members of the organization with recognizable identities and presented them as heroic figures whose actions embodied the values promoted by IS. Conversely, enemies were frequently represented through processes of dehumanization, humiliation, anonymity, and physical defeat. Corpses, prisoners, hostages, and defeated adversaries were often stripped of individuality or presented primarily as symbols of the weakness and moral inferiority of the out-group. The simultaneous individualization and glorification of the in-group and the dehumanization of the out-group therefore emerge as complementary visual mechanisms through which *Dabiq* reinforced a binary worldview based on belonging, exclusion, moral superiority, and antagonism.

The findings further demonstrate that violence itself was framed differently depending on the identity of those represented. The deaths of IS members were generally associated with martyrdom, heroism, sacrifice, and religious transcendence, whereas violence against adversaries was more frequently connected to humiliation, punishment, defeat, and dehumanization. Similarly, images of civilian victimization were particularly visible in the earlier issues and were used to attribute responsibility for Muslim suffering to IS's enemies. Taken together, these different representations contributed to constructing a moral framework in which violence committed by the organization could be presented as legitimate, necessary, defensive, or divinely sanctioned, while violence attributed to its adversaries reinforced narratives of injustice and existential threat.

These findings are relevant to the study of radicalization, although the relationship must be interpreted with methodological caution. The research does not demonstrate that exposure to particular images directly causes individual radicalization, nor does it measure audience reception or behavioral change. Rather, it identifies visual mechanisms capable of supporting narratives associated with radicalization processes. By reinforcing collective identity, establishing clear distinctions between the in-group and the out-group, legitimizing violence, glorifying fighters and martyrs, constructing narratives of victimization, and dehumanizing adversaries, the images analyzed create a symbolic environment potentially conducive to the acceptance of extremist interpretations and violent action. In this sense, the contribution of the study is not to establish a causal relationship between images and radicalization, but to identify and systematically analyze the visual frames through which extremist propaganda may contribute to broader processes of ideological socialization, legitimization of violence, and mobilization.

More broadly, the study contributes to the literature on extremist propaganda by demonstrating the analytical value of examining visual content longitudinally rather than treating an organization's propaganda as a homogeneous body of material. The comparison of the three publication periods, *Dabiq* 1–5, 6–10, and 11–15, shows that visual framing changed alongside IS's strategic circumstances. This suggests that extremist visual propaganda can function as an adaptive communication system in which images are selected and emphasized according to changing organizational priorities, military

conditions, and political narratives. Visual propaganda should therefore be analyzed not only in terms of what it represents, but also in terms of how those representations evolve over time.

The study nevertheless has limitations. As a qualitative analysis of the content produced by IS, it examines the messages constructed by the organization rather than their reception by audiences. Consequently, no direct causal inference can be made regarding the effect of individual images on radicalization, recruitment, or mobilization. Future research could address this limitation by combining visual content analysis with audience studies, interviews, experimental approaches, or analyses of individuals who consumed extremist propaganda. Comparative research involving other IS publications, such as *Rumiyah*, or propaganda produced by other jihadist organizations could also determine whether the visual patterns identified in *Dabiq* represent distinctive features of IS communication or broader characteristics of contemporary jihadist propaganda.

Ultimately, the analysis demonstrates that the visual dimension of *Dabiq* was not secondary to its ideological message. Images constituted a central mechanism through which IS represented itself, its political project, its fighters, its victims, and its enemies. The principal contribution of this article is therefore to show that IS's visual propaganda combined different and evolving frames of state legitimacy, military power, heroism, victimization, collective identity, and enemy dehumanization, while adapting their relative prominence to the organization's changing strategic circumstances. By identifying these patterns across the complete corpus of *Dabiq*, the study provides a more nuanced understanding of how extremist organizations use visual communication to construct legitimacy, normalize violence, and create symbolic narratives potentially conducive to ideological radicalization.

12. References

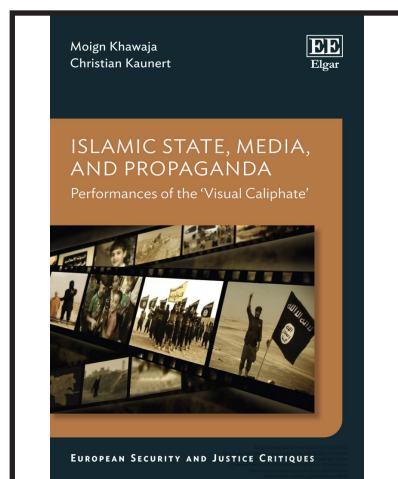
- Anfinson, A. (2021). The treachery of images: Visualizing "statehood" as a tactic for the legitimization of non-state actors. *Terrorism and Political Violence*, 33(4), 720–742.
- Baele, S. J., Boyd, K. A., & Coan, T. G. (2019). Lethal images: Analyzing extremist visual propaganda from ISIS and beyond. *Journal of Global Security Studies*, 4(4), 514–537.
- Berger, J. M. (2018). *Extremism*. MIT Press.
- Bunzel, C. (2015). *From paper state to caliphate: The ideology of the Islamic State* (Analysis Paper No. 19). The Brookings Project on U.S. Relations with the Islamic World.
- Cottee, S. (2023). *Radicalisation discourse: Consensus points, evidence base and blind spots*. Commission for Countering Extremism.
- El Damanhoury, K., & Winkler, C. (2018). Picturing law and order: A visual framing analysis of ISIS's Dabiq magazine. *Arab Media & Society*, (25), 1–30.

- Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, 43(4), 51–58.
- Fahmy, S. S. (2020). *The age of terrorism media: The visual narratives of the Islamic State Group's Dabiq magazine*. ResearchGate.
- Gambhir, H. K. (2014). *Dabiq: The strategic messaging of the Islamic State*. Institute for the Study of War.
- Herbers, L. J. (2016). *Media wars: The caliphate strikes back. Islamic State's propaganda magazine Dabiq as a possible paradigm shift in visual war reporting and propaganda* (Master's thesis, Lund University). LUP Student Papers.
- Hoffman, A., & Zeidel, R. (2021). ISIS in its own words: The history, strategy and ideology of the Islamic State [Book review]. *Strategic Assessment*, 24(1).
- Hooker, D. (2015). *Leadership in the reborn caliphate: Thematic network analysis of ISIL's e-zine Dābiq* (Master's thesis, Macquarie University). Macquarie University ResearchOnline.
- Ingram, H. J. (2017). An analysis of Inspire and Dabiq: Lessons from AQAP and Islamic State's propaganda war. *Studies in Conflict & Terrorism*, 40(5), 357–375.
- Ingram, K. M. (2023). An analysis of Islamic State's gendered propaganda targeted towards women: From territorial control to insurgency. *Terrorism and Political Violence*, 35(2), 338–354.
- Kaczkowski, W. (2019). Qualitative content analysis of images of children in Islamic State's Dabiq and Rumiya magazines. *Contemporary Voices: St Andrews Journal of International Relations*.
- Lakomy, M. (2019). Danse macabre: Gore images in the Islamic State's "Dabiq" magazine as a propaganda device. *The International Journal of Intelligence, Security, and Public Affairs*, 21(2), 143–161.
- Qi, Y. (2024). Propaganda in focus: decoding the media strategy of ISIS. *Humanities and Social Sciences Communications*, 11.
- Rasoulkolamaki, S., & Kaur, S. (2021). How ISIS represented enemies as ineffectual in Dabiq: A multimodal critical discourse analysis. *Discourse & Communication*, 15(6), 650–671.
- Rasoulkolamaki, S., Kaur, S., Zhdanava, A., & Mat Isa, N. A. N. (2025). In-group and out-group identity construction in extremist discourse: A critical multimodal approach. *Behavioral Sciences of Terrorism and Political Aggression*, 17(4), 377–395.
- Skoler, M. (2014, September 4). ISIS has a new hand sign — and it means far more than 'We're #1'. *The World from PRX*.
- Toguslu, E. (2019). Caliphate, hijrah and martyrdom as performative narrative in ISIS Dabiq magazine. *Politics, Religion & Ideology*, 20(1), 94–120.
- Venkatesh, V., Podoshen, J. S., Wallin, J., Rabah, J., & Glass, D. (2020). Promoting extreme violence: Visual and narrative analysis of select ultraviolent terror propaganda videos produced by the Islamic State of Iraq and Syria (ISIS) in 2015 and 2016. *Terrorism and Political Violence*, 32(8), 1753–1775.

Winkler, C., El-Damanny, K., Saleh, Z., Hendry, J., & El-Karhili, N. (2021). Intersections of ISIS media leader loss and media campaign strategy: A visual framing analysis. *Media, War & Conflict*, 14(4), 401–418.

Winter, C. (2020). Framing war: Visual propaganda, the Islamic State, and the battle for east Mosul. *Cambridge Review of International Affairs*, 33(5), 667–689.

Author's Note on the Use of Artificial Intelligence: *This document was prepared with the assistance of artificial intelligence (AI) tools, particularly for aspects of document structure and the review of some citations and references. All AI-assisted suggestions and text were reviewed and edited by the authors to ensure accuracy, clarity, appropriate academic tone, and consistency with the authors' own analysis. The final content reflects the authors' ideas and arguments.*



Islamic State, Media, and Propaganda: Performances of the 'Visual Caliphate'

Aarón Ferrando-Mkarbel

AUTHORS: Moign Khawaja and Christian Kaunert

YEAR OF PUBLICATION: 2025

EDITORIAL: Edward Elgar Publishing

Islamic State, Media, and Propaganda: Performances of the 'Visual Caliphate', by Moign Khawaja and Christian Kaunert, is a valuable contribution to terrorism studies because it shifts the analytical focus away from the spectacular violence of the Islamic State toward a more precise problem: how a terrorist organization sought to be perceived as a state through a systematic politics of images. This is its principal virtue. Rather than revisiting the debate over how much of the organization was genuinely "Islamic", the work interrogates its claim to "statehood" on the basis of a broad, carefully defined sample analyzed with methodological competence.

The authors proceed from a simple yet highly productive intuition: if the self-proclaimed Islamic State wished its subjects and sympathizers to recognize its claim to statehood and to support a political project with aspirations of permanence, it had to produce visible evidence of that statehood. Hence the notion of the "Visual Caliphate", understood as a propagandistic regime that not only proclaims authority but exhibits it, stages it and endows it with a documentary appearance. The book accordingly asks how the organization projected a form of "modern stateness" in its official videos and for what purposes it did so. The answer is articulated through a longitudinal visual analysis of 374 official videos published between July 2014 and July 2017, extracted after a rigorous screening of approximately 700 pieces located on social networks and digital repositories (pp. 12–13).

The methodological design is one of the text's major strengths. The research is not limited to the most celebrated productions or to the videos of extreme violence that circulated most widely in the press and on social media; rather, it analyses materials addressing themes such as population, territory, governance and foreign relations. This decision is important because it reconstructs Islamic State propaganda not merely as a display of terror but as a technology of legitimation. In other words,

Aarón Ferrando-Mkarbel, is a predoctoral researcher in the Department of Communication Sciences at Universitat Jaume I (Castellón).

Khawaja and Kaunert show that the organization did not seek only to intimidate; it also sought to persuade its audiences by projecting the appearance of a functioning political order.

The structure of the book responds clearly to this objective. After a prologue of strong interpretive weight, the second chapter situates the historical transition from the “paper state” to the territorial caliphate; the third develops the category of “modern stateness” on the basis of the Montevideo Convention; and the following four chapters analyze, respectively, the “performances” linked to population, territory, governance and foreign relations (pp. 37–38). The final chapter synthesizes the findings and offers a global reading of the Islamic State’s audiovisual project as a combination of theatricality, propagandistic calculation and the administration of visibility.

The scene of Abu Bakr al-Baghdadi in the Al-Nuri Mosque in Mosul in July 2014 is interpreted not as a simple historical document but as a carefully constructed staging. The authors describe the piece as a video “full of anomalies and theatrics” and turn that scenic dimension into the starting point of the analysis. The question is not whether the Islamic State was or was not a state in the full sense of the term, but rather how it sought to appear as one, what attributes it projected and what kind of recognition it sought to obtain from its subjects, its sympathizers and its enemies.

The empirical chapters are, taken together, the most solid part of the book. The chapter devoted to population shows how the propaganda stages an everyday life that appears normalized and ordered under the norms of the caliphate. The example of *A Visit to Mosul* is especially illustrative. The video combines the favorable testimony of a resident with the tour of a foreign fighter through various enclaves of Mosul. References to the conquest alternate with images of commercial activity, urban circulation, children playing in a park and sharia courts, culminating in the promise of a justice based on the word of God (p. 70). Here the propagandistic operation consists not only in informing but in producing an experience of itinerary. The city is presented as a governed, intelligible and administered space. This reading helps one understand why the content produced by the Islamic State cannot be reduced to a mere aesthetics of cruelty, since a substantial part of its efficacy depended on displaying an apparent normality.

The chapter devoted to territoriality is equally convincing. The work identifies a three-phase strategy of authentication: locating targets by means of maps, drones and other technical resources; attacking and occupying them; and, finally, exhibiting control over the population and infrastructures (pp. 114–116). The analysis is persuasive because it shows that technology performs a dual function. It serves to operate militarily, but also to persuade. In this context, the drone and the map operate as markers of technical rationality, as signs intended to present the state project not as a mere slogan but as a machinery supposedly capable of planning, conquering and governing.

The chapter on governance, for its part, adds a decisive nuance. Here the Islamic State appears caught between two necessities: presenting itself as a provider of order while continuing to exploit terror as one of its distinguishing marks. Khawaja and Kaunert show how certain pieces adopt conventions

proper to television formats of criminal investigation and procedural documentary in order to wrap violence in a visual grammar of evidence, confession and punishment (p. 151). The section on foreign relations completes that logic. The executions of Western hostages are seen as a form of informal “foreign policy” and as messages directed both at the adversary and at international public opinion. Propaganda therefore does not function as a simple showcase but as an instrument for strategically administering which facets of the organization are made visible and which remain hidden (pp. 171–173; 220).

From this point onward, the distinctive contribution of the book lies in systematizing that intuition through a longitudinal sample and in linking the images of government to a broader strategy of projecting that supposed state capacity. This finding is both novel and revealing for terrorism studies, for it compels one to think of propaganda not only as an instrument of radicalization or recruitment but also as a form of symbolic administration of power. The book is precise, moreover, in insisting that these stagings must not be taken at face value, since they are carefully scripted, edited and presented in order to project a favorable image of the caliphate in a context of low real state capacity and intense public scrutiny.

The volume nevertheless presents two limits that should be noted. The first derives from its own approach. Reception is inferred from the staging but is not triangulated with data on consumption or on the effective interpretation by audiences. This observation does not invalidate the findings, yet it does delimit their scope, for the book explains how the spectator is designed, not how each public has actually responded to those pieces. The second limit is temporal. The 2014–2017 delimitation is fully coherent with the object “caliphate”, but it leaves outside the more recent transformations in the circulation and diffusion of propaganda, especially those relating to automation and algorithmicizing.

Comparison with three recent works helps to specify its contribution more precisely. Against *ISIS’ Propaganda Machine*, by Ahmed Al-Rawi, which maps a much broader ecosystem of channels and formats, Khawaja and Kaunert renounce breadth in order to gain explanatory depth. Against *The Film of the Islamic State*, a reference work by Yorck Beese, they share the attention to audiovisual language but not the same diagnosis. Where Beese emphasizes the cinefication of media jihadism, Khawaja and Kaunert inscribe the aesthetics within a political strategy of political legitimation. And, when set against *Radicalization at High Speed*, by Katarzyna Maniszewska, the book can be read as an antecedent of the repertoires of authentication and affective administration that today circulate in an environment of greater technological automation.

In short, *Islamic State, Media, and Propaganda* is a serious, well-constructed and useful book. Its principal merit resides in treating the Islamic State with sufficient analytical distance to understand it as an actor that pursues recognition through various audiovisual proofs. Thanks to this, the work compels one to think of terrorism not only as a form of violence but also as a dispute over the regime of verisimilitude: what is accepted as evidence, what is perceived as order and what is interpreted as

a display of authority. It constitutes a relevant contribution, not because it puts an end to the debate on the legitimacy of terrorism, but because it offers a robust and replicable analytical matrix for continuing to study how violent organizations construct and disseminate their legitimacy through screens.

PIRA PROVISIONAL IRISH REPUBLICAN ARMY (OGLAIGH NA HÉIREANN)



ORGANIZATION TYPE:

Non-state, terrorist

IDEOLOGY:

Irish nationalist, republican

FOUNDERS:

**Seán Mac Stíofáin, Ruairi Ó Brádaigh,
Joe Cahill**

MAIN LEADERS:

**Seán Mac Stíofáin, Seamus Twoney,
Martin McGuinness, Kevin McKenna,
Thomas "Slab" Murphy**

PLACES OF ACTUATION:

**Northern Ireland, Ireland Republic,
Great Britain**

YEARS OF ACTIVITY:

1969-2005

ALLIANCES AND SYMPATHIZERS:

ETA, OLP, Gadafi's regimen, NORAIID

ESTIMATED MEMBERS:

8.000-10.000 along their existence

The Provisional IRA (Provisional Irish Republican Army), which called itself Óglaigh na hÉireann (The Irish Republic), was formed in December 1969 as a splinter group of the historic IRA. The split occurred at an Irish Republican Army convention held in County Roscommon: one faction accused the official leadership of abandoning armed struggle in favor of a political strategy. Seán Mac Stíofáin was the first Chief of Staff of the new organization. Its stated objective was to force the British withdrawal from Northern Ireland and the reunification of the island.

During the 1970s, the group transitioned from a relatively open battalion structure to a more cellular model of Active Service Units, which was more difficult for security services to penetrate. In parallel, Sinn Féin functioned as its political arm; figures like Gerry Adams and Martin McGuinness embodied the transition from armed struggle to negotiation.

The Provisional IRA was the deadliest organization in the Northern Ireland conflict: it is responsible for 1,768 of the more than 3,500 deaths during the Troubles, including over 450 British soldiers and hundreds of civilians. Among its most notorious actions were Bloody Friday in Belfast (1972), the assassination of Lord Mountbatten (1979), the bombing of the Grand Brighton Hotel during the Conservative Party conference (1984), and the Enniskillen bombing (1987). The group declared a ceasefire in 1994 and again in 1997, accepted the Good Friday Agreement of 1998, and announced the end of its armed campaign on July 28, 2005. On September 26 of that year, the Independent Disarmament Commission certified the decommissioning of its arsenal.

The Marrakech Attack, 24 August 1994

Historical and Contextual Background

An adequate understanding of the 1994 attacks in Morocco requires situating them within the evolution of Islamist extremism in the Maghreb, a region marked by incomplete decolonization, leadership rivalries between Rabat and Algiers, and the emergence of an armed jihad that, originating in Algeria, began to spill across borders. Morocco, an Alawite monarchy of authoritarian tradition under Hassan II, presented itself at the time as a pole of relative stability against the Algerian conflagration: a state that controlled official Islam through the Ministry of Habous and a network of loyal ulama, that had endured the so-called “Years of Lead”, and that based a substantial part of its international image and foreign-currency earnings on European tourism. That image of a secure enclave was precisely the symbolic target that the 1994 commando sought to pierce.

The immediate precursor was not a large-scale endogenous Moroccan movement, but the Algerian civil war. After independence in 1962, Algeria consolidated itself as a single-party socialist state under the National Liberation Front. In the late 1980s, economic deterioration, youth unemployment, and corruption opened the way to political Islamism. In December 1991 the Islamic Salvation Front (FIS) was on the verge of winning the legislative elections. The army annulled the process, dissolved the party, and launched a brutal repression. What followed was the “Black Decade”: a civil war between the security forces and armed Islamist groups, above all the Armed Islamic Group (GIA), which claimed between 150.000 and 200.000 lives. Massacres of civilians, assassinations of intellectuals, journalists, and foreigners, and a spiral of extreme violence marked those years and generated a militant diaspora that found in Europe (especially France) rear bases, recruitment, and financing.

From this matrix support networks emerged in the French banlieues. The cités of Seine-Saint-Denis (in particular the cité des 4000 in La Courneuve) and the outskirts of Lyon became spaces of radicalization. Young people of Algerian and Moroccan origin, many with records of minor delinquency, approached Salafist mosques and preachers who presented the Algerian jihad as a religious duty. Some traveled to training camps in Afghanistan or took part in the Bosnian war. From these networks the commando that operated in Morocco was organized. Behind the street-level executors operated figures such as

Abdelilah Ziyad (known as Rachid) and Mohamed Zinedine (Saïd), linked to the Moroccan Islamic Youth Movement and to contacts with the GIA.

The immediate geopolitical context was equally decisive. Rabat and Algiers maintained a deep rivalry centered on Western Sahara, occupied by Morocco after the Green March of 1975, and on leadership of the Maghreb. In 1993 Hassan II had handed over to the Algerian authorities Abdelhaq Layada, one of the founders of the GIA, a gesture that, according to later accounts, was not well received by certain sectors of the Algerian intelligence services (DRS). Some analysts and subsequent testimonies have maintained that elements of those services may have facilitated or tolerated actions intended to destabilize Morocco, although this thesis was never conclusively proven in a court of law. Marrakech was selected as a target for its symbolism: a tourist paradise that, in the eyes of the militants, represented the opening of the “apostate” regime toward the West and the presence of foreign “infidels” on Muslim soil, thereby maximizing the psychological, economic, and diplomatic impact.

The assault on the Atlas Asni was not an isolated incident but the visible culmination of an escalation that had begun in 1993. On 2 September of that year an assault took place on the first McDonald’s restaurant opened in Africa, located in Casablanca, which left three dead and eleven wounded. Shortly afterward, an attack on a banking entity in Oujda, near the Algerian border, left several security agents dead and a substantial haul. These events were initially attributed to ordinary crime, but the later confessions of those detained in 1994 forced their reinterpretation as the first steps of a jihadist campaign aimed at striking the stability of the kingdom and its tourist industry.

Planning and Preparation of the Attacks

Planning of the attacks began several months earlier, revealing a coordinated operation from France, orchestrated by a Franco-Maghrebi network inspired by the Algerian jihad and connected to the GIA. Preparations involved a group of young men recruited in the banlieues. Among them were Stéphane Aït Idir, a 22-year-old Franco-Algerian from La Courneuve; Redouane Hammadi, a 24-year-old Franco-Moroccan, also from the same cité; Tarek Felah; Kamal Benachka; Abdesslam Guerrouaz; Hamel Marzoug and others. According to Aït Idir’s own confessions before the examining magistrate in Fez, he had traveled to Morocco “to take part in the holy war” and had been promised “one of the best places in paradise”.

Training included the handling of Uzi automatic weapons, Kalashnikovs, and combat shotguns, rapid-assault tactics, and ideological indoctrination that presented Hassan II’s regime as illegitimate and European tourists as part of a Western presence to be expelled. Logistics contemplated the transfer of weapons across the eastern border and the use of stolen or rented vehicles. The principal target was tourism, the kingdom’s main source of foreign currency, and in particular Marrakech, a city symbolic

of prosperity and openness to the Western world. The Atlas Asni hotel, located in the Guéliz district, was carefully chosen: it was a high-category establishment that regularly housed European tourists, especially Spaniards and French. The attackers knew the building: they entered via a little-visible service corridor and chose the hour when the previous day's cash was being tallied. The intention was not solely robbery, since they took only a modest sum, around 10.000 dirhams, but to generate terror, maximize media impact, and send a clear political message to the palace.

This preparatory phase illustrates the hybrid nature of the commando: it was not a hierarchical organization of regional scope, but a small, transnational, and relatively amateur cell, fed by preachers, neighborhood networks, and geographical contiguity with the Algerian war. The operation involved at least a dozen individuals, with roles divided among recruitment and ideology (Ziyad and Zinedine), logistics (weapons transfer and lodging), execution (the trio that stormed the Atlas Asni), and supporting actions in other cities. Nevertheless, errors such as the use of stolen vehicles abandoned a short distance away, the concentration of an arsenal in relatives' homes, and the ease with which several members were located in Fez, Taourirt, and Aknoul revealed a limited organizational level, although this did not prevent the punctual lethality of the main assault.

Course of the Attacks

On 24 August 1994, a Wednesday in high tourist season, Marrakech was teeming with activity as thousands of European visitors thronged the medina, Jemaa el-Fna square, and the hotels of the Guéliz extension. The sequence of events concentrated around 10:30 a.m., at a moment calculated to coincide with the hotel's cash operations and with the presence of a small group of tourists in the lobby.

Three hooded men, Stéphane Aït Idir, Redouane Hammadi, and Tarek Felah, burst into the lobby of the Atlas Asni hotel through a service corridor. They opened fire indiscriminately, headed for the cash desk, and took approximately 10.000 dirhams. They shot at the small group of tourists present. Antonia Cuevas, aged 35, and Salvador Torras Turrel, aged 43, both Spanish, were killed. A French citizen was seriously wounded. The hotel director would later state that the attackers knew the building and the cash-operation timetable perfectly. The assailants fled in a stolen vehicle that they abandoned shortly afterward.



Figure 1: The Atlas Asni hotel in Marrakech, scene of the principal attack of the summer of 1994.

It was not an isolated incident. In the following days further actions by the same milieu occurred. On 25 August a group opened fire on police in Fez without causing casualties. Shootings and threats were recorded in Casablanca, including an attack on the wall of the Jewish cemetery. The Moroccan authorities linked these events to the 1993 assaults on the McDonald's and the banking entity in Oujda. The pattern was clear: small, highly motivated groups that combined robbery with the will to cause civilian casualties and to destabilize the country's security climate. Tarek Felah managed to escape to Europe. The others were arrested in the following days in Fez, Taourirt, and Aknoul. In the home of relatives of one of the detainees an arsenal was discovered consisting of rifles, grenades, ammunition, and portable radios. The confessions of those captured revealed the existence of a wider network and the intention to continue with similar attacks in other tourist cities.

The immediate chaos at the Atlas Asni was brief but intense, as eyewitnesses described: shots in a closed lobby, tourists lying on the floor, a receptionist threatened with a weapon to the temple, and the assailants' hurried flight toward a vehicle they soon abandoned. Material damage to the building was limited, but the human and symbolic damage was immediate. The choice of target and timing was strategic: a high-category hotel in the most emblematic city of Moroccan tourism, with guaranteed European victims, maximizing repercussions in the Spanish and French press and forcing the regime to acknowledge that the Algerian jihad had crossed the border.

Victims, Immediate Consequences, and Humanitarian Response

The final toll of the 1994 campaign confirmed two persons of Spanish nationality killed at the Atlas Asni and several wounded, among them a French citizen, Moroccan citizens, and security agents.

The response of the security forces, directed by the powerful Interior Minister Driss Basri, was rapid and forceful. In the hours and days after the assault most of the commando were arrested. Bomb threats occurred at the central station in Rabat and at the Congress Palace in Marrakech; these proved false but generated panic and demonstrated the groups' capacity to create alarm. Hassan II's government officially accused the Algerian intelligence services of being behind the operation, an accusation that Algiers rejected with virulence. On 27 August 1994 Morocco unilaterally closed the land border with Algeria, a measure that remains in force to this day and that symbolized the total rupture between the two countries.

Economically, Marrakech tourism suffered an immediate blow: massive cancellations of reservations and a perception of insecurity that the regime hastened to combat through an intense communication campaign and a visible reinforcement of police presence. The material cost was limited by comparison with later attacks such as those of Casablanca 2003 or Marrakech 2011, but the symbolic damage was enormous. Morocco, which presented itself as a stable and secure destination against Algerian violence, was forced to acknowledge the permeability of its borders and the existence of jihadist cells with external connections. The border closure with Algeria had lasting economic and human consequences for populations on both sides.

Investigation, Arrests, and International Collaboration

The investigation, led by the Moroccan Interior Ministry under Driss Basri, involved forced but decisive collaboration with France (country of residence of the majority of the detainees) and close monitoring by Spain, given the nationality of the two fatalities. Operational leads included the stolen vehicle abandoned after the assault, the testimonies of hotel staff, and above all the location of an arsenal in Aknoul. These leads produced a rapid series of arrests in Fez, Taourirt, and Aknoul.

The arrests made it possible to reconstruct the network. Interrogation of the detainees supplied details on recruitment in the banlieues, indoctrination, weapons logistics, and the intention to repeat attacks in other tourist cities. France was obliged to collaborate: arrests and searches were carried out in several French cities. Judge Jean-Louis Bruguière opened an investigation that revealed links with Algerian Islamist networks and recruitment in the cités. The French authorities found themselves caught between pressure from Rabat, which demanded firm action, and the reality of a Maghrebi community that viewed any hardening of counter-terrorist policies with suspicion.

This investigative phase exposed the transnational character of the phenomenon: it was not a local gang of robbers, as had been believed in 1993, but a jihadist cell with rear bases in France, inspiration

drawn from the Algerian war, and a declared objective in Moroccan tourism. At the same time, the thesis of direct control by the Algerian services, vigorously advanced by Rabat, was never conclusively demonstrated, and Algiers rejected it as a diplomatic maneuver. The “international collaboration” of 1994 was therefore unequal and laden with suspicion: effective in arresting most of the commando, insufficient to resolve the geopolitical enigma that the attack left open between the two shores of the Maghreb.



Figure 2: Stéphane Aït Idir on 27 January 1995, leaving the trial held in Fez in which he was sentenced to death.

Trials, Sentences, and Retrospective Justice

The trials opened in Fez on 10 January 1995 and concluded on 28 January before the Court of Appeal. Seventeen defendants, of whom seven were Franco-Maghrebi and the remainder local, appeared in a process that the regime presented as a demonstration of state firmness. Stéphane Aït Idir, Redouane Hammadi, and Hamel Marzoug were sentenced to death. Others received life imprisonment or terms of between six and twenty years. Amnesty International denounced procedural irregularities, allegations of torture during detention, and a trial it considered precipitate. Ultimately the death sentences were not carried out.

In 1996 another trial of the network was held in Paris. Abdelilah Ziyad admitted having organized the attack on the Atlas Asni and assumed responsibility for having ordered the assailants to attack tourists. Links with the GIA and with Algerian commanders were partially clarified, although the thesis of direct control by the Algerian services was never conclusively proven. These proceedings highlighted ethical and diplomatic tensions: criticism of the rigor of the Moroccan procedure, the French dilemma between counter-terrorist cooperation and consular protection, and the debate over whether the episode was a radicalized common crime or the first act of an exported jihad. The episode

formed part of the context that, months later in the summer of 1995, would culminate in the wave of GIA attacks in France, carried out by another cell (that of Khaled Kelkal), but with similar ideological and recruitment roots.

Long-Term Impact and Lessons Learned

The 1994 attacks and the 1995 trial compelled Morocco to reinforce its internal security apparatus and to tighten cooperation with France and Spain. Surveillance of Islamist networks and of arms flows toward Algeria was intensified. At the regional level, the border closure became a symbol of the rupture between the two countries and of the inability of the Arab Maghreb Union to advance. For the Moroccan authorities the episode demonstrated that the kingdom was not immune to the export of Algerian jihad. For France it highlighted the problem of radicalization in the banlieues years before it erupted with greater force in 1995 and, later, in the 2010s.

Tourism in Marrakech recovered over time and the city demonstrated resilience, yet the memory of those days remained as a reminder of the fragility of security in a context of transnational radicalization. The recollection of the Atlas Asni receded into the background beside the major later attacks (the already-mentioned Casablanca 2003 and Marrakech 2011), which far exceeded the lethality of 1994 and forced a deeper redesign of the kingdom's counter-terrorist architecture. Nevertheless, the events of August 1994 constituted the first serious warning that Islamist terrorism had reached Morocco, and that the borders of the Maghreb no longer fully isolated either of the two shores of the Mediterranean.

Although the death sentences were not carried out and some of those convicted later became the object of proceedings in Europe, the message of state firmness remained clear. Key lessons include the need not to underestimate threats that appear "imported" or of low intensity, the importance of shared intelligence with the countries of residence of the attackers (in this case France), the risk that hotels and tourist enclaves concentrate the symbolic calculus of small cells, and the lasting geopolitical cost of a security crisis that is read simultaneously as a jihadist crime and as an episode of Maghrebi rivalry. The Atlas Asni was, above all, the moment when a kingdom that believed itself sheltered discovered that contemporary jihad was already operating on its territory.

EPHEMERIS



16TH MAY 2026

A joint operation conducted by United States and Nigerian forces in Borno (Nigeria) neutralizes Abu Bilal al-Minuki, a senior commander within the global structure of Islamic State. Several of his closest collaborators were also killed. Al-Minuki's death is seen as one of the most significant losses suffered by the organization in recent years.

1



15TH MAY 2026

Mohammad Baqer al-Saadi is arrested in Turkey. He is identified as the principal figure responsible for the campaign of attacks carried out in Europe under the cover of Harakat Ashab al-Yamin al-Islamiyya (HAYI). This organization claimed responsibility for approximately twenty antisemitic and anti-American actions in various European countries during the months of March and April.

2



30TH MAY 2026

In the wake of the violence in Paris following Paris Saint-Germain's victory in the UEFA Champions League final, leaders of the far right - among them Jordan Bardella, president of the National Rally - intensify their discourse focused on security and immigration. Prominent European figures associated with this ideological current call for mass deportations.

3



17 JUNE 2026

Islamic State fighters in the Sahel Province launch a coordinated assault on a military base in Inâtes (Tillabéri, Niger), resulting in the deaths of 71 Nigerian soldiers. The Islamic State affiliate in the Sahel has intensified its operations in an attempt to seize territorial control from its rival JNIM (an Al-Qaeda affiliate) and from government forces.

4



18TH JUNE 2026

JNIM claims responsibility for an attack on Diori Hamani International Airport in the Nigerien capital, Niamey. This constitutes the second assault on the airport in 2026, following the attack of 29 January carried out by factions affiliated with Islamic State. These offensives demonstrate the terrorists' capacity to project violence against critical infrastructure in the country.

5



19TH JUNE 2026

The Swiss government submits a report to Parliament proposing a new specific law to prohibit Nazi symbols in public spaces. At present, the Swiss Criminal Code only permits the prosecution of the use of Nazi symbols for propagandistic purposes, thereby leaving a legal gap for those who display such symbols without the intention of disseminating extremist ideas.

6



23RD JUNE 2026

Fourteen members of the Bangsamoro Islamic Freedom Fighters (BIFF) surrender to the authorities in Maguindanao del Sur. The jihadist landscape in Southeast Asia in general, and in the Philippines in particular, is becoming a residual phenomenon, largely thanks to the counter-terrorism efforts of the region's security forces.

7



6TH JULY 2026

1. A large-scale operation by the Spanish National Police conducted in Toledo, Madrid, Barcelona and Ceuta results in the arrest of four individuals who had embraced the ideology of Islamic State and displayed highly radicalized and violent profiles. The detainees are also accused of alleged offences of indoctrination, self-training and glorification of terrorism.

8



17TH AUGUST 2026

Nine years have passed since the terrorist attacks in Barcelona and Cambrils, in which a cell inspired by Islamic State attacked pedestrians on Las Ramblas in Barcelona and, hours later, in Cambrils. The attacks caused the deaths of 16 civilians and injured more than 130 people, ranking among the most serious terrorist attacks suffered by Spain in recent decades.

9



25TH JULY 2026

An individual drives a van into people gathered near the Christopher Street Day celebrations in a Berlin park. The attacker subsequently continues the assault using a bladed weapon. The casualty toll stands at one Polish woman killed and at least 29 injured.

10

DID YOU KNOW THAT...?

On December 22, 2001, just three months after 9/11, British national Richard Reid, known since then as the "shoe bomber," boarded American Airlines Flight 63, en route from Paris to Miami, with explosives concealed in the soles of his shoes.

Once on board, he attempted to detonate the device and was subdued by the crew and several passengers. The diverted plane landed in Boston. Reid, who had been converted and trained by Al-Qaeda, was sentenced to life imprisonment. This incident explains why, since then, countless airports around the world have asked travelers to remove their shoes at security checkpoints.



On April 9, 1985, Sana Yusuf Muhaydli, a 16-year-old Lebanese militant of the Syrian Social Nationalist Party (SSN), drove a vehicle loaded with explosives into an Israeli checkpoint and convoy near Jezzine, in southern Lebanon. Israeli soldiers were killed in the attack, and according to some accounts, a Lebanese soldier was also killed.

Muhaydli was not a jihadist: the SSN is a secular nationalist organization with Syrian roots, at the time part of the Lebanese National Resistance Front against the Israeli occupation of southern Lebanon.

Hours earlier, she had recorded a farewell video, sitting at a table, speaking in the tone of someone reading a statement. That same April 9, the video was broadcast on Tele Liban news and later circulated on VHS tapes. The Beirut press dubbed her "the bride of the South." Researchers of the phenomenon agree that she was the first woman to commit a suicide attack in the contemporary era, and her recording was one of the first video testaments broadcast on television.



Following the attack on the Munich Olympic Village on September 5, 1972, West Germany decided to create an anti-terrorist force. On September 26, 1972, Interior Minister Hans-Dietrich Genscher ordered the creation of Grenzschutzgruppe 9 (GSG9) within the Federal Border Guard.

Five years later, on October 13, 1977, in the midst of the "German Autumn" (a campaign of mass bombings carried out by the RAF), a commando unit linked to the PFLP hijacked Lufthansa Flight 181, which was flying from Palma de Mallorca to Frankfurt, and demanded the release of prisoners belonging to the Red Army Faction (RAF).

After stopovers in the Middle East, the murder of Captain Jürgen Schumann, and the landing in Mogadishu, a GSG 9 team led by Wegener himself stormed the aircraft in the early hours of October 18th in Operation Feuerzauber. Within minutes, the four hijackers were killed or wounded, and all the remaining hostages on board were freed.



In colaboración with:



The “Traitors” of ETA

Inés Gaviria

Terrorist organizations do not only need weapons, militants and a cause with which to justify their crimes. They also need to impose obedience. Anyone who joins them cannot leave freely, question their decisions or acknowledge that using violence to achieve political objectives is always illegitimate. A terrorist group can scarcely tolerate dissent, because the existence of someone who has known the organization from the inside and has decided to leave it demonstrates that there was always another option. That is why ETA turned some of its former members into enemies and marked them with a word that, within its totalitarian logic, was equivalent to a death sentence: “traitor”.

But abandoning a terrorist organization is not a betrayal. To betray would have been to persevere in murder after understanding its radical injustice. To rectify, to refuse to kill or to defend the view that the weapons had to disappear means breaking with a discipline based on fear and recovering the capacity to decide freely. Those who took that step did not thereby erase the responsibility deriving from their crimes or from their previous militancy. Having ended up as victims of ETA does not automatically render legitimate everything they did before. Nevertheless, none of this diminishes their status as victims or justifies the crime committed against them.

María Dolores González Katarain, “Yoyes”, is perhaps the best-known case. She had risen to form part of the leadership of ETA military but ended up profoundly disillusioned with the organization. She left for Mexico, started a family and, after several years abroad, decided to return to the Basque Country to rebuild her life. She had no pending cases with the justice system and had provided no information to the security forces. Her crime, in ETA’s eyes, was to demonstrate publicly that it was possible to have belonged to the organization and afterwards to live outside it. ETA murdered her on 10 September 1986 in Ordizia, during the local festivities and in the presence of her three-year-old son.

Her murder had an exemplary purpose. ETA did not only intend to eliminate “Yoyes”, but to use her death to close the path to other terrorists who might be considering leaving the organization. It had to be shown that no one could decide on their own to abandon ETA. “Yoyes” represented a threat precisely because her life outside ETA could become a precedent. This 10 September 2026 marks the fortieth anniversary of her murder.

Two years earlier, ETA had murdered Miguel Francisco Solaun Angulo, “Mikel”, another former member of the terrorist organization. Solaun had taken part in the historic escape from Basauri prison in 1970 and had subsequently benefited from the 1977 amnesty. In the early 1980s, ETA forced him, through threats against his family, to collaborate in an attack against a building in Algorta intended to house a Civil Guard barracks. The terrorists planted fifty kilograms of explosives and intended to detonate them during the inauguration, when the building would be full of people.

Solaun refused to connect the device. As he left in writing, he did not do so because he was not a murderer. He also tried to alert the authorities to the existence of the explosives and ended up personally indicating where they were hidden. He was arrested and convicted for his initial collaboration, received a brutal beating from other ETA prisoners in jail, and lived his final months convinced that the organization would eventually kill him. On 4 February 1984, a terrorist shot him in a café in Algorta in the presence of his family. ETA accused him of being a “traitor and collaborator with the police” and presented his murder as a warning to those seeking an individual way out of the organization. His killers would later explain with terrifying clarity the mentality behind the crime: in a war, they said, every traitor had to be executed.

The case of Eduardo Moreno Bergaretxe, “Pertur”, presents important differences. Pertur was not a former member of ETA who had returned to civilian life, but one of the principal leaders of ETA politico-military when he disappeared in the French Basque Country on 23 July 1976. He defended the need to subordinate terrorism to political action and had set out his positions in the Otsagabia paper. His theses clashed with those of the more militarist sector of the organization, especially with the so-called *comandos bereziak*.

The authorship of his disappearance has never been clarified and his body remains missing. Over the years different hypotheses have been put forward, including the participation of extreme-right groups. Nevertheless, numerous testimonies and indications point to the conclusion that Pertur was eliminated by members of his own organization because of his internal disagreements and his commitment to giving priority to the political route. The last time he was seen alive he was with two members of the *bereziak*. For as long as those who know what happened continue to keep silent, his family will remain deprived of the truth and of the possibility of recovering his remains. On 23 July of the present year, 2026, fifty years have passed since his disappearance.

The trajectory of Juan María Jáuregui was different and allows one to observe the persistence of that logic long afterwards. During his anti-Franco youth, he briefly belonged to ETA, within its cultural

front. When the Sixth Assembly raised the question of the continuity of the armed route, Jáuregui broke with it. He later belonged to the Communist Party, joined the Socialist Party of Euskadi and became civil governor of Gipuzkoa. His political life was marked by the defense of human rights and of the rule of law, including against abuses committed in the anti-terrorist struggle.

ETA murdered him on 29 July 2000 in the café of the Beotibar fronton in Tolosa. He was shot in the back while talking with a friend. Decades had passed since his brief youthful militancy, and his murder was not presented as an internal purge but formed part of ETA's offensive against political representatives and constitutionalist citizens. Yet his story contains a revealing paradox: a man who had known the organization from the inside, who had rejected violence and who had devoted his adult life to defending democratic institutions ended up being murdered by that same organization.

The cases of “Yoyes”, “Pertur”, Solaun and Jáuregui are not interchangeable. Their previous responsibilities, their processes of rupture and the circumstances in which they were murdered were different. Nor had all of them travelled the same path of self-criticism with regard to their militancy. Remembering them as victims does not mean idealizing them or turning their biographies into simple narratives of redemption. It means recognizing an elementary principle: nothing entitles a terrorist organization to arrogate to itself the right to execute anyone who disagrees, leaves its ranks or decides to defend another way of doing politics.

There is a reason why these cases are especially uncomfortable for the narrative with which ETA justified its existence. “Yoyes”, “Pertur”, Solaun and Jáuregui knew the organization. They could not be presented as people alien to the supposed “Basque conflict” or as enemies incapable of understanding its motivations. They had shared, at different moments and to different degrees, its ideological universe. Precisely for that reason, their dissent was far more dangerous: it demonstrated that knowing the reasons invoked by ETA did not oblige one to accept its crimes, and that defending a particular identity or political project did not require killing.

Terrorism does not end completely when it stops killing. It is also necessary to dismantle the moral categories it constructed to justify its murders. Among them is the idea that leaving ETA, collaborating with the justice system or rejecting terrorist violence constituted a disloyalty deserving of punishment.

That is why we must remember these stories with all their nuances. They were members of ETA and some of them bore criminal responsibilities within the organization. But they were also its victims. ETA murdered them, or allegedly made them disappear in the case of “Pertur”, because they represented different forms of disobedience: questioning the primacy of the weapons, preventing a massacre, leaving the organization or openly defending democracy. In ETA's logic they were “traitors”. In reality, what they did was to demonstrate that even from within fanaticism there is always the possibility of choosing another path.

EDUARDO MORENO BERGARETXE

Born in: San Sebastián

Age: 25

Children: 0

Marital State: Single

Occupation: Leader of ETA politico-military

Date of the attack: 23/07/1976

Place of the attack: San Juan de Luz

Murdered by: ETA



Description of the attack:

Eduardo Moreno Bergaretxe, “Pertur”, disappeared on 23 July 1976 in the French Basque Country. The last time he was seen alive he was in the company of Francisco Javier Garayalde, “Erreka”, and Miguel Ángel Apalategui, “Apala”, members of the comandos bereziak of ETA politico-military. His body has never been found and no one has been convicted for his disappearance.

Pertur was one of the principal ideologues of ETA politico-military. He defended the view that the organization should subordinate armed activity to political direction and had taken part in drafting the Otsagabia paper. His positions provoked a growing confrontation with the militarist sector. Although different hypotheses have been advanced concerning his disappearance, numerous indications and testimonies point to the conclusion that he was kidnapped and murdered by members of the organization itself because of his internal disagreements.

MIGUEL FRANCISCO SOLAUN ANGULO

Born in: Basque Country

Age: 39

Children: 2

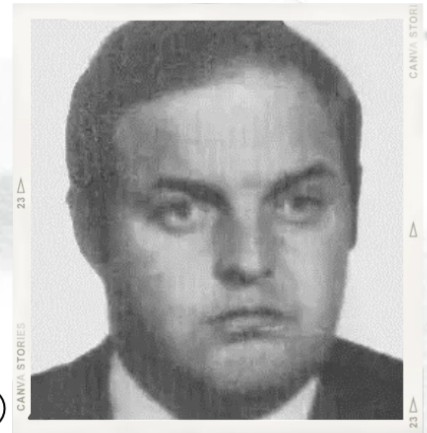
Marital status: Married

Occupation: Industrial engineer and construction contractor

Date of the attack: 04/02/1984

Place of the attack: Algorta, Getxo (Bizkaia)

Murdered by: ETA



Description of the attack:

On 4 February 1984, Miguel Francisco Solaun Angulo was with his family in a café in Algorta when a member of ETA shot him in the back. The organization claimed the murder, labelled him a “traitor and collaborator with the police” and presented the crime as a warning against those seeking an individual way out of the band.

Solaun had belonged to ETA during the Franco dictatorship and had organized the escape of fifteen prisoners from Basauri prison in 1970. Years later, ETA forced him, through threats against his family, to facilitate the placing of fifty kilograms of explosives in a building destined to become a Civil Guard barracks. Solaun refused to connect the bomb and helped the authorities locate it. He was arrested, convicted for collaboration and later pardoned. During his time in prison, he had been brutally assaulted by ETA prisoners. After regaining his freedom, he lived under threat until the organization carried out its warning.

MARÍA DOLORES GONZÁLEZ CATARAIN

Born in: Ordizia (Gipuzkoa)

Age: 32

Children: 1

Marital status: Married

Occupation: Economist

Date of the attack: 10/09/1986

Place of the attack: Ordizia (Gipuzkoa)

Murdered by: ETA



Description of the attack:

On 10 September 1986, María Dolores González Katarain, “Yoyes”, was walking through Ordizia with her three-year-old son during the local festivities. ETA member Antonio López Ruiz, “Kubati”, approached her and shot her at close range. Yoyes died instantly. Her murder had been ordered by the leadership of ETA to punish publicly her abandonment of the organization and to prevent her return to the Basque Country from encouraging other militants to follow the same path.

Yoyes had been one of the first women to reach positions of responsibility within ETA military. After the murder of José Miguel Beñarán, “Argala”, and her growing disagreements with the organization’s strategy, she left the band and moved to Mexico. There she studied, worked for the United Nations and started a family. She returned to Spain in 1985 with no pending cases before the courts and with the purpose of rebuilding her life. ETA turned that personal decision into an affront and punished it with death.

JUAN MARÍA JÁUREGUI APALATEGUI

Born in: Legorreta (Gipuzkoa)

Age: 48

Children: 1

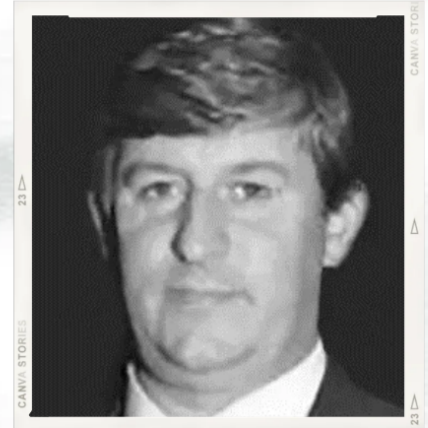
Marital status: Married

Occupation: Business executive and former civil governor of Gipuzkoa

Date of the attack: 29/07/2000

Place of the attack: Tolosa (Gipuzkoa)

Murdered by: ETA



Description of the attack:

On 29 July 2000, Juan María Jáuregui was talking with a friend in the café of the Beotibar fronton in Tolosa when two members of ETA approached him and shot him in the back. Jáuregui was then living in Chile for professional reasons and had returned to the Basque Country for a few days' holiday.

In his youth he had briefly belonged to ETA within the cultural front, but he broke with the organization when he rejected the continuation of violence. He later belonged to the Communist Party and to the Socialist Party of Euskadi. Between 1994 and 1996 he served as civil governor of Gipuzkoa, a period during which he defended the action of the democratic institutions against ETA and also promoted the investigation of possible police abuses. The terrorist organization murdered him decades after he had broken with it and after he had devoted a large part of his life to the defense of the rule of law.

About RIET

The Revista Internacional de Estudios sobre Terrorismo (RIET), is an electronic e-journal publication born from the idea of offering investigators a platform through which to publish academic articles related to the study of terrorism from any of its different approaches and perspectives (anti-terrorist strategies, security, prevention of violent radicalism, intelligence, etc.). The journal will provide flexibility in terms of content, style and length of the articles, without neglecting professional academic standards.

The research articles and other contents of the journal will be reviewed by members of the Scientific Committee, academic experts and external professionals prior to publication. They will provide the author with feedback, corrections, and pertinent notes if they were necessary.

Publishing every four months, RIET intends to become a reference for those authors who wish to publish in Spanish or English. RIET also intends to be the priority option of consultation for the Spanish-speaking public looking for contrasted quality content in the area of terrorism.

RIET is an Observatorio Internacional de Estudios sobre Terrorismo (OIET) initiative. All RIET content is accessible through the following web page: <https://rietjournal.org/>

RIET is indexed in Dialnet, REBIUN, Academic Index and Google Scholar.

Publication criteria

Articles and reviews sent to the journal must have scientific rigor. They must be original documents that have not been previously published or submitted for review in any other publication. Articles related to the study of terrorism from any of its multiple approaches will be accepted.

The evaluation system of the content submitted will be carried out through a peer review, guaranteeing the author's anonymity. Said review will be done by two members of the Scientific Committee or specialists external to the journal. The suitability of the subject, originality of the content, contribution in academic terms and its scientific rigor will be subject to evaluation.

The evaluators will present their opinion on the content, deciding whether it meets the conditions required to be published or if modifications are necessary. In the event that the analyzed text does not meet the minimum requirements they may also decide it is not valid for publication. The author will be informed of the reception of the article within a week. The evaluation process will take less than eight weeks from the moment the article is received. For those articles that must undergo modifications, the maximum time to send the definitive version of the article will be ten days from the moment the author is informed. The definitive version will then be reevaluated. In these cases, corrections should be limited to errors, restricting the possibility of adding content.

About **the periodicity**, the journal will be published every four months. There will be three annual issues published in the first week of the months of April, August and December. The deadline for submissions will be three months before the publication of each issue. If the content is received later than the stipulated date, it will be incorporated into the review for the next issue.

The submission of the original manuscripts must be sent to the Editorial Team through the e-mail jy@observatorioterrorismo.com. The e-mail must be carbon copied (CC) to the direction: c@observatorioterrorismo.com.

Two files must be sent in Word format. One including the author's name, professional affiliation and a brief description of the author's CV at the footer, and the other with an anonymous version of the paper.

Instructions for authors

- The papers can be written both in Spanish and English.
- The papers must comply with the spelling standards of the Royal Spanish Academy, following the 2019 update of the 2010 edition.
- The minimum length of scientific articles will be 4,000 words, and the maximum of 5,000, excluding references and footnotes. The latter should not exceed 2,000 words. Every article must include a maximum 200-word abstract, and maximum 5 keywords. Both the abstract and the keywords must be included in Spanish and English. Bibliographic reviews will have a maximum length of 1,500 words.
- The structure of scientific articles must be:
 - Title, centered.
 - Name of the author or authors along with their institutional affiliation. Under the title and with the surnames in capital letters.
 - Introduction
 - Main sections must be numbered and highlighted in bold (1.), the first one being the introduction.
 - Second level sections must be numbered and in italics (1.1).
 - Third level sections must be numbered and underlined (1.1.).
 - Conclusions
 - Bibliographic references arranged alphabetically.
- The text must follow Arial 12 style with 1.5 line spacing. Double space will not be used except in the heading of each main section. Tabs will be avoided, with exceptions. The paper must present a justified alignment.
- Citations longer than four lines must be tabulated and spaced from the upper and lower paragraphs.
- The citation model will be based on APA format, adding in the text in parentheses the surname(s) of the authors along with the year of publication of the work and the page, if necessary (González, 2015:35). It will be fully cited in the final section of bibliographic references. Footnotes will be reserved for clarifications, comments or punctuations, and used with moderation.
- Numerically ordered tables or graphs may be included. All of them must have a short description beginning with FIGURE X. (FIGURE 4. EVOLUTION TABLE OF ATTACKS). It will be necessary to indicate the origin of the source at the end of the description, whether it is from another author or self-elaborated (SOURCE: own elaboration).

Code of ethics and plagiarism detection

All parties involved in the publication of all RIET content, including authors, journal editors and reviewers, must adhere to the standards of ethical behavior expected in the Committee on Publication Ethics (Code of Conduct and Best Practices Guidelines for Journals Editors, COPE). RIET's policy is to publish original work, so a specific procedure is implemented to avoid malpractice, especially plagiarism. Before starting the evaluation process, Internet search tools and online software are used in order to corroborate originality and avoid plagiarism practices. Reviewers are also asked to pay attention to possible malpractices related to plagiarism during their evaluation.

Copyright

All published content is licensed under a Creative Commons Attribution 4.0 International license.

- The authors will keep their copyright and guarantee the magazine the right of first publication of his work.
- Authors may publish their work in other media or magazines, provided RIET is indicated as the original source of their work.
- The authors may give public diffusion of their work through their institutions, Internet channels or other means assigned for the diffusion of knowledge, as long as the original source is correctly cited.
- The authors are responsible for obtaining the necessary licenses and permissions for all material included in their work that requires them to do so.
- Authors should not make any payment for the evaluation/publication of their articles in RIET.

Open and free access policy

With the aim of contributing to the dissemination of knowledge among specialists and the general public, RIET is an open and free access academic platform.

All published content is licensed under a Creative Commons Attribution 4.0 International license

Copying, distribution and public communication is permitted as long as the author of the text and the source are cited, and the citation that accompanies each article is recommended. No commercial use or derivative works may be made. The rights of the published articles belong to their authors.



This work is [licensed under Creative Commons International Attribution 4.0 License](#)