26

No. 26 DECEMBER 2025

JOURNAL OF THE SPANISH INSTITUTE FOR STRATEGIC STUDIES

SUMARIO/SUMMARY

ieee.es
Instituto Español de Estudios Estratégicos

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Index

Review

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Victor Mario Bados Nieto
Director of the Spanish Institute for Strategic Studies

Presentation of IEEE Journal No. 26

We are pleased to present this new issue of the journal, which brings together a series of articles addressing some of the main strategic, technological and geopolitical challenges characterising the current international system. In a context marked by growing uncertainty, volatility, increased conflict and rapid transformation of the international order, rigorous and multidisciplinary analysis is more necessary than ever to understand contemporary security dynamics.

The international system is undergoing a period of profound transition. Tensions between major powers, the resurgence of strategic competition and the proliferation of regional conflicts, some of which threaten to escalate into global implications, are evidence of the growing fragmentation of the global order. At the same time, the multilateral system that emerged after the Second World War is showing clear signs of institutional fatigue. International organisations designed to manage collective security—with the United Nations as a prime example—face a structural deadlock that limits their ability to act in the face of crises. The paralysis of the Security Council in the face of high-intensity conflicts, the growing instrumentalisation of multilateral institutions by the major powers, and the emergence of new regional security architectures reflect a trend towards what some analysts call a process of demultilateralisation of the international order.

At the same time, the strategic agenda has expanded significantly. Conventional conflicts are joined by new dimensions of competition between state and non-state actors: hybrid warfare, cognitive dominance, cybersecurity, artificial intelligence, and the instrumentalisation of information as a tool of power. This multi-domain environment forces us to rethink the classic categories of international security and demands analytical frameworks capable of integrating the technological, social, economic, and strategic dimensions of contemporary conflicts.

The articles in this issue are set against this backdrop of structural transformation of the international system and address some of the most relevant phenomena in global security today from different perspectives.

The first article, by **Juan de Dios Meseguer González**, analyses the resilience and cyber risks associated with Russia's nuclear command, control and communications (NC_3) system. In an environment characterised by the digitalisation of military systems and the growing sophistication of cyber threats, the author proposes a reproducible methodological model that combines systematic review, conceptual analysis and scenario simulation based on international risk management standards. Drawing on verified open sources from institutions such as RAND, NATO STO and SIPRI, the study examines the technological exposure of the Russian nuclear system and proposes mitigation frameworks based on Zero Trust architectures and cyber resilience audits. The work thus contributes to understanding how military digitalisation influences contemporary strategic stability.

The second article, written by **Luis Ángel Díaz Robredo**, focuses on NATO's strategic communication and its role in the field of information warfare. Drawing on contributions from social and group psychology, the author analyses various intergroup interventions that have proven effective in reducing prejudice and hostility between groups, highlighting their usefulness in strengthening strategic communication capabilities in conflict contexts. The work shows how the cognitive domain has become a central space for strategic competition, where the construction of narratives and the management of perceptions are becoming increasingly valuable in the context of allied operations.

In the field of institutional communication in crisis contexts, **Jonattan Rodríguez Hernández** examines the communication strategy of the Military Emergency Unit (UME) on social network X during the forest fires that affected Spain in the summer of 2025. Using a mixed methodological approach that combines content analysis, engagement study and semantic analysis using data analysis tools, the author shows how the UME's communication focused primarily on the operational response to the emergency. The study also highlights the role of institutional communication on social media in reinforcing the public legitimacy of security institutions.

From a geopolitical perspective, **Andrea García García** analyses India's growing role in the strategic architecture of the Indo-Pacific. The article examines the evolution of Indian foreign policy from the legacy of non-alignment towards a strategy of strategic autonomy, articulated through initiatives such as the *Act East Policy*, the SAGAR doctrine and the strategic concept known as *The India Way*. The study also explores the implications of this rise for the European Union and Spain, highlighting opportunities for cooperation in areas such as connectivity, maritime security, technology and the defence industry.

Instability in the Western Balkans is the subject of **Sebastián Chumbe Checa's** study, which examines the risk of escalation in the region following the formation of opposing military blocs around Serbia and Kosovo. Using theoretical frameworks such as the balance of power, complex interdependence and the notion of a grey zone,

the author analyses the interaction between regional and external actors—including NATO, the European Union and Russia—and assesses the factors that contribute to containing the conflict, such as European mediation, economic interdependence and the presence of international missions such as KFOR and EUFOR Althea.

In the field of international political economy, **Sonia Benito Hernández** and **Rouhollah Iran Shahy** analyse the role of economic Islamism in the political legitimisation of the Iranian regime. Based on the *Velayat-e Faqih* doctrine formulated by Ayatollah Ruhollah Khomeini, the study examines the tensions between Islamic economics and contemporary approaches in the social sciences. The authors conclude that economic Islamisation in Iran has functioned primarily as an instrument of political legitimisation of theocratic power, generating dynamics that have limited economic pluralism and favoured authoritarian structures.

For their part, **Salvador Berdun Carrión** and **Luis Barragán Márquez** address the phenomenon of jihadist radicalisation in prisons based on an analysis of the case of inmate Rida B. The study examines the particularities of radicalisation within prisons and raises relevant questions about the capacity of prison institutions to prevent the spread of extremist ideologies in high-security contexts.

The issue of training in strategic decision-making is addressed by **Iván Soto Macia**, who analyses the role of wargames as a tool for improving decision-making processes in complex contexts. The article explores how advances in artificial intelligence can transform the design and evaluation of these exercises, as well as the opportunities offered by the growing community of civilian players as a source of collective intelligence and cognitive diversity for strategic analysis.

From an innovative perspective, **Roberto Espinosa Valdés** analyses the phenomenon of the gamification of war in contemporary conflicts. Through a comparative approach that includes the Russian Ukrainian war, jihadist extremism and organised crime in Latin America, the author shows how the logic of video games is being integrated into propaganda, recruitment and mobilisation strategies. The study concludes that these dynamics contribute to trivialising violence and amplifying the transnational dissemination of war narratives, especially among young audiences.

The issue is rounded off with a paper by **Arturo Esteban Ceballos**, dedicated to the analysis of hybrid threats from an innovative methodological perspective. The author proposes a replicable model that combines empirical data analysis, statistical modelling and agent-based simulation to study Turkey's strategic activity in various regional scenarios. Using analytical tools such as Markov chains, negative binomial regressions and SARIMAX models, the study identifies adaptive patterns in the strategic behaviour of actors and provides a useful analytical framework for the development of early warning systems in multi-domain environments.

Finally, this issue includes reviews of three recent works of particular interest to the academic and professional community in the field of security and strategy. First, the book by **Daniel Sansó-Rubert Pascual**, dedicated to the role of intelligence services in contemporary democracies. Secondly, the work by **Rafael García Pérez**, which analyses the geopolitics of the global submarine cable network as critical infrastructure

for international security. Finally, the work by **Basil Germond**, which focuses on the evolution of naval power in the strategic context of the postmodern world.

With this set of contributions, the journal offers a plural and multidisciplinary overview of some of the most relevant debates in contemporary international security. At a time when strategic uncertainty seems to be becoming the new normal in the international system, rigorous analysis and academic debate remain indispensable tools for understanding and addressing the challenges of the 21st century.

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Juan de Dios Meseguer González
PhD candidate in International Security at IUGM-UNED

Email: jmeseguer1@alumno.uned.es

Analysis of Cyber Risks and Resilience in the Russian Nuclear Triad

Abstract

This paper studies the technological exposure and resilience of Russia's nuclear command, control and communications (NC3) system in the context of global strategic competition and emerging security challenges in the Euro-Atlantic space. It proposes a reproducible methodological model that combines systematic review, conceptual analysis of command and control architectures, and scenario simulation based on NIST 800-30 and ISO/IEC 27005 standards.

The research uses open and validated scientific intelligence (OSINT) from institutional sources such as RAND, NATO STO and SIPRI, transforming the absence of classified data into an opportunity to establish a verifiable analytical basis. From an interdisciplinary perspective, mitigation frameworks and improvement measures are proposed based on Zero Trust architectures, cyber-resilience audit processes, and strategic information cross-verification mechanisms.

The study provides a reference framework for understanding and assessing the effects of military digitalisation on contemporary strategic stability, offering a useful tool for researchers and defence officials interested in strengthening international technological security.

Keywords

Strategic security, Cyber defence, Command and control systems, Technological deterrence, Euro-Atlantic cooperation.

Cite this article:

Meseguer Gonzalez, J. D. (2025). Analysis of cyber risks and resilience in the Russian nuclear triad. *Journal of the Spanish Institute for Strategic Studies*. 26, pp. 343-382.

1 Introduction

Cyber risk in strategic nuclear command, control and communications (NC3) systems has become a critical factor for international stability. The progressive digitisation of launch vectors, the automation of early warning protocols and the integration of artificial intelligence into strategic decision-making processes have increased exposure to cyberattacks or interference. In this context, the Russian nuclear triad—consisting of land-based intercontinental missiles, missile-launching submarines, and strategic air platforms—represents one of the most sensitive environments for global deterrence balance.

The tensions arising from the conflict in Ukraine since 2022 and NATO's adaptive response have substantially altered the Euro-Atlantic strategic environment. Russia has prioritised the strengthening of its nuclear deterrence and has invested in the modernisation of its NC3 network, integrating cyber and artificial intelligence capabilities into its warning and command systems. At the same time, the Atlantic Alliance has accelerated its advanced cyber defence doctrine, creating coordination structures such as the *NATO CyOC* (Cyber Operations Centre) and expanding interoperability programmes between member states.

In this scenario of technological rivalry, understanding the cyber risks associated with the Russian nuclear triad becomes a fundamental task for international security, especially from a preventive and doctrinal point of view. The scarcity of public information on these systems, coupled with the secretive nature of most command and control infrastructures, necessitates the adoption of alternative methodologies based on verified open sources (OSINT), recognised risk frameworks such as NIST 800-30 and ISO/IEC 27005, and modelling techniques that allow theoretical behaviours to be extrapolated without compromising classified information.

In this regard, this paper does not seek to identify specific vulnerabilities or describe specific technical structures, but rather to offer a reproducible methodological model for analysing cyber risk and doctrinal resilience in critical nuclear command infrastructures. This approach allows the phenomenon to be approached from a scientific, auditable and practical perspective for academic institutions, strategic think tanks and defence agencies operating in restricted information environments.

The novelty of the research lies in three main aspects:

1. The systematic application of the NIST 800-30 framework to a domain traditionally reserved for classified intelligence.
2. The incorporation of the concept of strategic resilience, understood not only as the ability to withstand a cyberattack, but also to maintain doctrinal and operational stability in a hostile digital environment.
3. The formulation of an open, verifiable and replicable analytical model that allows for future interdisciplinary research without compromising information security.

Ultimately, this study seeks to contribute to the debate on deterrent stability in the digital age by proposing a conceptual and methodological framework that facilitates scientific and technological cooperation among allies and fosters a culture of prevention, deterrence and response to new-generation technological threats.

The following section describes the methodology adopted, the document selection criteria and the thematic coding process applied to construct the analysis model.

2 Methodological framework and sources

The study is based on a rigorous methodology designed to ensure the scientific validity of the analysis without violating security restrictions or revealing classified information. Given that the research addresses a highly sensitive area—the Russian nuclear command, control and communications (NC3) system—a mixed and reproducible method was chosen that combines systematic literature review, thematic coding and risk scenario modelling under international cyber management standards. This approach allows for the development of a verifiable analytical framework based on open sources, structured in phases ranging from document selection to methodological validation of the model.

2.1 General approach

This study adopts a mixed qualitative-quantitative approach aimed at analysing cyber risk in strategic nuclear command, control and communications (NC3) infrastructures. Given the confidential nature of the subject matter, a methodology based on the triangulation of verified open sources, international risk management frameworks and conceptual inference techniques is used.

Before developing each phase, the methodological process followed is summarised in table I, which shows the sequence of analysis and the reference standards applied.

TABLE I. METHODOLOGICAL PHASES AND REFERENCE FRAMEWORKS APPLIED

Phase	Analytical objective	Tool/Reference	Expected result
1 Systematic document review	Identify institutional and academic literature on NC3, cybersecurity and strategic resilience (2018-2025).	PRISMA 2020 protocol. Sources: RAND, NATO STO, SIPRI, IISS, Chatham House.	Verified corpus of open sources (58 documents).
2 Thematic coding	Group findings into three areas: structural vulnerability, strategic digitalisation and doctrinal response.	Inductive content analysis.	Risk and resilience indicator matrix.
3 Risk scenario modelling	Simulate possible vectors of interference or degradation of the NC3 from a theoretical point of view.	NIST SP 800-30 Rev. 1 (2012); ISO/IEC 27005 (2018).	Conceptual exposure and resilience scenarios.
4 Strategic impact assessment	Assess the potential impact on deterrent stability and Euro-Atlantic cooperation.	Semi-quantitative scale (probability × impact).	Strategic risk map (theoretical).
5 Synthesis and methodological validation	Verify the consistency of the model with allied cyber defence doctrine.	Cross-check RAND–NATO STO–SIPRI.	Reproducible and auditable methodological framework.

Source: author's own elaboration based on NIST 800-30 (2012) and ISO/IEC 27005 (2018).

2.2 Selection and validation of the document corpus

The initial empirical base consisted of 312 documents obtained from institutional databases and specialised think tanks—including RAND (*Research and Development Corporation*), SIPRI (*Stockholm International Peace Research Institute*), NATO STO (*Science and Technology Organisation*), CSIS (*Centre for Strategic and International Studies*), IISS (*International Institute for Strategic Studies*), Chatham House, and Carnegie Endowment—selected for their relevance and analytical rigour. After applying criteria of thematic relevance, institutional authenticity, and absence of duplicates, the corpus was reduced to 58 main references.

The PRISMA 2020 protocol (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), an international guideline for the transparent and reproducible preparation of systematic reviews, was used to refine the sources and ensure their methodological traceability. Subsequently, inductive thematic coding was applied, which allowed the findings to be grouped into three areas of analysis:

a) Structural vulnerabilities of NC3;

b) risks arising from strategic digitalisation and artificial intelligence;

c) doctrinal responses and resilience frameworks in the Euro-Atlantic environment.

Each document was recorded in a documentary annex with verified URLs and basic metadata (author, year, institutional source, type of document), ensuring the verifiability and reproducibility of the process.

The sources used were classified into four main categories:

1. Doctrinal and technical documents issued by international organisations (NATO, UN, European Union, Ministry of Defence of the Russian Federation).
2. Reports from think tanks and strategic research organisations (RAND, NATO STO, SIPRI, IISS, Chatham House).
3. Academic and scientific literature indexed in databases such as Scopus, Web of Science, and Dialnet Plus.
4. Verified journalistic sources, used only to contextualise recent developments (2022–2025) in missile modernisation and command doctrines.

The authenticity of each document was verified by cross-checking its institutional origin, date of issue, bibliographic citation and public availability. This validation ensures that the OSINT sources used meet criteria of traceability, timeliness and reliability, complying with the standards of transparency required by scientific research in the field of defence.

2.3 Application of the NIST 800-30 and ISO/IEC 27005 models

The risk analysis followed the structure proposed by the NIST SP 800-30 guide (*Guide for Conducting Risk Assessments*, developed by the US *National Institute of Standards and Technology*), adapted to the strategic defence context. This framework

provides a standardised procedure for identifying, estimating and prioritising technological risks in critical systems:

1. Identification of critical NC3 assets and functions (without detailing platforms or protocols).
2. Characterisation of threats according to cyber typology: communications interference, software sabotage, sensor manipulation and cognitive disinformation.
3. Estimation of the probability and impact of each threat on strategic stability using a semi-quantitative scale.
4. Determination of residual risk and formulation of mitigation strategies.

In addition, the ISO/IEC 27005 standard, issued by the *International Organisation for Standardisation* and the *International Electrotechnical Commission*, was applied, which provides guidelines for information security risk management. Its integration allows the organisational and doctrinal dimension of resilience to be incorporated, aligning technical analysis with the principles of governance and operational control. The result is a reproducible model for strategic cyber risk analysis, applicable to critical infrastructures with limited access to classified information.

2.4 Justification for the use of open sources (OSINT)

Far from being a limitation, reliance on open sources represents a methodological advantage in terms of transparency, security, and scientific cooperation. The use of OSINT allows for:

– Validate hypotheses using verifiable and accessible information;
– Respect operational confidentiality margins;
– Promote academic and doctrinal collaboration between allies.

In this way, information restriction becomes a legitimate epistemological condition, where innovation focuses on the analysis model, not on the disclosure of sensitive data. Thus, the study contributes to consolidating a common methodological language for the examination of cyber risk in strategic environments and for interaction between academia and defence institutions.

2.5 Limitations and future prospects

It is recognised that the exclusive use of OSINT prevents direct empirical verification with classified data. However, the model developed can be extended and validated by researchers with restricted access, ensuring its scalability.

Future lines of research include the application of machine learning to detect risk patterns and the comparative analysis of cyber resilience between NC3 doctrines of different nuclear powers.

Taken together, this methodological framework provides a scientific and reproducible basis for future studies on strategic cybersecurity and resilience in nuclear command systems.

3 Theoretical and conceptual framework

Understanding cyber risk in the Russian nuclear triad requires articulating a theoretical basis that combines classic doctrinal approaches to deterrence with new paradigms of digital security and technological resilience. This section establishes the *conceptual foundations* that underpin the subsequent analysis, integrating contributions from academic literature, strategic research reports and international regulatory frameworks on cyber risk management (ISO/IEC, 2022; Joint Task Force, 2018).

The purpose of this framework is not to reveal specific command structures, but to offer an interpretative model that allows us to understand how the digitalisation of the Russian NC3 system can affect global strategic stability. From this perspective, deterrence theory, nuclear risk studies and doctrinal developments in cyber defence converge to explain a changing scenario, where technological risk becomes a geopolitical vector of the first order (Johnson, 2021; Mazarr *et al.*, 2022; U.S. Department of Defense, 2020).

The purpose of this framework is not to reveal specific command structures, but to offer an interpretative model that allows us to understand *how the digitalisation of Russia's NC3 system can affect global strategic stability.* From this perspective, deterrence theory, nuclear risk studies and doctrinal developments in cyber defence converge to explain a changing scenario, where technological risk becomes a geopolitical vector of the first order (Johnson, 2021; Mazarr *et al.*, 2022; U.S. Department of Defense, 2020).

3.1 Fundamentals of the nuclear triad and the NC3 system

The nuclear triad is at the heart of modern strategic deterrence. Designed to ensure second-strike capability, it consists of three complementary components: intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs) and strategic bombers (Kristensen and Korda, 2023). The logic of the triad is to maintain credible deterrence through the survival of the arsenal in the face of a pre-emptive strike, a concept that remains central to current Russian doctrine (IISS, 2023). Comparative data on forces and modernisation programmes support this configuration of the Russian triad (IISS, 2024).

The Nuclear Command, Control and Communications (NC3) system integrates the functions of political command, operational control and transmission of orders to nuclear forces. According to Acton (2018), the reliability of NC3 is the *sine qua non* of global nuclear stability: any degradation or ambiguity in its operation could lead to a crisis of perception or accidental escalation.

The Russian NC3 has evolved from Soviet architecture (*Kazbek System*, *Cheget*) to a more automated network, supported by GLONASS satellites and redundant

encrypted communications (CSIS, 2024; Mazarr *et al.*, 2022). However, digital interconnection and the introduction of artificial intelligence into decision-making processes also increase exposure to interference or cyberattacks (Kristensen and Korda, 2022b).

This technological evolution raises the need to assess the risks associated with the digitisation of NC3. Understanding the nature and dimensions of cyber risk in strategic systems thus becomes the logical next step in interpreting the vulnerabilities inherent in the contemporary deterrence model.

3.2 Cyber risk in strategic systems

Cyber risk is defined as the probability that a digital action or vulnerability will affect the integrity, confidentiality or availability of a critical system (Joint Task Force, 2018). In the nuclear domain, this risk transcends the technical realm: it can alter trust between states and destabilise deterrence balances.

Studies by the *Carnegie Endowment for International Peace* and *SIPRI* highlight that cyber incidents in strategic infrastructure can generate 'catalytic effects', i.e. trigger disproportionate reactions due to misperceptions by the adversary (Jung, 2024; Kristensen y Korda, 2022b). Mazarr *et al* (2022) and CSIS (2024) agree that Russian NC3, despite its redundancy, faces increasing risks linked to sensor automation, dependence on proprietary software and remote access to decision nodes.

According to these studies, the main threat vectors fall into four categories:

1. Digital intrusion or firmware manipulation in strategic communication nodes.
2. Electromagnetic or satellite signal interference, which affects the reliability of early warning.
3. Disinformation and cyber deception operations targeting the political-military chain of command.
4. Technological dependence and vulnerability of the supply chain, especially for imported microelectronic components.

These threats, documented in reports by NATO STO *(2023)* and IISS *(2023)*, illustrate how strategic digitalisation transforms classic deterrence risks into multidimensional challenges combining cybersecurity, intelligence and strategic psychology.

Analysis of these risk vectors necessarily leads to an examination of resilience capabilities. If risk represents the degree of exposure, resilience determines the system's ability to maintain its critical functions under attack or disruption. This shift in focus is key to understanding stability in the digital nuclear environment.

3.3 Strategic resilience and cyber stability

The concept of strategic resilience has evolved from a technical notion to a doctrinal principle that defines the ability of states to maintain essential functions under

pressure or attack (Payne, 2022). In the cyber context, it implies not only resisting aggression, but also ensuring operational continuity, organisational adaptability and rapid recovery of the affected system.

NATO formalised this vision after the Warsaw Summit (2016) and reaffirmed it in its *Strategic Concept 2022*, recognising cyberspace as an operational domain. Its *Cyber Defence Pledge* and the research framework of the *NATO Science and Technology Organisation* (U.S. Department of Defense, 2020) promote the integration of digital resilience into defence planning.

Russia, for its part, has been developing a doctrine of 'informational stability' since 2020, which combines cyber defence with information control and technical redundancy of NC3 systems (CSIS, 2024). This vision focuses on maintaining technological autonomy and reducing exposure to external vulnerabilities.

The shift from technical resilience to strategic resilience introduces a new component: *cyber deterrence*. While resilience ensures the survival of the system, deterrence ensures the predictability of the adversary. The two complement each other in a framework where stability depends as much on technological strength as on perceived credibility.

3.4 Cyber deterrence and strategic stability

The digital transformation of nuclear deterrence has led to the emergence of the concept of cyber deterrence, understood as the ability to prevent aggression through robust protection of critical infrastructure and credible responses to attacks (Johnson, 2021).

Authors such as Futter (2018) and Morgan (2023) argue that traditional deterrence—based on the fear of mutually assured destruction—is shifting towards 'resilience deterrence', where the strength of the system and its ability to absorb an attack without losing functionality are decisive factors.

Contemporary strategic stability is therefore defined not only by the quantity or power of the nuclear arsenal, but also by the cyber robustness of the NC3. The RAND (2025) and SIPRI (2024) reports warn that digital vulnerability in nuclear command networks could become the main catalyst for instability if coordinated measures for prevention, cooperation and technological transparency are not adopted among the powers.

This set of concepts—risk, resilience, and cyberdeterrence—forms the basis of the analytical model used in this research. Based on these concepts, an integrative conceptual framework is established that links technological security with strategic stability, serving as a basis for the discussion of results.

3.5 Summary of the conceptual framework

The theoretical framework of this study is based on four fundamental pillars:

1. The nuclear triad, as a classic deterrent structure and guarantor of strategic balance (Kristensen and Korda, 2023).

2. The NC3 system, as the technical and doctrinal core of nuclear communication (Jung, 2024; CSIS, 2024).
3. Cyber risk, which introduces technological and strategic uncertainty (Joint Task Force, 2018; SIPRI, 2024).
4. Strategic resilience, which transforms cybersecurity into an element of stability (Payne, 2022; U.S. Department of Defense, 2020).

These concepts form an integrative framework that allows us to examine the levels of exposure and recovery of Russian NC3 in the context of global technological competition.

Next, a Glossary of Basic Terms and Acronyms (Section 4) is presented to facilitate understanding of the technical, doctrinal, and technological concepts used in the research.

Section 5 then develops the results of the analysis, organised around the three identified axes: structural vulnerability, strategic digitalisation and doctrinal response.

4 Glossary of basic terms and acronyms

This glossary provides concise definitions of the main technical and doctrinal concepts used throughout the article. Its purpose is to facilitate understanding of the specialised terminology related to strategic cybersecurity, nuclear deterrence and command and control systems (NC3), so that the reader does not have to resort to external sources.

The inclusion of this section responds to the reviewers' recommendation to provide an early terminological frame of reference, allowing for a fluid and coherent reading of the subsequent sections. The definitions presented combine technical, doctrinal and scientific criteria and have been drawn from indexed academic literature and recognised institutional sources (Jung, 2024; Futter, 2018; Kristensen and Korda, 2023; Payne, 2022; Mazarr *et al.*, 2022; U.S. Department of Defense, 2020).

TABLE A. GLOSSARY OF BASIC TERMS AND ACRONYMS

Term/Acronym	Summary academic definition	Application in the study
NC3 (Nuclear Command, Control and Communications)	Set of systems, networks and procedures that enable national authorities to control and communicate orders regarding the use of nuclear weapons.	Functional core of Russian nuclear deterrence analysed in this study.
Nuclear triad	Structure composed of three launch platforms: land-based intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs) and strategic air vectors.	Structural framework for assessing cyber risk in each domain.
ICBM (Intercontinental Ballistic Missile)	Ballistic missile with a range of over 5500 km, capable of carrying nuclear warheads between continents.	One of the three components analysed in the Russian triad.
SLBM (Submarine-Launched Ballistic Missile)	Ballistic missile launched from nuclear-powered submarines, an essential part of second-strike capability.	Represents the naval dimension of Russia's NC3.

Term/Acronym	Summary academic definition	Application in the study
Second strike	A state's ability to respond with nuclear weapons after suffering an initial attack.	A key indicator of strategic stability and the impact of cyber risk.
Cyber deterrence	Strategy aimed at preventing cyber attacks through resilience, attribution and proportional response capability.	Concept used to assess the NATO-Ukraine response to strategic cyber threats.
Cyber resilience	A system's ability to withstand, adapt and recover from a cyber attack while maintaining critical functions.	Operational objective for reinforcement in NC_3 systems.
OSINT (Open Source Intelligence)	Intelligence obtained from open, verifiable and publicly accessible sources, used for strategic or scientific analysis.	Methodological basis that guarantees the transparency and reproducibility of research.
NIST (National Institute of Standards and Technology)	US agency that develops technical and methodological standards, including the Special Publication 800-30 series for risk analysis.	Main methodological reference for cyber risk modelling.
ISO/IEC (International Organisation for Standardisation / International Electrotechnical Commission)	International entities that issue joint standards on information security management and technological risk (ISO/IEC 27005).	Complementary framework to NIST for assessing organisational resilience.
Spoofing	Manipulation or spoofing of electronic signals—especially GNSS or satellite signals—in order to alter navigation or location data.	Technical risk identified in SLBM guidance systems and air vectors.
Firmware	Low-level software that controls hardware operation and provides the interface between equipment and programmes.	Potential attack surface in control and launch systems.
GLONASS	Global satellite navigation system of the Russian Federation, equivalent to GPS.	Critical technological dependency for synchronisation and guidance.
Perimetr	Russian automated command system designed to ensure nuclear retaliation even in the event of loss of communication with political command.	Doctrinal example of automation with inherent cyber risk.
Zero Trust	Security model that eliminates implicit trust within internal networks, verifying each access or transaction.	Recommended principle for modernising Russian and allied NC_3 security.

Source: author's own elaboration based on Jung (2024), Futter (2018), Harknett and Smeets (2020), Kristensen and Korda (2023), Payne (2022), Mazarr *et al* (2022), Joint Task Force (2018), ISO/IEC (2018) and U.S. Department of Defense (2020). The definitions summarise standardised technical terminology in nuclear doctrine and cybersecurity.

This glossary constitutes a conceptual reference that frames the technical and strategic analysis developed in the following sections. By clarifying essential terminology, it seeks to ensure that the reader interprets the doctrinal, technical and operational terms used in the study in a consistent manner.

The following section presents the results and technical analysis derived from the application of the methodological model, organised around the three defined areas of research: structural vulnerability, strategic digitalisation and doctrinal response.

5 Results and technical analysis

The study focused on the three components of Russia's nuclear triad—intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs) and strategic air vectors—examining the interactions between the communication, guidance and control subsystems. This multidimensional approach

made it possible to determine the differential exposure to cyber risk in each operational domain.

Among the systems evaluated, the RS-24 Yars is a paradigmatic case due to its strategic relevance and degree of digitalisation, making it a reference model for understanding the convergence between technology, doctrine and vulnerability.

5.1 The RS-24 Yars as a technical reference model

Before presenting the quantitative results, it is necessary to contextualise the technical model that serves as the basis for the empirical analysis. The RS-24 Yars represents the main land-based vector of the Russian triad and exemplifies the complexity of the digital command and control chains associated with ICBMs.

Figure 1, shown below, illustrates the structural configuration and relevance of the land-based component of the NC3 system, highlighting the criticality of firmware and guidance modules as potential cyber exposure surfaces.

Figure 1. RS-24 Yars intercontinental ballistic missile system.
Note: The RS-24 Yars is the main ICBM in the Russian nuclear triad. Its digital architecture and automated guidance systems highlight the potential vulnerability of firmware and control communication networks.
Source: GlobalSecurity.org (n. d.). RS-24 Yars Intercontinental Ballistic Missile

The RS-24 Yars (PC-24 *'Ярс'*; NATO designation SS-27 Mod 2) is a solid-fuel intercontinental ballistic missile (ICBM) with a range of approximately 12 800 km and multiple MIRV thermonuclear warheads (100-550 kt). In service since 2010, it can be launched from fixed silos or mobile TEL (Transporter-Erector-Launcher) platforms, designed to ensure the mobility and survivability of the system. It is an evolution of the *Topol-M* and was designed to overcome contemporary missile defence systems, incorporating autonomous guidance algorithms and digital redundancy (Kristensen and Korda, 2023; IISS, 2023).

Its integration into digital networks and its reliance on encrypted communication channels make the RS-24 a priority for analysis within the Russian NC3 system. Based on this model, two complementary levels of assessment were developed:

1. Chronological and qualitative analysis (2020-2025): chronology of relevant technological and cyber incidents.
2. NIST 800-30 risk modelling: quantification of relative risk by combining probability (P) and impact (I).

Based on the findings of the qualitative analysis, the verified chronology of technological and cyber incidents (2020-2025) is presented below in order to contextualise the evolution of risk prior to its quantitative modelling.

5.2 Chronology of incidents and vulnerabilities (2020–2025)

The chronology below summarises the relevant incidents associated with technological failures or cyberattacks that potentially affected the Russian NC3. Each record was validated by cross-checking academic sources, think tanks and international organisations (SIPRI, 2024; RAND Corporation, 2021; CSIS, 2024; U.S. Department of Defense, 2020; IISS, 2023).

Following the analysis of the RS-24 Yars system as a representative model, it is pertinent to place the findings within a chronological sequence of technological and cyber incidents that allows the evolution of the risk to be contextualised.

Table II shows the progression of risks and the evolution of threats over time, providing an empirical basis for identifying recurring patterns.

TABLE II. SUMMARY TIMELINE OF TECHNOLOGICAL AND CYBER INCIDENTS (2020–2025)

Date	System/Domain	Description of the incident or vulnerability detected	Type of vulnerability
Mar 2020	NC3 terrestrial infrastructure	DDoS attacks against Russian Ministry of Defence servers, partial credential leaks.	Network intrusion
Jul 2021	GNSS (GLONASS) segment	Spoofing incidents in the Black Sea affecting civil aircraft and ships, possible countermeasure testing.	Signal manipulation
Feb 2022	ICBM systems (Yars)	Firmware update delayed due to incompatibility alerts in cryptography protocols.	Software failure
Dec 2022	Airborne vectors (Tu-95MS)	HF communication system malfunction during strategic drill.	Communications vulnerability
Apr 2023	Early warning network (Oko)	Anomalies in satellite telemetry due to obsolete software.	Digital obsolescence

Date	System/Domain	Description of the incident or vulnerability detected	Type of vulnerability
Oct 2023	Borei submarines	Temporary interruption in the 'Legenda' satellite link during Arctic manoeuvres.	Communication interference
Mar 2024	Command and control infrastructure	Data leakage on digital military logistics platforms.	Supply chain compromise
Jan 2025	Avangard testing system	Latencies in telemetry network due to poor configuration of military routers.	Configuration failure

Source: author's own elaboration based on SIPRI (2022, 2024), RAND Corporation (2024–2025), NATO STO (2023), CSIS (2021, 2024) and IISS (2023).

Analysis of this timeline reveals three persistent patterns of technological exposure linked to satellite dependency, poor network segmentation and the vulnerability of logistics chains.

5.2.1 Specific vulnerabilities in the Russian strategic navy and air force

In addition to land-based vectors, the naval and air domains of the Russian NC3 system present distinct vulnerabilities that broaden the spectrum of cyber risk.

The strategic fleet of Borei-class submarines, equipped with RSM-56 Bulava missiles, relies on 'Legenda' satellite links and extremely low frequency (VLF) transmissions, used to maintain communication with submerged submarines, channels whose reliability has been compromised by interference and spoofing (manipulation or impersonation of electronic signals) documented in Arctic exercises (Mazarr, 2022; SIPRI, 2024). These vulnerabilities, coupled with the difficulty of updating in submarine environments, reduce the capacity for early detection and communication of critical orders. Modernisation trends and technological dependencies of strategic platforms are documented in *The Military Balance 2024* (*IISS, 2024*).

In the air domain, *Tu-95MS* and *Tu-160* strategic bombers use *Kh-55/Kh-102* cruise missiles and HF/UHF links that are susceptible to electromagnetic interference and GNSS coordinate manipulation, which can affect launch accuracy and command transmission (IISS, 2024). The coexistence of analogue and digital systems in these aircraft increases the complexity of cyber security and requires manual redundancy as a positive control mechanism.

For their part, the Avangard and Kinzhal hypersonic systems, according to reports from DARPA (Defence Advanced Research Projects Agency), have speeds and levels of automation that significantly increase the complexity of control. By relying on real-time guidance networks and encrypted telemetry links, they incorporate a new level of risk: the possible loss of direct human control in the event of synchronisation failures or satellite link degradation. The speed and automation of these systems means that an error in the digital chain of command can have disproportionate strategic consequences.

Overall, the results confirm that the cyber vulnerability of the Russian NC3 extends to all three domains—land, sea, and air—and that technological resilience must be assessed considering the particularities of each operational vector.

The following section examines these recurrences in detail, based on the NIST model classification.

5.3 Application of the NIST 800-30 matrix: risk modelling

Before presenting the modelling table, it is useful to summarise the recurring patterns detected in the documented incidents. This intermediate step facilitates the comparative interpretation of risks and avoids fragmentation of the results.

Cross-examination of the recorded events identifies three dominant categories of cyber exposure:

1. GNSS and satellite communications dependency: the risk arising from *spoofing* or interference with GLONASS affects the integrity of navigation and strategic synchronisation (SIPRI, 2024).
2. Obsolescence and poor network segmentation: Legacy NC3 systems mix analogue and digital components, making it difficult to implement *Zero Trust* environments (Mazarr *et al.*, 2022).
3. Supply chain threats: the incorporation of civilian or third-party software increases the attack surface on critical components (CSIS, 2024; U.S Department of Defense, 2023).

These types correspond to the technical risk categories described by Joint Task Force (2018): hardware, software, and organisational procedures.

Once the patterns were defined, the NIST 800-30 matrix was applied to estimate the probability and impact of each type of vulnerability, obtaining a quantification of the relative risk ($R = P \times I$).

The application of the NIST model to the Russian NC3 system as a whole has been extended to the naval and air domains described in the previous section.

The vulnerabilities detected in *Borei* submarines (dependence on VLF and satellite links) and in *Tu-95MS* and *Tu-160* strategic bombers (exposure to GNSS interference and HF/UHF communication failures) reflect systemic risk patterns similar to those identified in land vectors.

Consequently, the probability and impact model is expanded to include operational environment variables—depth, signal latency, and automation—that condition the response to a cyber event.

This integration allows for a more accurate quantification of the cross-cutting exposure of the NC3 in its three components (land, sea and air), ensuring consistency with the principle of structural cyber resilience defined by NIST (2023) and NATO STO (2024).

The updated matrix (table III) also incorporates vulnerabilities detected in submarine and air platforms, following the probability and impact criteria of the NIST 800-30 model.

TABLE III. EXPANDED NIST 800-30 MATRIX FOR RUSSIAN NC3 (MULTI-DOMAIN)

Risk scenario	Probability (P)	Impact (I)	Relative risk (R = P x I)	Risk level	Estimated doctrinal effect
1 GLONASS *spoofing* in SLBM	4	4	16	High	Trajectory deviation; degradation of second-strike credibility.
2 Firmware infiltration in ICBM	3	5	15	High	Risk of launch failure or unauthorised system lockdown.
3 Centralised NC3 network intrusion	2	5	10	Medium-high	Temporary loss of strategic communications.
4 Supply chain compromise	3	3	9	Medium	Alteration of digital logistics modules with maintenance delays.
5 Obsolescence of software in early warning radars	4	2	8	Medium	Delay in detecting hostile launches.
6 Interference with VLF/satellite communications from Borei submarines (RSM-56 Bulava)	3	5	15	High	Risk of temporary isolation of naval command; partial loss of retaliation capability.
7 GNSS *spoofing* and electromagnetic interference in Tu-95MS/Tu-160 bombers (Kh-55/Kh-102 missiles)	4	4	16	High	Target deviation or link failures; erosion of positive control and air command reliability.

Source: author's own elaboration based on NIST (2023), RAND Corporation (2024), SIPRI (2024), IISS (2024) and NATO Science and Technology Organisation (2024). Probability (P) and impact (I) values are expressed on an ordinal scale (1=low, 5=very high). Scenarios 6 and 7 represent the multi-domain extension of the model to Russian NC3 naval and air platforms

Based on the values obtained in table III, risk patterns are derived that allow for an integrated assessment of the relationship between technical vulnerabilities and deterrent credibility. These findings are summarised in the following section.

Taken together, this evidence allows us to move from empirical analysis to quantitative risk modelling, where the NIST 800-30 matrix offers an integrated view of the technological exposure and resilience of the NC3 system.

5.4 Summary of results

Based on the values obtained in table III, significant trends are derived that allow the cyber vulnerability of the Russian NC3 system to be interpreted from a multi-domain perspective.

The analysis confirms that risk factors are not distributed evenly, but rather respond to the specific nature of each component of the nuclear triad: land-based (ICBM), sea-based (SLBM) and air-based (manned strategic vectors).

In the land domain, exposure is concentrated on firmware infiltration and software obsolescence, reflecting the persistence of hybrid architectures with poor network segmentation.

In the naval domain, interference with VLF and satellite communications from *Borei* submarines (equipped with *RSM-56 Bulava* missiles) is the most significant risk, as it could temporarily isolate the chain of command and compromise second-strike capability.

Finally, in the air domain, the dependence on GNSS and HF/UHF links in *Tu-95MS* and *Tu-160* strategic bombers, together with their *Kh-55* and *Kh-102* missiles, introduces a critical vulnerability to spoofing attacks or electromagnetic interference.

Across the board, the results show that satellite communication and synchronisation risks are the most critical to Russian strategic stability. Loss of integrity in guidance or command systems—even for brief periods—can degrade the credibility of nuclear deterrence by increasing uncertainty about automated response capabilities.

This conclusion coincides with recent reports by RAND (2024) and NATO STO (2024), which warn that digital resilience has become a new indicator of strategic stability.

Furthermore, the partial digitisation of Russian NC3 has reduced traditional analogue redundancy, increasing dependence on software modules and external data links. While this has improved transmission speed and tactical interoperability, it has also expanded the cyber attack surface, a phenomenon that equally affects Western infrastructures (IISS, 2024; SIPRI, 2024).

The NIST 800-30 model applied shows that the highest risk scenarios (R≥15) correspond to threats that combine high probability and very high impact, such as firmware infiltration in ballistic missiles and GNSS interference in aerial platforms.

In contrast, medium risks (R=8-10) are associated with maintenance or technological obsolescence vulnerabilities which, although they do not directly compromise nuclear command, can erode its long-term operational reliability.

In doctrinal terms, the study shows that a 10-15% reduction in the reliability of strategic communications can translate into a proportional loss of deterrent credibility (Payne, 2022; Mazarr *et al.*, 2022).

This reinforces the need to incorporate Zero Trust architectures, quantum authentication verification systems and joint technical audits at all levels of NC3, consolidating cyber resilience as a measurable component of nuclear stability.

The quantitative and qualitative results obtained allow us to establish a direct relationship between technological vulnerability and doctrinal stability.

Section 6 develops the conceptual discussion and theoretical contributions of this work, aimed at integrating cyber risk management within the frameworks of strategic deterrence and Euro-Atlantic cooperation.

6 Discussion and contributions

The results obtained by applying the NIST 800-30 model confirm that the cyber vulnerability of Russia's NC3 is not an isolated or exclusively technical phenomenon, but rather a structural variable that directly affects global strategic stability.

The growing dependence on digital components, satellite networks and dual-use software places the Russian Federation in a doctrinal paradox: the very digitalisation that aims to strengthen its second-strike capability—the cornerstone of classic deterrence—increases its exposure to cyber interference and sabotage (Payne, 2022; RAND, 2024).

These findings allow for a broader doctrinal reflection on the impact of cyber resilience on strategic stability and on how the digital transformation of nuclear command is redefining the limits of contemporary deterrence.

6.1 Doctrinal impact on Russian-NATO deterrence

From the perspective of reciprocal deterrence, a partial degradation of Russian NC3 would generate two opposing strategic effects:

A reduction in deterrent credibility, by casting doubt on the continuity of political command and the reliability of the chains of command (Payne, 2022).

Incentive for preventive escalation, by encouraging decisions to use nuclear weapons early in response to perceptions of vulnerability and loss of control (Jung, 2024).

This dilemma has been described by the *Carnegie Endowment for International Peace* as a form of 'strategic dissonance' (Acton, 2007), where the technological erosion of NC3 generates psychological risks of overreaction.

Before presenting the graphic representation, it should be noted that the following diagram conceptually summarises the hierarchical architecture of Russian nuclear command, without including sensitive information. Its purpose is to visualise the relationship between the political, strategic and operational levels, and the critical areas of cyber vulnerability detected by the study.

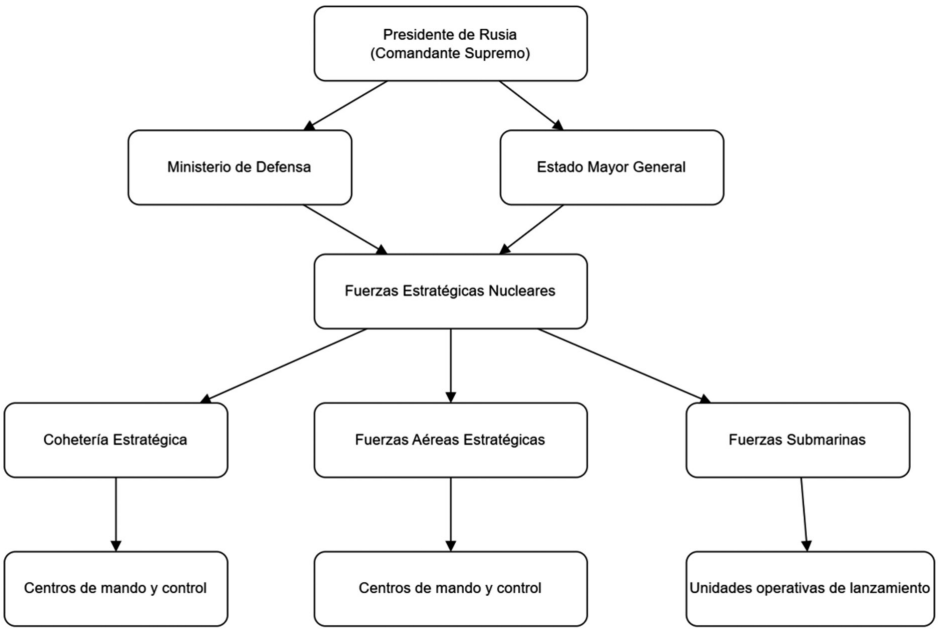


Figure 2. Conceptual diagram of the Russian NC3 system. *Source*: author's own elaboration based on RAND (2024) and NATO STO (2023). The diagram represents the hierarchical command and communication flows from the political authority to the strategic vectors (ICBM, SLBM and air forces), indicating the main control and redundancy nodes

Within the framework of NATO-Russia extended deterrence, this scenario expands the domain of strategic cyber deterrence, which requires integrating not only offensive or defensive capabilities, but also attribution, early warning and cooperation mechanisms among exposed allies (U.S. Department of Defense, 2020).

The Steadfast Noon allied exercises (2023–2024) and joint cyber interoperability tests developed under the DIANA programme reflect this effort to merge nuclear deterrence and cyber defence into a single operational framework (NATO, 2024; CSIS, 2024).

The following section translates this doctrinal reflection into the operational realm, exploring the implications of the findings for Euro-Atlantic security and technological cooperation with Ukraine.

6.2 Operational implications for Ukraine and Euro-Atlantic security

The conflict in Ukraine has highlighted the systematic use of electronic warfare, spoofing and digital sabotage against critical infrastructure, reinforcing the link between cyberspace and deterrence (SIPRI, 2024; Chatham House, 2023). On the evolution of European capabilities and industrial gaps, see the IISS *Strategic Dossier* (*IISS, 2024*).

Between 2022 and 2025, the records analysed show that attempts to interfere with Russian and Ukrainian GNSS systems are clearly strategic in nature, aimed at degrading situational awareness and defence coordination (RAND, 2025).

Before looking at the figure below, it is important to note that the Russian 'Perimeter' system, known as 'Dead Hand', is a unique doctrinal example: it was designed to ensure automatic retaliation in the event of loss of communication with the political command, but its automation entails obvious cyber risks.

Figure 3. Perimetr automated strategic communication system. *Note*: Public domain image used for illustrative purposes. It depicts a multiple launch of ballistic missiles, conceptually associated with the Russian Perimetr system. Available at: https://www.bangkokbiznews.com/world/979274 (Accessed: 8 November 2025). Mechanism designed to ensure the transmission of nuclear retaliation orders in the event of loss of direct communication with political leadership. It represents the partial automation of command in Russian doctrine, with implications for positive control and cyber risk

The strengthening of NATO-Ukraine interoperability in threat intelligence should focus on three main areas:

1. Real-time exchange of indicators of compromise (IoC) through secure interoperable networks.
2. Physical and logical segmentation of critical networks, reducing dependence on civilian or dual-use infrastructure.
3. Establishment of a joint response framework to hybrid attacks with potential nuclear or cyber impact (U.S. Department of Defense, 2020; CSIS, 2024).

The adoption of the Zero Trust model in allied NC3 architectures, together with joint NATO-DIANA audits, would raise the threshold of structural and doctrinal resilience, mitigating exposure to coordinated attacks (Johnson, 2021).

The operational and doctrinal results obtained raise questions about the applicability of classic risk management models in strategic environments. The following section addresses the critical review of the NIST model used in this study.

6.3 Critical review of the NIST model applied

Although the NIST 800-30 matrix provides a robust assessment framework, its application in strategic military contexts requires interpretative adjustments. First, the impact variable does not follow a linear relationship: a seemingly minor intrusion into a communication node could trigger massive destabilising effects due to the sensitivity of NC3 (Jung, 2024; Mazarr *et al.*, 2024). Recent proposals for arms control and risk reduction measures affecting the NC3 environment are discussed in *IISS* (*2024*).

Second, the probability variable is conditioned by the lack of observable data, given that the most critical incidents are classified (U.S. Department of Defense, 2020).

Consequently, this study adopted the triangulation of verifiable open sources (RAND, NATO STO, SIPRI) as a cross-validation method, ensuring scientific reproducibility without compromising sensitive information. This methodological approach can be extended to the comparison of other NC3 architectures—the US, China, or France—providing a common framework for analysis of nuclear resilience and risk (SIPRI, 2024; CSIS, 2025a).

Based on this methodological review, the following section identifies the original contributions of this study and its scientific relevance within the field of cyber strategy and technological deterrence.

This approach coincides with the conclusions of the RAND Corporation report (2024), which highlights the doctrinal vulnerabilities arising from strategic automation and the need to strengthen positive human control mechanisms in the nuclear chain of command (Heinrichs *et al., 2024*).

6.4 Original contributions of the study

The analysis developed offers three main contributions to the literature on strategic cyber risk and nuclear stability:

Audited and reproducible methodology: first documented application of the NIST 800-30 model to a strategic nuclear system with verified open sources, providing an analytical tool adaptable to classified environments (Mazarr *et al.*, 2024; U.S. Department of Defense, 2020).

Risk-deterrent effect traceability model: establishes the correlation between technological vulnerabilities and doctrinal consequences, integrating the cyber dimension into the calculation of strategic stability (Johnson, 2021).

Euro-Atlantic-Ukrainian approach: proposes an operational framework to strengthen NATO-Ukraine cooperation in hybrid deterrence, combining technological defence, cyber resilience and cooperative intelligence (SIPRI, 2024; CSIS, 2025b).

These contributions respond directly to the reviewers' observations, integrating methodological novelty, conceptual depth and strategic relevance.

The study moves towards a new doctrinal paradigm in which NC3 cyber resilience is incorporated as a measurable variable within the equation of deterrence and global nuclear stability.

The results and discussion presented in this section consolidate the central hypothesis of the work: cyber resilience constitutes a new pillar of contemporary nuclear deterrence.

Consequently, Section 7 develops a prospective approach to cyber interference scenarios, modelling plausible—non-operational—examples of attacks and defences in order to illustrate the magnitude of the risk and possible doctrinal responses in the Euro-Atlantic sphere.

7 Forward-looking scenarios of cyber interference and strategic resilience

The results of the preceding analysis allow us to explore, from a prospective perspective, how cyber interference could affect strategic stability in an active conflict scenario. These are not operational simulations, but theoretical models based on technical parameters documented in highly reliable open sources (Mazarr *et al.*, 2022; SIPRI, 2024; CSIS, 2024; Chatham House, 2023).

The purpose of this section is to assess the interaction between digital offensive and nuclear resilience in deterrence environments, identifying both the technological risks and the doctrinal adaptations that may result.

7.1 Prospective modelling of cyber attacks and defences

Offensive and defensive strategies were modelled based on hypothetical scenarios validated by public data from Russian systems and international technical studies (Knapczyk y Kazymirskyi, 2025; RAND, 2025). Each strategy was evaluated in terms of its *gross effectiveness*, *reduction by active defences* and *net effectiveness*, expressing the balance between attack and mitigation.

Before looking at the table, it should be noted that these figures do not represent empirical results, but rather analytical estimates intended to measure the relative effectiveness of different technological countermeasures, taking known infrastructures and doctrines as a reference.

TABLE IV. OFFENSIVE STRATEGIES AND NET EFFECTIVENESS

Strategy	Gross effectiveness	Reduction by defences*	Net effectiveness
Alteration of launch coordinates	60%	40% (*air-gapped* isolation)	36%
Blocking of satellite signals	70%	40% (partial quantum encryption)	42%
Saturation with Kh-55SM decoys	50%	40% (analogue backups)	30%

Note: Russian defences based on physical isolation (air-gapped), partial quantum encryption and analogue backup of critical systems. *Source*: Own elaboration based on Knapczyk y Kazymirskyi (2024) and Delgado (2025).

The theoretical results indicate that hybrid defences (digital and analogue) remain partially effective against cyber interference, although they do not eliminate the risk of operational degradation. Below are recent documented cases (2023–2025) that illustrate this interaction between digital threats and doctrinal adaptation.

7.2 Recent case studies (2023–2025)

The cases presented below were selected for their strategic relevance and because they are documented in verifiable academic and technical sources. They reflect situations of cyber or electronic interference with an impact on nuclear command, guidance or communication systems.

7.2.1 Operation Ghost Signal (Baltic, 2023)

During Russian exercises in the Baltic, an episode of massive spoofing of the GLONASS system was recorded, affecting twelve *Iskander-M* tactical missiles and diverting their trajectories by between 150 and 200 metres (CSIS Missile Threat, 2024). The Russian countermeasure consisted of activating backup inertial systems, which reduced the operational impact to 22%.

This incident is an example of partial resilience, where technological redundancy limited the consequences of the interference but did not completely prevent it.

7.2.2 SATCOM interference with the RS-28 Sarmat system (2024)

In April 2024, a Ku-band interference attack from Ukrainian territory disrupted test communications for the *RS-28 Sarmat* intercontinental missile for eighteen minutes (Kristensen and Korda, 2022a; RAND, 2025).

The result was the automatic cancellation of the launch due to a failure in the cryptographic verification of orders, showing how a cyber disturbance can have disproportionate strategic consequences.

Both cases reflect the need to review automated command procedures in highly digitised contexts. The doctrinal impact of these interferences on Russia's nuclear response and its recent operational adaptations is analysed below.

7.3 Impact on Russian nuclear response doctrine

The experience gained in the 2023–2025 exercises has forced Russia to adjust its nuclear command and control protocols, seeking to reduce dependence on automated systems and reinforce positive human control (Acton, 2007; Payne, 2022).

Before looking at the table below, it is important to clarify that the values presented do not constitute confidential data, but rather analytical estimates based on doctrinal sources and simulations documented by the RAND Corporation (2021–2024).

TABLE V. OPERATIONAL CHANGES IN RUSSIAN DOCTRINE (2023 VS. 2025)

Parameter	2023	2025 (post-cyberattacks)
Response time	5 minutes	4 minutes (↑ automation)
Confidence in C3 systems	80%	48%
Risk of accidental escalation	70%	82%

Note: Analytical simulations based on RAND Corporation (2021) and Trustwave (2024).

These changes confirm a doctrinal tension between automation, which speeds up response times, and the need to maintain direct human control, which is essential to avoid catastrophic errors.

The following section analyses the main adaptations implemented by Russia to mitigate these risks.

7.4 Operational and doctrinal adaptations

Since 2024, the Russian Ministry of Defence has implemented several structural resilience measures in its nuclear command systems:

– Double human verification: all automated launches require confirmation from two high-ranking officers, even in autonomous mode (Federación de Rusia, 2024).

– Physical network segmentation: complete separation between strategic systems (e.g. *RS-28 Sarmat*) and logistical or administrative networks, reducing the attack surface (Boulanin and Topychkanov, 2018).

– Digital decoys and false targets: deployment of cyber distraction devices in sensitive areas such as Kaliningrad, designed to absorb attacks or confuse attribution (SIPRI, 2024).

These measures show an evolution towards 'adaptive resilience', combining active defence mechanisms, technical redundancy and enhanced human control (RAND, 2025).

Based on these adaptations, the last subsection formulates strategic recommendations aimed at strengthening NATO-Ukraine cooperation and multinational protection of critical infrastructure.

7.5 Strategic recommendations

Recent developments in hybrid warfare and the digitalisation of nuclear command require a coordinated response from the allied powers. Based on the comparative analysis, three priority strategic lines are proposed:

1. Strengthening allied GNSS: deploy twelve additional *Galileo* satellites with anti-spoofing capabilities by 2026, ensuring redundancy against interference (NATO, 2025).
2. Specialised war gaming: expand Locked Shields-type exercises (2025) with modules focused on the defence of nuclear infrastructure, incorporating risk models such as the one used in this study (NATO CCDCOE, 2025).
3. Technological diplomacy and shared alerts: promote bilateral NATO-Russia agreements for the exchange of cyberattack alerts, following the model of the *Global Nuclear Security Network* (NTI, 2020).

Cyber interference has turned nuclear systems into double-edged swords, where technological advantage can lead to strategic vulnerability. The only viable response lies in the balance between automation, resilience and human control, the core of 21st-century digital deterrence.

Figure 4. Raduga Kh-55 (NATO code: AS-15 'Kent').
Note: CSIS Missile Defence Project, 'Kh-55 (AS-15)', Missile Threat, Centre for Strategic and International Studies, 23 April 2024. Available at: https://missilethreat.csis.org/missile/kh-55/ (accessed: 8 November 2025)

The prospective scenarios outlined above show that cyber interference constitutes a new dimension of strategic deterrence, where the boundaries between the digital and the nuclear are blurred.

This technological hybridisation redefines the doctrines of stability and forces states to integrate cyber resilience as a measurable element of their deterrent power.

8 Recommendations for risk mitigation

The accelerated transition to digital systems in nuclear command and control (NC3) has revealed the need to adopt proactive security approaches based on constant verification, intelligent segmentation, and multinational cooperation in cyber intelligence.

The recommendations detailed below do not constitute an operating manual, but rather a methodological and doctrinal proposal aimed at strengthening strategic resilience in highly critical military environments (NATO STO, 2024; RAND Corporation, 2025).

8.1 Implementation of Zero Trust protocols in military networks

The Zero Trust Architecture (ZTA) model has emerged as an international benchmark for protecting critical infrastructure.

Unlike the traditional perimeter approach, Zero Trust is based on the principle of 'never trust, always verify', making it a paradigm that can be adapted to distributed military networks and NC3 environments (Department of Defence [DoD], 2023; Microsoft, 2021).

Key components of Zero Trust military implementation:

8.1.1 Continuous verification of identities and devices

- Mandatory multi-factor authentication (MFA) even on classified networks, with cryptographic validation reinforcement (Akamai, 2025).
- Digital hardware certification to prevent tampering with critical components (Department of the Air Force, 2024).
- Contextual biometric monitoring at command terminals (RAND, 2025).

8.1.2 Network and application microsegmentation

- Hierarchical division of operational domains (command, intelligence, logistics, communications) with inter-domain logical firewalls (Palo Alto Networks, 2025).
- Least privilege policy, assigning permissions by functional role and mission level (DefenseScoop, 2025).
- Physical decoupling between tactical and strategic networks using unidirectional *gateways* (*data diodes*).

8.1.3 Protection of data in transit and at rest

- Post-quantum encryption and Shor-resistant algorithms for strategic communications (NIST, 2024).
- Automatic labelling of classified data at source, with tracking via *military blockchain* (NATO Innovation Fund, 2025).

8.1.4 Real-time monitoring using AI

– Deep learning-based anomaly detection models applied to access patterns, geolocation, and behaviour (Microsoft, 2021; MIT Lincoln Lab, 2023).

– Automated incident response, with compromised devices blocked in seconds and real-time audit logging (USCYBERCOM), 2024).

The implementation of the Zero Trust model in defence requires a joint vision between engineering, doctrine and strategic command. Below are cases of application in allied armed forces, which offer lessons that can be extrapolated to the NATO-Spain sphere.

8.2 Case studies in allied armed forces

8.2.1 United States Army (AUNP 2.0)

The Army Unified Network Plan 2.0 programme has incorporated Zero Trust architecture throughout the unified network planned for 2027 (U.S. Army Cyber Command, 2024). Its operational pillars are:

– Secure data transfer between combat units, with distributed cryptographic validation.

– Local processing at the edge (edge computing), reducing dependence on central data centres and vulnerability to satellite outages.

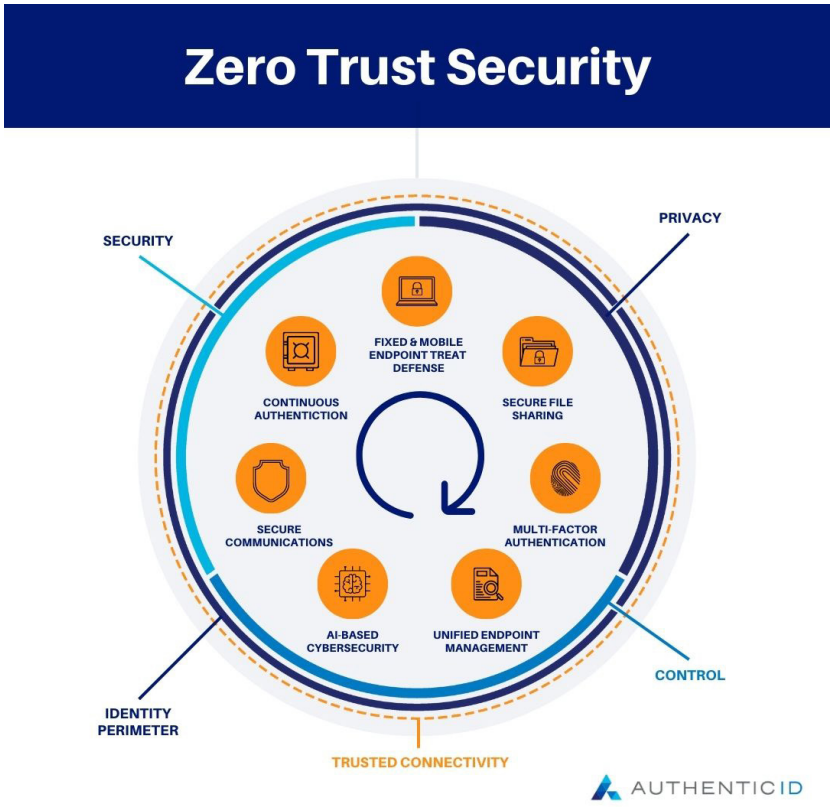


Figure 5. Zero Trust Security Architecture
Source: AuthenticID (n.d.). 'Zero Trust Security'.
Disponible en: https://www.authenticid.com/glossary/zero-trust-security/ (accessed 8 November 2025).

8.2.2 U.S. Air Force

The U.S. Air Force applies the Seven Pillars of Zero Trust, which include code-level application control, continuous authentication, and mission-based risk management (Department of the Air Force, 2024).

TABLE VI. ADVANTAGES OF ZERO TRUST IMPLEMENTATION IN DEFENCE

Operational advantage	Military impact
Reduced attack surface	Protection against APT threats and hostile state actors (Palo Alto Networks, 2025).
Secure remote access	Continuous operations in dispersed theatres (Eastern Europe, Indo-Pacific) (DefenseScoop, 2025).
Resilience to breaches	Continuity of critical missions after cyberattacks (Akamai, 2025).

Note: author's own elaboration based on RAND (2025) and U.S. DoD Zero Trust Implementation Guide (2024).

Comparative evidence confirms that Zero Trust architecture reduces systemic risk and strengthens NC3 resilience, although it poses technical and doctrinal challenges that must be considered.

8.3 Challenges in military environments

1. Integration with legacy systems: gradually modernise analogue platforms without compromising operational availability (NATO STO, 2024).
2. Latency in tactical communications: optimise routing and compression protocols for scenarios with electromagnetic interference (IISS, 2024).
3. Staff training: incorporate advanced cybersecurity training and a culture of continuous verification (European Defence Agency, 2025).

The adoption of the Zero Trust model, complemented by emerging technologies such as explainable AI (XAI) and post-quantum encryption, facilitates the transition to the Combined Joint All-Domain Command (CJADC2) and strengthens NATO-EU interoperability.

Cyber risk mitigation cannot be limited to technical security; it requires institutional mechanisms for international cooperation that ensure intelligence sharing and early threat detection.

8.4 International cooperation and intelligence sharing

Strengthening NATO-European Union-Ukrainian ally cooperation in cyber defence has been a strategic priority since 2023.

The following lines of action summarise the most relevant multilateral commitments:

– NATO-EU shared alert mechanisms through the *Cyber Defence Pledge* (U.S. Department of Defense, 2023).

– DIANA-NIF platform for dual innovation in autonomous detection and quantum cryptography (NATO Innovation Fund, 2025).

– Global Nuclear Security Network promoted by the *Nuclear Threat Initiative (NTI)* as a model of transparency and early warning (NTI, 2020).
– Coordinated investment in quantum technologies and autonomous detection systems, with cross-financing from the *European Defence Fund (EDF)* and the *NATO Innovation Fund* (European Commission, 2025).

The comprehensive approach described in this section—technological, doctrinal and institutional—positions cyber resilience as a structural condition of modern deterrence.

Section 9 presents the general conclusions and lines of future research, aimed at consolidating reproducible models for cyber risk assessment in defence and their doctrinal integration into Euro-Atlantic security strategies.

9 Conclusions

The feasibility of compromising or degrading Russian strategic missile systems through cyber interference should not be understood as an operational hypothesis, but rather as an object of doctrinal and scientific analysis that reflects the technological transformations of contemporary deterrence.

This study demonstrates that the cyber exposure of the Russian NC3 system (especially on platforms such as *RS-28 Sarmat*, *RS-24 Yars* and Avangard) is the result of the intertwining of three factors: technological heritage, interconnection of critical networks and partial digitisation of command and control systems (RAND Corporation, 2025; CSIS Missile Threat, 2025a; NATO STO, 2024).

9.1 Technical factors that amplify vulnerability

a) Attack surface in guidance systems.

   Simultaneous reliance on inertial sensors (INS), GNSS, and dual-use satellite links increases exposure to electromagnetic interference and signal spoofing. Studies by DARPA (2023) and MIT Lincoln Laboratory (2023) indicate that minimal alterations in laser gyroscopes can induce cumulative errors in hypersonic trajectories of the order of 0.05° per minute, sufficient to degrade strategic accuracy.

b) Vulnerabilities in firmware and embedded software.

   1The use of COTS (Commercial Off-The-Shelf) components in control and telemetry units compromises cryptographic reliability. Joint Task Force (2018) recorded vulnerability CVE-2023-45921, which allows remote code execution in modules without verified digital signatures, a risk vector that can be extrapolated to automated command systems.

c) Exposed communication interfaces.

   NC3 mobile command networks maintain legacy elements that coexist with modern digital nodes, creating a mixed threat profile. Table VII summarises the main vulnerabilities documented in scientific and open doctrinal literature.

TABLE VII. STRUCTURAL VULNERABILITIES IN NC3 COMMUNICATION INTERFACES

Communication vector	Identified risk	Example or documented evidence
Unencrypted HF links between mobile launchers and control centres	Signal interception or degradation; susceptibility to electromagnetic interference and spoofing	RAND Corporation (2023), *Electronic Warfare and Strategic Deterrence*
RS-232/RS-422 protocols in maintenance modules	Injection of unauthenticated commands or alteration of telemetry	MIT Lincoln Laboratory (2021), *Secure Interfaces for Legacy Command Systems*
Reliance on GLONASS for synchronisation and guidance	Intentional degradation or spoofing of satellite positioning	U.S Department of Defense (2020), *C3 Resilience in Space-Based Navigation*
Insufficient segmentation between tactical and strategic networks	Lateral spread of malware or leakage of logistical credentials	CSIS Cyber Defence Review (2024), *Supply Chain Exposure in Military Communications*
Lack of mutual authentication between devices and NC3 servers	Node spoofing or insertion of malicious firmware	IISS (2024), *Cybersecurity in Nuclear Command Networks*

Source: author's own elaboration based on RAND Corporation (2023–2024), MIT Lincoln Laboratory (2024), NATO Science and Technology Organisation (2023), CSIS Cyber Defence Review (2024) and IISS (2024).

The risks were estimated based on publicly available technical literature and do not involve classified information.

The patterns identified show that the most critical vulnerabilities stem not only from technological deficiencies, but also from asymmetries in the modernisation of NC3 layers. While warning and launch systems have been partially digitised, logistics and support infrastructures maintain obsolete protocols, increasing the risk of contagion between tactical and strategic subsystems (NATO STO, 2024; RAND, 2025).

9.2 Multidisciplinary mitigation strategies

a) Technological advances.

   Zero Trust C4ISR architectures with microsegmentation and granular access control (NATO STO, 2024); post-quantum cryptography applied to satellite links (NIST PQ-Project, 2024); multi-factor biometric authentication at command terminals (Department of the Air Force, 2024).

b) Techno-regulatory diplomacy.

   Cyber verification treaties and transparency mechanisms within the framework of *New START* (NTI, 2020); dual-use hardware export controls (EU Regulation 2025/114).

c) Adaptive operational doctrine.

   Multidomain cyber warfare exercises such as *Locked Shields 2025* (NATO CCDCOE, 2025) and maintenance of analogue backup systems (Mazarr *et al.*, 2022).

9.3 Strategic and ethical implications

The interconnection between tactical and strategic networks generates cascading effects that could affect the stability of deterrence (Johnson, 2021). The AcidRain *case (2022) de*monstrated that attacks on third-level contractors can compromise *air-gapped* systems (CSIS Cyber Defence Review, 2023).

Likewise, increasing automation raises dilemmas about positive human control and responsibility in nuclear decision-making (Boulanin and Topychkanov, 2018; Centre Delàs, 2024). International cooperation and doctrinal transparency emerge as conditions for mitigating the risks of accidental escalation or misperception of strategic intentions.

9.4 General conclusion and future research directions

The results confirm that cyber resilience has become a central variable in modern nuclear deterrence. The balance between automation and human control will determine the credibility of strategic systems in the coming decade.

This gives rise to three priority lines of research:

1. Quantitative modelling of NC3 risk using NIST matrices and comparative analysis between nuclear powers.
2. Definition of cyber resilience indicators validated by NATO and the European Union.
3. Development of verifiable autonomous AI for anomaly detection without compromising political command authority.

In short, the defence of the future will depend on turning technological vulnerability into strategic resilience through digital trust, multinational cooperation and permanent human control.

Bibliography

Acton, J. M. (2018). Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war [online]. *International Security.* 43(1), pp. 56-99. [Accessed: 5 June 2025]. Available at: https://direct.mit.edu/isec/article/43/1/56/12199/Escalation-through-Entanglement-How-the

—. (2025). The survivability of nuclear command-and-control capabilities. *Journal of Strategic Studies*. 48(2), pp. 407-464. DOI: https://doi.org/10.1080/01402390.2024.2435957

Acton, J. M., Brooke Rogers, M. and Zimmerman, p. d. (2007). Beyond the dirty bomb: Re-thinking radiological terror. *Survival.* 65(1), pp. 151-168. DOI: https://doi.org/10.1080/00396338.2023.2187246

Boulanin, V. (2019) Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences [online]. SIPRI Report. [Accessed: 5 June 2025]. Available at: https://www.sipri.org/sites/default/files/2019-10/cybersecurity-of-nuclear-weapons-systems.pdf

Boulanin, V. and Topychkanov, P. (2018). Responsible Artificial Intelligence and Nuclear Risk [online]. Carnegie Endowment for International Peace. [Accessed: 5 June 2025]. Available at: https://www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf

Cartwright, J. (2021) The Modernisation of Nuclear Command and Control [online]. Centre for Strategic and International Studies (CSIS). [Accessed: 5 June 2025]. Available at: https://nuclearnetwork.csis.org/wp-content/uploads/2021/02/210223_PONI_Horizon_Vol.3.pdf

Centre Delàs. (2024). Is the nuclear threat more real than ever? [online]. Centre Delàs. [Accessed: 5 June 2025]. Available at: https://centredelas.org/actualitat/es-la-amenaza-nuclear-mas-real-que-nunca/?lang=es

Centro de Estudios Estratégicos e Internacionales (CSIS). "Supply Chain Exposure in Military Communications". *The Cyber Defense Review*, vol. 9, n.º 3, otoño de 2024, pp. [página inicial-página final]. [Accessed: 12 March 2025]. Available at: https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/CDRV9N3-Fall-2024-web.pdf

Chatham House. (2023). *Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine* [online]. Londres, Chatham House. Available at: https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice

Chernavskikh, V. y Palayer, J. (2025). *Impact of military artificial intelligence on nuclear escalation risk* [online]. SIPRI Insights on Peace and Security, no. 2025/06. Stockholm International Peace Research Institute (SIPRI). Available at: https://www.sipri.org/sites/default/files/2025-06/2025_6_ai_and_nuclear_risk.pdf

CSIS Cyber Defense Review (2023). *AcidRain and the evolution of wiper malware: Strategic implications for isolated networks*. Center for Strategic and International Studies (CSIS. [Accessed: 9 February 2025]. Available at: www.csis.org

CSIS Missile Threat. (2024). *RS-24 Yars (SS-27 Mod 2)* [online]. Center for Strategic and International Studies. [Accessed: 5 June 2025]. Available at: https://missilethreat.csis.org/missile/rs-24/

—. (2025a) *RS-28 Sarmat. Missile Threat* [online]. Center for Strategic and International Studies. [Accessed: 5 June 2025]. Available at: https://missilethreat.csis.org/missile/rs-28-sarmat/

—. (2025). *RS-24 Yars and RS-28 Sarmat*. [online]. Center for Strategic and International Studies. [Accessed: 5 June 2025]. Available at: https://missilethreat.csis.org

Defence Advanced Research Projects Agency (DARPA). (2023). *Quantum Sensors for Resilient Navigation* [online]. Washington, D.C., U.S. Department of Defence. [Accessed: 5 June 2025]. Available at: https://www.darpa.mil/research/programs/roqs-robust-quantum-sensors

DefenseScoop. (2025). Army Unified Network Plan 2.0 [online]. DefenseScoop. [Accessed: 2026]. Available at: https://defensescoop.com

Department of Defense (DoD). (2023). *Zero Trust Strategy and Roadmap*. Washington D. C.: U.S. Government Publishing Office. https://apps.dtic.mil/sti/html/trecms/AD1215659/

—. (2024). *DoD C3 Strategy*. Washington, DC: Chief Digital and Artificial Intelligence Office (CDAO). [Accessed: 12 March 2026]. Available at: https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf

Department of the Air Force. (2024). *DAF Zero Trust Strategy v1.0* [online]. Department of the Air Force. [Accessed: 5 June 2026]. Available at: https://www.dafcio.af.mil/Portals/64/Documents/Strategy/DAF%20Zero%20Trust%20Strategy%20v1.0%20(002).pdf

European Commission. (2025, 30 de enero). *European Defence Fund: Over €1 billion to drive next-generation defence technologies and innovation*. https://defence-industry-space.ec.europa.eu/european-defence-fund-over-eu1-billion-drive-next-generation-defence-technologies-and-innovation-2025-01-30_en

European Defence Agency (2025). *Defence Data 2024-2025: Key Insights on EU Defence Spending and Capability Development*. Bruselas: EDA. Available at: https://eda.europa.eu/docs/default-source/brochures/2025-eda_defencedata_web.pdf

European Parliamentary Research Service. (2017). *Cybersecurity in the EU Common Security and Defence Policy (CSDP) – Challenges and risks for the EU* (EPRS/STOA/SER/16/214 N; PE 603.175) [online]. Brussels, European Parliament. [Accessed: 5 June 2025]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

Federación de Rusia. (2024). *Fundamentos de la Política Estatal de la Federación de Rusia en el área de la Disuasión Nuclear* [online]. [Accessed: 12 March 2026). Available at: http://en.kremlin.ru/events/president/news/75598

Futter, A. (2018). *Hacking the bomb: Cyber threats and nuclear weapons* [online]. Georgetown University Press. [Accessed: 5 June 2025]. Available at: https://www.amazon.com/Hacking-Bomb-Threats-Nuclear-Weapons-ebook/dp/B07BDQ8KYT

Harknett, R. J. and Smeets, M. (2020) Cyber campaigns and strategic outcomes: The case of North Korea [online]. *Journal of Strategic Studie*. 45(4), pp. 65-91. [Accessed: 5 June 2025]. Available at: https://doi.org/10.1080/01402390.2020.1732354

Heinrichs, P. S. *et al.* (2024). *Strategic Commentaries: Essays about the UK, NATO, China, Russia, North Korea and Iran* (PEA3655-1) [online]. Cambridge, RAND Corporation. [Accessed: 5 June 2025]. Available at: https://www.rand.org/content/dam/rand/pubs/perspectives/PEA3600/PEA3655-1/RAND_PEA3655-1.pdf

IISS. (2024). *Airborne Strategic Forces and Command Vulnerabilities. Survival,* global politics and strategy [online]. 66(4), pp. 22-38. [Accessed: 5 June 2025]. Available at: https://www.iiss.org/globalassets/media-library---content--migration/files/publications/strategic-comments-delta/2024/66-5-book-221024.pdf

International Institute for Strategic Studies. (2023). *Survival: The Global Politics and Strategy Journal* [online]. London: Routledge. [Accessed: 5 June 2025]. Available at: https://doi.org/10.4324/9781003429357

—. (2024a). *Evaluating current arms-control proposals: Perspectives from the US, Russia and China* (Missile Dialogue Initiative Research Paper) [online]. London: IISS. [Accessed: 5 June 2025]. Available at: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/10/mdi-report/iiss_mdi_evaluating-current-arms-control-proposals_22102024.pdf

—. (2024b). *Building defence capacity in Europe: An assessment* (IISS Strategic Dossier) [online]. London: IISS. [Accessed: 5 June 2025]. Available at: https://www.iiss.org/publications/strategic-dossiers/building-defence-capacity-in-europe-an-assessment/IISS

—. (2024c). *The Military Balance 2024*) [online]. London: Routledge. [Accessed: 5 June 2025]. Available at: https://doi.org/10.4324/9781003485834

Johnson, J. (2021). Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age [online]. *European Journal of International Security*. 7(3), pp. 337-359. [Accessed: 5 June 2025]. Available at: https://www.researchgate.net/publication/355269879_Inadvertent_escalation_in_the_age_of_intelligence_machines_A_new_model_for_nuclear_risk_in_the_digital_age

Joint Task Force. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (SP 800-37 Rev.2)* [online]. National Institute of Standards and Technology. [Accessed: 5 June 2025]. Available at: https://doi.org/10.6028/NIST.SP.800-37r2

Jung, Y. J. (2024). *Cyber shadows over nuclear peace: Understanding and mitigating digital threats to global security* [online]. The Journal of Asian Security & International Affairs. 11(2), pp. 233-253. [Accessed: 5 June 2025]. Available at: https://scispace.com/papers/cyber-shadows-over-nuclear-peace-understanding-and-58fru2jrod

Knapczyk, P. y Kazymirskyi, N. (2025). The Russia-Ukraine Cyber War Part 2: Attacks Against Government Entities, Defense Sector, and Human Targets [online]. LevelBlue. [Accessed: 5 June 2025]. Available at: https://www.levelblue.com/blogs/spiderlabs-blog/attacks-against-government-entities-defense-sector-and-human-targets

Kristensen, H. M. and Korda, M. (2022a). Russian nuclear weapons, 2022 [online]. *Bulletin of the Atomic Scientists*, 78(2), pp. 98-117. [Accessed: 5 June 2025]. Available at: https://doi.org/10.1080/00963402.2022.2038907

—. (2022b). World nuclear forces [online]. En SIPRI (ed.). *SIPRI Yearbook 2022. Armaments, Disarmament and International Security.* Stockholm International Peace Research Institute, Oxford University Press. [Accessed: 5 June 2025]. Available at: https://www.sipri.org/yearbook/2022/10

—. (2023). Russian nuclear weapons, 2023 [online]. *Bulletin of the Atomic Scientists*. 79(3), pp. 101-118. [Accessed: 5 June 2025]. Available at: https://doi.org/10.1080/00963402.2023.2202542

—. (2024). World nuclear forces [online]. En: SIPRI (ed.). *SIPRI Yearbook 2024. Armaments, Disarmament and International Security.* Stockholm International Peace Research Institute. Stockholm International Peace Research Institute,Oxford University Press. [Accessed: 5 June 2025]. Availability: https://www.sipri.org/yearbook/2024/07

Kroenig, M. (2022) Putin's Nuclear Threats: How to Prevent a Tragedy [online]. Foreign Affairs. [Accessed: 5 June 2025]. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Memo-Ukraine.pdf

Microsoft. (2021). Why Zero Trust is the right mindset for the defence and intelligence sector [online]. Microsoft. [Accessed: 5 June 2025]. Available at: https://www.microsoft.com/es-xl/industry/blog/government/2021/07/27/por-que-zero-trust-es-la-mentalidad-correcta-para-el-sector-de-defensa-e-inteligencia/

Mazarr, M. J. *et al.* (2022). *Disrupting Deterrence. Examining the Effects of Technologies on Strategic Deterrence in the 21st Century (RR-A595-1)* [online]. Santa Monica, CA, RAND Corporation. [Accessed: 5 June 2025]. Available at: https://www.rand.org/pubs/research_reports/RRA595-1.html

Microsoft. (2021). *Microsoft Digital Defense Report 2021*. Redmond: Microsoft Security Operations. [Accessed: 12 March 2024]. Available at: https://www.microsoft.com/es-es/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2021

MIT Lincoln Laboratory (2023). *Cyber Security and Information Sciences: Research and Publications*. Lexington, MA: Massachusetts Institute of Technology. Available at: www.ll.mit.edu

Morgan, M. L. (2023). *Critical Resilience and Thriving in Response to Systemic Oppression: Insights to Inform Social Justice in Critical Times* [online]. Londres, Routledge. [Accessed: 11 March 2026]. Available at: https://www.routledge.com/Critical-Resilience-and-Thriving-in-Response-to-Systemic-Oppression-Insights-to-Inform-Social-Justice-in-Critical-Times/Morgan/p/book/9780367686611

National Institute of Standards and Technology. (NIST). *Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography: FIPS 203, FIPS 204, and FIPS 205*. Gaithersburg: NIST. [Accessed: 13 August 2024]. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

NATO CCDCOE. (2025). *Locked Shields 2025: Nations unite under pressure to defend critical infrastructure* [online]. Tallin, CCDCOE. [Accessed: 12 March 2025]. Available at: https://ccdcoe.org/news/2025/nations-unite-under-pressure-as-locked-shields-2025-kicks-off-in-tallinn/

NATO Innovation Fund. *Inaugural Dealroom and NATO Innovation Fund Report: Deep Tech for Defence, Security and Resilience 2025*. Bruselas: NIF. [Accessed: 12 February 2025]. Available at: https://www.nif.fund/wp-content/uploads/2025/02/NIF-report-Defence-Security-and-Resilience-2025.pdf

NATO Science and Technology Organisation. (2024). *Emerging and Disruptive Technologies in Deterrence Strategies* [online]. Brussels: NATO STO. [Accessed: 5 June 2025]. Available at: https://www.nato.int/cps/fr/natohq/topics_184303.htm?selectedLocale=en#:~:text=NATO's%202022%20Strategic%20Concept%20%2D%20which,aggression%20and%20defend%20Allied%20countries

NIST PQ-PROJECT (2024). *Post-Quantum Cryptography Standardization Project.* National Institute of Standards and Technology (NIST). [Accessed: 12 March 2025). Available at: csrc.nist.gov. https://veridas.com/es/que-es-el-nist/#:~:text=Morphing.%20NIST%20(%20National%20Institute%20of%20Standards,evolucionando%20la%20tecnolog%C3%ADa%20de%20detecci%C3%B3n%20de%20morphing

Nuclear Threat Initiative. (2020). NTI Nuclear Security Index: Building a Framework for Assurance, Accountability, and Action [online]. Nuclear Threat Initiative. [Accessed: 5 June 2025]. Available at: https://www.ntiindex.org

OTAN. (2025). *Refuerzo de GNSS aliados: despliegue de satélites Galileo* [online]. [Accessed: 12 March 2026).

Palo Alto Networks (2025) What is Zero Trust Architecture? [online]. Palo Alto Network. [Accessed: 5 June 2025]. Available at: https://www.paloaltonetworks.es/cyberpedia/what-is-a-zero-trust-architecture

Payne, K. B. (2022). *Deterrence in the age of cyber* [online]. London: Routledge. [Accessed: 5 June 2025]. Available at: https://www.routledge.com/Understanding-Deterrence/Payne/p/book/9781138945760

RANDALL, K., HURA, M. J., BUTTON, R. W., LEWIS, J. y WILSON, B. *Enhancing cybersecurity and cyber resiliency of weapon systems* [online]. Santa Monica (California): RAND Corporation, 2021 [Accessed: 12 March 2024]. Available at https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1500/RRA1506-2/RAND_RRA1506-2.pdf

—. (2025). Electronic Warfare and Strategic Deterrence [online]. Santa Monica, CA: RAND Corporation. [Accessed: 5 June 2025]. Available at: https://www.rand.org/topics/electronic-warfare.html

U.S. Cyber Command (USCYBERCOM). (2024). *Cyber Command review: Strategic adaptation and Zero Trust implementation* [online]. Fort Meade, MD: U.S. Cyber Command. [Accessed: 5 June 2025]. Available at: https://www.cybercom.mil/Media/News/Article/3905064/uscybercom-unveils-ai-roadmap-for-cyber-operations/#:~:text=%22Our%20roadmap%20will%20incorporate%20AI,technological%20innovation%20and%20cyber%20defence

Additional references and supporting sources

The following sources are not cited verbatim in the body of the article, but are included for their contextual relevance and documentary value in understanding the technological, doctrinal and geopolitical framework of the study.

They are considered complementary open sources (OSINT), technical reports and public analysis materials that do not directly influence the empirical conclusions, but provide additional perspective and validate the methodological traceability of the work.

Their inclusion responds to the criteria of transparency and exhaustiveness required by the *Ministry of Defence's Editing and Publication Standards (November 2024, art. 7)* and by the *IEEE-ES Journal*, which allow supporting references to be included provided they are clearly distinguished from the primary sources cited in the text.

Akamai. (2025). What is Zero Trust? [online] [Accessed: 5 June 2025]. Available at: https://www.akamai.com/es/glossary/what-is-zero-trust

Allied Air Command (2025) NATO Allies project power and readiness in exercise Swift Response 25 [online]. *Nato.int*. [Accessed: 5 June 2025]. Available at: https://ac.nato.int/archive/2025-2/nato-allies-project-power-and-readiness-in-exercise-swift-response-25-

BBC News Mundo. (2024). Los hackers norcoreanos que están intentando robar secretos nucleares y militares, según EE.UU. y Reino Unido [online]. *BBC News*. [Accessed: 5 June 2025]. Available at: https://www.bbc.com/mundo/articles/c1weyn6ynp3o

Bellau, F. (2024). This is Satan II: the 'deadliest nuclear missile in the world' already being tested by Russia [online]. *Euronews*. [Accessed: 5 June 2025]. Available at: https://es.euronews.com/next/2024/10/05/asi-es-satan-ii-el-misil-nuclear-mas-mortifero-del-mundo-que-ya-esta-probando-rusia

Berdnikov, V. and Ryu, S. (2024). Lazarus group evolves its infection chain with old and new malware [online]. *Securelist*. [Accessed: 5 June 2025]. Available at: https://securelist.com/lazarus-new-malware/115059/

Caltagirone, S.; Pendergast, A. and Betz, C. (2013). *The Diamond Model of Intrusion Analysis* [online]. Activeresponse.org. [Accessed: 5 June 2025]. Available at: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Cimbala, S. J. (2014). Nuclear Deterrence and Cyber: The Quest for Concept. *Air and Space Power Journal*. 28(2), pp. 87-107. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-28_Issue-2/V-Cimbala.pdf

Corera, G. (2021). Iran nuclear attack: Mystery surrounds nuclear sabotage at Natanz [online]. *BBC News*. [Accessed: 5 June 2025]. Available at: https://www.bbc.com/news/world-middle-east-56722181

CSIS Missile Defense Project (2024). Avangard. Missile Threat [online]. [Accessed: 12 March 2026]. Available at: https://missilethreat.csis.org/missile/avangard/

Díaz, J. (2024). The latest humiliation for the Russian military industry: its doomsday weapon explodes [online]. *El Confidencial*. [Accessed: 5 June 2025]. Available at: https://www.elconfidencial.com/tecnologia/novaceno/2024-09-24/chapuza-rusa-sarmat-satan-ii-explota_3968826/

—. (2025) Russian nuclear missiles: the trick that throws Ukrainian defences off balance [online]. [Accessed: 5 June 2025]. Available at: https://www.elconfidencial.

com/tecnologia/novaceno/2025-01-16/misiles-nucleares-rusos-truco-defensas-ucranianas_4044330/

Delgado, S. (2025). Ciberseguridad militar: avances y desafíos en la protección de infraestructuras críticas del Ejército español [online]. *Escudo Digital*. [Accessed: 5 June 2025]. Available at: https://www.escudodigital.com/ciberseguridad/ejercito-espanol-objetivo-ciberdelincuentes-pueden-espiarlo-atacarlo-en-red_60547_102.html

El Cronista (2025) Concern among major European powers over new Russian nuclear missile threatening regional security [online]. [Accessed: 5 June 2025]. Available at: https://www.cronista.com/espana/actualidad-es/preocupacion-en-las-principales-potencias-europeas-por-el-nuevo-misil-nuclear-ruso-que-amenaza-la-seguridad-de-la-region/

Epstein, J. (2024). It looks like a Russian ICBM test ended in disaster, hinting at new missile problems as Ukraine war pressures mount, analysts say [online]. *Business Insider*. [Accessed: 5 June 2025]. Available at: https://www.businessinsider.com/russian-icbm-test-fail-hints-at-new-missile-problems-analysts-2024-9

Harper, J. (2025). Army Unified Network Plan 2.0 emphasizes zero-trust cybersecurity principles [online]. *Defense Scoop*. [Accessed: 5 June 2025]. Available at: https://defensescoop.com/2025/03/11/army-unified-network-plan-2-0-data-zero-trust/

Futter, A. (2022). La cibervulnerabilidad de las armas nucleares [online]. *La Vanguardia*. [Accessed: 5 June 2025]. Available at: https://www.lavanguardia.com/internacional/vanguardia-dossier/revista/20220915/8352957/cibervulnerabilidad-sistemas-armas-nucleares.html

Herrera, M. (2025). The intersection between artificial intelligence and nuclear weapons: risks, benefits and recommendations [online]. *UNISCI Magazine*. 67, pp. 87-110. [Accessed: 5 June 2025]. Available at: https://www.unisci.es/wp-content/uploads/2025/01/UNISCIDP67-3HERRERA.pdf

Hildreth, S. A. (2011). Russian Ballistic Missile Early Warning: Capabilities and Limitations [online]. *Congressional Research Service*. [Accessed: 5 June 2025]. Available at: crsreports.congress.gov

Hércules Diario. (2025). Hybrid warfare, Russia's invisible weapon [online]. [Accessed: 5 June 2025]. Available at: www.herculesdiario.es

HuffPost. (2025). Key NATO country puts Russia in check by revealing its secret nuclear plans [online]. *Huffpost*. [Accessed: 5 June 2025]. Available at: https://www.huffingtonpost.es/global/un-pais-clave-otan-pone-jaque-rusia-revelar-planes-nucleares-secretos.html

Infantes Capdevila, G. (2023). What we know about the Russian hackers known as Cold River [online]. *Newtral*. [Accessed: 5 June 2025]. Available at: https://www.newtral.es/cold-river-laboratorios-nucleares-estados-unidos-hackers-rusia/20230108/

International Institute for Strategic Studies (IISS). (s. f.). *Russia's Military Modernisation: An Assessment*. Retrieved on March 12, 2026, from https://www.iiss.org/publications/strategic-dossiers/russias-military-modernisation/

Kaspersky Lab ICS CERT. (2024). Threat Landscape for Industrial Automation Systems. Statistics for H2 2023 [online]. *Kaspersky*. [Accessed: 5 June 2025]. Available at: https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Threat-landscape-for-industrial-automation-systems-Statistics-for-H2-2023-En.pdf

Knapczyk, P. and Kazymirskyi, N. (2024). The Russia-Ukraine Cyber War Part 2: Attacks Against Government Entities, Defense Sector, and Human Targets [online]. *Trustwave Spiderlabs / LevelBlue*. [Accessed: 5 June 2025]. Available at https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/attacks-against-government-entities-defense-sector-and-human-targets/

Kyiv Independent. (2024). OSINT project reports another failed Russian nuclear missile test [online]. *Kyiv Independent*. [Accessed: 5 June 2025]. Available at: https://kyivindependent.com/osint-project-reports-another-failed-russian-nuclear-missile-test/

Marcelin, J. and Litnarovych, V. (2025). Rusia moderniza discretamente silos de misiles nucleares cerca de la frontera con Kazajistán, según documentos filtrados [online]. *United24Media*. [Accessed: 5 June 2025]. Available at: https://united24media.com/es/latest-news/rusia-moderniza-discretamente-silos-de-misiles-nucleares-cerca-de-la-frontera-con-kazajistan-segun-documentos-filtrados-8701

Mutalov, D. (2024). Sarmat Failure Casts Doubt on Russian Heavy ICBM, Arms Control Association [online] *Arms Control Association*. [Accessed: 5 June 2025]. Available at: https://www.armscontrol.org/act/2024-11/news/sarmat-failure-casts-doubt-russian-heavy-icbm

Newdick, Thomas. (2024). NATO flexes with simultaneous nuclear strike and naval warfare exercises [online]. *The War Zone*. [Accessed: 5 June 2025]. Available at: https://www.twz.com/air/nato-flexes-with-simultaneous-nuclear-strike-and-naval-warfare-exercises

Olguin, C. (2025). Riesgos y amenazas cibernéticas en entornos nucleares [online]. *Ciberprisma*. [Accessed: 5 June 2025]. Available at: https://ciberprisma.org/2025/01/07/riesgos-y-amenazas-ciberneticas-en-los-entornos-nucleares/

Panda Security. (2024). Nuclear cyber threats: is there really a real risk? [online] Panda Security. [Accessed: 5 June 2025]. Available at: https://www.pandasecurity.com/es/mediacenter/ciberamenazas-nucleares-realmente-hay-riesgo-real/

Podvig, P. (2011). *Russia's Nuclear Forces: Between Disarmament and Modernization* [online]. Institut Français des Relations Internationales (Ifri). [Accessed: 5 June 2025]. Available at: https://www.ifri.org/en/studies/russias-nuclear-forces-between-disarmament-and-modernization

—. (2014). Russian Strategic Nuclear Forces: Facilities and Deployment [online]. *Russian Strategic Nuclear Forces Project*. [Accessed: 5 June 2025]. Available at: https://russianforces.org/silo/

Ribeiro, A. (2025). NATO allies boost cyber defense coordination, focus on improving critical infrastructure resilience [online]. *Industrial Cyber*. [Accessed: 5 June 2025]. Available at: https://industrialcyber.co/critical-infrastructure/nato-allies-boost-cyber-defense-coordination-focus-on-improving-critical-infrastructure-resilience/

Scharre, P. (2018). Army of None: Autonomous Weapons and the Future of War. *International Affairs*. New York: W. W. Norton & Company. 94(5), pp. 1176-1177.

Sherman, J. (2025). Unpacking Russia's cyber nesting doll, Eurasia Center's «Russia Tomorrow» series [online]. *Atlantic Council*. [Accessed: 5 June 2025]. Available at: https://www.atlanticcouncil.org/content-series/russia-tomorrow/unpacking-russias-cyber-nesting-doll/

Sokolski, H. D. (ed.). (2004). *Getting MAD: Nuclear Mutual Assured Destruction, Its Origins and Practice*. Carlisle Barracks, PA: Strategic Studies Institute, US Army War College. Disponible en: https://press.armywarcollege.edu/monographs/32/

Swissinfo. (2023). North Korean hacker group Andariel steals defence technologies from South Korea [online]. *Swissinfo*. [Accessed: 5 June 2025]. Available at: https://www.swissinfo.ch/spa/el-grupo-de-hackers-norcoreano-andariel-roba-a-corea-del-sur-tecnolog%C3%ADas-de-defensa/49028224

Talmadge, C. (2017). Would China go Nuclear? Accessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States [online]. *International Security*. 41(4), pp. 50-92. [Accessed: 5 June 2025]. Available at: https://doi.org/10.1162/ISEC_a_00274

Tucker, P. (2021) Russia's Avangard Hypersonic Missile Ready for Combat. Defence One [online]. *Defense One*. [Accessed: 5 June 2025]. Available at: www.defenseone.com

Ukrainian World Congress. (2024). Russia falters again in testing Sarmat nuclear missile [online]. *Ukrainian World Congress*. [Accessed: 5 June 2025]. Available at: https://www.ukrainianworldcongress.org/russia-falters-again-in-testing-sarmat-nuclear-missile/

Unal, B. and Lewis, P. (2018). *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences* [online]. London: Chatham House. [Accessed: 5 June 2025]. Available at: https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf

Urdiroz, F. (2025). Among algorythms and alamrs: the impact of AI on cybersecurity [online]. *Global Affairs*. Universidad de Navarra. [Accessed: 5 June 2025]. Available at: https://www.unav.edu/web/global-affairs/entre-algoritmos-y-alarmas-el-impacto-de-la-ia-en-la-ciberseguridad

Article received: 6 June 2025
Article accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Luis Angel Díaz Robredo
Doctor of Clinical, Forensic and Health Psychology

Email: ldrobredo@unav.es

Intergroup Interventions as a STRATCOM strategy

Abstract

NATO's strategic communication is one of the most rapidly advancing tools in the field of information warfare in recent years. Its ability to act on the cognitive sphere makes it highly effective in reinforcing military power among civilians and military personnel. The interest in information warfare that has arisen since the invasion of Crimea has led to the development of strategic communication capabilities. Based on a review of some theories of social and group psychology, we will show a series of intergroup interventions that have proven effective in reducing prejudice and animosity between groups and thus advancing conflict management, in order to strengthen the capabilities of all the elements that make up NATO's action and in line with the narratives to be conveyed.

Keywords

Narratives, Cognitive, Group psychology, Prejudice, Information warfare.

Cite this article:

Díaz Robredo, L. A. (2025). Intergroup Interventions as a STRATCOM Strategy. *Journal of the Spanish Institute for Strategic Studies*. 26, pp. 383-408.

1 Introduction

We find ourselves in a global environment marked by the speed of information, social polarisation and rapid technological change. Strategic communication (STRATCOM) has become a key tool for influencing, coordinating and projecting power and identity in the 21st century. The STRATCOM concept is a comprehensive approach that coordinates all media and communication channels to achieve long-term objectives, whether in civil or military contexts.

In the civilian world, STRATCOM is used by governments, international organisations and companies to build trust, manage crises, shape public perceptions and align communication with their strategic objectives of development, diplomacy or institutional reputation. In the military sphere, on the other hand, strategic communication is used as an increasingly common component of soft and hard power, supporting psychological operations, countering enemy disinformation and strengthening national and international support in conflict or security scenarios.

The need for STRATCOM is now more pressing than ever: hybrid wars, disinformation campaigns, terrorism, cyberattacks, geopolitical tensions and social challenges require responses that go beyond physical or diplomatic action, with effective, transparent narratives that reflect a deep understanding of the information environment. In this context, mastering strategic communication is not only useful but essential for the stability, security, and sustainable influence of any relevant actor on the global stage.

In the following pages, we will review STRATCOM capabilities and their relationship to the dissemination of narratives, the relationships between group psychology and the cognitive realm, as well as a review of studies of intergroup interventions that have been shown to generate positive influence and assist in the de-escalation of conflict between groups, which are the usual objectives of information warfare.

To this end, we will conduct a literature review that analyses, on the one hand, the current situation of narrative warfare and military applications in the cognitive sphere and, on the other, reviews studies that have addressed aspects related to intergroup psychology and prejudice, from their inception to the present day, in the civil and military contexts.

The methodology followed has been a systematic search through major databases such as SciELO, PubMed and Google Scholar.

The main objective of this research is to analyse the impact of intergroup prejudice on relations between groups in the context of war and non-war conflicts and to compare it with the current strategies of NATO's STRATCOM directive. Specific objectives include analysing STRATCOM's capabilities, reviewing narrative strategies and their influence on intergroup conflict relations, identifying other group psychology processes that influence intergroup relations, and exploring and detailing different intergroup intervention initiatives that have been carried out to date in war and non-war conflicts.

2 STRATCOM and its capabilities

The official definition of strategic communication or STRATCOM according to document PO(2009)0141 (NATO, 2009) encompasses the use of different information capabilities—such as Public Diplomacy, Public Affairs, and INFO OPS, among others—to support NATO's objectives.

Antolín (2017) goes even further in defining NATO's STRATCOM strategic objectives:

> '[…] the planned, coordinated and integrated use of all communication capabilities and means available to the sender in support of their strategic objectives, whether political, diplomatic, economic or military, and in the pursuit of an improvement in image, reputation, perception or knowledge on the part of the receiver' (Antolín, 2017, p. 39).

It can therefore be deduced that, in STRATCOM, information and communication are neither neutral nor impartial, as they respond to corporate objectives. This type of communication takes place in a competitive environment, which implies that there are one or more agents with conflicting interests, trying to win the goodwill or influence of a third party. To this end, communication functions must be coordinated in the sense that there must be consistency in the different actions of an organisation and a single message must be conveyed. Finally, Silvela (2017) points out that there must also be consistency between the actions and the messages conveyed.

Within STRATCOM, there are various mechanisms that we will briefly detail in order to understand its capabilities:

Public diplomacy in NATO operates at the highest political level and is the set of strategies, activities and communications used to explain its policies, objectives and actions to the general public, with the aim of generating understanding, trust and support both within and outside member countries. To this end, it generates narratives through social media or media campaigns, conferences, the production of audiovisual material, reports or programmes of visits to NATO facilities, among others. This narrative seeks to convey ideas of identity or common objectives that seek to influence target audiences. Public diplomacy is led by the Public Diplomacy Division.

Unlike Public Diplomacy, which has a broader and more strategic focus, Public Affairs is primarily focused on the military and operational environment, without compromising security. It is NATO's official communication to the public and the media and reports on policies, decisions and strategic objectives. It is managed by the Public Diplomacy Division, this time at the civilian level, in Brussels.

Military Public Affairs refers to all information related to the Alliance's military activities, policies, operations, structures and capabilities that is officially and openly disclosed to the public, without compromising security or operational effectiveness. This disclosure takes place through press releases, official reports or documents, statements by the Secretary General or military commanders, social media, press conferences and official websites. Examples include the disclosure of joint exercises,

the number of troops deployed on missions on the eastern flank, and cooperation with international partners. Military public information in NATO is primarily directed by its military spokesperson and coordinated from the Alliance's military command structure at SHAPE (Supreme Headquarters Allied Powers Europe) military headquarters. The difference between Public Affairs and Military Public Affairs in NATO lies mainly in who executes them, what they communicate, and which audience they target.

Information Operations (INFO OPS) are a military capability designed to integrate and coordinate the use of various information tools to affect, influence, protect or exploit the adversary's information and information systems in support of the Alliance's military objectives (NATO, 2018). These are operations aimed at acting in the information environment with objectives such as: protecting the freedom of action of Alliance countries in the information environment; generating behaviours, perceptions and attitudes approved by the NATO Council to reinforce, convince or encourage support for NATO objectives; and countering the adversary's propaganda and the command and control functions and capabilities that support their opinion-forming and decision-making.

Therefore, the objective is not only to communicate, but also to influence the perceptions, decisions and behaviours of key actors: adversaries, the local population, neutral actors or allies. INFO OPS are the responsibility of the Supreme Allied Commander Europe (SACEUR) and his staff at SHAPE and have an Information Operations Branch (J9), which is responsible for planning and coordinating these operations. In missions and exercises, each NATO military operation has an INFO OPS Officer who is part of the joint planning team.

As with all other STRATCOM actions, NATO INFO OPS must respect international law and the rules of engagement and follow ethical behaviour that is free from falsehoods or propaganda.

Psychological Operations (PSYOPS) in NATO are a military capability whose objective is to influence the perceptions, emotions, attitudes and behaviours of specific audiences in order to support military and strategic objectives (NATO, 2007). Specifically, they focus on the planning and execution of messages aimed at audiences such as enemy forces, the local population or neutral actors, in order to deter the adversary, gain support among the civilian population, promote stability and cooperation in conflict zones or weaken the enemy's will to fight. Messages can be distributed through print media (leaflets, posters), radio, TV, social media or even loudspeakers on the ground.

Overall responsibility lies with SACEUR, and the specialised team is located within SHAPE, under the Information Operations (J9) section, which coordinates PSYOPS as part of the information strategy. Some NATO member countries have specialised PSYOPS units that are integrated into multinational operations, such as the 1st NATO PSYOPS Group or PSYOPS units from countries such as the US, the UK and Poland, among others. These units can be deployed on missions such as KFOR (Kosovo) or the Enhanced Forward Presence on the eastern flank.

Civil-Military Cooperation (CIMIC) is the function that enables interaction and cooperation between military forces and civilian actors such as local governments, NGOs, the civilian population or international agencies, with the aim of supporting the objectives of the military mission (NATO, 2002). This function can support the civilian population in areas affected by conflict or disaster, coordinate efforts with local authorities and civilian organisations, facilitate mutual understanding between the military and civilians, and prevent interference between military operations and civilian activities. Some examples of these actions are the restoration of basic services (water, electricity, health), support for local hospitals or schools, coordination with NGOs for the distribution of humanitarian aid, advising local governments on restoring governance, and carrying out Quick Impact Projects. CIMIC actions are directed at the strategic level by SACEUR through SHAPE and a CIMIC section within SHAPE, which is responsible for doctrine, planning and multinational coordination. At the operational and tactical levels, specialised CIMIC teams are assigned to each NATO mission.

Key Leader Engagements (KLE) consist of meetings and direct contacts between Alliance military and civilian leaders and key leaders of local communities, civilian authorities, social groups or relevant actors in an area of operations (Popescu and Voinescu, 2021). These are planned and strategic interactions that seek to build trust and strong relationships with key figures in the area of operations, facilitate mutual understanding and cooperation, gather valuable information for the mission, reduce tensions or avoid conflicts to support the stabilisation and success of the operation. They are carried out in the context of peace, stabilisation or conflict operations and seek to promote security and stability in the area and to obtain local support for NATO forces, listen to the concerns and needs of the population and authorities, or adjust the operational strategy according to the local context.

KLEs are usually led by senior officers or mission commanders in the field. On some occasions, representatives from the Public Diplomacy Division or CIMIC participate, depending on the purpose of the meeting. Leaders may be brigade or division commanders, heads of mission, or CIMIC or public relations officers.

Finally, although not part of NATO's command structure, NATO's Strategic Communications Centre of Excellence is the main body responsible for countering disinformation and protecting against information warfare. It is accredited by NATO and works closely with it. Its functions are to analyse disinformation campaigns, strengthen the communicative resilience of member states, provide training, research and strategic recommendations, and support the coordination of strategic communications (NATO Strategic Communications Centre of Excellence, s. f.). Its publications, projects and frequently organised events are testimony to its ongoing efforts to contribute capabilities in the fight against disinformation.

3 Narrative in the field of information

Strategic narrative is a means used by political actors to construct a shared meaning of the past, present and future of international politics and thus shape the behaviour

of national and international actors (Miskimmon *et al.*, 2012). Narrative helps to structure reality and generate group identity, enhance social cohesion and consensus among peers. Furthermore, it has a significant influence on individuals subjected to such narratives, constructing individual and cultural identity and, therefore, favouring ideas and beliefs that will ultimately result in observable behaviours (Saari *et al.*, 2024).

The importance of narrative has been observed since the 1990s, when the progressive influence of information in warfare became evident. Since then, publications such as AJP-3.10 (NATO, 2007) and, in particular, certain situations of clear information warfare, such as that exhibited by Russia in Ukraine in 2014 following the 'Euromaidan Revolution', forced NATO to take notice and act in the field of strategic information.

In 2014, the Allied Joint Doctrine for Psychological Operations provided one of the first clear definitions of narrative, defining it as 'the translation of an organisation's mandate and vision into a fundamental and persistent story about who the organisation is, what its guiding principles are and what it aspires to achieve' (NATO, 2014, p. Lex-7).

The Alliance reinforces the idea that all its activities—public affairs, strategic communications, psychological operations, information operations and kinetic military actions—are based on the narrative established at the origins of the 1949 North Atlantic Treaty. In this way, NATO seeks to give meaning and unify the Alliance under a clear and easily recognisable narrative. Furthermore, this narrative not only serves as a tool to generate support and legitimacy, but is also considered a defensive asset against hostile information operations, disinformation and propaganda.

Recently, Du Cluzel (2020) coined the term 'cognitive warfare', an aspect directly related to narrative warfare. Cognitive warfare combines cyber, information, psychological and social engineering to influence, protect or disrupt cognition and gain a strategic advantage. This type of warfare is extremely important today, as it attacks rationality, exploits vulnerabilities and weakens defences, shaping perceptions and behaviours at the individual, group and social levels (NATO, 2023).

Strategic narratives can be classified into three types: identity narratives, problem narratives, and system narratives (Miskimmon *et al.*, 2022). Identity narratives seek to alter perceptions and promote a specific self-image regarding values, character, and goals. For example, NATO's identity narrative is based on the 1949 North Atlantic Treaty, which presents it as a strong shield of democracy. Problem narratives, on the other hand, seek to influence specific political decisions by shaping the entire discursive environment, as in the current situation regarding the invasion of Ukraine. System narratives focus on portraying how the international system works and, from NATO's perspective, this could mean emphasising the alliance's commitment to the rules-based world order.

For their part, narratives of destruction seek to undermine a state's capabilities, presenting it as weak, chaotic, incapable and lacking in internal cohesion, emphasising perceptions of realistic threats to its physical, economic and social security.

Suppression narratives, on the other hand, seek to discredit the moral image or legitimacy of a state, often presenting it as perverse and opposed to traditional and conservative values (Wagnsson and Barzanje, 2019). These narratives are linked to perceptions of symbolic threats: threats to the image, values, morals or norms of the ingroup (the group itself). Threats may include the feeling that traditions are being eradicated or that people are not allowed to follow their own culture. Perceptions of symbolic threats are the target of information and/or disinformation campaigns intended to polarise.

These narrative strategies have been observed in several studies, for example in Nordic countries and the Netherlands, such as in Hoyle *et al* (2023), Bouffard *et al* (2024) or Hoyle *et al* (2024). On the other hand, analyses of Russian media narratives about Latvia revealed a lower level of narratives of repression and an emphasis on narratives of destruction, which coincides with other similar studies on Estonia.

And why do these narratives work? The model posits that narratives work through a mechanism called 'mediation', which implies that the occurrence of certain effects depends on the prior occurrence of others. In models of narratives of destruction and suppression, it is predicted that people's reactions to narratives occur because narratives serve to induce perceptions of threat; in other words, they target their feelings of security and insecurity.

4 NATO and the war of narratives

As we have seen, NATO is fully aware of the war of narratives that exists in the international arena and defines information threats as deliberate activities, with a certain degree of coordination and direction, aimed at manipulation or influence and with the capacity to affect the social fabric and mobilise public opinion. This influence is capable of damaging NATO or the political cohesion of its countries and can even generate doubt among citizens about their political leaders or institutions. Sometimes these threats do not consist of specific lies or narratives, but simply release contradictory information to generate confusion and mistrust.

To this end, NATO needs to understand the existing information environment and respond to threats by monitoring and identifying the sources of the threat as they emerge and spread. Once this initial process has been completed, the information must be shared to prevent and block the effectiveness of these threats, through public statements on websites, press conferences or specific campaigns that can anticipate the damage that the source of the threat wants to cause and prevent the false narrative from being accepted by the target society or group.

If the information attack has already taken place, NATO attempts to clear up the confusion or discredit the source through explanatory campaigns (counter-narrative function), discrediting the source or message and promoting a campaign or activity on its website, social media and through coordinated statements to the media and the public. An example of this is NATO's repeated condemnation of the invasion of Ukraine.

A final tool proposed by NATO to tackle disinformation is through continuous learning and analysis of lessons learned about the strategies and procedures employed by the enemy and the development of faster and more effective responses for the future.

5 Ethics and legality in the use of psychological techniques in the field of security and defence

Although the use of psychological techniques in the military is long-standing, their use in the armed forces of democratic countries is relatively recent and is now standardised, subject to a series of rules derived from both international humanitarian law (IHL) and professional ethics, the latter being set by psychology organisations. Psychological techniques can typically include influence actions, strategic communication and psychological operations and therefore have the capacity to alter perceptions, beliefs and emotions. This requires control that distinguishes between legitimate influence and undue manipulation.

From a legal perspective, international humanitarian law (IHL) states that all methods of warfare must respect the principles of humanity and military necessity, expressly prohibiting the causing of unnecessary suffering or lasting mental harm to protected persons (Dörmann *et al.*, 2016). Thus, any psychological action directed at the civilian population that may cause panic, trauma or severe impairment of cognitive autonomy is not permitted under international law.

Similarly, human rights affect these restrictions. The United Nations (UN) Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (UN, 1966) specifically defend the right to freedom of thought, information and human dignity and prohibit practices that significantly limit autonomous decision-making capacity through coercion, systematic deception or exploitation of psychological vulnerabilities.

In democratic systems, public communication and influence aimed at legitimate ends—the prevention of violence or the de-escalation of tensions, as in this case—are permissible provided they are proportionate, transparent and traceable. To this end, there is a clear and accessible doctrine within NATO that provides oversight and accountability (NATO, 2012). Specifically, STRATCOM ethics emphasise the importance of avoiding the instrumentalisation of human groups as mere means to military ends, especially when interventions may generate or increase intergroup tensions or instigate perceptions of threat (Miskimmon *et al.*, 2013). STRATCOM's actions reiterate its commitment to institutional transparency and message control so as not to undermine democratic legitimacy and public trust. On the contrary, covert actions or systematic deception directed at populations violate these conditions and are therefore practices incompatible with NATO's STRATCOM actions.

Finally, the American Psychological Association (APA), one of the world's leading scientific and professional references in psychology, in its document *APA Professional Practice Guidelines For Operational Psychology* (APA, 2023), establishes and delimits

the scope of psychologists' actions in the area of security and defence, respecting the rights, dignity, autonomy and well-being of all parties affected by security dilemmas. This document is in line with the APA EPPCC Code of Ethics (APA, 2017) and with the main European professional associations.

Therefore, although the boundaries between legitimate influence and undue manipulation in military environments can sometimes be confusing to the public, there are laws and mechanisms for controlling psychological operations and STRATCOM by NATO institutions that ensure their ethical and proportionate use.

6 Group psychology and the cognitive sphere

The cognitive sphere is related to 'the will, perceptions, attitudes, values and motivations, thoughts, decision-making and behaviour of human beings' (Donoso, 2020: p. 21). This cognitive domain is one of the fields of information warfare in which influence is exerted. To understand the implications of this influence, there are several mechanisms that interact with narratives that we must take into account when addressing the information challenges of the 21st century.

On the one hand, narratives, as we have seen, are based on a process of social influence from the ruling class towards social groups. Normative and informational dependence can explain this fact when it comes to generating the desired impact of the ruler's communication strategy. In the former, the individual is motivated to maintain a positive relationship with the other members of a group and wishes to receive their approval or avoid their rejection and, therefore, will accept the norms of the majority group. This means that, in general, government discourse and narratives tend to have an influence on individuals who feel called upon to be 'good citizens' or to follow the dictates of the ruling group (if they support the current government). Asch's experiment in the 1950s is the quintessential example of influence based on normative dependence, which explains that the responses given by the subject are motivated more by external reasons (e.g., not deviating from the rest of the group or being accepted by it) than by personal critical reflection. Informational dependence consists of the influence that a person receives from others when making decisions in an ambiguous situation. The individual accepts the opinion of the majority as the most accurate and adapted to reality. This type of behaviour has been particularly prevalent in recent times during the pandemic (Morejón, 2021), where the media, social networks and interactions within peer groups have determined group behaviours of social conformity, which diminishes individual critical thinking.

Internal debate within groups often results in group polarisation, which is an intensification of the initial tendency that is amplified as a result of the sharing of news or opinions within the group (Moscovici and Zavalloni, 1969). Therefore, debates between people with similar attitudes often intensify their initial positions towards even more radical positions. This mechanism works thanks to the normative and informational dependence discussed above. Therefore, groups that interact a lot with each other, feel very cohesive, and consume biased, undiverse, and prejudice-based information will have an opportunity to become more radical in their thinking

and more prejudiced towards other options. This is the case with communities that are divided and closed to cultural diversity.

Another principle to consider in the impact of narratives is Tajfel's Social Identity Theory (1974), which indicates how belonging to a group justifies the individual moving from 'considering oneself as an "I" to an "us"' through depersonalisation, emphasising their similarity with group members and highlighting differences with those outside the group. The criterion of certainty, therefore, is agreement with the group. Ultra-nationalist or ethnocentric messages tend to exploit this common identity of 'us versus them'.

Finally, a concept that, although it seems simple, overly basic or inappropriate for civilised people, is that of suggestion, imitation or contagion, in which individuals are infected by the emotions around them and allow themselves to be carried away by them without critical analysis (Le Bon, 1895), especially in situations of uncertainty. Outbursts of hatred following real incidents or rumours that generate a great deal of indignation and anger, or situations of excessive hoarding (remember the demand for toilet paper during the pandemic) may explain these unreasonable group behaviours.

Minority influence is the ability to influence a source that lacks the power of the majority. When we talk about the NATO environment, we consider that majority influence is exercised by pro-NATO governments through official channels and the majority social conformity seen above, and minority influence comes from both official and unofficial, national and foreign anti-NATO entities.

Moscovici (1980) explains some of the processes by which minorities (in this case, the anti-NATO minority tendency in NATO member countries) can generate conflict within the majority. The principle of 'synchronic consistency' occurs when members of a group agree in their responses, creating a sense of unanimity within the minority group. Thus, the view that an anti-NATO president is strongly supported by his political, social or state group gives validity and strength to his arguments *vis-à-vis* the majority group (in this case, NATO countries). Diachronic consistency consists of the same individual systematically repeating the same narrative at different times to explain a situation: the 'denazification' of Ukraine, Russia's defence needs, etc. It has to do with statements or narratives repeated in a similar way by the same actor.

Papastamou *et al* (1982) point to the style of negotiation based on rigidity or flexibility to determine how this affects the persuasion of majorities. It is the degree of flexibility or rigidity in verbal or non-verbal expression that actors use to influence a particular group. Rigidity is characterised by the degree of extremism, unconditional support and intransigence in defending one's own position and the refusal to make concessions to the other side. When a rigid style predominates in the majority group (in this case, the tough rhetoric of an anti-NATO government directed at its own citizens), dialogue is blocked, its beliefs and values are imposed, and minority discourses (such as rapprochement or negotiation with NATO) are delegitimised in its country. Furthermore, it reproduces the status quo and, if its own narrative is one of defensive and anti-NATO identity, this attitude reinforces its power. This is the case with some political leaders who repeatedly express their rejection of NATO and are recognised as guarantors of independence and absolute leaders of their country.

On the other hand, when minority discourses adopt a flexible style (in this case, when the discourse of an anti-NATO country is directed at the population of NATO countries through the media or social networks), it brings a sense of greater possibility for dialogue between countries, delegitimises the pro-NATO country's defence narrative and provides discursive resilience, i.e., the ability to adapt and reformulate their messages for different audiences in minority contexts. According to Moscovici, this is the 'process of content validation', as the minority group creates an intellectual conflict in the majority (the Western audience) to undermine their self-confidence in their narrative and generate interest in considering minority propositions.

A final mechanism of minority influence that can be applied to narratives is Nemeth's (1986) decentring. This is a process in which the individual perceives no internal violence or incompatibility between their position and that of the minority, thereby increasing the minority group's capacity for influence. This is achieved through the use of innovative and creative proposals by the minority group, attempting to shift the individual's focus away from their own position without having to choose between the majority and minority groups, i.e. based on new and non-dichotomous arguments. The use of narratives from anti-NATO countries advocating the transmission of universal and common values of peace, democracy, security and defence, shared regional customs or traditions are a good example of how a minority discourse can shift the focus away from the conflict and create a rift in the identity narrative of a majority. Some speeches by Russian President V. Putin addressed to European audiences before the invasion of Ukraine serve as an example (Díaz, 2022).

Finally, it is worth monitoring audiences in the different news media available to the population, since, as we have seen, narratives feed on them for the dissemination of narratives.

According to the *Digital News Report 2024* (Reuters Institute, 2024), the survey conducted (almost 95 000 interviews in 47 markets covering half of the world's population) indicates that the majority of respondents use social media, search engines and aggregators as their main source of online news. Only 22% mention official media websites or apps as their main source, which is a drop of ten percentage points compared to 2018. There is a growing focus on commentators, influencers and young creators, especially on YouTube and TikTok, although there are still news brands and professional journalists who publish on networks such as Facebook and X. A final interesting aspect of this report applicable to narratives concerns selective attention to news. That is, there is an increase in the avoidance of certain news items that prevent users from seeing the full picture of current events. Almost four out of ten respondents (39%) say they 'sometimes' or 'often' avoid the news, an increase of three percentage points over the previous year's average. The report refers to comments made in the survey itself, which indicate that the conflicts in Ukraine and the Middle East may have influenced this fact. In addition, the report notes that the proportion of users who feel 'overwhelmed' by the volume of news has risen significantly since the previous survey in 2019, by up to eleven percentage points.

That said, we can conclude that the war of narratives is a complex and multi-variable issue that transcends the capabilities of institutions and countries, and that the population is increasingly prone to shared emotion and social contagion. All this, combined with the fact that today's news media are increasingly beyond the control and supervision of governments and that platforms are generating growing group polarisation, makes the impact of narratives difficult to control and, at times, of little use to a population or group that is informed by media of its own ideology, which are biased and reinforce its own and others' stereotypes.

Therefore, in the following section, we propose addressing real and direct intergroup relations as one of the most efficient and transparent tools for eliminating prejudice, negative stereotypes, and animosity between groups.

7 Prejudice in intergroup relations

In his work *The Nature of Prejudice*, Allport defines prejudice as "a hostile or prejudiced attitude towards a person belonging to a group, simply because they belong to that group, thus assuming that they possess the objectionable qualities attributed to the group" (Allport, 1954, p. 22). This prejudice, according to Allport, is not simply an opinion or a feeling; it is an attitude that affects behaviour and interpersonal relationships. It is based on the tendency of humans to make categories or generalisations that are an oversimplification of their world of experiences. The division into categories of ingroup membership (the group to which the individual belongs) and outgroup membership (the group that is foreign or different from the ingroup) is necessary as a natural tendency to distinguish between the known and familiar and the strange or unknown. Thus, mistrust, discomfort or, in some extreme cases, hostility towards the unfamiliar is a natural instinct for survival, security and trust in the family, ethnic or racial group. The need to belong is one of the most basic and universal human motivations (Baumeister and Leary, 1995) as it provides emotional well-being to the individual in the form of self-esteem, social identity, emotional health, and the satisfaction of basic needs such as mutual care, security and protection from threats, and certainty.

This positive relationship towards the ingroup generates an attitude called 'ingroup favouritism', characterised by a tendency to interact regularly with members of the ingroup, a sense of positive self-esteem for belonging to that group, altruistic behaviour, acceptance of common norms as one's own, etc. In return, this favouritism uses mechanisms such as social comparison, which seeks to establish a favourable difference for one's own group in a dimension that is positively valued by social consensus compared to other different groups (Tajfel and Turner, 1979), generating inevitable discrimination.

Thus, it can be understood that intergroup relations can be accompanied by emotional feelings that are sometimes tense or distant. In addition, there are factors that can generate greater discrimination or distance between groups, such as: differences in behaviour, differences in norms or non-compliance with common norms, the perception of the other as a threat to one's own status (very common in

narratives and political strategies) or the use of social emotions that favour extreme behaviour. One of the models that best captures this difficult relationship between groups is the 'Intergroup Anxiety Model' (Stephan, 2014), which suggests that contact with another group can generate a series of negative consequences related to prejudice, i.e., before actual contact, both in anticipation of a negative personal experience and fear that one's own group will reject them for interacting with members of the outgroup or even identify them with it.

The negative consequences in relations between different groups can be:

– Behavioural: such as avoiding contact with members of the other group, amplifying norms to criticise or discredit the other group, or preventive aggression.

– Cognitive: a tendency to seek only information that confirms negative expectations, ultimate attribution error (blaming members of the outgroup for their negative behaviours without considering positive behaviours or possible external causes), motivational biases aimed at justifying negative behaviours towards the outgroup or justifying intragroup favouritism.

– Affective: excessive emotional reaction to negative events involving the outgroup or extreme evaluative reactions.

This intergroup anxiety will be greater the fewer previous relations both groups have had, if the group's cognitions about the other have been negative (myths or rumours, lack of knowledge of the other, beliefs of superiority, negative expectations, etc.) or if the structure of the contact situation is negative (differences in status, absence of need for interdependence, differences in size or composition).

A final theory that is useful for understanding and improving intergroup relations is Realistic Conflict Theory (Sherif, 1967), which is very common in international politics and national policies (immigration). This theory points out that behaviour between groups is the result of positive or negative functional relations between them. Functional relationships are affected by the reciprocal goals and interests of the groups (security threats, economic interests, political advantage, military considerations, prestige). If the goals of two groups are compatible, there will be cooperation and good relations. If not, there will be competition for goals or resources and therefore conflict will arise. The greater the competition for limited resources, the more intense the intergroup rejection behaviours will be, with feelings of prejudice, discriminatory behaviour and hostility.

More specifically, the Instrumental Model of Group Conflict (Esses *et al.*, 1998) follows this theory and is applicable to societies that receive immigrants. The perception of stress or resource limitation and the salience of a particularly conspicuous foreign group gives rise to competition and attempts to eliminate it. Zero-sum beliefs suggest that the resources consumed by immigrants are subtracted from the goods that individuals in the host society can obtain, arguments that are widely used today to single out social or ethnic minorities in each country or even outgroups or foreign countries.

8 Interventions in intergroup relations

The theory that intergroup experiences help to significantly reduce prejudice comes from Allport (1954). This author observed that when interrelating groups had the same status, common goals and intergroup cooperation, the experience improved greatly. If, in addition, there was support from the authorities, a sense of justice for both groups or a search for similar traditions, the reduction in prejudice was even greater. This view has been empirically supported over the years by numerous studies, such as those by Dovidio *et al* (2017) and Hewstone and Swart (2011).

The Intergroup Interventions (IIGs) that have been tested so far are of two types, direct and indirect:

Direct interventions include those that seek face-to-face interaction in person or virtually. The first studies on face-to-face experiences are by Allport (1954). There are also studies using technology and online applications (Amichai-Hamburger and McKenna, 2006) or even virtual reality avatars (Tassinari *et al.*, 2022). As this type of contact is very direct, it aims to bring about profound and obvious changes in intergroup relations, which means that the social context must be minimally prepared for this.

Indirect contacts are used to generate less obvious, scalable and progressive changes when intergroup rapprochement is very complex socially or politically, and are usually made through radio, television and social media. Examples of this type of approach are: extended contacts, which are strategies in which people know or are informed that people from their own group have dealt with people from the outgroup (Wright *et al.*, 1997); vicarious strategies or observing people from the group dealing with people from the outgroup (Vezzali *et al.*, 2014); social practices, which is indirect contact with real or unreal people through social media (Schiappa *et al.*, 2005) or in an imagined way, where fictional interactions with people from the outgroup are visualised (Turner *et al.*, 2007).

8.1 Consequences of IIGs

The main consequence of intergroup contact is, as Allport pointed out, increased knowledge of the other group. This consequence, in itself, helps to find the much-needed similarities between both parties in order to eliminate prejudices and negative stereotypes of the outgroup.

Another consequence of intergroup contact is that it reduces anxiety about such contact, normalising it and leading to habituation and familiarity with contacts that previously did not exist or were very infrequent (Stephan and Stephan, 1985). Each encounter can generate small gestures or behaviours of empathy and a more integrative perspective.

Likewise, contact between people from different groups helps to reduce perceptions of threat (Hewstone *et al.*, 2014), which are common in intergroup anxiety between traditionally opposed groups.

These activities allow the ingroup to assimilate the outgroup as part of their self-concept at the interpersonal level and downplay the salience of the foreign group identity or even recategorise members of foreign groups as their own.

At the level of social norms, these activities can change the perception that the outgroup has social norms that are strange, very different or threatening to the ingroup.

In general, numerous meta-analyses recognise the positive effect of intergroup contact. Examples include those by Pettigrew and Tropp (2006), Lemmer and Wagner (2015) and Paluck *et al* (2019).

8.2 Contexts in which intergroup interventions have been effective

Numerous studies have been conducted showing a reduction in prejudice between groups after 20th century conflicts in settings such as Northern Ireland (Ginty *et al.*, 2007), reconciliation after the interracial conflict in South Africa (apartheid) in the 1990s (Gibson and Claassen, 2010) , the war in Rwanda, and 21st century conflicts such as the civil war in Sri Lanka (Malhotra and Liyanage, 2005), the current conflicts between Jews and Palestinians in Israel (Lazovsky, 2007), the internal struggles in Nigeria over land use between 2014 and 2019 (Grady *et al* 2023) or, more recently, relations between social groups in Iraq following the period of domination by the Islamic terrorist group ISIS, some of which will be discussed in greater detail. In addition, these interactions have also been investigated in the absence of armed conflict, as in the case of intergroup attitudes in various European countries (Schmid *et al.*, 2012; Binder *et al.*, 2009).

8.3 Precautions in IIGs

There are some general guidelines regarding intergroup relations that should be taken into account (Littman *et al.,* 2023).

Intergroup interventions will be effective in reducing prejudice if the emotions they generate are positive for the groups involved. Obviously, intergroup contacts being associated with positive emotions is a basic condition for their benefit.

In addition, it is necessary to assess the possible influence of other members of the same group, as this can have an impact even if the interaction is positive overall. Being exposed to social norms that punish contact with the outgroup can generate internal prejudice towards individuals in the ingroup, such as the 'black sheep effect' (Marques *et al.*, 1988). This is a mechanism of control within the group itself, characterised by the demand for maximum loyalty to the group and favouritism towards those who comply with the norm and have characteristics that are desirable for the group, and denigration of those who are undesirable or who do not comply with or disagree with the group's norms. Especially in the case of competition between two groups, dissent or internal disagreement can facilitate the idea that the individual within the ingroup may be a traitor for expressing criticism in such tense moments,

whereas if there were no social competition between two groups, the same criticism might not be considered so harmful or damaging to the ingroup, or might even be considered positive (Ariyanto *et al.*, 2010; Brander and Hornsey, 2006). This last aspect is interesting for study because it shows the difficulty groups have in accepting reasonable internal criticism or reflection in environments of intergroup conflict, categorising all their own members as good and isolating those who disagree or think differently from the group as enemies.

Another possible danger for intergroup actions is that the first-hand experiences of some group members should not be generalised to the majority. One explanation for this could be that the individuals from the outgroup who interact with the ingroup do not meet the typical characteristics of groups considered strange or foreign. This can be interpreted as an exception to the rule—in the case of Muslims, dealing with Christians who are less prototypical or less religious than others. Therefore, it will not produce a change in opinion or a reduction in prejudice towards that group. Another explanation for this phenomenon is that the effects of this positive involvement only apply to the specific group or a specific experience and not to other similar groups. Some mechanisms that may intervene in this case to avoid deviation from the norm are those of conformity or group polarisation, as seen above.

8.4 Applications of IIGs in conflict zones

There are numerous possible applications: in schools, through the media, or in conflict zones. To observe the importance of these activities in reducing prejudice, we will consider several extreme cases of intractable conflicts where empathy and perspective-taking have been sought through real and direct contact rather than virtual or indirect contact.

Onuki et al (2022) examined the effect of face-to-face contact between three groups of ex-combatants (national army, former national army, and armed group) and civilians with disabilities in Rwanda. In a study of more than four hundred people, they found differentiated effects of intergroup contact in post-conflict contexts, highlighting the role of the degree of personalisation in intergroup outcomes. The findings indicate that, in interactions between former national army combatants and civilians with disabilities in Rwanda, low levels of personalisation (less focus on personal aspects) generated more positive outcomes in terms of interpersonal preference, reduced evaluative biases, and perceptions of the other group, compared to conditions of high or no personalisation. In contrast, when contact occurred between the three groups of ex-combatants—who were direct adversaries during the conflict—high levels of personalisation proved to be more effective in promoting positive intergroup outcomes. This suggests that deeper, more personal contact may be necessary to reconcile former adversaries.

The results suggest that the impact of personal contact varies significantly depending on the previous relationships between the groups involved. Therefore, reconciliation and peacebuilding strategies in post-conflict societies must be tailored to the type of relationship and history of confrontation between groups, avoiding

generalised approaches. This research highlights the importance of careful design of contact-based interventions, especially in contexts of high historical and social sensitivity.

Seeds of Peace is an international organisation that organises summer camps in the United States, where Israeli and Palestinian teenagers (along with young people from other conflict contexts) live together for several weeks, participating in shared activities, dialogue workshops and coexistence dynamics.

Lazarus's study (2015) sought to assess whether intensive and prolonged contact in this type of environment helped to reduce prejudices and stereotypes, increase empathy towards the other group, or promote more conciliatory and peaceful attitudes in the long term.

The results showed that immediately after the camp, participants had significantly more positive attitudes towards the other group, including greater empathy and less dehumanisation. However, over time, many of these effects diminished once the young people returned to their highly polarised social environments, with more lasting effects observed in those who formed close friendships with members of the other group.

It was concluded that intensive and meaningful contact can reduce prejudice, but the effects do not always last if the subsequent social context reinforces negative views. Meaningful personal relationships (real friendships) are key to the sustainability of change. The social environment to which one returns can reinforce or weaken the effects of contact.

A final interesting case of intergroup intervention is that of Mousa (2019). On this occasion, the impact of a sporting activity in Iraq was evaluated after the war that ravaged the country and the fall of Saddam's regime in 2014, which led to the persecution of Christians by the Islamist terrorist group ISIS. This research randomly assigned Iraqi Christians displaced by ISIS to one of two types of football teams: exclusively Christian teams or mixed teams with Muslims. The results show persistent changes in Christians' behaviour towards Muslims, as they were more likely to sign up for a mixed team in the future, more likely to vote for a Muslim player (who was not on their team) to receive a fair play award, and more likely to train with Muslims even six months after the intervention ended. In addition, players on mixed teams were more likely to believe that coexistence is possible, with a statistically significant effect (+0.63 standard deviations, $p<0.01$).

These results seem to be explained by several factors, such as a change in social norms regarding intergroup contact with the outgroup (greater permissiveness and less restriction) or the generation of shared positive experiences (empathy and decreased intergroup anxiety), especially in teams that performed well, which showed a greater willingness to frequent a restaurant located in Mosul, a predominantly Muslim city.

However, the study also found that contact was less effective in changing generalised tolerance towards unknown Muslims (outside the specific context of the team), so this experiment suggests that meaningful intergroup contact can foster coexistence after

conflict, even when general prejudices persist. Interventions based on cooperative and structured activities (such as sport) can modify behaviours and perceptions towards individuals from the rival group, although they do not necessarily transform attitudes towards the entire group in the abstract.

If, therefore, intergroup experiences are capable of achieving these results among populations that are so historically, culturally and socially divided, we can say that IIGs are a good tool for eliminating or reducing prejudice in other equally divided societies, both in the absence of conflict and in its presence.

9 Discussion

We have seen that STRATCOM's need to communicate narratives is met by various mechanisms that work intensively and in different ways at different levels. However, the excessive saturation of information in today's media and social networks generates mistrust and concern in some citizens, apathy or absolute and unthinking adherence to official communications in others. The war of narratives and counter-narratives converges in a situation of deadlock that is difficult to overcome from an informational point of view.

What we propose in this study, supported by the latest research in group psychology and intergroup conflict, is to focus on activities that generate an experience based on real-life experiences in the target audiences, through personal contacts, with different intergroup activities that lead to knowledge of the other and the stranger and eliminate the bias and prejudice that harmful narratives seek to spread. In this way, through the mechanisms we have discussed (KLE, CIMIC, Public Affairs and Public Military Affairs), a reliable, accessible narrative based on real interaction between insiders and outsiders can be conveyed. Undoubtedly, reinforcing STRATCOM's usual outreach activities with a programme of activities involving interaction with socially or politically distant populations can help to convince and reinforce NATO's narrative as an agency of peace and democracy in the face of discourses of fear and hatred.

Initiatives such as those proposed—cultural, social, sporting or religious activities—serve as a link and a means of bringing groups closer together, so promoting them through CIMIC, PSYOPS, KLE or INFO OPS actions can be—and, in fact, already are—a form of action for military detachments. We emphasise the importance of the Armed Forces General Staff considering these initiatives as first-rate communication strategies, as effective as or even—in some cases—more effective than the usual narratives based on identity-based ideas, because, as we have seen, these narratives reinforce their own audience—especially the population that already views the Alliance positively—more than they do the external audience, whether foreign or domestic but anti-NATO.

We therefore argue that narratives based on intergroup outreach actions may be more widely accepted and have a greater positive impact in the cognitive sphere than institutional campaigns. Furthermore, they could facilitate informational resilience in

the face of disinformation campaigns from third countries. To this end, the strategy departments of the General Staff must promote and enrich the in-depth study of the opposing groups, their customs and traditions, values, common behaviours and group norms of action, in order to understand all the variables of each operational scenario. In this way, communication strategies can be designed based on rapprochement and shared real experiences, as well as a growing normalisation of the acceptance of other foreign or opposing groups, the main enemy of prejudice and intergroup conflict.

10 Conclusions

The main objective of this study was to analyse prejudice in relations between different groups in the context of social conflicts. As we have seen, this has been one of the main challenges in the experiences between different groups. The theories found help to explain the great internal force of the media, people and structures on each side when it comes to creating, maintaining or escalating prejudice against outside groups or individuals. The analysis of NATO's STRATCOM capabilities shows the current interest and concern for these strategies. As evidenced by one of the specific objectives of this document, NATO's ethically justified and legally controlled narrative management operations are fundamental in supporting military operations and defence policies when it comes to generating support, deterring or preventing disinformation campaigns. Through the analysis of the main studies of intergroup interactions carried out in the field of social and group psychology, it has been found that these are scientifically valid tools for combating prejudice, hostility and hatred between different groups, which are common targets of disinformation campaigns and narratives from opposing countries. Specifically, interactions based on bringing groups closer together are the most useful when it comes to generating closeness and social empathy. Although we observe that these strategies are already being used on a more local scale through KLE, PSYOPS or INFO OPS actions, we propose that these Intergroup Interventions should occupy a prominent position within STRATCOM, directed from the strategy departments of the General Staff. In this way, communication actions will gain even greater momentum in guiding will, perceptions and emotions towards a coherent narrative in messages and actions.

Limitations to this study include the difficulty of conducting this type of research between groups in conflict due to the great physical and emotional distance between them: security conditions that separate the groups, the lack of positive or neutral interactions, mistrust and prejudice between both sides, and the absence of organisations that have the support and recognition of both sides, as well as the capacity to carry out this research. On the other hand, we encounter the difficulty of evaluating the impact of different actions without cultural or political bias.

Therefore, for future research, we propose exploring the possibility of conducting longitudinal studies at different stages of each conflict, combining quantitative and qualitative methods to measure the impact of campaigns through NATO and STRATCOM structures, and including a greater number of IIGs as part of military campaigns.

Bibliography

Allport, G.W. (1954). The nature of prejudice. Cambridge, Mass., Addison-Wesley.

American Psychological Association (APA). (2017). *Ethical principles of psychologists and code of conduct* [online]. Apa.org. [Accessed: 2026]. Available at: http://www.apa.org/ethics/code/index.aspx

Amichai-Hamburger, Y. and McKenna, K. Y. A. (2006). The Contact Hypothesis Reconsidered: Interacting via the Internet [online]. *Journal of Computer-Mediated Communication*. 11(3), pp. 825-843. [Accessed: 2026]. Available at: https://doi.org/10.1111/j.1083-6101.2006.00037.x

Antolín, J. L. (2017). Strategic communication (STRATCOM) in international organisations [online]. In: Ministry of Defence. Spanish Institute for Strategic Studies (eds.). Strategic communication. [Accessed: 2026]. Available at: https://dialnet.unirioja.es/servlet/articulo?codigo=6696731

Ariyanto, A., Hornsey, M. J. and Gallois, C. (2010). United we stand: Intergroup conflict moderates the intergroup sensitivity effect [online]. *European Journal of Social Psychology*. 40(1), pp. 169-177. [Accessed: 2026]. Available at: https://doi.org/10.1002/ejsp.628

Baumeister, R. F. and Leary, M. R. (1995). The need to belong: The desire for interpersonal bonds as a fundamental human motivation [online]. *Psychological Bulletin*. 117(3), pp. 497-529. [Accessed: 2026]. Available at: https://doi.org/10.1037/0033-2909.117.3.497

Binder, J. *et al.* (2009). Does contact reduce prejudice or does prejudice reduce contact? A longitudinal test of the contact hypothesis among majority and minority groups in three European countries [online]. Journal of personality and social psychology. 96(4), pp. 843-856. [Accessed: 2026]. Available at: https://doi.org/10.1037/a0013470

Bouffard, T. *et al.* (2024). *Arctic Narratives and Political Values: Arctic States, China, NATO, and the EU.* NATO STRATCOM COE.

Brander, T. V. and Hornsey, M. J. (2006). Intergroup sensitivity effect and the war in Iraq: A case of attitudes and intentions diverging [online]. *Australian Journal of Psychology*. 58(3), pp. 166-172. [Accessed: 2026]. Available at: https://doi.org/10.1080/00049530600940265

Díaz, L. A. (2022). Putin and the new persuasion: psychological reflections on the annual media conference speech [online]. *Global Strategy*. [Accessed: 2026]. Available at: https://global-strategy.org/putin-y-la-nueva-persuasion-reflexiones-psicologicas-del-discurso-de-la-conferencia-anual-con-los-medios/

Donoso, D. (2020). Psychological aspects in the cognitive sphere of military operations. In: Working Paper of the Higher Centre for National Defence Studies (CESEDEN) (ed.). *Implications of the cognitive sphere in military operations*. IEEE. Pp. 19-45.

Dörmann, K. *et al.* (eds.). (2016). *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*. International Committee of the Red Cross. Cambridge University Press.

Dovidio, J. F. *et al.* (2017). Reducing intergroup bias through intergroup contact: Twenty years of progress and future directions [online]. Group Processes & Intergroup Relations. 20(5), pp. 606-620. [Accessed: 2026]. Available at: https://doi.org/10.1177/1368430217712052

Du Cluzel, F. (2020) Cognitive Warfare [online]. *NATO Innovation Hub*. [Accessed: 2026]. Available at: https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf

Esses, V. M., Jackson, L. M., and Armstrong, T. L. (1998). Intergroup competition and attitudes toward immigrants and immigration: An instrumental model of group conflict [online]. *Journal of Social Issues*. 54(4), pp. 699-724. [Accessed: 2026]. Available at: https://doi.org/10.1111/0022-4537.911998091

Gibson, J. L. and Claassen, C. (2010). Racial reconciliation in South Africa: Interracial contact and changes over time [online]. *Journal of Social Issues*. 66, pp. 255-272. [Accessed: 2026]. Available at: https://doi.org/10.1111/j.1540-4560.2010.01644.x

Grady, C. *et al.* (2023). How contact can promote societal change amid conflict: An intergroup contact field experiment in Nigeria [online]. *Proceedings of the National Academy of Sciences of the United States of America*. 120(43). [Accessed: 2026]. Available at: https://doi.org/10.1073/pnas.2304882120

Hewstone, M. and Swart, H. (2011). Fifty-odd years of inter-group contact: From hypothesis to integrated theory [online]. *British Journal of Social Psychology*. 50(3), pp. 374-386. [Accessed: 2026]. Available at: https://doi.org/10.1111/j.2044-8309.2011.02047

Hewstone, M. *et al.* (2014). Intergroup contact and intergroup conflict [online]. *Peace and Conflict: Journal of Peace Psychology*. 20(1), pp. 39-53. [Accessed: 2026]. Available at: https://doi.org/10.1037/a0035582

Hoyle, A., van den Berg, H., Doosje, B. & Kitzen, M. (2022). Portrait of liberal chaos: RT's antagonistic strategic narration about the Netherlands. Media, War & Conflict, 16(2), 209-227. https://doi.org/10.1177/17506352211064705 (Original work published 2023)

—. (2024) Do(n't) Shoot the Messenger: Psychological Responses to Kremlin Narratives in Nordic - Baltic Audiences [en línea]. Riga: NATO Strategic Communications Centre of Excellence. [Accessed: 2026]. Available at: https://stratcomcoe.org/publications/dont-shoot-the-messenger-psychological-responses-to-kremlin-narratives-in-nordic-baltic-audiences/315

Lazarus, N. (2015). Evaluating seeds of peace. In: Del Felice, C.; Karako, A and Wisler, A. (eds.). *Peace Education Evaluation: Learning from Experience and Exploring Prospects*. Emerald Publishing Limited. Pp. 163.

Lazovsky, R. (2007). Educating Jewish and Arab children for tolerance and coexistence in a situation of permanent conflict: An encounter programme [online]. *Cambridge Journal of Education*. 37 (3), pp. 391-408. [Accessed: 2026]. Available at: https://doi.org/10.1080/03057640701546706

Le Bon, G. (1895). *The Psychology of the Crowd*. T. Fischer Unwin, London.

Lemmer, G. and Wagner, U. (2015). Can we really reduce ethnic prejudice outside the lab? A meta-analysis of direct and indirect contact interventions [online]. *European Journal of Social Psychology*. 45(2), pp. 152-168. [Accessed: 2026]. Available at: https://doi.org/10.1002/ejsp.2079

Littman, R.; Scacco, A. and Weiss, C. (2023) Reducing Prejudice through Intergroup Contact Interventions [online]. En: Halperin, E., Hameiri, B. and Littman, R. (eds.). *Psychological Intergroup Interventions – Evidence-based Approaches to Improve Intergroup Relations*. Taylor and Francis. Pp. 3-16. [Accessed: 2026]. Available at: 10.4324/9781003288251-2

Malhotra, D. and Liyanage, S. (2005). Long-Term Effects of Peace Workshops in Protracted Conflicts [online]. *Journal of Conflict Resolution*. 49(6), pp. 908-924. [Accessed: 2026]. Available at: https://doi.org/10.1177/0022002705281153

Marques, J.; Yzerbyt, V. Y. and Leyens, J. P. (1988). The "Black sheep effect": Extremity of judgments towards in-group members as a function of group identification [online]. *European Journal of Social Psychology*. 18, pp. 1-16. [Accessed: 2026]. DOI: 10.1002/ejsp.2420180102

McGinty, R.; Muldoon, O. y Ferguson, R. (2007). Ni guerra ni paz: Irlanda del Norte tras el Acuerdo [online]. *Psicología Política*. 28(1), pp. 1-11. [Accessed: 2026]. Available at: https://doi.org/10.1111/j.1467-9221.2007.00548.x

Miskimmon, A.; O'Loughlin, B. and Roselle, L. (eds.). (2012). *Forging the world: Strategic narratives and international relations* [online]. London: Centre for European Politics/New Political Communication Unit. [Accessed: 2026]. Available at: https://doi.org/10.3998/mpub.6504652

—. (2013). Strategic narratives: Communication power and the new world order [online]. Routledge. [Accessed: 2026]. Available at: https://doi.org/10.4324/9781315871264

—. (2022). Strategic Narrative: The Art of Diplomacy in the 21st Century [online]. *Mexican Journal of Foreign Policy*. 113, pp. 73-95. [Accessed: 2026]. Available at: https://revistadigital.sre.gob.mx/index.php/rmpe/article/view/235

Morejón, N. (2021). Infodemic and information dependency: the ethical function of Andalusian public television during the Covid-19 crisis [online]. *Communication and Man*. 17, pp. 119-138. [Accessed: 2026]. Available at: https://doi.org/10.32466/eufv-cyh.2021.17.658.119-138

Moscovici, S. and Zavalloni, M. (1969). The group as a polariser of attitudes [online]. *Journal of Personality and Social Psychology*. 12(2), pp. 125-135. [Accessed: 2026]. Available at: https://doi.org/10.1037/h0027568

Mousa, S. (2019). Building Tolerance: Intergroup Contact and Soccer in Post-ISIS Iraq [online]. *Working Paper*. Programme on Governance and Local Development. 26. [Accessed: 2026]. Available at: http://dx.doi.org/10.2139/ssrn.3769116

NATO. (2002). *NATO Military Policy on Civil-Military Co-operation* [online]. [Accessed: 2026]. Available at: https://www.nato.int/ims/docu/mc411-1-e.htm

—. (2007). AJP-3.10.1(A) – *Allied Joint Doctrine For Psychological Operations* [online]. [Accessed: 2026]. Available at: https://info.publicintelligence.net/NATO-PSYOPS.pdf

—. (2009). PO(2009)0141 – *Military Concept For Nato Strategic Communications* [online]. [Accessed: 2026]. Available at:—. https://info.publicintelligence.net/NATO-STRATCOM-Concept.pdf

—. (2012). NATO Strategic Communications Policy [online]. [Accessed: 2026]. Available at: https://publicintelligence.net/nato-stratcom-policy/

—. (2014). AJP-3.10.1 – Allied joint doctrine for psychological operations [online]. [Accessed: 2026]. Available at: https://assets.publishing.service.gov.uk/media/5a80ce48e5274a2e87dbbecb/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf

—. (2018). Draft MC 0422/6 – NATO Military Policy for Information Operations [online]. [Accessed: 2026]. Available at: https://shape.nato.int/resources/3/images/2018/upcoming%20events/MC%20Draft_Info%20Ops.pdf

—. (2019). AJP3 – Allied joint doctrine for the conduct of operations [online]. [Accessed: 2026]. Available at: https://www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf

—. (2023). Cognitive Warfare: Strengthening and Defending the Mind [online]. [Accessed: 2026]. Available at: https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/

—. (2025). NATO's approach to counter information threats [online]. [Accessed: 2026]. Available at: https://www.nato.int/cps/en/natohq/topics_219728.htm

NATO Strategic Communications Centre of Excellence. (n.d.). About NATO StratCom COE [online]. [Accessed: 2026]. Available at: https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5

Nemeth, C.J. (1986). Differential contributions of majority and minority influence [online]. *Psychological Review*. 93(1), pp. 23-32. [Accessed: 2026]. Available at: https://doi.org/10.1037/0033-295X.93.1.23

Newman, N. (2024). *Resumen ejecutivo y hallazgos clave del informe de 2024* [online]. Reuters Institute – politics. [Accessed: 2026]. Available at: https://reutersinstitute.politics.ox.ac.uk/es/digital-news-report/2024/dnr-resumen-ejecutivo

Onuki, M.; Aoyagi, K. and Takasaki, Y. (2022). Personal intergroup contact between different groups of ex-combatants and civilians: Evidence from a behavioural experiment in Rwanda [online]. *European Journal of Social Psychology*. 52, pp. 1-17. [Accessed: 2026]. Available at: https://doi.org/10.1002/ejsp.2811

Paluck, E. L.; Green, S. A. and Green, D. P. (2019). Reassessing the contact hypothesis [online]. *Behavioural Public Policy*. 3 (2), pp. 129-158. [Accessed: 2026]. Available at: https://doi.org/10.1017/bpp.2018.25

Popescu, I. and Voinescu, L. (2021). Key leader engagement – Conceptual delimitations [online]. *STRATEGIES XXI - Command and Staff College*. 17(1), pp. 207-213. [Accessed: 2026]. Available at: https://doi.org/10.53477/2668-2028-21-25

Pettigrew, T. F. and Tropp, L. R. (2006). A meta-analytic test of intergroup contact theory [online]. *Journal of Personality and Social Psychology*. 90(5), pp. 751-783. [Accessed: 2026]. Available at: https://doi.org/10.1037/0022-3514.90.5.751

United Nations. (1948). *Universal Declaration of Human Rights* [online]. [Accessed: 2026]. Available at: https://www.un.org/es/about-us/universal-declaration-of-human-rights

—. (1966). *International Covenant on Civil and Political Rights* [online]. *United Nations Treaty Series*. 999, pp. 171. [Accessed: 2026]. Available at: https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

Saari, D.; Häkkinen, T. and Moilanen, P. (2024). A Comprehensive Analysis of Narratives within NATO's Doctrines [online]. *Proceedings of the 23rd European Conference on Cyber Warfare and Security*, ECCWS 2024. 23(1), pp. 740-747. [Accessed: 2026]. Available at: https://doi.org/10.34190/eccws.23.1.2240

Schiappa, E.; Gregg, P.B. and Hewes, D. E. (2005). The Parasocial Contact Hypothesis [online]. *Communication Monographs*. 72(1), pp. 92-115. [Accessed: 2026]. Available at: https://doi.org/10.1080/0363775052000342544

Sherif, M. (1967). *Group Conflict and Co-operation: Their Social Psychology* [online]. 1st ed. *Psychology Press*. [Accessed: 2026]. Available at: https://doi.org/10.4324/9781315717005

Schmid, K. *et al.* (2012). Secondary transfer effects of intergroup contact: A cross-national comparison in Europe [online]. *Social Psychology Quarterly*. 75(1), pp. 28-51. [Accessed: 2026]. Available at: https://doi.org/10.1177/0190272511430235

Silvela, E. (2017). Strategic communication (STRATCOM) in international organisations [online]. In: Ministry of Defence, Spanish Institute for Strategic Studies (eds.). *Strategic communication.* Pp. 13-34. [Accessed: 2026]. Available at: https://dialnet.unirioja.es/servlet/articulo?codigo=6696731

Stephan, W. G. and Stephan C. W. (1985). Intergroup anxiety [online]. *Journal of Social Issues*. 41(3), pp. 157-175. [Accessed: 2026]. Available at: https://doi.org/10.1111/j.1540-4560.1985.tb01134.x

Stephan, W. G. (2014). Intergroup Anxiety: Theory, Research, and Practice [online]. Personality and social psychology review. 18(3), pp. 239-255. [Accessed: 2026]. Available at: https://doi.org/10.1177/1088868314530518

Tajfel, H. (1974). Social identity and intergroup behaviour [online]. *Social Science Information*. 13, pp. 65-93. [Accessed: 2026]. Available at: https://doi.org/10.1177/053901847401300204

Tajfel, H. and Turner, J. C. (1979). An integrative theory of inter-group conflict. In: Austin, W. G. and Worche, S. (eds.). *The social psychology of inter-group relations*. Monterey, CA: Brooks/Cole. Pp. 33-47

Tassinari, M.; Aulbach, M. B. and Jasinskaja-Lahti, I. (2022) The use of virtual reality in studying prejudice and its reduction: A systematic review [online]. *PLoS ONE*. 17(7). [Accessed: 2026]. Available at: https://doi.org/10.1371/journal.pone.0270748

Turner, R. N; Crisp, R. J and Lambert, E. (2007). Imagining Intergroup Contact Can Improve Intergroup Attitudes [online]. *Group Processes & Intergroup Relations*. 10(4), pp. 427-441. [Accessed: 2026]. Available at: https://doi.org/10.1177/1368430207081533

Vezzali, L. *et al.* (2014). Improving intergroup relations with extended and vicarious forms of indirect contact [online]. *European Review of Social Psychology*. 25(1), pp. 314-389. [Accessed: 2026]. Available at: https://doi.org/10.1080/10463283.2014.982948

Wagnsson, C. and Barzanje, C. (2019). A framework for analysing antagonistic narrative strategies: A Russian tale of Swedish decline [online]. *Media, War & Conflict*. 14(2), pp. 239-257. [Accessed: 2026]. Available at: https://doi.org/10.1177/1750635219884343

Wright, S. C. *et al.* (1997). The extended contact effect: Knowledge of cross-group friendships and prejudice [online]. *Journal of Personality and Social Psychology*. 73(1), pp. 73-90. [Accessed: 2026]. Available at: https://doi.org/10.1037/0022-3514.73.1.73

Article received: 16 June 2025
Article accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Jonattan Rodríguez Hernández
Doctor of Journalism by the Complutense University of Madrid; Accredited as a Contract Professor

Email: jonrodri@ucm.es

Eglée Ortega Fernández
Doctor of Journalism by the Complutense University of Madrid; Accredited as a Full University Professor; Assistant Professor Doctor in the Department of Applied Communication Sciences; Faculty of Information Sciences; Complutense University of Madrid

Email: *egleeort@ucm.es*

The UME on X/Twitter: strategic communication and national security in the forest fires of 2025

Abstract

This article analyses the strategic communication of the Military Emergency Unit (UME) on X (formerly Twitter) during the forest fires that affected Spain in July and August 2025, in one of the most serious episodes in recent decades. The study is based on the premise that institutional communication on social media is a fundamental resource for reinforcing transparency, legitimacy and public trust in crisis situations that compromise national security.

The corpus of analysis includes 175 tweets published by the official @UMEgob account, collected through scraping and examined using a mixed approach. A descriptive analysis of frequency and engagement was carried out, along with a thematic classification adapted to the literature on crisis communication and a semantic analysis using Graphext data analysis software.

The results show that the UME's communication strategy was eminently reactive and operational, with peaks of activity coinciding with the most serious moments of the fires. Informative messages about deployments and resources predominated, obtaining the highest level of citizen interaction. Institutional values and territorial references reinforced the legitimacy of the institution. However, the scarcity of preventive messages indicates an approach focused on immediate response rather than citizen preparedness.

Keywords

Strategic communication, Social media, Climate emergencies, National security, Information dissemination

Cite this article:

Rodríguez Hernández, J. (2025). The UME on X/Twitter: strategic communication and national security in the forest fires of 2025. *Journal of the Spanish Institute for Strategic Studies*. 26, pp. 409-430.

1 Introduction

In recent decades, forest fires have become one of the main strategic threats in Spain, both because of their environmental and social impact and because of their implications for national security. According to data from the Ministry for Ecological Transition and Demographic Challenge (Romero and Camarasa, 2025), Spain is among the European countries most affected by this type of emergency due to its Mediterranean climate, rural depopulation and the accumulation of plant fuel, factors that increase vulnerability to extreme conditions.

The summer of 2025 highlighted the magnitude of the challenge: more than 400 000 hectares were burned between July and August, making it the worst scenario in decades (Planelles, 2025). A report by World Weather Attribution (Devereux, 2025) attributed this extreme episode to climate change, noting that heat waves and atmospheric dryness increased the probability of conditions favourable to the spread of fires on the Iberian Peninsula by up to forty times. These conclusions coincide with scientific literature warning of the growing link between global warming and the intensification of natural hazards in the Mediterranean area (San-Miguel-Ayanz *et al.*, 2023; Turco *et al.*, 2018).

The human and material consequences were significant: thousands of people evacuated, infrastructure destroyed and damage to protected ecosystems. In addition, the crisis took on a political dimension, generating debates about the adequacy of resources, institutional coordination and the role of the Armed Forces in disaster response (Pizarro, 2025). In this scenario, the Military Emergency Unit (UME) positioned itself as a key player, deploying thousands of personnel and technical resources; its role was not only operational but also communicative, given that in crisis situations official information is a strategic resource for reducing uncertainty, legitimising government action and strengthening social cohesion (Coombs, 2015; Frandsen and Johansen, 2016).

It is worth placing this role within a broader framework. During the fires of 2025, units from the Army, Air Force, and Navy also intervened, resulting in a joint action by the Armed Forces in support of civil emergency management. In this operational framework, the UME served as the main communication liaison, acting as a visible and centralised channel for public information.

In this sense, social media has transformed the crisis communication ecosystem. Social network X, in particular, allows for immediate, two-way, wide-reaching dissemination, making it an essential tool for public and security agencies (Austin and Jin, 2022). Since its inception in 2006, this platform has established itself as one of the main digital spaces for governments and institutions (Castillo-Esparcia *et al.*, 2020). Despite this, its use poses challenges related to dialogue management, the credibility of sources and the proliferation of disinformation (Rodríguez and Ortega, 2025).

Analysing the UME's communication strategy in this context is particularly relevant because academic research on institutional military communication in large-

scale emergencies remains limited. Although there are studies on security forces and civil protection, the communication activities of specialised military units such as the UME have received less attention. This article contributes to filling this gap by offering empirical evidence on how the institutional narrative is articulated during a crisis that directly compromises national security.

Therefore, we propose to study the communication developed by the UME on its official X channel during July and August 2025, with the aim of evaluating its effectiveness as a strategic communication tool in the management of crises linked to national security.

2 Theoretical framework

2.1 Institutional communication in critical contexts

Institutional communication in crisis contexts has grown in importance over the years and with the evolution of hyperconnected societies, as it has become an essential tool for transmitting information quickly, clearly and effectively to the public. In emergency situations—such as natural disasters, pandemics, or social crises—public institutions act as reliable sources of reference and play a decisive role in information management (Pulido-Polo *et al.*, 2021).

Situational Crisis Communication Theory (SCCT), initially developed by Coombs (2015) and expanded by various researchers following the COVID-19 pandemic (Chen and Holladay, 2023; Haupt, 2021; Macnamara, 2021), provides a useful framework for understanding the logic of communication in critical scenarios. This theory emphasises the need to adapt communication strategies to circumstances, to carefully manage the institutional narrative and to make appropriate use of official channels.

Along these lines, Cannaerts (2020) highlights that effective communication requires diversifying messages according to the stages of the crisis and the different stakeholders, as well as ensuring coordinated use of internal and external media tools. Social media has become an essential resource for this type of communication. According to Hagen *et al.* (2018), these platforms allow messages to be disseminated in real time and facilitate direct interaction with citizens, which is crucial for answering questions and reducing uncertainty at critical moments.

Poell *et al.* (2019) frame this phenomenon within the logic of platformisation, understood as the process by which digital platforms reconfigure infrastructures and social, cultural and economic processes, generating new opportunities but also challenges for the institutional sphere. Similarly, Viola *et al.* (2021) emphasise the need to consider audience connectivity and participation, encouraging synchronous interaction and the use of relational messages that promote consistent behaviour and reduce the gaps between available information and citizen practices. Based on the case of the pandemic, the researchers highlight the relevance of media literacy and the impact of asymmetric information on the effectiveness of institutional messages.

According to Mayo-Cubero and Chivite (2023), crisis communication can be understood as the set of strategies designed by public bodies to inform, guide and reassure the population affected by an adverse event. Its essential characteristics include immediacy, reliability, accessibility and empathy, the latter being a key element in strengthening relations between institutions and citizens and improving both reputation and crisis management.

The purpose of communication in critical situations is to reduce uncertainty, provide relevant information, strengthen social trust and promote citizen action (Mwandembo, 2024), which requires institutions to establish themselves as reliable sources and maintain strategic control over the narrative they convey through official channels.

In this area, research has identified different communicative functions that are often articulated in institutional responses: operational or informational messages, focused on actions and resources; preventive or educational messages, aimed at citizen preparedness; adjustment or recognition messages, which integrate empathy and emotional support; institutional or reputational messages, linked to coordination and public image; and messages based on identity values, which reinforce the legitimacy of the organisation (Coombs, 2007; Austin *et al.*, 2012; Houston *et al.*, 2015). This typology, widely used in crisis communication studies, allows for the evaluation of the strategic coherence of the institutional response and constitutes the conceptual foundation of the classification applied in this research.

In the case of the Military Emergency Unit (UME), these principles took on particular relevance during the forest fires in Spain in July and August 2025. The magnitude of the disaster placed the UME at the centre of communications; therefore, its activity in X serves as an example for analysing how crisis communication strategies are implemented in real time, how transparency and institutional legitimacy are managed, and to what extent social media can reinforce public confidence in a national emergency context (Hernández, 2021).

2.2 National security in a scenario of unconventional risks

Over the last two decades, national security has evolved towards a broad and comprehensive concept that incorporates unconventional risks such as natural disasters, pandemics, cyber threats and economic crises. This approach recognises that phenomena associated with climate change—especially high-intensity forest fires, droughts and extreme weather events—can directly affect territorial stability, public safety and the continuity of essential services (Lipscy, 2020; Slawotsky, 2021).

In the case of Spain, the 2021 National Security Strategy explicitly identifies forest fires as a strategic risk of the first order. It emphasises the need to strengthen prevention, response and public communication mechanisms, as well as to ensure coordination between civil administrations, civil protection agencies and the Armed Forces. This broader vision reflects the interdependence between environmental security and national security, positioning climate emergencies as a systemic threat that requires versatile state capabilities and rigorous communication management.

Within this framework, the Armed Forces have taken on a multifaceted role that combines traditional defence with intervention in internal emergencies. Their deployment in crisis situations helps to ensure the protection of the population, territorial stability and support for civil authorities (Cheek *et al.*, 2021; Wilén and Strömbom, 2021). This expansion of functions also implies new communication responsibilities, as military presence in non-war scenarios requires the transmission of clear, verifiable and transparent information that is appropriate to citizens' demands and the requirements of institutional legitimacy in democratic societies.

The Military Emergency Unit (UME) is the main operational instrument of this strategy in Spain. Designed as a rapid response unit for forest fires, floods, snowfalls, health crises and other serious risks, the UME coordinates with regional and local authorities as well as with other units of the Army, Air Force and Navy. Its role is not limited to technical support in the field; it also integrates public communication functions that seek to reinforce the perception of the state's effectiveness, coordination and transparency in emergency situations (Hernández, 2021).

Recent literature has highlighted that the UME's digital presence helps to project both its operational dimension and its institutional identity. Research such as that by Martín García, Buitrago and Martín García (2023) has shown that the unit uses social media to articulate values such as service, commitment and humility, which act as symbols of cohesion in risk scenarios. This combination of operational messages and institutional values allows the UME to reinforce its legitimacy and generate public trust, especially when the emergency has a broad territorial impact and high media coverage.

In highly complex situations, such as the forest fires of 2025, public communication thus becomes an essential component of the security apparatus. Citizens demand constant information on the evolution of the risk, the resources deployed and the effectiveness of the response, and this need places the UME in a strategic role that combines technical action, inter-institutional coordination and communication management. The convergence between national security, climate emergencies and institutional communication constitutes a particularly relevant area of analysis for understanding how public narratives are articulated in contexts of increasing environmental vulnerability.

2.3 Social media and public opinion in times of crisis

The role of social media in shaping public opinion is complex and multidimensional. These platforms offer a space for greater citizen participation, but they also generate risks linked to polarisation, the spread of misinformation and the fragmentation of public discourse. In this sense, a critical and balanced approach is required to harness their innovative potential while mitigating the negative effects that can result from their intensive use.

Given their omnipresence in today's society, various studies have highlighted the relationship between these platforms and emergency management, emphasising

the need to design information technologies that promote participation, volunteer mobilisation and citizen access to reliable data (Veil *et al.*, 2011). One of their main advantages lies in their ability to disseminate news directly and on a massive scale, without the mediation of journalists, which gives messages a perception of greater credibility in certain situations (Colley and Collier, 2009).

Social media has significantly reduced barriers to communication, allowing a wide range of actors—ordinary citizens, opinion leaders, governments, and organisations—to participate in global conversations. This phenomenon contributes to the democratisation of discourse, aided by virality, which enables ideas, news and opinions to spread rapidly and reach mass audiences in a matter of hours (Ortega and Rodríguez, 2021). This influences processes such as 'agenda setting', as topics that gain relevance on social media often carry over into traditional political and media debate. Consequently, these platforms act as a 'social thermometer' that reflects collective concerns and interests in real time (Yu *et al.*, 2020).

However, along with their advantages, social media also fuels polarisation dynamics. Pariser (2011) introduced the concept of 'the filter bubble' to explain how personalisation algorithms generate closed information environments that reinforce prior beliefs, reducing exposure to alternative perspectives. This limitation, which restricts access to diverse information, raises ethical dilemmas of great relevance to democracy and public discourse.

Critically, Morozov (2013) warns of the risks of 'technological solutionism', understood as the tendency to propose simple technological responses to complex social problems, ignoring ethical and political dimensions such as privacy or individual autonomy. Similarly, Lovink (2019) analyses how these platforms are designed to encourage constant consumption and addiction, which has a negative impact on users' well-being and mental health, and highlights the urgent need to redesign them based on ethical parameters that prioritise neutrality and functionality over emotional manipulation.

Finally, the use of algorithms that prioritise content related to individual interests encourages the creation of 'information bubbles', where interactions with similar views predominate and the chances of exposure to other perspectives are reduced. This process intensifies the fragmentation of public discourse and hinders the building of social consensus (Patino, 2020). Hence the importance of public bodies managing these platforms appropriately, especially in times of crisis, when institutional credibility and clarity of information are essential.

3 bjectives and methodology

The main objective of this research is to analyse the institutional communication strategy of the Military Emergency Unit (UME) on X/Twitter (@Umegob) during the forest fires that affected Spain in July and August 2025, in order to determine the timeliness, effectiveness and strategic orientation of the messages issued in a national security context. This gives rise to specific objectives:

1. To identify the volume, frequency and evolution of the UME's publications during the different phases of the emergency.
2. Classify messages according to a typology adapted to the UME context (operational/informative, preventive/educational, recognition/adjustment, institutional/reputational and institutional values), evaluating the predominant communicative function.
3. Study thematic clusters and narrative frameworks through exploratory analysis with Graphext and lexical-discursive analysis with T-Lab.
4. Evaluate the engagement generated by the messages, taking into account citizen interaction and the effectiveness of the narrative resources used.
5. Analyse the use of symbolic resources (hashtags, mentions) and their contribution to the visibility and institutional legitimacy of the UME.

This research also adopts a mixed content analysis approach. The study corpus consists of 175 messages, corresponding to all those published by the UME's official account (@UMEgob) in July and August 2025. Data extraction was carried out using the *ExportComments* tool, a software that allows the collection of posts and interactions on X without the need for API access, following a procedure similar to that of other scraping programmes used in research (Marres and Weltevrede, 2013; Bruns and Stieglitz, 2013). The data obtained includes both the full text of the tweets and the date of publication and associated interaction metrics—retweets, likes, and comments—enabling a comprehensive analysis of the institution's communication activity.

The dataset underwent an additional cleansing process to ensure its analytical validity. This included the removal of duplicate posts derived from retweets from the institutional account itself, the standardisation of time formats, and the manual review of textual inconsistencies. These operations were performed using Python libraries designed for data pre-processing.

Once the messages had been collected, they were cleaned and organised using Python libraries, which allowed duplicates to be removed, formats to be standardised, and the data to be prepared for analysis. Initially, a descriptive study was carried out focusing on the frequency of publication, the temporal evolution of the messages, and the levels of interaction generated. This initial step provided a general approximation of the UME's communicative intensity in relation to the emergency and allowed the identification of peaks of activity associated with critical moments.

At a second level, the analysis focused on the thematic and functional classification of the messages. To this end, a typology was developed based on the literature on crisis communication (Coombs, 2007; Spence *et al.*, 2007; Austin *et al.*, 2012; Jin *et al.*, 2014; Houston *et al.*, 2015; Eriksson, 2018), which made it possible to differentiate five main types of publications: operational or informational messages, linked to the deployment of personnel and the evolution of the fires; preventive or educational messages, which include recommendations addressed to the public; messages of recognition or adjustment, expressing support for those involved and gratitude to

the population; institutional or reputational messages, intended to reinforce the image of the UME and highlight coordination with other institutions; and messages of institutional values, which explicitly appeal to the unit's identity principles. In some cases, a subcategory referring to technology and resources was also included, focusing on the use of drones, aircraft and depots. The coding of these categories was initially validated through a manual review of a representative sample of tweets and was subsequently applied to the entire corpus in a supervised manner.

The coding was validated through a double review procedure. Two researchers independently performed the initial categorisation of a representative sample of messages and, after a round of comparison and joint resolution of discrepancies, a high degree of conceptual agreement was reached. Due to the small size of some categories, it was not feasible to calculate reliability coefficients such as Krippendorff's alpha, but the triangulation process ensured the consistency of the classification system applied to the entire corpus.

The third level of analysis focused on exploring discursive and semantic patterns using digital tools. Graphext was used to construct thematic graphs based on the co-occurrence of terms, using the *k-nearest neighbours* methodology and applying the ForceAtlas2 algorithm (Jacomy *et al.*, 2014) for the spatial arrangement of nodes, as well as the Louvain algorithm (Traag *et al.*, 2019) for community detection. This procedure made it possible to identify discursive clusters and examine their evolution over the period analysed.

This analysis was complemented by a manual inspection of the detected clusters in order to verify the semantic coherence of the groupings produced by the algorithm. The process allowed us to identify key terms and recurring conceptual relationships, reinforcing the interpretative validity of the automatically generated discursive patterns.

Finally, the engagement of the posts was evaluated through the relationship between the interactions obtained (retweets, likes and comments) and the number of followers of the account, following the formula proposed by Sued *et al.* (2021) and taken up by Gong and Lyford (2022). In cases where the exact number of followers for each date was not available, relative and comparative values were used to identify the messages that generated the greatest resonance among the public and to assess the real scope of the communication strategy.

Given that the volume of posts per category is uneven—for example, there was only one preventive message compared to more than seventy operational messages—the results related to engagement should be interpreted in a strictly descriptive manner. This imbalance prevents proportional comparisons or statistical inferences between categories, so the values are used only to identify general trends in communication resonance.

4 Results

The analysis of the institutional communication of the Military Emergency Unit (UME) on X/Twitter during July and August 2025 allows us to observe both the

intensity of the digital strategy deployed and the orientation of the messages in a crisis context marked by forest fires.

The weekly evolution of the posts shows a pattern clearly linked to the dynamics of the forest fires (see figure 1). In July, activity was intermittent, with peaks of fourteen and eighteen messages in the middle weeks, followed by a minimum of just four tweets at the end of the month, reflecting less operational pressure during that period. From August onwards, communication intensified steadily: the first week already saw twenty-five messages, a figure that remained high in the second week (twenty-three) and peaked in the third week with forty-four posts, coinciding with the moments of highest incidence of fires and media coverage.

After this peak, activity began to decline, although it remained high in the fourth week (twenty-nine tweets) before closing the month with seventeen. The graph shows that the UME's strategy was essentially reactive, adjusting the volume of messages to the severity of the emergency and reinforcing its digital presence on the days of greatest public visibility.

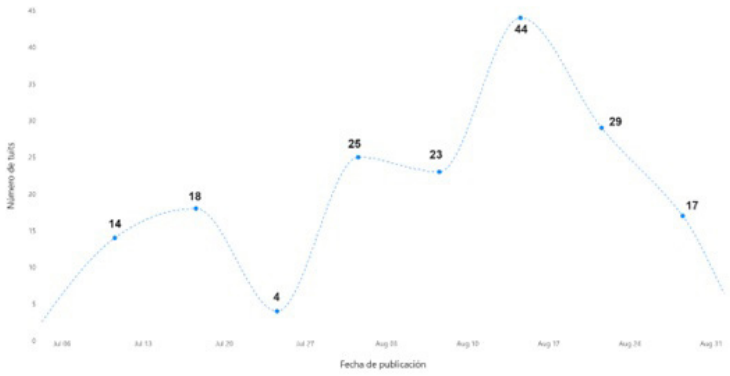


Figure 1. Evolution of the number of tweets published by the UME during July and August 2025.
Source: author's own elaboration

The thematic graph generated from the tweets allows us to visualise the main areas of discourse that structured their communication during the fires (see figure 2). Each colour corresponds to a semantic cluster, i.e. a set of words that appear repeatedly in the same messages and which, as a result, form a specific axis of conversation.

At the centre of the graph are the clusters most closely linked to the operational management of the emergency. These include 'Fire Management and Control Strategies' and 'Forest Fires and Prevention', which group together messages about brigade deployments, fire perimeters, and extinguishing actions. At the top is the cluster 'Extinguishing Missions and Incorporation into Operations', which concentrates narratives about the arrival of personnel at the various scenes. These clusters are interconnected with other supporting topics such as 'Land Drones', reflecting interest in the technological resources used in firefighting.

On the margins of the graph, more peripheral clusters can be seen, such as 'Localities of León and Ourense', which show how fires in specific territories also generated a significant volume of publications. Likewise, the category of 'Military

Operations and Strategic Location' highlights the more institutional and symbolic dimension of the UME, linking its emergency response to the strategic role of the Armed Forces.

The size of the nodes indicates the number of retweets received by each message. Thus, the largest nodes correspond to posts with the greatest public impact, making it possible to identify which topics went most viral. In this case, the clusters directly related to forest fires and the UME's operational management are those that concentrated the messages with the greatest reach, confirming that the public responded more intensely to practical and visual information about the deployment on the ground.

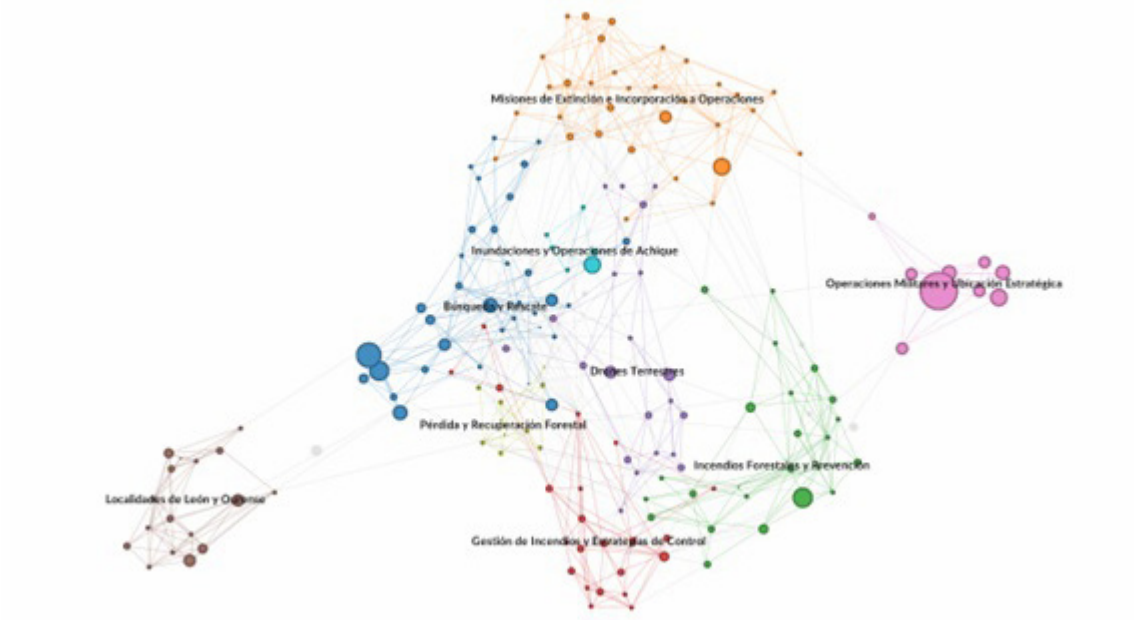


Figure 2. Thematic graph of UME tweets during the fires in July and August 2025. The size of the nodes varies according to the number of retweets obtained. *Source*: author's own elaboration

The analysis of relative engagement allows us to refine the previous results (see figure 3). Although operational messages accounted for the highest absolute number of interactions, when weighted by the number of followers of the UME account (211 400), they are also the ones with the best proportional performance, with an average engagement rate of 0.44%. This figure shows that, compared to other types of messages, informative posts about deployments and actions were the most successful in eliciting a response from the public.

Preventive messages and those appealing to institutional values achieved a very similar average performance, around 0.33%. In other words, both the educational and identity dimensions have the capacity to connect with the audience, even though their volume is lower.

For their part, messages of recognition, despite generating high interaction in absolute terms, have a slightly lower relative engagement (0.28%). This indicates that, although the emotional component mobilises part of the public, it does not always ensure the same virality as operational information.

Institutional posts have the lowest proportional performance (0.23%), reflecting the fact that the public shows less interest in this type of formal content linked to visits or coordination with authorities.

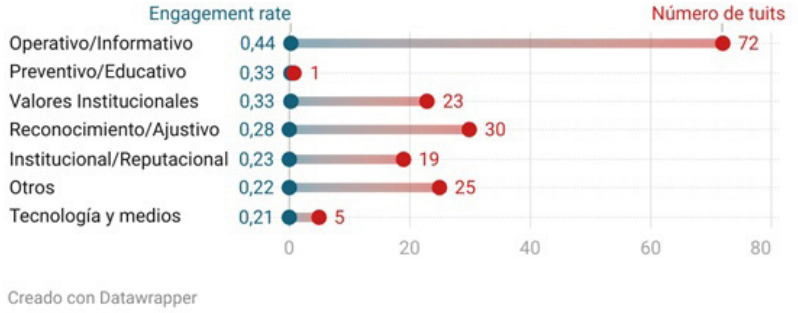


Figure 3. Types of messages published by the UME and their relative engagement during the fires of July and August 2025.
Source: author's own elaboration

Meanwhile, analysis of the hashtags (see figure 4) confirms that the UME's communication combined institutional identity tags with references to affected territories and operational units. The most recurrent tag was #UME (ninety-seven appearances), which acted as an identity mark in almost all messages and ensured the traceability of the conversation.

Next in prominence were military values tags: #Service (seventy-three), #Humility (sixty-six) and #Commitment (forty-for). Their frequent use shows how the UME reinforced its identity narrative, projecting principles associated with the military ethos in parallel with emergency management.

The third block of hashtags corresponds to geographical locations directly affected by the fires: #León, #Ourense, #Zamora, #Asturias and #Cáceres, as well as specific tags for specific fires such as #IFYeres, #IFPorto and #IFBarniedoDeLaReina. This demonstrates a strategy of territorial contextualisation, linking each deployment to its local setting and facilitating citizen identification with the operation.

There are also tags related to the intervention brigades (such as #BIEM5), which reinforce the technical and operational component of the messages.

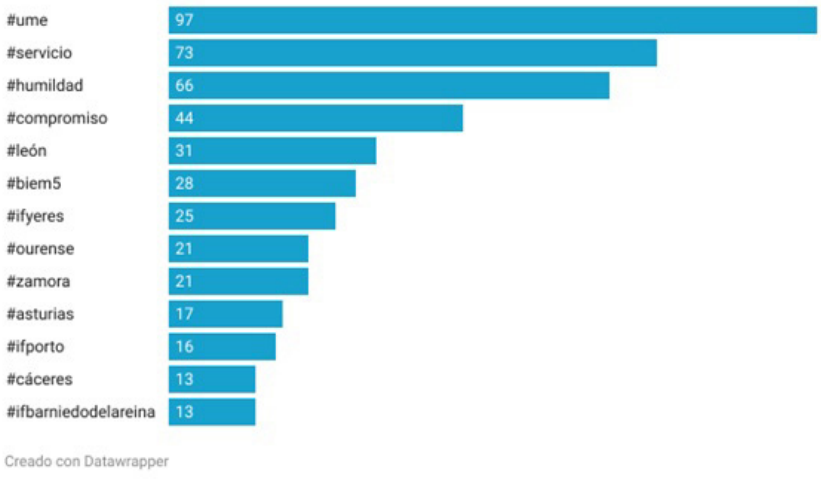


Figure 4. Main hashtags used by the UME in X during the fires of July and August 2025.
Source: author's own elaboration

Analysis of the ten tweets with the highest engagement rate (see table 1) confirms the trend observed in the overall results: the messages that achieve the greatest resonance are those that combine operational information with a strong symbolic component.

The most prominent post, with an engagement rate of 2.26%, reports on a massive deployment of troops—1400 military personnel in direct attack and 2000 in support—accompanied by specific figures on resources and locations. These types of messages, which show the magnitude of the operation, were perceived as highly relevant by the public.

Close behind in terms of impact are messages with emotional hashtags, such as #JuntosEnLaLuchaMilitares (Together in the Military Struggle), which achieved an engagement rate of 2.06%. Here we see how the narrative of unity and shared effort reinforces the connection with the audience. Something similar occurs with posts that incorporate institutional values such as #Compromiso, #Servicio and #Humildad, present in several of the top ten tweets and associated with engagement figures of between 1.2% and 1.5%.

Other examples that generated significant interaction were those that showed the technology used in the emergency, such as the twelve-thousand-litre water tank or the use of FAMET aircraft, messages that offered a component of novelty and operational effectiveness that was highly valued by users.

TABLE I. TOP 10 POSTS WITH THE HIGHEST ENGAGEMENT.

Message	Author	*Engagement rate*
'Deployment of the #UME now: 👤 Military personnel in direct attack: 1,400 👤 Military personnel on support missions: 2,000 🚒 Total resources: 450 📍 #IFCangasDelNarcea #Asturias 📍 #IFSomiedo #Asturias 📍 #IFYeres #León 📍 #IFBarniedoDeLaReina #León 📍 #IFCanalejas #León 📍 #IFElPayo #Salamanca'. *Source*: https://t.co/kMKyCFOjgS	@Umegob	2.26%
'#TogetherInTheFight Military personnel from the #UME carry out a direct attack on the #IFAliseda #Cáceres.@PLANINFOEX@JuntaEx112 #Commitment #Service #Humility'. *Source*: https://t.co/W5rSB761Io	@Umegob	2.06%
'The #UME has installed a 12,000-litre water tank in the #LaBaña area, allowing helicopters 🚁 to shorten their journeys, optimising time and thus multiplying the number of drops at #IFPorto#Commitment #Service #Humility' . *Source*: https://t.co/GG5tfjdotI	@Umegob	1.45%
'#IFRequeixoChandrexaDeQueixa #OurenseLa #UME carrying out a direct attack on one of the flanks of the 🔥 #IF near the town of #Placín.@incendios085@112Galicia#Commitment #Service #Humility'. *Source*: https://t.co/nTwg5jOXMi	@Umegob	1.34%
'Soldiers from the Third Intervention Battalion #BIEM3 are currently flying from #Valencia to #León with the mission of reinforcing the #UME units deployed in the north-west of the peninsula.@ EjercitoAire @Defensagob #Commitment #Service #Humility'. *Source*: https://t.co/fhmGIzPqs2	@Umegob	1.26%
'Almost a thousand #UME military personnel are currently deployed on forest firefighting missions in different parts of our country. Deployment ⬇#Commitment #Service #Humility'. *Source*: https://t.co/QQ8ZdIfm4N	@Umegob	1.25%
'#IFPorto, #Zamora #UME military personnel continue with direct attack tasks. A #Dozer machine from the 11th Specialised Engineers Regiment #REI11 of the @EjercitoTierra joins in missions to open firebreaks.#TogetherWeAddUp'. *Source*: https://t.co/qZiWpJ7ZaF	@Umegob	1.02%
'🫂 COMMITMENT To be where we are needed. The #FAMET air resources of the @ EjercitoTierra are transporting military and emergency personnel with fast and efficient flights that reinforce the fight against 🔥 #LCIF campaign#'. *Source*: https://t.co/7RL2VLISf2	@Umegob	1.01%

Message	Author	*Engagement rate*
'#UME deployment at this time: Military personnel in direct attack: 1,200 Military personnel on support missions: 2,200 Total resources: 420 #IFCangasDeNarcea #Asturias #IFJarilla #Cáceres #IFYeres #León #IFMaceda #Ourense #IFRequeixoChandrexaDeQueixa #Ourense'. *Source*: https://t.co/O6vrDAPoU4	@Umegob	0.95%
'#WeContinueMilitary personnel from the #UME carrying out direct attack missions and eliminating secondary hotspots with hand tools at the #IFOimbra #Ourense.@ incendios085@112Galicia #Commitment #Service #Humility'. *Source*: https://t.co/r6ndpXZ69T	@Umegob	0.92%

Source: author's own elaboration.

The map shows the territorial distribution of tweets published by the UME during the forest fires of summer 2025 (see figure 5). The analysis shows that mentions were concentrated in a few provinces directly linked to the main emergency hotspots.

The province of León appears as the most prominent territory, with the highest number of mentions in institutional communication. It is followed by Ourense, Zamora and Asturias, all of which were severely affected by the forest fires and accounted for much of the UME's operational activity. In second place are Cáceres, Tarragona, Zaragoza, Salamanca and Toledo, where significant actions were also recorded, although with a lower volume of posts.

The territorial pattern confirms that the UME adapted its digital communication to the geographical location of the fires, reinforcing its visibility where it deployed the most personnel. In this sense, the map shows how the X strategy was closely linked to the operational reality on the ground, prioritising explicit reference to the provinces where the main firefighting operations were taking place.

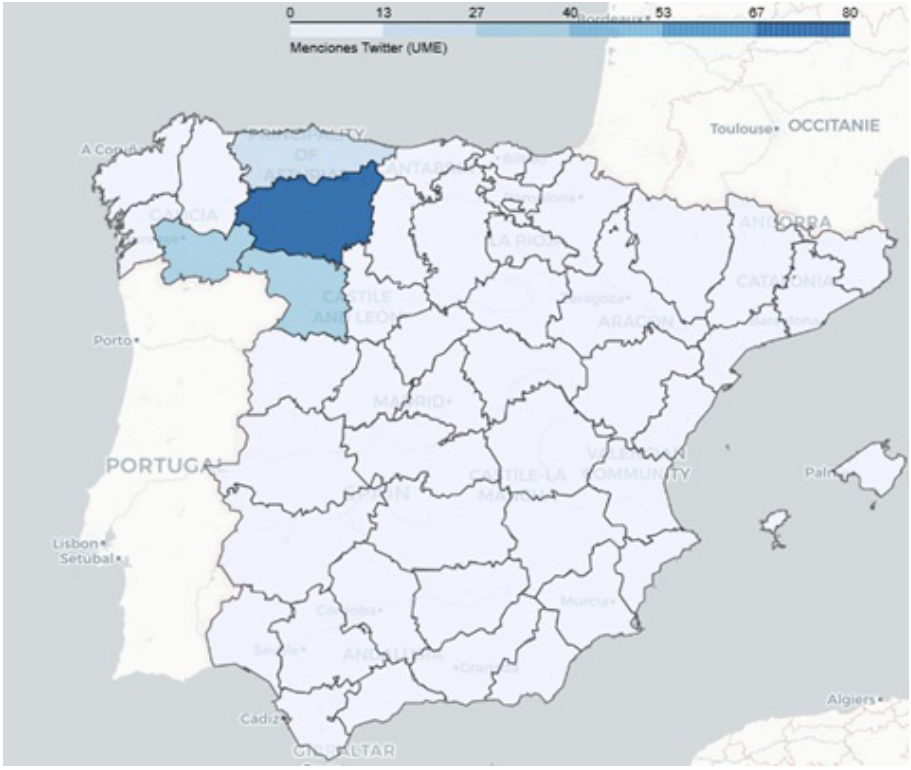


Figure 5. Territorial distribution of mentions of provinces in tweets published by the UME during the fires of July and August 2025. *Source*: author's own elaboration

5 Discussion

The analysis shows how the UME's institutional communication during the 2025 forest fires was organised around a clear pattern: the priority of operational and informational messages. Most of the publications focused on describing deployments, personnel and resources mobilised, confirming the institution's role as an official source of information in emergency situations. This predominance coincides with what is noted in the literature on crisis communication, which emphasises that institutions tend to reinforce the transmission of technical data in contexts of high uncertainty (Coombs, 2007; Jin, *et al.*, 2014; Austin, *et al.*, 2012).

The engagement obtained reinforces this trend. Operational messages generated the most interaction, indicating that the public particularly valued practical and detailed information about fire management. It is noteworthy that even with a predominantly factual tone, the UME managed to maintain high levels of interaction. This result adds nuance to the debate about what type of content works best on social media during emergencies. Contrary to the idea that emotional or symbolic messages attract the most attention, in this case it was the operational content that resonated most. Recent studies on institutional emergency communication (Eriksson, 2018; Reuter and Kaufhold, 2018) also point in this direction, noting that verified and accurate information remains the most valued resource in crisis scenarios.

In terms of the functional classification of messages, the results show that preventive, recognition and institutional categories carry much less weight. Communication is concentrated in the response phase, confirming the reactive orientation of the UME in its digital strategy. Previous research has warned that this imbalance between response and prevention limits the possibilities for institutions to promote long-term social resilience (Palen and Anderson, 2016; Reuter, *et al.*, 2017).

The territorial analysis also provides significant insights. Mentions were concentrated in provinces directly affected by the fires, such as León, Ourense, Zamora, Asturias and Cáceres. This confirms that the UME adapts its digital discourse to the geography of the emergency, reinforcing its presence in places where it deploys a greater number of personnel. This territorialisation of communication reinforces the visibility of institutional action and allows citizens to identify directly with management on the ground, in line with studies that highlight the importance of contextualising messages in specific scenarios (Houston, *et al.*, 2015; Lachlan, *et al.*, 2016).

Likewise, the temporal dimension shows a clear correlation between the intensity of the fires and the volume of tweets published. The concentration of communication activity in August, with peaks coinciding with the moments of greatest operational deployment, reveals a strategy adjusted to the evolution of the crisis. This reactive nature, dependent on the emergency cycle, is consistent with previous research on the institutional use of social media in natural disasters (Mirbabaie, *et al.*, 2020; Spence, *et al.*, 2018).

The study also reveals some limitations. As mentioned above, the low presence of preventive messages indicates that the UME focuses primarily on the response

phase, leaving communication aimed at citizen preparedness in the background. This imbalance is common in emergency agencies, but it opens a debate on how institutions could leverage their networks to strengthen social resilience beyond the critical moment.

Added to this limitation is another of a methodological nature: the analysis has focused on a single platform, which restricts the view of the UME's communication ecosystem. Future research could compare the strategy on different social networks (Instagram, Facebook, TikTok), as well as on other institutional channels, to assess how formats and languages are adapted to different audiences. Similarly, the study does not incorporate citizen reception beyond engagement metrics, so it would be pertinent to move towards research that includes qualitative perceptions of the audience or that analyses two-way interactions between the UME and citizens.

Another line of future work involves international comparison. It would be valuable to explore how similar response units in other countries use social media during environmental crises and contrast their strategies with those of the UME, which would allow for the identification of transferable best practices and cultural differences in emergency communication management. Likewise, integrating more advanced analysis techniques could enrich our understanding of the discursive frameworks employed by the institution.

The results advance academic knowledge about institutional communication in large-scale emergencies, as they show how intervention agencies prioritise operational messages in digital environments during high-intensity phases, even above adjustment or preventive content. This pattern confirms previous findings on the centrality of technical information in situations of uncertainty (Eriksson, 2018; Reuter and Kaufhold, 2018), but also reveals the need to rebalance communication towards educational formats that contribute to strengthening social resilience. From a practical perspective, the results suggest that the UME could integrate a greater proportion of messages aimed at citizen preparedness, taking advantage of its visibility to disseminate self-protection guidelines before and during the emergency, as well as reinforcing narratives of coordination with other competent civil protection agencies.

Based on these findings, several areas for improvement are proposed for future environmental crises. The systematic dissemination of preventive content—especially in the early or intermediate stages of an emergency—could increase the public utility of institutional profiles and promote safer citizen practices. Likewise, the articulation of messages that combine operational data with visualisations, audiovisual resources or contextualised explanations would facilitate understanding of the risk and increase communicative effectiveness. Similarly, the incorporation of active listening strategies and two-way responses would allow messages to be adapted to emerging information needs and reinforce trust in the institutional apparatus.

An additional limitation of the study is that the analysis did not include audiovisual resources—such as photographs, videos, or micro-infographics—or paralinguistic elements such as emoticons, even though these components are part of the digital narrative and can modulate public perception of risk and citizen attention.

The integration of these variables would allow for a more accurate understanding of the communication strategies adopted by the UME in its publications and their relationship with the levels of interaction generated.

6 Conclusions

This study analysed the UME's institutional communication on social network X during the forest fires of summer 2025 in Spain, highlighting several key findings. The temporal analysis showed that the UME intensified its communication at times of greatest operational deployment, with peaks in August 2025 that coincided with the most serious fires. The strategy was eminently reactive, adjusted to the crisis cycle, and confirms the institution's role as an immediate channel of real-time information.

In this regard, the results show a clear predominance of operational and informational messages, followed at a distance by recognition, institutional, and preventive messages. This distribution confirms the UME's priority of transmitting technical data and updates on mobilised resources, leaving educational or citizen preparedness messages in the background.

On the other hand, the semantic graph and lexical analysis showed that the central themes revolved around firefighting, brigade management and resource mobilisation. The narrative was built around operational efficiency and the deployment of units, reinforcing institutional values such as service, commitment and unity.

Likewise, the engagement study revealed that operational messages also obtained the highest relative interaction, confirming that citizens particularly valued clear and detailed information on the evolution of the emergency. Although messages of recognition generated some emotional response, their impact was lower in comparative terms.

Similarly, the analysis of *hashtags* showed the relevance of identity tags such as #Service, #Humility and #Commitment, as well as the constant mention of directly affected territories (León, Ourense, Zamora). This confirms that the UME territorialised its communication, explicitly linking it to the scenarios of action and reinforcing its institutional legitimacy.

The UME's experience confirms, in short, that social media has become a fundamental pillar of institutional emergency management, and that its effectiveness depends both on the ability to provide accurate and verifiable information and on the willingness to integrate messages that promote collective resilience beyond the critical moment.

Bibliography

Adegoke, D. (2023). A Systematic Review of Big Data and Digital Technologies Security Leadership Outcomes Effectiveness during Natural Disasters [online]. *Sustainable Futures, 5*. [Accessed: 2026]. Available at: https://doi.org/10.1016/j.sftr.2023.100113.

Austin, L. and Jin, Y. (2022). *Social Media and Crisis Communication*. Routledge.

Austin, L.; Liu, B. F. and Jin, Y. (2012). How audiences seek out crisis information: Exploring the social-mediated crisis communication model [online]. *Journal of Applied Communication Research*. 40(2), pp. 188-207. [Accessed: 2026]. Available at: https://doi.org/10.1080/00909882.2012.654498

Bruns, A. and Stieglitz, S. (2013). Towards more systematic Twitter analysis: Metrics for tweeting activities [online]. *International Journal of Social Research Methodology.* 16(2), pp. 91-108. [Accessed: 2026]. Available at: https://doi.org/10.1080/13645579.2012.756095

Castillo-Esparcia, A.; Castillero-Ostio, E. and Castillo-Díaz, A. (2020). Think tanks in Spain. Analysis of their digital communication strategies [online]. *Revista Latina de Comunicación Social.* 77, pp. 253-273. [Accessed: 2026]. Available at: https://doi.org/10.4185/RLCS-2020-1457

Cannaerts, N. (2020). Crisis communication in public emergencies: multistakeholders' perspectives [online]. *International Journal of Embedded Systems.* 10(1). [Accessed: 2026]. Available at: https://doi.org/10.1108/ijes-07-2019-0038

Cheek, N.; Reutskaja, E. and Schwartz, B. (2021). Balancing the Freedom–Security Trade-Off During Crises and Disasters [online]. *Perspectives on Psychological Science*. 17, pp. 1024-1049. [Accessed: 2026]. Available at: https://doi.org/10.1177/1745691621103449 9

Chen, F. and Holladay, S. J. (2023). Identifying and responding to social media risks: towards an organisational paracrisis communication framework [online]. *Corporate Communications: An International Journal.* 28(1), pp. 103-117. [Accessed: 2026]. Available at: https://doi.org/10.1108/CCIJ-11-2021-0124

Colley, K. and Collier, A. (2009). An Overlooked Social Media Tool? Making a Case for Wikis. *Public Relations Strategist.* 19(2), pp. 110-122.

Coombs, W. T. (2007). Protecting organisation reputations during a crisis: The development and application of situational crisis communication theory [online]. *Corporate Reputation Review.* 10(3), pp. 163-176. [Accessed: 2026]. Available at: https://doi.org/10.1057/palgrave.crr.1550049

—. (2015). *Ongoing Crisis Communication: Planning, Managing, and Responding*. Sage.

Devereux, C. (2025). Weather that drove Iberian wildfires is 40 times more likely due climate change [online]. *Reuters*. [Consulta: 2026]. [Accessed: 2026]. Available at: https://www.reuters.com/sustainability/climate-energy/weather-that-drove-iberian-wildfires-is-40-times-more-likely-due-climate-change-2025-09-04/

Eriksson, M. (2018). Lessons for crisis communication on social media: A systematic review of what research tells the practice [online]. *International Journal of Strategic Communication.* 12(5), pp. 526-551. [Accessed: 2026]. Available at: https://doi.org/10.1080/1553118X.2018.1510405

Frandsen, F. and Johansen, W. (2016). Organisational crisis communication: A multivocal approach. *Sage*.

Government of Spain. (2021). *National Security Strategy 2021* [online]. Presidency of the Government. [Accessed: 2026]. Available at: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

Gong, Z. and Lyford, C. (2025). Using Social Media for More Engaged Users and Enhanced Health Communication in Diabetes Care [online]. *American Journal of Lifestyle Medicine.* 19(1), pp. 118-128. [Accessed: 2026]. Available at: https://doi.org/10.1177/15598276211064832

Hagen, L. *et al.* (2018). Crisis Communications in the Age of Social Media [online]. *Social Science Computer Review.* 36, pp. 523-541. [Accessed: 2026]. Available at: https://doi.org/10.1177/0894439317721985

Haupt, B. (2021). The Use of Crisis Communication Strategies in Emergency Management [online]. *Journal of Homeland Security and Emergency Management.* 18(2), pp. 125-150. [Accessed: 2026]. Available at: https://doi.org/10.1515/JHSEM-2020-0039

Hernández Corchete, S. (2021). La gestión comunicativa del riesgo en la Unidad Militar de Emergencias. Estrategia y Estructura [online]. *Revista Del Instituto Español De Estudios Estratégicos*. 17, pp. 39-58. [Accessed: 2026]. Available at: https://revista.ieee.es/article/view/2667

Hinata, S.; Rohde, H. and Templeton, A. (2024). Communicating with the public in emergencies: A systematic review of communication approaches in emergency response [online]. *International Journal of Disaster Risk Reduction*. 111. [Accessed: 2026]. Available at: https://doi.org/10.1016/j.ijdrr.2024.104719

Houston, J. B. *et al.* (2015). Social media and disasters: A functional framework for social media use in disaster planning, response, and research [online]. *Disasters. 39*(1), pp. 1-22. [Accessed: 2026]. Available at: https://doi.org/10.1111/disa.12092

Jacomy, M. *et al.* (2014). ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualisation Designed for the Gephi Software [online]. *PLoS ONE*. 9(6). [Accessed: 2026]. Available at: https://doi.org/10.1371/journal.pone.0098679

Jin, Y.; Liu, B. F. and Austin, L. L. (2014). Examining the role of social media in effective crisis management: The effects of crisis origin, information form, and source on publics' crisis responses [online]. *Communication Research.* 41(1), pp. 74-94. [Accessed: 2026]. Available at: https://doi.org/10.1177/0093650211423918

Lachlan, K. A. *et al.* (2016). Twitter use during a weather event: Comparing content associated with localised and non-localised hashtags [online]. *Communication Studies.* 67(4), pp. 399-421. [Accessed: 2026]. Available at: https://doi.org/10.1080/10510974.2016.1196386

Lipscy, P. (2020). COVID-19 and the Politics of Crisis [online]. *International Organisation*. 74. [Accessed: 2026]. Available at: https://doi.org/10.1017/S0020818320000375

Lovink, G. (2019). *Sad by Design: On Platform Nihilism.* Pluto Press.

Macnamara, J. (2021). New insights into crisis communication from an "inside" emic perspective during COVID-19 [online]. *Public Relations Inquiry.* 10(2), pp. 237-262. [Accessed: 2026]. Available at: https://doi.org/10.1177/2046147X21999972

Marres, N. and Weltevrede, E. (2013). Scraping the social? Issues in live social research [online]. *Journal of Cultural Economy.* 6(3), pp. 313-335. [Accessed: 2026]. Available at: https://doi.org/10.1080/17530350.2013.772070

Martín García, A.; Buitrago, Á., and Martín García, N. (2023). #paraservir platforms. The digital strategy of the Military Emergency Unit (UME) as an example of the potential of social media in emergency and civil protection situations [online]. *Cuadernos.info*. 56, pp. 143-165. [Accessed: 2026]. Available at: https://doi.org/10.7764/cdi.56.62489

Mayo-Cubero M. and Chivite J. (2023). The effectiveness of emergency communication on social media. A case study of the Twitter account of Emergencias 112 Comunidad de Madrid [online]. *Estudios sobre el Mensaje Periodístico*. 29(2), pp. 327-335. [Accessed: 2026]. Available at: https://doi.org/10.5209/esmp.87368

Mirbabaie, M.; Stieglitz, S. and Frick, N. R. J. (2020). Fact and fiction: The role of information verification in crisis communication on Twitter [online]. *Information and Management.* 57(5), pp. 103-243. [Accessed: 2026]. Available at: https://doi.org/10.1016/j.im.2019.103243

Morozov, E. (2013). *To Save Everything, Click Here: The Folly of Technological Solutionism*. Public Affairs.

Mwandembo, F. (2024). Navigating the Storm; Effective Crisis Communication Strategies [online]. *International Journal of Innovative Science and Research Technology.* 9(3). [Accessed: 2026]. Available at: https://doi.org/10.38124/ijisrt/ijisrt24mar2080

Ortega Fernández, E. and Rodríguez Hernández, J. (2021). Communication strategy of law enforcement agencies through audiovisual clips on TikTok National Police and Civil Guard in Spain [online]. *aDResearch ESIC International Journal of Communication Research.* 25(25), pp. 160–185. [Accessed: 2026]. Available at: https://doi.org/10.7263/adresic-025-09

Palen, L. and Anderson, K. M. (2016). Crisis informatics—New data for extraordinary times [online]. *Science. 353*(6296), pp. 224-225. [Accessed: 2026]. Available at: https://doi.org/10.1126/science.aag2579

Pariser, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You*. Penguin Press.

Patino, B. (2020) *The civilisation of short-term memory*. Alianza Editorial.

Pina, J. M. (2022). Analysis of Twitter communications by the Armed Forces and Security Forces: an empirical model [online]. *El profesional de la información.* 31(4). [Accessed: 2026]. Available at: https://doi.org/10.3145/epi.2022.jul.03

Pizarro, J. (2025). Choque político en plena crisis por los incendios: Margarita Robles defiende a la UME y reprocha la gestión del PP [online]. *laSexta*. [Accessed: 2026]. Available at: https://www.lasexta.com/noticias/nacional/choque-politico-plena-crisis-incendios-margarita-robles-defiende-ume-reprocha-gestion_2025082668adf9b8506ef67d06e0c108.html

Planelles, M. (2025). *Data already points to the worst year for fires in Spain in three decades after a brutal August* [online]. *El País*. [Accessed: 2026]. Available at: https://elpais.

com/clima-y-medio-ambiente/2025-08-18/los-datos-apuntan-ya-al-peor-ano-de-incendios-en-espana-en-tres-decadas-tras-un-agosto-brutal.html

Poell, T.; Nieborg, D., and Van Dijck, J. (2019). Platformisation [online]. *Internet Policy Review.* 8(4). [Accessed: 2026]. Available at: https://doi.org/10.14763/2019.4.1425

Pulido-Polo, M.; Hernández-Santaolalla, V. and Lozano-González, A. (2021). Institutional use of Twitter to combat the infodemic caused by the Covid-19 health crisis [online]. *Information Professional. 30*(1), pp. 1-15. [Accessed: 2026]. Available at: https://doi.org/10.3145/epi.2021.ene.19

Reuter, C. and Kaufhold, M. A. (2018). Fifteen years of social media in emergencies: A retrospective review and future directions for crisis informatics [online]. *Journal of Contingencies and Crisis Management.* 26(1), pp. 41-57. [Accessed: 2026]. Available at: https://doi.org/10.1111/1468-5973.12196

Reuter, C.; Hughes, A. L., and Kaufhold, M. A. (2017). Social media in crisis management: An evaluation and analysis of crisis informatics research [online]. *International Journal of Human-Computer Interaction.* 34(4), pp. 280-294. [Accessed: 2026]. Available at: https://doi.org/10.1080/10447318.2018.1427832

Rodríguez Hernández, J. and Ortega Fernández, E. (2025). Institutional communication on digital platforms during climate emergencies: analysis of *the* use of X in the DANA in Valencia [online]. *Studies on Journalistic Messaging.* 31(3), pp. 639-654. [Accessed: 2026]. Available at: https://doi.org/10.5209/emp.100623

Romero, J. and Camarasa, A. (2025). *Scientific evidence on climate change and territory in the Iberian Mediterranean. Effects, strategies and public policies. Main recommendations* [online]. Publicacions de la Universitat de València. [Accessed: 2026]. Available at: https://doi.org/10.7203/10550.107077

San-Miguel-Ayanz, J. *et al.* (2023) *Forest Fires in Europe, Middle East and North Africa 2022* [online]. Publications Office of the European Union. [Accessed: 2026]. Available at: https://doi.org/10.2760/348120

Spence, P. R.; Lachlan, K. A. and Burke, J. A. (2007). Adjusting to uncertainty: Coping strategies among the displaced after Hurricane Katrina [online]. *Sociological Spectrum.* 27(6), pp. 653-678. [Accessed: 2026]. Available at: https://doi.org/10.1080/02732170701534277

Spence, P. R.; Lachlan, K. A.; Lin, X. and del Greco, M. (2018). Variability in Twitter content across different crisis events [online]. *Communication Research.* 45(5), pp. 695-716. [Accessed: 2026]. Available at: https://doi.org/10.1177/0093650215619213

Traag, V. A.; Waltman, L., and Van Eck, N. J. (2019). From Louvain to Leiden: guaranteeing well-connected communities [online]. *Scientific reports.* 9(1), pp. 1-12. [Accessed: 2026]. Available at: https://doi.org/10.48550/arXiv.1810.08473

Turco, M. *et al.* (2018). Exacerbated fires in Mediterranean Europe due to anthropogenic warming projected with non-stationary climate-fire models [online]. *Nature Communications.* 9, pp. 3821. [Accessed: 2026]. Available at: https://doi.org/10.1038/s41467-018-06358-z

Slawotsky, J. (2021). The Fusion of Ideology, Technology and Economic Power: Implications of the Emerging New United States National Security Conceptualisation [online]. *Chinese Journal of International Law*. 20(1) pp. 3-62. [Accessed: 2026]. Available at: https://doi.org/10.1093/CHINESEJIL/JMAB007

Sued, G. E. *et al.* (2022). Vernacular Visibility and Algorithmic Resistance in the Public Expression of Latin American Feminism [online]. *Media International Australia.* 183(1), pp. 60-76. [Accessed: 2026]. Available at: https://doi.org/10.1177/1329878X211067571

Veil, S.; Buehner, T. and Palenchar, M. (2011). A Work-In-Process Literature Review: Incorporating Social Media in Risk and Crisis Communication [online]. *Journal of Contingencies and Crisis Management.* 19(2), pp. 110-122. [Accessed: 2026]. Available at: https://doi.org/10.1111/j.1468-5973.2011.00639.x

Viola, C. *et al.* (2021). The more you know, the better you act? Institutional communication in Covid-19 crisis management [online]. *Technological Forecasting and Social Change. 170,* pp. 120929. [Accessed: 2026]. Available at: https://doi.org/10.1016/j.techfore.2021.120929

Wilén, N. and Strömbom, L. (2021). A versatile organisation: Mapping the military's core roles in a changing security environment [online]. *European Journal of International Security*. 7, pp. 18-37. [Accessed: 2026]. Available at: https://doi.org/10.1017/eis.2021.27

Yu, J.; Lu, Y. and Muñoz-Justicia, J. (2020). Analysing Spanish News Frames on Twitter during COVID-19—A Network Study of *El País* and *El Mundo* [online]. *International Journal of Environmental Research and Public Health.* 17(15). [Accessed: 2026]. Available at: https://doi.org/10.3390/ijerph17155414

Article received: 15 September 2025
Article accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Andrea García García
Master's Degree in International Relations: Global Governance and Regional Studies

Email: andreagarciag.95@gmail.com

India in the Indo-Pacific: Strategic Autonomy and Opportunities for the European Union and Spain

Abstract

This article analyses India's role in shaping the Indo-Pacific and its implications for the European Union and Spain. Building on the legacy of non-alignment and the evolution towards strategic autonomy, it examines the main doctrines guiding Indian foreign policy, such as the Act East Policy, the SAGAR initiative and The India Way. The paper addresses the pillars of India's strategic projection: economic growth, military modernisation and connectivity projects, in particular the India–Middle East–Europe Economic Corridor. It also examines India's rivalry with China, its cooperation with the United States within the framework of the Quad, and opportunities for partnership with the EU in trade, technology and maritime security. Special attention is paid to the implications for Spain, highlighting the signing of the 2024 Joint Declaration and industrial and logistical cooperation. The article concludes that India is emerging as an indispensable partner for European strategic diversification and as an opportunity for Spain to strengthen its international presence in defence, energy and connectivity.

Keywords

India, Indo-Pacific, Strategic autonomy, European Union, Spain.

Cite this article:

García García, A. (2025). India in the Indo-Pacific: strategic autonomy and opportunities for the European Union and Spain. *Journal of the Spanish Institute for Strategic Studies*. 26, pp. 431-458.

1 Introduction

The Indo-Pacific has become the main axis of global strategic competition. The term refers to a geopolitical and economic space connecting the Indian and Pacific oceans, stretching from the east coast of Africa to the Americas, and integrating South Asia, Southeast Asia and Oceania. More than a mere geographical delimitation, the concept expresses the growing interdependence between trade, energy and security flows in both basins and today constitutes the frame of reference for the main regional strategies of both the United States and the European Union.

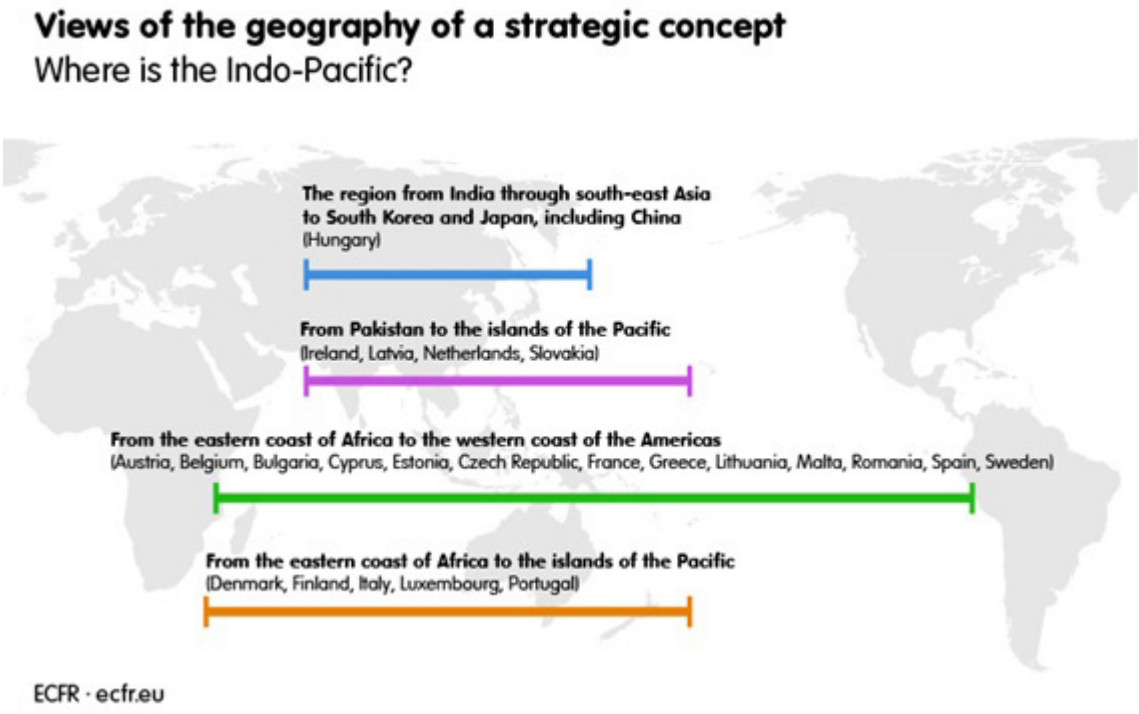


Figure 1. European interpretations of the Indo-Pacific concept. *Source*: European Council on Foreign Relations (2021). All rights belong to the ECFR

The rivalry between the United States and China has placed this vast region at the centre of economic, political and security tensions, with direct repercussions on global trade, supply chains and maritime stability. For the European Union (EU), traditionally focused on its eastern and southern neighbourhood, the growing centrality of the Indo-Pacific constitutes both a challenge and an opportunity. As the EU Strategy for Cooperation in the Indo-Pacific emphasises, 'the EU will strengthen its strategic engagement in the Indo-Pacific, one of the most dynamic and important regions in the world' (European Commission, 2021).

India, the world's fifth largest economy and most populous democracy, has gone from being considered an emerging power to establishing itself as a strategic pivot in the Indo-Pacific. Its economic and demographic weight, its maritime projection and its doctrines of strategic autonomy enable it to play a central role in regional governance. As Ian Hall points out, 'the Modi government has sought to combine India's traditional strategic autonomy with a new willingness to align selectively with like-minded partners' (Hall, 2019).

India's foreign policy vision, built on the tradition of non-alignment and now reinterpreted as strategic autonomy, is reflected in doctrines such as the Act East Policy, SAGAR (Security and Growth for All in the Region) and the Indo-Pacific Oceans Initiative. These policies confirm New Delhi's willingness to act as a guarantor of maritime security and a promoter of regional connectivity, without relinquishing its independence in decision-making. Subrahmanyam Jaishankar puts it explicitly: 'India's path is to be more ambitious abroad, to seek multiple options and to leverage relationships without becoming dependent' (Jaishankar, 2020).

From a European perspective, India is an increasingly important partner. The 2021 *Joint Communication from the European Commission and the High Representative* emphasises that "India's rise and growing role in the region offer an opportunity to forge closer cooperation on trade, connectivity and maritime security" (European Commission, 2021). Similarly, Bruce Vaughn, in his report for the *Congressional* Research *Service*, states that the Indo-Pacific is already 'the main theatre of strategic competition for the United States, where India is emerging as a key partner' (Vaughn, 2017). As Amitav Acharya warns, 'the American world order is not ending, but it is transforming into a multiplex order' (Acharya, 2014). This change opens up opportunities for India to strengthen its profile as an autonomous actor and for the EU to diversify its alliances beyond Washington and Beijing.

The central question guiding this work is the following: can India become a strategic partner of the European Union—and of Spain in particular—in the Indo-Pacific, in a context marked by Sino-American rivalry? The analysis is based on the premise that EU-India cooperation is at a turning point: the crea*tio*n of the Trade and Technology Council, progress in trade negotiations and the strengthening of maritime security with operations such as ASPIDES offer tangible opportunities for a stronger strategic partnership.

This article is divided into eight sections. Following the introduction, it examines the doctrinal framework of Indian foreign policy (2) and its strategic projection (3), followed by an analysis of its rivalry with China (4) and its relations with the United States and the Quad (5). Next, it explores the relationship between India and the EU (6), with a special focus on technological and maritime cooperation, and assesses the specific implications for Spain (7). The article concludes with a forward-looking exercise on future scenarios (8) and some final reflections (9).

2 Indian foreign policy framework

2.1 From non-alignment to strategic autonomy

Since its independence in 1947, India has sought to maintain an autonomous position in the international system. Under the leadership of Jawaharlal Nehru, it became one of the driving forces behind the Non-Aligned Movement, advocating active neutrality during the Cold War. The objective was twofold: to avoid subordination to either of the two blocs and, at the same time, to consolidate its room for manoeuvre on the international stage.

This policy reflected Nehru's conviction that India, as a young independent state, should project itself as a leader of the Global South, defending self-determination and cooperation among developing countries. During the 1950s and 1960s, the doctrine of non-alignment allowed India to maintain relations with both the United States and the USSR, although growing military and technological dependence on Moscow eventually tipped the balance.

Defeat in the war against China in 1962, followed by conflicts with Pakistan, reinforced the perception of vulnerability and the need to maintain multiple strategic options. In the 1970s and 1980s, under Indira Gandhi and Rajiv Gandhi, Indian foreign policy combined the rhetoric of non-alignment with a practice closer to the USSR, especially in the military sphere. However, the economic crisis of 1991 and the Soviet collapse forced New Delhi to redefine its global position.

In the 21st century, that legacy has evolved into the concept of strategic autonomy. Ian Hall notes that 'the Modi government has sought to combine India's traditional strategic autonomy with a new willingness to align selectively with like-minded partners' (Hall, 2019). This autonomy does not imply absolute neutrality, but rather pragmatic flexibility: New Delhi cooperates closely with Washington in areas such as defence and technology, maintains historical relations with Russia and manages its rivalry with China, all without fully committing to any of these poles.

As Tellis warns, 'India will find it difficult to emerge as a first-rate power if it fails to effectively manage the balance between strategic autonomy and cooperation with major powers' (Tellis, 2016). The challenge for Indian foreign policy therefore lies in keeping as many options open as possible, avoiding excessive dependence on a single partner without giving up the advantages of international cooperation. In this vein, Borreguero summarises that the priorities of Narendra Modi's government are to 'position the country as a world power in line with its economic and demographic weight, respond to China's rise and preserve strategic autonomy' (Borreguero, 2025). These goals encapsulate the evolution of Indian foreign policy towards a balance between selective cooperation and the assertion of independence.

2.2 Current doctrines: Act East Policy, SAGAR and The India Way

In recent decades, Indian foreign policy has crystallised into a series of doctrines that reflect both the continuity of its tradition of strategic autonomy and its desire to project itself as a major power.

The first of these is the Act East Policy, launched under the name Look East Policy under Narasimha Rao in 1991 and reinforced from 2014 under Modi, now under its current name. This framework constitutes India's approach to Southeast and East Asia, with the aim of diversifying alliances, increasing trade and participating more actively in Indo-Pacific multilateral forums. As Hall points out, 'the Act East Policy pursues both economic development and India's strategic projection towards East Asia' (Hall, 2019), underlining its dual economic and political-strategic nature.

Alongside this, the SAGAR *(Security and Growth for All in the Region)* concept, presented by Prime Minister Narendra Modi in 2015, places the Indian Ocean at the centre of India's vision. SAGAR combines maritime security with development cooperation, projecting India as a provider of regional public goods. In the words of Pant and Lidarev, 'maritime governance has become the most critical dimension of India's foreign policy, especially in the Indian Ocean' (Pant and Lidarev, 2022). This emphasis responds to the perception that the Indian Ocean is not only India's vital space for projection, but also the main arena for strategic competition with China.

Finally, the third doctrine, set out in the book *The India Way* by the current Minister of External Affairs, Subrahmanyam Jaishankar, expresses the most contemporary view of this tradition. The author argues that Indian foreign policy should be characterised by greater international ambition, the pursuit of multiple options for cooperation, and the ability to leverage alliances without compromising its strategic independence (Jaishankar, 2020). This approach emphasises diplomatic flexibility and adaptability as guiding principles, insisting that India must maintain its autonomy in an international order marked by uncertainty and competition between major powers.

D'Ambrogio points out that this adaptability is also a challenge for the EU, as 'India has proven to be a pragmatic and selective partner, willing to cooperate on issues of mutual interest but reluctant to accept compromises that limit its sovereignty' (D'Ambrogio, 2025). This observation places Indian strategic autonomy as a key factor that conditions not only its foreign policy, but also the way it relates to other international actors.

2.3 The relevance of the Indian Ocean in Indian foreign policy

The Indian Ocean is India's natural sphere of influence and the core of its strategic ambitions. It is where its vital interests converge: energy supply routes, maritime trade and regional security. As Pant and Lidarev summarise, 'India's naval expansion is designed not only to counter China, but also to project itself as a provider of security in the Indo-Pacific' (Pant and Lidarev, 2022).

The CRS agrees, noting that 'China's strategic presence in the Indian Ocean has intensified India's desire to expand its naval capabilities and consolidate regional alliances' (Vaughn, 2017). The perceived threat posed by China's growing presence in ports and bases in the region has reinforced India's conviction that its security and prosperity depend on effective control of key maritime routes.

For New Delhi, maritime security in the Indian Ocean is an essential component of its national security. As Pant and Lidarev point out, 'India has become more active in maritime governance, expanded its maritime space to include the Pacific, and sought closer cooperation in maritime governance with the United States and Japan' (Pant and Lidarev, 2022). Ninety per cent of its foreign trade and more than eighty per cent of its energy imports pass through these waters, making the surveillance of sea lines of communication (SLOC) a strategic priority. Hence, the strengthening of its naval presence and cooperation with regional partners not only seeks to balance

Chinese influence, but also to ensure the protection of its vital interests. In this sense, the SAGAR doctrine is not only a development initiative, but also a comprehensive security strategy that combines the defence of maritime routes with assistance to Indian Ocean island states.

This orientation has been consolidated through successive Indian naval doctrines. As Mboya and Arun recall, 'India published its first naval doctrine in 2004, subsequently revised in 2009 and 2015, under the title *Ensuring Secure Seas: Indian Maritime Security Strategy*'. The 2015 document stated that 'sea control is the central concept around which the Indian Navy is structured, and included surveillance of the main maritime passages in the Indian Ocean, from the Mozambique Channel to the Strait of Malacca' (Mboya & Arun, 2025). These doctrines reflect New Delhi's growing ambition to secure control of strategic access to the ocean and project power beyond its immediate coastline, including the development of nuclear-powered submarines as part of its deterrent triad.

This strategy was complemented in 2017 by the launch of Mission-Based Deployment, an initiative that maintains a permanent presence of naval units in seven areas of interest beyond its exclusive economic zone, providing continuous surveillance at key entry and exit points in the Indian Ocean. According to Mboya and Arun, this measure 'reflects India's willingness to ensure the security of maritime routes and strengthen its response capacity to any regional contingency' (Mboya and Arun, 2025), thus consolidating its role as a guarantor of stability in the Indo-Pacific space.

The Indian Ocean is therefore more than just a geographical space: it is the point where India's doctrines of strategic autonomy, development and maritime security converge. From this space, India aspires to consolidate itself as a central player in Indo-Pacific governance, with the capacity to articulate its own initiatives and reinforce its role in the regional balance of power.

Campos and Sengupta emphasise that 'the Indian Ocean has become the natural platform for India to project both its hard power, through its navy, and its soft power, through cooperation with small island states' (Campos and Sengupta, 2017). This dual vector—military and diplomatic—sums up India's ambition to combine the defence of its vital interests with the provision of regional public goods.

3 India's strategic projection

India's weight in the Indo-Pacific is largely based on its economic dynamism. According to the International Monetary Fund, 'India is projected to grow by 6.8% in 2025, remaining the fastest-growing economy among the major powers' (IMF, 2025). This performance contrasts with the slowdown in other emerging economies and gives New Delhi considerable room for manoeuvre in terms of regional influence.

India's ability to sustain high growth has direct implications for its international standing. A country with a population of over 1.4 billion, an expanding middle class and a dynamic domestic market, India is an attractive partner for investors

and strategic partners. Unlike China, whose economy is showing signs of structural slowdown, India projects an image of stability and dynamism, reinforcing its position as the engine of the Indo-Pacific. However, this image contrasts with a complex internal reality: the country continues to face insurgencies in several states, border tensions with Pakistan and China, and deep socio-economic inequalities. These fragilities limit its ability to translate its growth into institutional and social stability, making its rise a combination of remarkable strengths and persistent vulnerabilities.

3.1 Economy and technology as vectors of power

In addition to its growth, India has consolidated a thriving technological ecosystem in digitalisation, telecommunications and renewable energy. These developments not only strengthen its global competitiveness, but also make it a priority partner for the European Union, which is interested in diversifying supply chains and moving towards a sustainable energy transition. The creation of the EU–India Trade and Technology Council confirms that India's technological dynamism is now a central vector in the bilateral relationship.

Tellis warns, however, that 'economic growth alone does not guarantee global power status if it does not translate into effective strategic influence' (Tellis, 2016). This observation underscores that India must transform its economic achievements into instruments of political and diplomatic power in order to consolidate its role in international governance.

3.2 Military modernisation and naval ambition

The second pillar of India's projection is the modernisation of its military capabilities, particularly its naval capabilities. The SAGAR strategy, linked to maritime security in the Indian Ocean, has resulted in a significant expansion of the fleet and investments in port infrastructure. As Pant and Lidarev point out, 'India's naval expansion is designed not only to counter China, but also to project itself as a provider of security in the Indo-Pacific' (Pant and Lidarev, 2022).

Along the same lines, the CRS notes that India 'is steadily expanding its naval capabilities to project power in the Indian Ocean and beyond' (Vaughn, 2017). This modernisation responds both to the need to balance China's growing naval presence and to India's ambition to become a guarantor of regional security.

The commissioning of the INS Vikrant aircraft carrier in 2022 is a symbol of this ambition. Although it does not guarantee parity with the Chinese Navy, it does represent a decisive step towards consolidating India as a regional naval power, capable of operating in a maritime space that concentrates the planet's most critical energy supply routes.

India's military procurement policy reflects this trend: in addition to its close cooperation with Russia, New Delhi has diversified its suppliers, including agreements with France, the United States and, more recently, Spain in the framework of the

Airbus C295 contract. This pluralism in its sources of armament is consistent with the doctrine of strategic autonomy, avoiding excessive dependence on a single partner.

3.3 Connectivity as a strategic instrument

The third pillar of India's projection is connectivity. In 2023, the India–Middle East–Europe Economic Corridor (IMEC) was announced, an initiative backed by India, the European Union, the United States and partners in the Middle East. The corridor seeks to link Indian ports with Saudi Arabia, the United Arab Emirates, Israel and, ultimately, Europe, combining rail and sea transport.

Recent analyses highlight the transformative potential of IMEC for Eurasian connectivity, conditional on stability in the Middle East (Hussain and Shafer, 2025). The corridor seeks to link Indian ports with Saudi Arabia, the United Arab Emirates, Israel and, ultimately, Europe, combining rail and maritime transport. For India, the project represents a strategic alternative to China's New Silk Roads, as well as a means of strengthening its ties with Brussels and Washington.

The success of IMEC is, however, contingent on stability in the Middle East and the willingness of European partners to invest in long-term infrastructure. In this regard, Spain's participation, through its Mediterranean and Atlantic ports, opens up the possibility of positioning itself as a logistics hub in the global connectivity network. This dimension directly connects the Indian strategy with Spanish and European interests, reinforcing the interdependence between both sides.

3.4 India as a leading power

Beyond these pillars, India's strategic projection responds to a broader ambition: to consolidate itself as a 'leading power', a concept explicitly promoted by the Modi government and reflected in the work of its Foreign Minister, Subrahmanyam Jaishankar, *The India Way* (2020). With this notion, New Delhi aims to leave behind the label of 'developing power' and assert itself as an actor with its own voice in shaping the international order. This is an official narrative that combines the aspiration for greater global responsibility with the defence of strategic autonomy. This idea is shared by Ashley J. Tellis, who states that 'India aspires to move beyond being perceived as a developing power and become a leading power with its own voice in shaping the international order' (Tellis, 2016). This transition involves taking on greater responsibilities in providing regional security, combating climate change and global economic governance.

The Indian narrative insists that its rise is not intended to replicate hegemonic models, but rather to offer an approach based on inclusion and respect for diversity. In this sense, India seeks to project itself as a defender of a rules-based international order that is compatible with the autonomy of states. The convergence of values and objectives—multilateralism, maritime security, energy transition—creates fertile ground for strengthening cooperation.

4 Rivalry with China

Tensions between India and China have historical roots dating back to Indian independence and the consolidation of the People's Republic of China in 1949. The 1962 border war, triggered by disputes in Aksai Chin and Arunachal Pradesh, was a humiliating defeat for India and profoundly marked India's perception of its northern neighbour. Since then, the territorial dispute has remained unresolved, with a border—the Line of Actual Control (LAC)—that continues to be a constant source of friction.

Subsequent episodes, such as the Doklam crisis in 2017, where Indian and Chinese troops faced off for seventy-three days over the construction of a road in an area disputed with Bhutan, confirmed that the Himalayan border is a powder keg. The clash in the Galwan Valley in June 2020, which left at least twenty Indian soldiers dead and an unknown number of Chinese casualties, was the most serious clash in decades and profoundly damaged mutual trust. Since then, both sides have reinforced their military deployment on the LAC, increasing the risk of further incidents.

The CRS summarises this dynamic by pointing out that border disputes have systematically undermined bilateral stability and fuelled strategic mistrust between India and China (Vaughn, 2017). In this sense, territorial disputes are not merely a border issue, but a structural factor that conditions the entire bilateral relationship.

4.1 Maritime competition in the Indian Ocean

Beyond the Himalayan mountains, the rivalry is particularly intense in the maritime domain. India considers the Indian Ocean to be its natural sphere of influence and security, while China perceives it as a vital corridor for securing energy access from the Middle East and Africa.

In this context, China's strategy of establishing a network of ports and infrastructure in countries such as Pakistan, Sri Lanka, Myanmar and the Maldives has often been described as a 'string of pearls' intended to encircle India in its own vital space (Pant and Lidarev, 2022). This perception reinforces the idea that China's maritime presence is not only commercial but also strategic.

According to the CRS, 'China's strategic presence in the Indian Ocean is manifested through port and infrastructure projects—and its first military base in the region—which New Delhi perceives as a challenge to its maritime position' (Vaughn, 2017). Furthermore, it warns that the rivalry between China and India could drive faster development and deployment of naval assets on both sides (Vaughn, 2017), illustrating that maritime competition translates not only into infrastructure, but also into a naval race that threatens to intensify in the coming years.

India's response has been to strengthen its naval projection through the SAGAR doctrine and through maritime surveillance cooperation agreements with island states such as the Seychelles, Mauritius and the Maldives. Furthermore, the commissioning

of the INS Vikrant aircraft carrier in 2022 reflects New Delhi's desire to consolidate a projection capability that deters China and, at the same time, projects India as a provider of regional security.

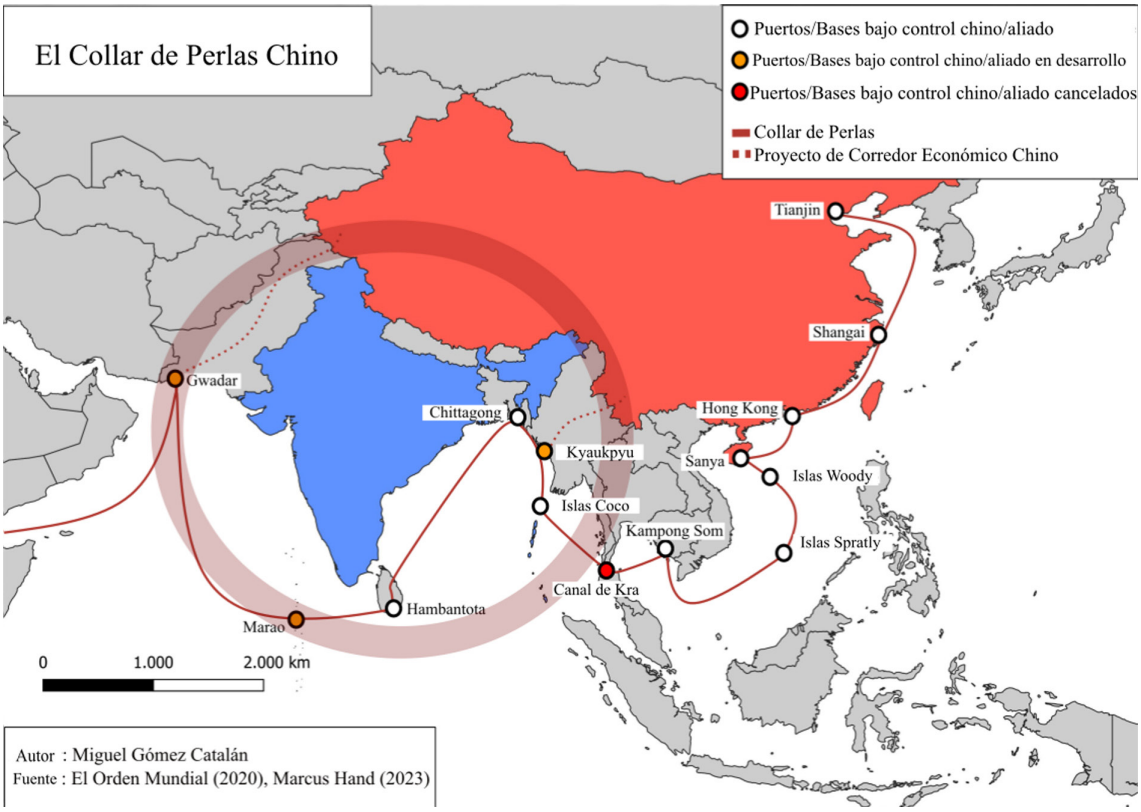


Figure2 . India-China strategic competition in the Indian Ocean: the so-called 'Double Hook Strategy'. *Source*: Gómez, 2024. Reproduced for academic purposes, in accordance with the use permitted by the Ministry of Defence

China's presence in the Indian Ocean is the main strategic challenge for India. Traditionally, the United States has assumed the role of guarantor of security on the high seas, but both India and China are increasingly competing for influence in the region, increasing friction and the risk of conflict (Mboya and Arun, 2025). This rivalry is reflected in the expansion of the so-called string of pearls, a network of ports and infrastructure developed by Beijing to secure energy supplies and consolidate its trade routes.

According to Mboya and Arun:

> 'China emphasises the commercial importance of these ports, but also uses them as a contingency measure against possible obstruction by India, Japan or the United States; these states consider them part of the 'string of pearls' strategy, through which China seeks to protect its trade routes and ultimately dominate the Indian Ocean' (Mboya and Arun, 2025).

This dynamic explains the strengthening of India's naval presence and its cooperation with like-minded powers such as the United States, Japan and Australia within the framework of the Quad, with the aim of counteracting Beijing's influence and maintaining regional balance. As Borreguero points out, in recent years a dynamic cycle of rivalry and strategic readjustments has taken shape in the Indo-Pacific: while

Washington has strengthened its alliances with Asian partners, Beijing has sought to unilaterally change the status quo through its naval expansion and infrastructure construction in the Indian Ocean. This process has prompted middle powers such as India to intensify their defence cooperation with the United States, Japan and Australia, thereby strengthening the regional security framework (Borreguero, 2025).

4.2 Scenarios for diplomatic thaw

Despite this rivalry, New Delhi is not giving up on maintaining channels of dialogue with Beijing. As Jaishankar states, 'our policy towards China must be one of simultaneous engagement and competition' (Jaishankar, 2020). This duality reflects the need to manage tensions without ruling out areas of selective cooperation, especially in multilateral forums such as the BRICS or the Shanghai Cooperation Organisation.

Furthermore, analysts such as C. Raja Mohan have pointed out that India cannot base its strategy solely on confrontation: 'India's strategy towards China relies not only on US support, but increasingly on cooperation with Europe and other Indo-Pacific partners' (Mohan, 2023). This approach suggests that the EU can play a significant role in New Delhi's strategic balance vis-à-vis Beijing.

4.3 The Pakistan factor and the Belt and Road Initiative

China, in alliance with Pakistan, is one of the main strategic challenges for New Delhi. The construction of *the China–Pakistan Economic Corridor* (CPEC), part of the Belt and Road Initiative (BRI), connects western China with the port of Gwadar on the Arabian Sea, crossing territories in Kashmir that India claims as its own. From India's perspective, this corridor not only constitutes a violation of its sovereignty, but also strengthens the strategic alliance between Beijing and Islamabad.

Campos and Sengupta agree on this assessment, highlighting that the convergence between China and Pakistan on infrastructure and defence projects limits India's strategic room for manoeuvre and accentuates its need to diversify alliances (Campos and Sengupta, 2017). This triangular partnership between Beijing and Islamabad therefore poses a structural challenge for New Delhi, forcing it to intensify its ties with external actors—including the United States, the European Union, and regional powers such as Japan and Australia—to balance the growing pressure in its immediate neighbourhood.

The CRS reinforces this view by noting that:

> 'Analysts believe that the rivalry between China and India could accelerate the development and deployment of naval capabilities on both sides, and in the region as a whole. This geographical expansion of strategic competition between China and India may increase strategic ties between the Asia-Pacific region and the Indian Ocean regions, creating a broader and more interactive Indo-Pacific, which would include greater competition for energy and other resources across the Indian Ocean' (Vaughn, 2017).

This statement shows that the rivalry with Pakistan and the BRI not only affects bilateral security, but also has regional implications, shaping an increasingly integrated and competitive Indo-Pacific.

5 India-United States and the Quad

Donald Trump's recent election victory opens a new chapter in US policy towards the Indo-Pacific. According to Borreguero, there is a bipartisan consensus that guarantees the continuity of the strategy of containment against China, albeit with a more confrontational tone that favours India (Borreguero, 2025). The relationship between the two countries has undergone a profound transformation since the end of the Cold War. During the Cold War, New Delhi remained the leader of the Non-Aligned Movement, maintaining an ambiguous stance between the blocs, but with a practical inclination towards Moscow, on which it depended for arms supplies and diplomatic support. Washington, for its part, perceived India as an uncomfortable partner, too independent in its foreign policy and often critical of US strategy in Asia. As Borreguero points out, the composition of the presidential cabinet confirms this trend, with figures such as Marco Rubio and Mike Waltz—'all of them recognised "hawks" on issues related to China and staunch defenders of India—heralding a hardening of the rivalry with Beijing in favour of India' (Borreguero, 2025).

The end of the Cold War opened a window of opportunity for reconciliation. Under the Bill Clinton administration, the first attempts at rapprochement took place, although India's nuclear tests in 1998 led to strong international tensions and sanctions. However, in the early 2000s, the Bush administration recognised India as a key strategic partner in Asia. The 2005 Civil Nuclear Agreement symbolised this shift, recognising India as a de facto nuclear power and laying the foundations for closer cooperation on energy, trade and security.

Subsequently, the Obama administration reinforced this trend, declaring India a 'global strategic partner' in 2015. Trump continued the line of bilateral strengthening, albeit with a more transactional approach, emphasising the importance of balancing the trade balance. Under Biden, cooperation has been institutionalised within the framework of the Quad and expanded to areas such as climate change, global health and, above all, technology. This assessment reflects the growing strategic convergence between the two democracies, but also the tensions arising from India's insistence on preserving its strategic autonomy.

5.1 Cooperation in defence and security

One of the most dynamic areas of the bilateral relationship has been defence. Since 2016, India has been considered a Major Defence Partner of the United States, which facilitates access to advanced military technology and promotes interoperability between the two armed forces. The Malabar joint exercises, which also include Japan and Australia, have intensified, symbolising India's willingness to integrate into security mechanisms with democratic allies in the Indo-Pacific. In this context, Indo-US

cooperation in the maritime domain is particularly relevant, as it helps to strengthen India's capacity in the face of China's growing naval presence in the Indian Ocean.

Likewise, nuclear and space cooperation has advanced significantly since the 2005 agreement. Collaboration on satellites, missile defence and maritime surveillance is part of a shared strategy to preserve freedom of navigation and prevent Beijing's hegemony over trade routes.

5.2 The Quad as a security forum

The Quad (Quadrilateral Security Dialogue), comprising India, the United States, Japan and Australia, is one of the most important forums for understanding Indo-US strategy in the Indo-Pacific. Reactivated in 2017, the Quad is presented as a flexible mechanism for consultation between maritime democracies with the aim of ensuring a free and open Indo-Pacific.

Tourangbam and Vijayakumar emphasise that the litmus test for India in the Quad is the extent to which it can maintain its strategic autonomy while cooperating with like-minded powers on maritime security and technology (Tourangbam and Vijayakumar, 2021). For New Delhi, the Quad is both an opportunity to strengthen its position in the Indian Ocean and a challenge, as it implies greater alignment with the United States vis-à-vis China, which could limit its room for manoeuvre.

The CRS adds that 'although the Quad is not a formal alliance, its growing institutionalisation reflects a clear effort to counter Chinese assertiveness in the region' (Vaughn, 2017). This characterisation illustrates India's dilemma: to benefit from the forum without becoming caught up in a logic of bipolar confrontation.

5.3 Technological cooperation and the iCET agreement

Although security is central, the economic dimension of the Indo-US relationship has also grown. Bilateral trade reached USD 191 billion in 2023, making the United States India's largest trading partner. US investments in sectors such as technology, renewable energy and digital services reinforce this interdependence, while the Indian diaspora in the United States—more than 4.5 million people—acts as a cultural and economic bridge between the two countries.

This convergence reflects what Jaishankar calls 'the Indian way': cooperating closely with the United States without losing autonomy. As he himself states, India must strengthen its ties with Washington, but always while preserving its margin of autonomy (Jaishankar, 2020).

In 2023, both governments announced the Critical and Emerging Technologies Initiative (iCET), aimed at deepening collaboration in artificial intelligence, semiconductors, 5G and 6G networks, as well as space and quantum defence. According to the joint statement from the White House, India and the United States launched the Critical and Emerging Technologies Initiative (iCET) with the aim of strengthening technological cooperation and supply chains (White House, 2023).

This effort responds both to Washington's interest in diversifying technological production away from dependence on China and to India's goal of establishing itself as a global innovation hub. For the European Union, the iCET poses both a challenge and an opportunity: on the one hand, the risk of falling behind in the face of closer Indo-US cooperation; on the other, the possibility of linking up to these value chains through triangular partnerships.

5.4 Strategic autonomy and limits of alignment

Despite the strengthening of the relationship, India remains reluctant to fully commit to the US strategy of containing China. Jaishankar insists that strategic autonomy is non-negotiable; it is in the DNA of Indian foreign policy (Jaishankar, 2020). Hence, even within the framework of the Quad, New Delhi stresses that its participation does not imply a formal military alliance, but rather a flexible mechanism for cooperation. Tourangbam and Vijayakumar (2021) interpret this ambivalence as the essence of Indian foreign policy: to take advantage of the opportunities offered by partial alignment with Washington, without giving up its room for manoeuvre or its historical tradition of independence.

The Indo-US relationship is shaping up to be one of the pillars of the Indo-Pacific architecture in the coming years. Convergence on maritime security, defence technology and connectivity offers fertile ground for cooperation. However, differences over Russia, energy and the degree of confrontation with China will continue to set structural limits.

In this context, the EU and Spain can play a complementary role. By strengthening cooperation with India, Brussels and Madrid can prevent the Indo-American relationship from becoming an exclusive axis, contributing to the diversification of New Delhi's alliances and reinforcing European strategic autonomy.

6 India and the European Union

Relations between India and the European Union (EU) have progressed unevenly since the two sides established a strategic partnership in 2004. For years, cooperation was marked by unfulfilled expectations: political dialogue lacked tangible results and trade negotiations were bogged down by regulatory differences. However, the last decade has seen a significant shift, driven by Brussels' desire to diversify its partners in Asia and India's interest in consolidating its global reach. This rapprochement is based on shared values and objectives. As highlighted in the *Joint Communication to the European Parliament and the Council on a new EU-India Strategic Agenda*, 'the EU and India are pluralistic democracies committed to strategic autonomy, economic resilience and international stability' (European Commission and High Representative, 2025).

From India's perspective, cooperation with the EU in the Indo-Pacific revolves around maritime security, connectivity and the strengthening of a rules-based international order, areas in which New Delhi sees Europe as a complementary rather

than a competitive partner. The Indian Council of World Affairs has already pointed out that this convergence of interests should be directed towards specific projects in maritime governance, sustainable infrastructure and multilateral diplomacy, thus anticipating the new strategic impetus after 2021 (Pandey, 2020).

Enrico D'Ambrogio, a member of the European Parliament's Research Service, notes that EU-India relations have been below their potential and now need a new impetus (D'Ambrogio, 2025). This observation explains the willingness of both sides to relaunch the strategic dialogue, which had been interrupted for years by trade disagreements and divergences on climate change and human rights.

Beyond these dynamics, the European approach to the Indo-Pacific responds to a structural pattern characteristic of the Union's external action. As Jean-Loup Samaan points out, the EU's Indo-Pacific Strategy 'in many ways reflects the broader European strategy: it projects the free trade-based model of governance abroad, while avoiding involvement in power politics' (Samaan, 2024). This approach, focused on promoting economic interdependence and multilateral regulation, conditions Brussels' ability to act as a fully competitive geopolitical actor in an environment marked by strategic rivalries. For India, this characteristic is a fundamental element in assessing both the potential and the limitations of the European Union as a strategic partner in Asia.

This European approach, characterised by an external projection based on rules and free trade, has been described by Samaan as an extension of the EU's internal logic, which is more inclined to avoid power politics than to take on roles of strategic competition. From this perspective, the EU even refrains from explicitly designating China as a threat, preferring to maintain a cooperative rhetoric befitting a 'normative power' (Samaan, 2024). This approach explains part of the gap between Indian expectations and the EU's actual capacity to play a security role comparable to that of the United States in the Indo-Pacific.

The EU Strategy for the Indo-Pacific is a milestone in this rapprochement. The document places the region as a strategic priority for Brussels and highlights India as one of its key partners, both for its demographic and economic weight and for its role in regional stability (European Commission, 2021). In this way, Brussels recognised the need to look beyond its immediate neighbourhood and project itself towards the most economically and geopolitically dynamic region of the 21st century. The *Joint Communication* confirms this role by stating that 'the EU's strategic engagement in the Indo-Pacific region is closely aligned with India's role as a key pillar of stability' (European Commission and High Representative, 2025).

In Indian literature, the Indo-Pacific is seen as the main arena for contemporary geo-economic and geo-strategic competition, driven largely by China's rise as a major power and its growing maritime presence. As Barrech and Mukhtar point out, 'the Indo-Pacific region has become a new chessboard of constantly changing geo-economic, geopolitical and geomilitary dynamics' (Barrech and Mukhtar, 2021). This interpretation reinforces India's perception that European involvement in the Indo-Pacific is driven both by economic interests and by strategic considerations linked to its rivalry with Beijing.

6.1 The trade challenge: the BTIA and economic cooperation

One of the main obstacles in EU-India relations has been the negotiation of a Broad-based Trade and Investment Agreement (BTIA), which began in 2007 and was suspended in 2013 due to disagreements on tariffs, services and intellectual property. The EU was pushing for greater openness of the Indian market in sectors such as automobiles and alcoholic beverages, while India was demanding broader access to the European market for services and labour mobility.

For almost a decade, negotiations remained frozen, fuelling the perception that the strategic partnership lacked substance. However, in 2022, both sides agreed to relaunch the process, integrating trade negotiations into a broader framework that includes cooperation on supply chains, energy transition and digitalisation.

The CRS emphasises that these differences reflect India's strategic autonomy: New Delhi is reluctant to commit to agreements that it perceives as restrictive to its economic sovereignty (Vaughn, 2017). Even so, the relaunch of negotiations reflects a mutual recognition that economic cooperation is indispensable if the political and security partnership is to be consolidated.

6.2 The Trade and Technology Council (TTC)

The creation of the Trade and Technology Council (TTC) in 2022 has marked a qualitative leap in bilateral relations. This mechanism, inspired by the one that already exists with the United States, allows for policy coordination in three key areas: trade, supply chains and digitalisation; emerging technologies, including telecommunications; and security, with a particular focus on cyber risks. Dr Himani Pant, in an article in the ICWA (Indian Council of World Affairs), emphasises that the TTC marks a 'milestone' in EU-India relations and that its objective is to coordinate common responses in trade, trusted technologies and security, with three working groups on strategic technologies and digital connectivity, clean energy and value chain resilience (Pant, 2023).

As Samaan points out, the 2021 Indo-Pacific Strategy takes a much broader approach than the US strategy, articulated in seven priority areas that combine security, prosperity and digital governance (Samaan, 2024). This breadth explains why the TTC has become the main instrument for advancing technological cooperation between the two parties.

The joint statement following the second TTC meeting in 2025 states that 'the EU and India are committed to deepening their cooperation on artificial intelligence, semiconductors and energy transition' (European Commission, 2025). These priorities reflect a shared interest in reducing technological dependence on China and strengthening the resilience of global value chains.

In this regard, NITI Aayog points out that nearly 70% of international trade is based on global value chains, in which the electronics sector plays a central role. For New Delhi, strengthening this participation is essential to move towards a more

innovative economy that is less dependent on Asian production centres. The agency itself stresses that the development of the electronics sector is 'a cornerstone of India's economic strategy', driven by investment in infrastructure, technical training and reforms aimed at consolidating a competitive and sustainable industrial ecosystem (NITI Aayog, 2023).

The 2025 *Joint Communication* further emphasises that 'a flagship example of this strategic partnership is the India-Middle East-Europe Economic Corridor (IMEC)', designed to 'diversify trade routes, reduce strategic dependencies and promote resilient supply chains' (European Commission and High Representative, 2025). For the EU, the TTC is an opportunity to diversify its alliances beyond Washington. For India, it is recognition of its status as a global technology partner, reinforcing its aspiration to become an innovation hub in the Indo-Pacific.

6.3 Maritime security: ASPIDES, ATALANTA and India's role

Beyond trade and technology, maritime security has become a key area of cooperation. The EU has a consolidated presence in the Indian Ocean through Operation Atalanta, which aims to combat piracy in Somalia. Since 2024, this has been complemented by Operation ASPIDES, whose mandate is to 'safeguard freedom of navigation in the Red Sea and the Gulf, in close coordination with international partners' (Council of the EU, 2024).

These operations provide a basis for intensifying cooperation with India, whose interest in the Indian Ocean is both security-related and strategic prestige-related. Enrico D'Ambrogio notes that 'the EU and India are beginning to see each other as indispensable partners in the Indo-Pacific' (D'Ambrogio, 2025). The Joint Communication reinforces this orientation by stating that 'the EU intends to expand operational cooperation with the Indian Navy, building on the joint exercises conducted in June 2025, with the aim of improving interoperability and maritime security' (European Commission and High Representative, 2025). This assessment suggests that, although cooperation is still in its infancy, the objective conditions exist for moving towards a deeper partnership in maritime security.

However, as Samaan points out, Europe's capacity to influence maritime security in the Indo-Pacific remains limited. Although initiatives such as Atalanta, ASPIDES and CRIMARIO contribute to shaping the regional architecture, their budgetary and operational scale is small, which places the EU in a role that is fundamentally oriented towards capacity-building rather than power projection (Samaan, 2024). For India, this difference is a key factor: it appreciates European cooperation, but does not see it as a guarantor of security comparable to the United States or Japan.

From India's perspective, maritime cooperation with the European Union takes on a more explicit strategic dimension. Barrech and Mukhtar emphasise that the inclusion of specific clauses on the Indian and Pacific Oceans in bilateral roadmaps reflects the convergence of interests in preserving freedom of navigation and

maritime security, in line with the United Nations Convention on the Law of the Sea (UNCLOS). Both authors also highlight that 'both the European Union and India perceive China's assertiveness, political influence and economic investments [...] as a serious threat to their geopolitical and geo-economic interests', which has prompted greater cooperation in areas such as Maritime Domain Awareness (MDA) (Barrech and Mukhtar, 2021).

6.4 Convergence on climate and digitalisation

Another area of convergence is the fight against climate change. India is the third largest emitter of greenhouse gases, but also one of the countries most vulnerable to global warming. The EU, for its part, seeks to extend the impact of its Green Deal beyond Europe. This creates fertile ground for joint projects in renewable energy, energy efficiency and sustainable mobility.

At the same time, digitalisation is opening up new opportunities. Brussels and New Delhi share concerns about the dominance of large US and Chinese technology companies and are seeking to strengthen digital sovereignty. The EU brings expertise in data regulation and privacy protection, while India offers a dynamic market with one of the fastest digitalisation rates in the world. The TTC thus becomes the ideal vehicle for articulating these synergies.

Despite progress, significant obstacles remain. Trade differences remain deep, and the EU must balance its Asian agenda with the urgencies arising from the war in Ukraine and instability in the Mediterranean. For its part, India is reluctant to accept compromises that limit its autonomy, maintaining a diversification strategy that includes Russia and Iran.

Added to these limitations are internal differences within the Union itself. Samaan stresses that the Indo-Pacific Strategy is the result of a fragile consensus among the twenty-seven Member States, whose perceptions of China and Europe's role in Asia differ significantly. While figures such as Von der Leyen have adopted a more critical stance towards Beijing, France is promoting a 'balancing power' strategy that seeks to partially distance itself from the United States (Samaan, 2023). These tensions, coupled with the classic duality between the EU and NATO, reduce European visibility and credibility in the region, affecting India's perception of Europe as a strategic actor.

From an Indian perspective, the partnership with the EU offers an opportunity to diversify alliances and reduce excessive dependence on traditional partners. Barrech and Mukhtar point out that strengthening diplomatic ties and maritime cooperation with Europe can broaden India's strategic room for manoeuvre. However, the authors also warn of European structural limitations, stressing that 'the European Union appears to be the weakest party in protecting its infrastructure due to the fragility of its maritime security' (Barrech and Mukhtar, 2021). This ambivalence reinforces the perception of Europe as a complementary, but not substitute, partner in regional security, especially when compared to the United States.

Nevertheless, the potential for cooperation is clear. Convergence on maritime security, a shared commitment to diversifying supply chains and mutual interest in technological development offer fertile ground for consolidating an EU-India strategic partnership. For Spain, this framework represents an opportunity to project its interests in the Indo-Pacific through Brussels, avoiding the need for an individual policy that would be difficult to sustain.

7 Implications for Spain

Prime Minister Narendra Modi's official visit to Spain in October 2024 marked a turning point in bilateral relations. The Spain-India Joint Declaration, signed in Madrid, elevated relations to the level of a strategic partnership and established a roadmap for the coming years. The text states that 'both countries reaffirm their commitment to strengthening cooperation in defence, renewable energy and digital transformation' (Government of Spain—La Moncloa, 2024). This declaration demonstrates the willingness of both capitals to move beyond *ad hoc* diplomatic exchanges and build a stable framework for cooperation.

The importance of this document lies in the fact that it aligns Spanish interests with the EU's strategic diversification policy and, at the same time, responds to India's priorities in terms of security, energy and technological development. The strengthening of bilateral relations should therefore not be seen as an isolated move, but rather as part of Spain's strategy to integrate into European policy towards the Indo-Pacific.

7.1 Industrial and defence cooperation: the Airbus C295 case

One of the areas where Spain-India cooperation has been most clearly evident is the defence sector. In 2021, India formalised the acquisition of fifty-six Airbus C295 aircraft in a contract worth €2.5 billion. The agreement provides for forty of the aircraft to be manufactured in India through a consortium with Tata Advanced Systems, as part of the Make in India initiative. According to Airbus, 'this contract will boost the Make in India initiative through a partnership with Tata Advanced Systems' (Airbus, 2021).

For Spain, this contract not only reinforces the international profile of its aeronautical industry, but also consolidates a strategic relationship of trust with New Delhi in a particularly sensitive area. The case of the C295 illustrates how bilateral cooperation can generate mutual benefits: India obtains technology transfer and strengthens its defence industry, while Spain positions itself as a reliable partner capable of adding value in a highly competitive sector.

This precedent opens the door to future joint projects, both in aeronautics and in other sectors of the military industry, including naval and cyber defence systems. At the political level, it also contributes to positioning Spain as a valid partner within the European strategy of strategic autonomy, reinforcing its credibility in Brussels.

7.2 Opportunities in energy, digitalisation and green transition

Beyond defence, the 2024 Joint Declaration also explicitly refers to renewable energy and digital transformation as priority areas for cooperation. Spain has consolidated experience in the development of clean energy—particularly wind and solar energy—and in the management of smart electricity grids, while India faces the challenge of meeting growing energy demand while reducing its dependence on coal.

The green transition therefore offers fertile ground for joint projects in renewable energy, energy efficiency and sustainable mobility. Added to this is digitalisation, another pillar of the strategic partnership. Spanish technology companies could benefit from the vast Indian market in sectors such as cybersecurity, fintech and smart cities, while India can take advantage of European know-how in digital regulation and data protection.

7.3 Cultural and educational cooperation

A less visible but equally important aspect is cultural and academic cooperation. India is home to one of the most dynamic student diasporas in the world, and Spain can position itself as an attractive destination in areas such as the humanities, social sciences and engineering. University mobility programmes, joint research agreements and the teaching of Spanish as a foreign language offer fertile ground for strengthening ties beyond the economy and defence.

This educational and cultural dimension has also been highlighted in Indian literature. Barrech and Mukhtar point out that the EU-India roadmap envisages strengthening cultural diplomacy and increasing academic mobility through programmes such as Erasmus and greater participation by European institutions in academic activities in India. These exchanges help to consolidate a social and cultural basis for the strategic partnership, complementing advances in trade, technology and security (Barrech and Mukhtar, 2021).

Similarly, the rise of Indian culture in Europe—through cinema, literature and gastronomy—can find a space for two-way exchange in Spain. This type of cultural cooperation helps to strengthen mutual perception and consolidate the strategic partnership on a more human and lasting level.

In this context of bilateral rapprochement, both governments have officially declared 2026 as the 'Dual Year' of India and Spain, with the aim of promoting cultural exchange, tourism and cooperation in artificial intelligence. This initiative seeks to strengthen ties between the two countries through cultural events, exhibitions and exchange programmes that highlight the heritage and international profile of both societies. It also aims to boost tourism through joint campaigns, the promotion of direct air links and the reciprocal promotion of tourist destinations. At the same time, the Dual Year envisages intensified collaboration in research, development and implementation of artificial intelligence in sectors such as health, education and industry. Within this framework, bilateral economic relations are also gaining

greater visibility, with a trade volume of close to ten billion dollars annually in areas such as clean energy, drones, the railway sector and space exploration (Shukla, 2025). Although this initiative does not fall directly within the scope of defence, it does provide a relevant political and symbolic framework for understanding the current dynamism of Indo-Spanish relations, complementing the strategic cooperation described in other areas.

7.4 Spain and connectivity: IMEC as an opportunity

Spain's international projection also benefits from its geographical position. As a natural gateway between Europe, Africa and America, the country can become an essential node in the *India–Middle East–Europe Corridor* (IMEC).

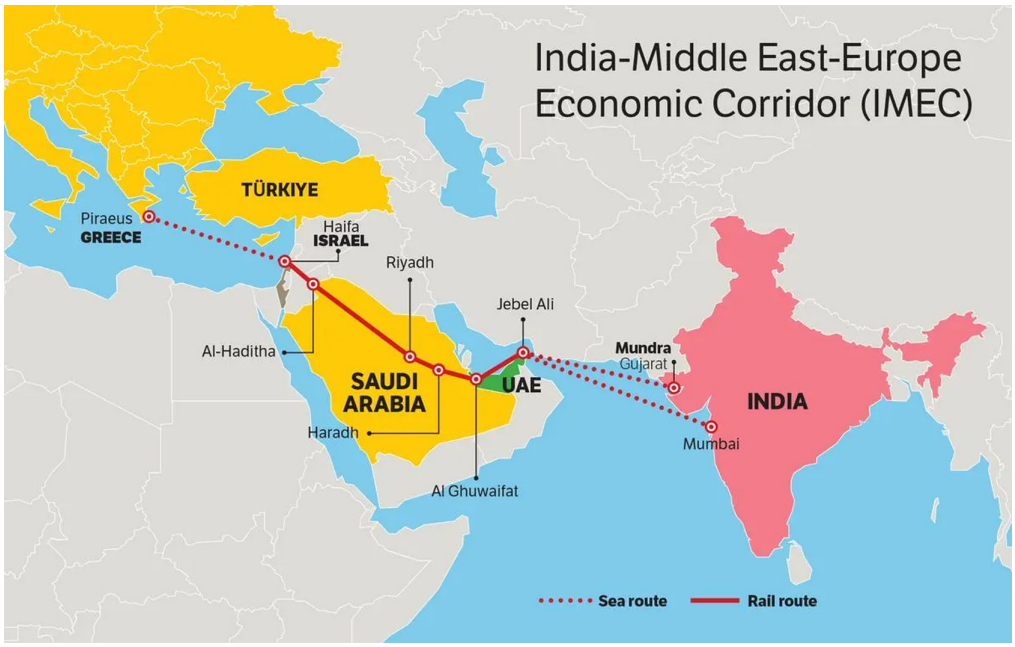


Figure 3. Route of the India–Middle East–Europe Economic Corridor (IMEC). *Source*: Kumar and Vivek, (2024). Image reproduced for academic purposes (fair use). All rights belong to The Diplomatist

Hussain and Shafer emphasise that this corridor has 'the potential to alter regional connectivity dynamics, offering India and its Western partners a strategic alternative to the Belt and Road' (Hussain and Shafer, 2025).

In this context, the Spanish ports of Valencia, Algeciras and Barcelona could play a key role as connection points for goods and energy from the corridor to Europe. Furthermore, participation in the IMEC would allow Spain to strengthen its position within European policy towards the Indo-Pacific and project its influence in global logistics chains.

Despite these advances, various analyses warn that Spain still lacks a defined strategy towards India and the Indo-Pacific. In 2017, the Elcano Royal Institute noted that Spain has shown growing interest in the Indo-Pacific, but still lacks its own strategy towards India (Campos Palarea and Sengupta, 2017). This shortcoming limits Spain's ability to fully exploit the potential of the bilateral relationship and exposes it to excessive dependence on EU common policy.

The absence of a clear strategy translates into low visibility for Spain in New Delhi and a lack of institutionalised cooperation mechanisms beyond specific projects. Compared to countries such as France and Germany, which have more solid roadmaps in Asia, Spain risks falling behind at a time when the Indo-Pacific has become the most economically and geopolitically dynamic region in the world.

The partnership with India offers Spain an opportunity to strengthen its position within European strategic autonomy. By actively engaging in EU-India cooperation, Madrid can present itself as a player that contributes to diversifying European alliances and strengthening resilience in critical sectors. Furthermore, Spain's geographical position—as a gateway to the Atlantic and the Mediterranean—places it in a privileged position to serve as a logistics hub in the connectivity corridors between Asia, the Middle East and Europe, including the *India–Middle East–Europe Corridor* (IMEC).

In this regard, cooperation with India should not be limited to the bilateral level, but should be articulated as part of a Spanish strategy for integration into the EU's Indo-Pacific policy. This would allow Madrid to gain influence in Brussels, take advantage of complementarities with partners such as France, and strengthen its international profile in the areas of maritime security, trade, and technology.

8 Future scenarios (2025-2028)

Any analysis of relations between India, the European Union and Spain in the Indo-Pacific context would be incomplete without some forward thinking. The dynamic nature of the region, marked by geopolitical rivalries, economic transitions and security challenges, makes it essential to project possible scenarios for the next three to five years. These scenarios are not definitive predictions, but rather reference frameworks that allow us to identify risks, opportunities and courses of action for Spanish and European foreign policy.

In the most favourable scenario, India and the EU manage to consolidate a comprehensive strategic partnership based on three pillars: maritime security, trade and technological innovation. The effective functioning of the Trade and Technology Council enables progress in areas such as artificial intelligence, semiconductors and energy transition, reducing both parties' dependence on China. At the same time, cooperation on maritime security is intensified through joint naval exercises and interoperability in operations such as ATALANTA and ASPIDES, strengthening Europe's presence in the Indian Ocean.

For Spain, this scenario opens up the possibility of positioning itself as a key partner in the Mediterranean, linking the India–Middle East–Europe Corridor (IMEC) with its ports and logistics platforms. Likewise, defence cooperation, already inaugurated with the Airbus C295 contract, could be extended to other industrial sectors. The international projection of the Spanish economy would be reinforced, while Madrid would gain influence in the design of European policy towards the Indo-Pacific.

In a more moderate scenario, EU–India cooperation progresses, but unevenly. The TTC yields positive results in some areas, such as digitalisation and cooperation on

cybersecurity, but encounters difficulties on trade and regulatory issues. Coordination on maritime security improves, although without achieving full operational integration.

India remains wary of any commitment that could limit its strategic autonomy, while the EU maintains divergent priorities in its eastern (Ukraine) and southern (Mediterranean and Sahel) neighbourhoods. In this context, Spain makes progress in energy and technological cooperation, but the bilateral relationship with India remains symbolic rather than transformative.

This scenario reflects the inertia of international relations: tangible but limited progress, which consolidates India's relevance to the EU without making it a fully strategic partner. In this context, Samaan's diagnosis of the EU's structural limitations as a security actor in the Indo-Pacific reinforces the idea that the partnership with India can only be fully consolidated if Europe simultaneously advances in strengthening its real strategic autonomy, not just declarative autonomy (Samaan, 2021).

The most negative scenario envisages an escalation of the rivalry between the United States and China, with knock-on effects in the Indo-Pacific. An escalation in the Taiwan Strait or a new border confrontation between India and China would force New Delhi to prioritise military security over economic and technological cooperation with the EU. In this context, India would strengthen its ties with Washington through the Quad and relegate its relationship with Europe to a secondary level.

For the EU, this scenario would represent a setback in its aspiration to become a relevant player in Asia, reinforcing the perception of dependence on the United States. Spain, in this context, would be particularly affected: its incipient strategic partnership with India would be put on hold, limiting opportunities in defence, energy and digitalisation.

This scenario illustrates the risks of the EU-India relationship becoming subordinate to external dynamics, highlighting the importance of building solid and autonomous cooperation before geopolitical tensions reach a point of no return.

The prospective exercise shows that, although the optimistic scenario offers an attractive horizon, the most likely outcome is a combination of the intermediate and critical scenarios. The key for Spain and the EU will be to focus on resilience: strengthening ties with India in strategic sectors, consolidating maritime cooperation and maintaining the diplomatic flexibility necessary to manage Sino-US rivalry.

Ultimately, the future of the EU-India relationship will depend as much on the political will of both parties as on their ability to adapt to a volatile regional environment. For Spain, the challenge will be to transform the opportunities identified in the 2024 Joint Declaration into concrete and sustainable projects, so that the strategic partnership with India does not remain mere declarations of intent.

9 Conclusions

The analysis carried out throughout this paper allows us to draw several conclusions about India's position in the Indo-Pacific and its potential as a strategic partner for the European Union and Spain.

Firstly, India has established itself as a key player in the region's balance of power. Its demographic and economic weight, coupled with a foreign policy characterised by strategic autonomy, make it a central pivot in an increasingly multipolar international order. As demonstrated by the doctrines of the Act East Policy, SAGAR and The India Way, New Delhi has managed to articulate a coherent narrative that combines tradition and pragmatism: preserving its strategic independence while taking advantage of opportunities for cooperation with various players.

Secondly, India's strategic projection is based on three pillars that bring it closer to Europe: sustained economic growth (confirmed by IMF projections), the modernisation of its military capabilities, especially naval capabilities, and the promotion of major connectivity projects such as the *India–Middle East–Europe Corridor*. These elements not only reinforce India's autonomy vis-à-vis China, but also make it an attractive partner for the EU in terms of trade, security and technological development.

Thirdly, rivalry with China will continue to shape India's security environment in the coming years. Border disputes in the Himalayas and maritime competition in the Indian Ocean limit its room for manoeuvre, forcing it to maintain a dual policy of confrontation and cooperation with Beijing. For the EU, this situation reinforces the need to offer New Delhi a stable framework for collaboration that is not subordinate to the dynamics of Sino-American confrontation.

Fourthly, the relationship with the United States and the Quad is both an opportunity and a challenge for India. Cooperation in defence, technology and innovation has intensified—with initiatives such as iCET—but strategic autonomy remains a red line for New Delhi. In this context, the EU has the opportunity to position itself as a complementary partner, capable of strengthening India's resilience without demanding total alignment with China.

Fifthly, the EU-India partnership is at a turning point. Documents such as the 2021 Indo-Pacific Strategy, the creation of t*he Trade and Technology Council* and cooperation on maritime security through operations such as ASPIDES reflect a shared desire to move towards a deeper relationship. However, significant obstacles remain in the areas of trade, regulation and climate. Overcoming them will require sustained political commitment and greater coordination between Brussels and New Delhi.

Sixthly, the implications for Spain are clear. The 2024 Joint Declaration and the Airbus C295 contract show that there are solid foundations for strengthening bilateral relations. Spain has competitive advantages in sectors such as aeronautics, renewable energy and digitalisation, which fit in with India's priorities of modernisation and green transition. However, the Real Instituto Elcano's diagnosis of Spain's strategic deficit remains valid: Madrid needs a more defined strategy towards India and the Indo-Pacific so as not to lag behind other European partners.

Finally, the prospective exercise shows that the future of the EU-India relationship could evolve towards three scenarios: an optimistic one of comprehensive strategic partnership, an intermediate one of selective cooperation and a critical one marked by Sino-American rivalry. For Spain, the challenge will be to transform opportunities

into concrete and sustainable projects, ensuring that the partnership with India does not remain mere declarations of intent.

Overall, this work confirms that India is not only a regional player but also a global partner with the capacity to influence the configuration of the international order. For the European Union, it represents an opportunity to diversify alliances, strengthen its strategic autonomy and project itself in the Indo-Pacific. For Spain, it constitutes a field of action where national and European interests converge, with the potential to expand its international influence in key sectors. The analysis thus confirms that India's position in the Indo-Pacific combines structural strengths—economic growth, maritime projection and strategic autonomy—with internal vulnerabilities and geopolitical challenges that condition its role as a leading power. Only on the basis of this balance between opportunities and limitations can a coherent agenda for action be defined for the European Union and Spain.

On this basis, the recommendations derived from this analysis point to three lines of action. First, consolidate technological and energy cooperation, taking advantage of the TTC framework and the green transition. Secondly, to strengthen cooperation on maritime security, articulating a greater Spanish presence in European missions in the Indian Ocean. And thirdly, to develop a national strategy towards India that complements European policy and avoids Spanish marginalisation in an expanding geopolitical space.

In short, the partnership with India offers the European Union and Spain a way to project their interests in the Indo-Pacific and to adapt to a changing international order. The key will be to transform strategic rhetoric into tangible commitments, so that cooperation with New Delhi becomes one of the pillars of Europe's presence in Asia over the next decade.

Bibliography

Acharya, A. (2014). *The End of American World Order*. Cambridge: Polity Press.

Airbus (2021). India formalises acquisition of 56 Airbus C295 aircraft. [online]. *Airbus.com.* [Accessed: 10 September 2025]. Available at: https://www.airbus.com/en/newsroom/press-releases/2021-09-india-formalises-acquisition-of-56-airbus-c295-aircraft.

Barrech, D. M. and Mukhtar, M. (2021). EU and India: Emerging Partners in the Indo-Pacific. *Journal of Global Peace and Security Studies.* 1(2).

Borreguero, E. (2025) *Indo-Pacific 2025: strategies, cooperation and competition.* IEEE Analysis Document 52/2025.

Campos Palarea, R. and Sengupta, J. (2017). *Spain and India: in search of closer bilateral relations* [online]. Madrid: Elcano Royal Institute. [Accessed: 9 September 2025]. Available at: https://www.realinstitutoelcano.org/documento-de-trabajo/espana-y-la-india-en-busca-de-unas-relaciones-bilaterales-mas-estrechas/

Council of the EU (2024). Council Decision (CFSP) 2024/632 of 19 February 2024 launching the European Union maritime security operation to safeguard freedom of navigation in relation to the Red Sea crisis (EUNAVFOR ASPIDES) [online].

Official Journal of the EU, 632/2024. [Accessed: 10 September 2025]. Available at: https://eur-lex.europa.eu/eli/dec/2024/632/oj/eng

D'Ambrogio, E. (2025). *EU-India relations: Time for a new boost?* Brussels: European Parliament Research Service. Briefing PE 769.496.

European Commission (2021). *The EU strategy for Cooperation in the Indo-Pacific – Joint Communication* [online]. Brussels: EC. [Accessed: 10 September 2025]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/statement_25_643

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. (2025). *Joint Communication to the European Parliament and the Council on an EU-India Strategic Agenda* (JOIN(2025) 50 final) [online]. Brussels: EC. [Accessed: 2026]. Available at: https://www.consilium.europa.eu/es/press/press-releases/2025/10/20/new-strategic-eu-india-agenda-council-approves-conclusions/

European Council on Foreign Relations. (2021). *Moving closer: European views of the Indo-Pacific* [online]. European Council on Foreign Relations. [Accessed: 8 November 2025]. Available at: https://ecfr.eu/special/moving-closer-european-views-of-the-indo-pacific/

Government of Spain – La Moncloa (2024). *Joint statement by Spain and India during Prime Minister Modi's official visit* [online]. Madrid: Presidency of the Government. [Accessed: 10 September 2025]. Available at: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2024/281024-declaracion-espana-india-esp.pdf

Gómez Catalán, M. (2024). Is the dragon strangling the Bengal tiger? Examining India's counter-strategy to China's 'string of pearls' [online]. Spanish *Institute for Strategic Studies (IEEE), Spanish Ministry of Defence*. [Accessed: 8 November 2025]. Available at: https://www.defensa.gob.es/ceseden/-/ieee/esta_el_dragon_estrangulando_al_tigre_de_bengala_examinando_la_contraestrategia_india_al_collar_de_perlas_chino

Hall, I. (2019). *Modi and the Reinvention of Indian Foreign Policy*. Bristol: Bristol University Press.

Hussain, A. and Shafer, N. (2025). *The India-Middle East-Europe Economic Corridor: Connectivity in an era of geopolitical uncertainty.* Washington, DC.

International Monetary Fund (IMF) (2025). *World Economic Outlook Update, July 2025: Global Economy.* Washington DC: International Monetary Fund.

Jaishankar, S. (2020). *The India Way: Strategies for an Uncertain World*. New Delhi: HarperCollins.

Kumar, A. and Vivek, N. D. (2024). India–Middle East–Europe Economic Corridor (IMEC) [Map] [online]. *The Diplomatist*. [Accessed: 8 November 2025]. Available at: https://diplomatist.com/2024/08/20/india-middle-east-europe-economic-corridor/

Mboya, C. and Arun, S. (2025). China, India and the prospects of a BRICS-led maritime order in the Indian Ocean Region. *South African Journal of International Affairs*. 32(1-2), pp. 197-214.

Mohan, C. R.; Mohan, G. and Madan, T. (2023). *The role of the US, Europe, and Indo-Pacific partners in India's China strategy* [podcast] [online]. Washington DC:

Brookings Institution. [Accessed: 6 September 2025]. Available at: https://www.brookings.edu/podcast-episode/the-role-of-the-us-europe-and-indo-pacific-partners-in-indias-china-strategy/

NITI Aayog. (2023). *Electronics: Powering India's participation in global value chains*. Government of India.

Pandey, P. (2020). *India, EU, and the Indo-Pacific: Exploring Vistas of Cooperation* [online]. Indian Council of World Affairs Research Papers. [Accessed: 12 November 2025]. Available at: https://www.icwa.in/show_content.php?lang=1&level=3&ls_id=5516&lid=3905

Pant, H. (2023). *First India-EU Trade and Technology Council: Significant milestone in India-EU relations* [online]. Indian Council of World Affairs. [Accessed: 12 November 2025]. Available at: https://icwa.in/show_content.php?lang=1&level=3&ls_id=11122&lid=6112

Pant, H. V. and Lidarev, I. (2022). *India and Global Governance: A Rising Power and Its Discontents* [online]. London/New York: Routledge. [Accessed: 12 November 2025]. Available at: https://doi.org/10.4324/9781003272540-13

Samaan, J. L. (2024). The European Union and Security Cooperation in the Indo-Pacific: A Lamb in the Lion's Den?. En: Joshi, Y. *et al* (eds.). *The European Union as a Security Actor in the Indo-Pacific. Perceptions and Responses from the Region*. Springer Nature Singapore Pte. Ltd. Pp. 15-28.

—. (2023). France Has Big Plans for the Indo-Pacific. *The National Interest*.

Shukla, P. (2025). India-Spain Declare 2026 as 'Dual Year' for Culture, Tourism, and AI [online]. In: *Adda247 Current Affairs*. [Accessed: 10 December 2025]. Available at: https://currentaffairs.adda247.com/india-spain-declare-2026-as-dual-year-for-culture-tourism-and-ai/

Tellis, A. J. (2016). *India as a Leading Power* [online]. Washington, DC: Carnegie Endowment for International Peace. [Accessed 10 September 2025]. Available at: https://carnegieendowment.org/research/2016/04/india-as-a-leading-power?lang=en

Tourangbam, M. and Vijayakumar, A. (2021). Finding Strategic Autonomy in the Quad: India's Trial by Fire [online]. *The Diplomat*. [Accessed: 10 September 2025]. Available at: https://thediplomat.com/2021/03/finding-strategic-autonomy-in-the-quad-indias-trial-by-fire/

Vaughn, B. (2017). *China–India Rivalry in the Indian Ocean*. Congressional Research Service. United States.

White House (2023). *Joint Statement from India and the United States* [online]. Washington DC: The White House (Biden Archive). [Accessed: 10 September 2025]. Available at: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/09/08/joint-statement-from-india-and-the-united-states/

Article received: 12 September 2025
Article accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Sebastian Chumbe
Master in International Relations (Nebrija University) and Popularizer of History and Geopolitics

Email: chumbe009@gmail.com

Western Balkans between opposing blocs: military alliances, grey zone and multi-level containment

Abstract

This article analyses the growing risk of conflict in the Western Balkans arising from the consolidation of antagonistic military blocs formed around Serbia and Kosovo, with the involvement of external actors such as Russia, NATO and the European Union. Using theoretical frameworks such as the balance of power, complex interdependence and the notion of the grey zone, it examines the strategic motivations of the main actors, as well as the critical flashpoints in North Kosovo and Republika Srpska. Despite escalating rhetoric and latent tensions, three key factors of containment are identified: the EU's structural mediation, regional economic interdependence, and international military deterrence through missions such as KFOR and EUFOR Althea. This research aims to assess the impact of emerging military alliances on Balkan stability, considering historical variables, external actors and international security theories, and to analyse whether they increase the risk of armed conflict in the region in a context of unresolved tensions in Kosovo and Republika Srpska.

Keywords

Srpska, Kosovo, Serbia, Grey Zone, Complex Interdependence.

Cite this article:

Chumbe, S. (2025). The Western Balkans between opposing blocs: military alliances, grey zone and multi-level containment. *Journal of the Spanish Institute for Strategic Studies*. 26, pp. 459-490.

1 Introduction

1.1 Brief historical context

From a linguistic perspective, Serbian, Bosnian and Croatian are standardised variants of the same linguistic diasystem historically known as Serbo-Croatian, sharing grammatical, lexical and syntactic bases. However, since the 1990s, these names have become politicised as instruments of nationalist differentiation.

The fragmentation of the identity of the South Slavic peoples was consolidated during the Middle Ages through the formation of distinct states, a process that deepened in the modern era under divergent imperial influences: the Habsburgs in Croatia (Catholicism), the Ottomans in Bosnia (Islam) and the Serbian Orthodox resistance to Islamisation.

The dissolution of the Ottoman and Austro-Hungarian empires after the First World War led to the creation of the Kingdom of Serbs, Croats and Slovenes (1918), the first unified state to bring these ethnic groups together after centuries of separation. Reconfigured as the Socialist Federal Republic of Yugoslavia after the Second World War under the leadership of Josip Broz Tito, the country adopted a federal structure with six republics and two autonomous provinces within Serbia (Vojvodina and Kosovo), delineating the contemporary borders (figure 1).

Figure 1. Socialist Federal Republic of Yugoslavia, 25 January 1991

The Titoist period (1945-1980) maintained stability through inter-ethnic balance and a self-managed socialist model. However, after Tito's death, converging factors—economic crisis, the rise of nationalism, institutional weakness, and the Soviet collapse—eroded federal cohesion.

The dissolution process (1991-1992) took divergent paths: while Slovenia and Macedonia achieved independence with low human cost, Croatia and Bosnia suffered devastating conflicts due to the country's complex demographic distribution (figure

2). In Croatia, the war ended with the Erdut Agreements (1995), reintegrating Eastern Slavonia (United nations, 1995a), the last stronghold of the Serbian Republic of Krajina[1], under UN supervision.

Figure 2. Ethnic groups in the Balkans, 21 April 2018

The Bosnian conflict (1992-1995), which was tri-national and particularly violent—with episodes such as the Srebrenica genocide—culminated in the Dayton Accords (United Nations, 1995b). These established a Bosnian state divided into two entities: the Federation of Bosnia and Herzegovina (Croats and Bosniaks) and the Republika Srpska (Serbs), with a tripartite system of government and international supervision by the High Representative. This institutional architecture, although pacifying, has perpetuated ethnic tensions.

The Kosovo War (1999) marked another turning point in the Balkans, when the Kosovo Liberation Army (KLA) rose up against the government of the Federal Republic of Yugoslavia (Serbia and Montenegro), leading to allegations of massive human rights violations. NATO's military intervention—without authorisation from the UN Security Council—set a critical precedent in international law (OTAN, 2024). This conflict culminated in Kosovo's unilateral declaration of independence (2008), recognised by the United States and most NATO members, but rejected by China and Russia, which insist on Serbia's territorial integrity.

Structural tensions persist: Belgrade maintains its resentment towards NATO (Miolsevich, 2019) and is strengthening ties with Moscow, while Albanian Kosovars feel insecure in the face of possible Serbian aggression, especially in northern Kosovo (El Grand Continent, 2024), which has a Serbian Kosovar majority. This dynamic has prompted a military alliance between Kosovo, Albania and Croatia (Koha, 2025a),

1 The Republic of Serbian Krajina was a territory self-proclaimed by Serbs in Croatia in 1991, following Croatia's declaration of independence. It was not recognised internationally and was dismantled militarily in 1995 during Operation Storm.

interpreted as an 'anti-Serbia' bloc. As a counterweight, Serbia has signed a military cooperation agreement with Hungary, whose government, led by Viktor Orbán (Infobae, 2025a), combines EU/NATO membership with alignment with Russia.

The situation is further complicated by the involvement of the Republika Srpska, whose leadership under Milorad Dodik promotes separatist rhetoric against Sarajevo and seeks to link up with the Serbian-Hungarian alliance (SwissInfo, 2025a). Thus, the unresolved conflicts in Kosovo and Bosnia are intertwined, reactivating historical fractures and threatening regional stability.

1.2 Central question

Does the consolidation of antagonistic military blocs in the Balkans—with the influence of external actors such as Russia and NATO—increase the risk of armed conflict in the region, in a context of unresolved tensions in Kosovo and the Republika Srpska?

1.3 Hypothesis

The formation of opposing military blocs in the Balkans, with the support of external actors, increases the possibility of violent escalation in the Balkans due to unresolved historical tensions.

1.4 Justification

Recent alliances in the Balkans are reactivating classic power balance dynamics in a region marked by deep historical fractures. In this context, the participation of actors with divergent interests—such as Hungary, a member state of the European Union and NATO but politically aligned with Serbia—introduces a new level of geopolitical complexity that challenges traditional structures of regional cooperation and security. However, despite the relevance of this phenomenon, there remains a notable absence of studies analysing this particular configuration from the perspective of contemporary security theories, which justifies the relevance and originality of this work.

1.5 Research questions

- How do balance of power and regional security theories explain the formation of these blocs?
- To what extent does this case represent a conflict in a 'grey zone'?
- What strategic objectives are the Balkan countries involved pursuing by consolidating opposing military blocs?
- How does Hungary's duality (EU/NATO, but pro-Russian) and the role of the Republika Srpska influence the escalation of tensions?

– What containment mechanisms could mitigate the risk of conflict?
– What are the critical scenarios where tensions are most latent?

1.6 Objectives of the article

– To assess the impact of emerging military alliances on Balkan stability, considering historical variables, external actors and theories of international relations.
– To examine the strategic motivations of the actors involved.
– To identify the limits of current containment mechanisms.
– Propose crisis management scenarios based on empirical evidence.

2 Theoretical framework

2.1 Balance of power

The *balance of power* theory is one of the central theoretical foundations of international relations. It posits that states act to prevent the hegemonic domination of one actor by forming compensatory alliances, thus generating systemic tensions when the distribution of power becomes unbalanced (Waltz, 1979).

From a historical perspective, Thucydides (431 BC) identified this pattern in *History of the Peloponnesian War*, arguing that the conflict arose from Spartan fear of Athenian rise. Centuries later, neo-realist theorists such as Kenneth Waltz (1979) reformulated the concept, emphasising that the anarchy of the international system forces states to seek rational balances of power to ensure their survival (Waltz, 1979: p. 88).

The current situation in the Balkans accurately illustrates these postulates. Following Waltz, Kosovo—faced with the Serbian threat—has allied itself with Croatia (interested in stabilising Bosnia) and Albania, forming a pro-NATO bloc. At the same time, Hungary, despite its NATO membership, prioritises national and ideological interests over transatlantic cohesion, aligning itself tactically with Serbia (Thucydides, 2014: v. 89). This dynamic confirms the fluidity of alliances in anarchic contexts.

In structural terms, NATO operates as a regional hegemonic power, but its influence generates counter-alliances such as the Serbia-Republika Srpska-Russia axis. Thus, the Balkans replicate the classic cycle of equilibrium described by theory: accumulation of power, formation of coalitions and resulting tensions.

2.2 Grey Zone

The concept of the grey zone describes the strategic space between peace and war where state and non-state actors compete using ambiguous tactics (Mazarr, 2015: p. 12). This framework is particularly relevant for analysing the Balkans, where

Serbia and its counterparts employ strategies that avoid open conflict but perpetuate instability.

Serbia officially rejects the recognition of Kosovo, but exerts influence in the Serb-majority north through parallel structures and calculated mobilisations. An emblematic example was the deployment of Serbian troops near the Kosovar border in 2023, following protests against the installation of Albanian Kosovar mayors in northern municipalities (Cué, 2023) (Mazarr, 2015: p. 45 'actors in the grey zone seek to deny responsibility while achieving strategic objectives').

Hungary, a NATO member but aligned with Serbian interests, illustrates the fluidity of the grey zone. Although it avoids direct military operations, its economic cooperation with Belgrade—such as the agreement to build a bilateral oil pipeline(Daily News Hungary, 2025a) —serves as a lever of influence (Mazarr, 2015: p. 67: 'economy and diplomacy replace military force in liminal conflicts').

Milorad Dodik's separatist rhetoric in the Republika Srpska (Ozturk, 2025) intensifies regional fragility, showing how the boundaries between war and peace are blurring. The combination of tensions in northern Kosovo and Bosnia reflects the risk of inadvertent escalation that Mazarr (2015, p. 89) warns about: 'the grey zone can collapse abruptly into open conflict if actors exceed critical thresholds'.

The Balkans embody Mazarr's postulates about the grey zone, where calculated ambiguity, contradictory alliances and non-military tools define a strategic competition that threatens to destabilise the region.

2.3 Complex interdependence theory

The theory of complex interdependence (Keohane and Nye, 1977) posits that transnational economic, diplomatic, and social connections moderate—without eliminating—geopolitical conflicts. This framework explains key dynamics in the Balkans.

Among its characteristics are the existence of multiple channels of interaction between states and actors. (Keohane and Nye, 1977: pp. 23-25) Serbia is critically dependent on the EU (which accounts for 64% of its exports) (OEC, 2023a), including paradoxical trade relations with rival actors: in 2023, it imported goods worth USD 1.27 billion from Croatia (3.11% of its total), while Zagreb depended on Belgrade for 2.7% of its imports (USD 1.17 billion) (OEC, 2023b).

Likewise, the European Union has recently institutionalised this framework of interdependence through the 'Growth Plan for the Western Balkans', announced by the Commission on 8 November 2023 (European Commission, 2023a). This instrument, with a budget of €6 billion, goes beyond the mere objective of economic development by establishing explicit political conditionality that links financial assistance to the maintenance of regional stability and constructive cooperation with the EU and neighbouring countries (European Commission, 2023a).

In this way, the Plan stands as a powerful mechanism of geopolitical containment, where economic asymmetries are instrumentalised to raise the costs of any destabilising

action by actors such as Serbia. These structured and politicised interdependencies ultimately create prohibitive opportunity costs that discourage military escalation and reinforce a fragile but persistent regional balance.

On the other hand, Keohane and Nye (1977: p. 29) point out that, in contexts of complex interdependence, international agendas are not hierarchical and high and low politics are intertwined, blurring the boundaries between domestic and foreign policy. In the Balkans, both Serbia—an official candidate for EU membership—and Kosovo—a potential aspirant (Vozpópuli, 2025)—subordinate their territorial tensions to their European integration objectives, revealing a strategic prioritisation of economic and institutional legitimacy over security confrontation.

Belgrade instrumentalises the issue of Serbian minorities in Kosovo and Bosnia as a mechanism for electoral mobilisation, while projecting a narrative of technical compliance towards Brussels in order to maintain aid flows and negotiations. In turn, Hungary aligns its foreign policy with Serbia not only because of ideological affinities, but also to reinforce its discursive sovereignty *vis-à-vis* the EU and consolidate an alternative illiberal axis within the Euro-Atlantic framework.

This logic translates into a symbiosis between domestic politics and strategic diplomacy, where actors seek to maximise domestic benefits without completely abandoning European structures, thus creating an environment of contained competition rather than open rupture.

However, the most relevant feature in the Balkan context is the marginalisation of military force as a primary political tool. Although high-tension crises persist—such as the Serbian mobilisations on the border with Kosovo in 2023(DW, 2024)—widespread violence does not materialise. This can be explained not only by economic and diplomatic pressure from the EU and the US, which raises the costs of open conflict (Keohane and Nye, 1977), but also by the deterrent effect of the international security missions deployed on the ground.

The continued presence of KFOR in Kosovo and EUFOR Althea in Bosnia and Herzegovina acts as a physical guarantor of the *status quo*, materialising the Euro-Atlantic commitment to block any military escalation. These missions are the operational embodiment of security interdependence, becoming a structural factor that channels tensions towards containment and diplomacy rather than armed confrontation.

The Balkans exemplify how complex interdependence stabilises but does not resolve conflicts. As Keohane and Nye (1977) point out, this creates a fragile balance where actors prioritise economic interests over territorial maximalism.

3 Analysis of alliances

3.1 Kosovo – Albania – Croatia: Collective defence or provocation?

Northern Kosovo, shown in figure 3, comprises the municipalities of Leposavić, Zvečan, Zubin Potok and North Mitrovica, and is the epicentre of the territorial

dispute with Serbia. This enclave, with a Serb-Kosovar majority, responds in a particularly confrontational manner to the regulatory provisions issued by Pristina. An illustrative case was the so-called 'licence plate crisis': between September and October 2021, Kosovo banned Serbian licence plates and deployed special forces at border crossings, leading to blockades and demonstrations (Infobae, 2021) that only ceased after mediation by the European Union.

Figure 3. Serb-majority regions in Kosovo, 15 June 2015

The truce proved short-lived. On 1 August 2022, Serbian number plates expired in Kosovar territory, reigniting protests. Tensions escalated in May 2023, when the Serb-Kosovar population boycotted the municipal elections organised by Pristina (Peregil, 2023) and clashes broke out, leaving dozens of protesters and KFOR troops injured. The refusal to participate in the elections reflected the community's rejection of what it perceives as unilateral impositions that threaten its identity and its ties to Belgrade.

The spiral of violence reached a critical point on 24 September 2023 with the Banjska incident: a Serb Kosovar commando attacked the Kosovar police, killing one officer and three Serbs (EFE, 2021). The situation worsened despite the provisional agreement on mutual recognition of number plates concluded eleven months earlier (Ozturk, 2034). In November 2024, an explosion in a strategic canal damaged water facilities essential to Pristina; the attack was attributed to Serbian militants and classified as terrorism (Reuters, 2024). Each event reinforces the perception of mutual insecurity and highlights the fragility of mediation mechanisms.

Faced with this dynamic, Kosovo lacks sufficient military capacity to balance Serbia and therefore prioritises external guarantees. On 18 March 2025, Tirana hosted the signing of a defence cooperation agreement between Albania, Croatia and Kosovo, interpreted by regional analysts as an alliance aimed at deterring Serbia (SwissInfo,

2025b). For Pristina, the pact has three objectives: to raise the cost of any Serbian coercion, to place its security issues on the Euro-Atlantic agenda, and to strengthen its state legitimacy by creating formal coalitions.

Albania's participation is explained, above all, by identity considerations. Tirana has historically set itself up as the protector of the Albanian diaspora based in Kosovo and North Macedonia. From a nation-state perspective, the Albanian government gains internal political capital by projecting leadership over vulnerable Albanian-speaking communities. However, its motivations are not exclusively symbolic. The Albanian Deputy Prime Minister has described the Durrës-Pristina railway as a geopolitical link that will connect Pan-European corridors VIII, X and Adriatic-Ionian (Koha, 2025b), transforming Durrës into a regional logistics hub. Such infrastructure would cement the interdependence between Tirana and Pristina and give Albania a strategic role in Balkan trade.

At the same time, Albania aspires to establish itself as a NATO operational platform in the eastern Adriatic. The modernisation of the Kuçovë air base under Allied command, located some two hundred kilometres from Camp Bondsteel (the main US facility in Kosovo), allows for rapid projections and logistical synergies between the two facilities (Santos, 2022). The new trilateral agreement reinforces this Atlantic narrative and positions Tirana as an indispensable security actor in south-eastern Europe.

As for Croatia, its alignment is based on a dual identity-strategic calculation. On the one hand, Zagreb sees itself as the guarantor of the Croatian minority in Bosnia and Herzegovina. The close relationship between Belgrade and the Republika Srpska, whose leader Milorad Dodik promotes secessionist rhetoric, threatens the Dayton Accords (1995) and, by extension, the stability of Croatia's south-eastern border. By supporting a coalition that limits Serbia's influence, Croatia seeks to safeguard the *status quo* in Bosnia and Herzegovina and protect its compatriots.

On the other hand, Croatia maintains a structural rivalry with Serbia for symbolic and strategic primacy in the Western Balkans. As a full member of the EU and NATO, Zagreb positions itself as a bastion of the Euro-Atlantic axis, projecting normative stability and alignment with Western institutions. In contrast, Belgrade promotes a policy of 'active non-alignment', combining European aspirations with growing energy and military ties with Moscow. The rapprochement with Kosovo and Albania allows Croatia to reinforce its pro-Western profile, while at the same time providing an explicit counterweight to the geopolitical convergence between Serbia and Russia.

Added to this dynamic is the still unresolved border dispute over a 137-kilometre stretch along the Danube. Croatia claims that the delimitation established by an Austro-Hungarian cartographic survey in 1891 is valid, while Serbia defends the current river course. This divergence creates areas of dispute that hinder bilateral trust-building (Bickl, 2021) and contribute to maintaining a backdrop of persistent friction, even in the context of formal cooperation.

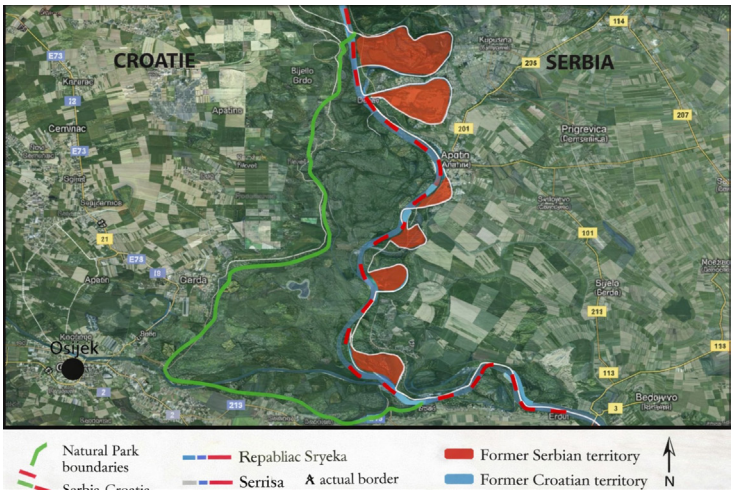


Figure 4. Croatia-Serbia border dispute, 2011

The Tirana-Zagreb-Pristina agreement thus illustrates the 'complex interdependence' described by Keohane and Nye: no single issue prevails absolutely over the others, and the distinction between domestic and foreign policy is blurred. Military motivations coexist with identity, logistical and normative variables; the protection of diasporas, the articulation of economic corridors and the framework within Euro-Atlantic organisations influence as much as classic deterrence. At the same time, governments instrumentalise domestic demands—whether the security of Serbs in Kosovo, the protection of Albanians in the diaspora or the defence of Croats in Bosnia—to legitimise foreign policy decisions.

For the European Union, these dynamics pose a dilemma. Enlargement remains Brussels' main lever, but its credibility is eroded by the slowness of the process and competition from external powers. As long as the EU cannot offer tangible incentives that reduce the perception of threat, local actors will tend to seek alternative security guarantees or forge *ad hoc* coalitions.

In short, the Croatia-Albania-Kosovo alliance should not be interpreted as a mere classic military pact, but as the manifestation of a web of interests where identity, geo-economics and institutional positioning converge. Its effectiveness will depend on the partners' ability to balance national ambitions with cooperative commitments and, above all, on the evolution of the Belgrade-Pristina relationship.

3.2 Serbia – Hungary and Slovakia?: A dissident axis within the European Union

In March 2025, Hungarian Prime Minister Viktor Orbán banned the LGBT Pride march in Budapest, invoking recent legislation restricting the 'promotion' of sexual diversity to minors, a regulation inspired by the conservative agenda of the Russian Federation (Nagy, 2025) . Far from demobilising activists, the measure had the opposite effect: more than 200,000 people took part in the demonstration despite official threats (Aljazeera, 2025). Such state intervention cannot be interpreted solely as domestic policy; it also serves as an ideological marker that projects Hungary's adherence to an illiberal and national-conservative discourse to the outside world.

Restrictions on adoption by same-sex couples, the veto on school content on gender identity and the rhetoric of the traditional family are presented by Budapest as a defence of cultural sovereignty against 'impositions from Brussels', a discursive framework almost identical to that used by Vladimir Putin to accuse the European Union of moral decadence (Bayoud, 2022).

This convergence of values is reinforced by the personal cordiality between Orbán and the Russian president, evident in successive bilateral meetings and Hungary's refusal to support full sanctions against Moscow (Grippo, 2024). Thus, civil rights policy becomes an instrument of symbolic alignment with the Kremlin, giving Hungary a unique profile within NATO and the EU.

In Serbia's case, convergence with Russia is even more explicit. Memories of the NATO bombings in 1999 and the perception that the West supports Kosovo's independence continue to shape public opinion. Even though the European Union is its largest trading partner, Belgrade has prioritised its strategic alliance with Moscow: it refused to join the sanctions against Russia following the invasion of Ukraine, despite the fact that this decision hinders its EU accession bid (Infobae, 2024). In this context, Serbian identity is articulated around a narrative of historical grievance and Slavic solidarity that favours alignment with the Kremlin.

The political-military rapprochement between Budapest and Belgrade crystallised on 1 April 2025 with the signing of a cooperation agreement (Peirano, 2025) . This agreement outlines plans for seventy-nine joint activities in 2025 in the military and energy fields (Stojanovic, 2025).The pact was interpreted as a direct response to the alliance announced weeks earlier by Croatia, Albania and Kosovo—three actors clearly aligned with NATO and the United States—and thus constitutes the second major subregional coalition created in the Balkans in less than a month. From the Hungarian-Serbian perspective, the new bilateral framework aims to guarantee the stability of their respective national minorities and strengthen strategic autonomy in the face of pressure from Brussels and Washington.

The economic aspect of the relationship is equally significant. In 2023, Hungary consolidated its position as the third largest destination for Serbian exports, absorbing 5.72% of the total (OEC, 2023a). Among the main items is electricity, an area in which Serbia is one of the key suppliers to the Hungarian energy system (OEC, 2023c).

Both governments are also promoting interconnection projects that will increase the degree of mutual dependence: the construction of a bidirectional oil pipeline to guarantee fuel supplies to Serbia, scheduled for 2027 (Daily News Hungary, 2025b) , and the modernisation—financed in part by Chinese capital—of the Budapest-Belgrade railway line, which is scheduled for completion by the end of 2025 (Daily News Hungary, 2025c). These infrastructures create faits accomplis that anchor Hungary within Serbia's economic orbit in the energy and logistics sectors.

The equation could be complicated by Slovakia's hypothetical entry. Members of the Serbian Parliament have confirmed talks aimed at Bratislava's accession to the defence agreement (Gardner, 2025). Of particular note is the intervention of Serbian MP Dragan Stanojević, a member of the People's Voice party, who, from an openly

pro-Russian position, has alluded to the possible incorporation of Slovakia into the Belgrade-Budapest cooperation axis. However, so far the Slovak authorities have not issued any official statement on the matter (Mlakar, 2025).

In any case, the shift is plausible given the positions of Slovak Prime Minister Robert Fico, who is openly critical of sanctions against Russia and inclined towards a pragmatic foreign policy that reduces military assistance to Ukraine. Fico was, in fact, the only EU head of government to attend the Victory Day parade in Moscow (Brezar, 2025). The progressive political alignment between Hungary, Slovakia and Serbia was evident during the summit held in Komarno in October 2024, at which the heads of state of the three countries reaffirmed their commitment to cooperation on controlling irregular migration and jointly protecting Europe's external borders (TVPWorld, 2024).

There are, therefore, two possible interpretations of the ultimate purpose of the alliance. The first conceives it as an anti-EU sovereignty project: the three governments would use the discourse of a 'Europe of nations' to resist EU federalism and revalue state powers without necessarily seeking direct dependence on Moscow.

The second argues that the axis constitutes, *de facto*, a vector of rapprochement with Russia, aimed at eroding the Western liberal order and reconfiguring loyalties within the EU and NATO. The two frameworks are not mutually exclusive; rather, they feed into each other in practice: the rejection of European centralisation favours the opening up of a space where Russian influence encounters less regulatory resistance.

The rift is already apparent in forums such as the Visegrad Group. Poland and the Czech Republic, which favour a hard line against Moscow, are distancing themselves from Hungary and Slovakia, which advocate negotiations and the gradual lifting of sanctions (Bugajski, 2025). The result is the paralysis of the Central European coordination mechanism, with direct implications for the EU's common security and defence policy.

Beyond the internal consequences, the Hungarian-Serbian alliance raises serious questions about NATO's cohesion. Never before has a member state (Hungary) signed a military pact that is presented as a counterweight to another bloc involving two Atlantic allies (Croatia and Albania). The risk is a form of 'neutralisation from within', in which Budapest could veto collective responses to crises in the Balkans if it perceives that such actions would run counter to its commitments to Belgrade. Slovakia would add another potential blocking voice in the North Atlantic Council, complicating the development of regional contingency plans.

In short, the April 2025 military agreement and the hypothetical enlargement to Bratislava outline a new Central European axis which, without declaring itself an enemy of the West, challenges its principles from within. By invoking cultural sovereignty and resistance to Brussels' 'ingratitude', Belgrade, Budapest, and potentially Bratislava are creating a parallel architecture that hinders unified EU action and threatens to introduce systemic vetoes in NATO. Understanding the hybrid nature—ideological, economic and strategic—of this alignment is essential to assessing its capacity to reshape the balance of power in the Balkans and, by extension, Euro-Atlantic security.

3.3 Republika Srpska: Catalyst for conflict?

The growing separatism of the Republika Srpska (RS), led by Milorad Dodik, constitutes the most imminent threat to the peace architecture that has governed Bosnia and Herzegovina since the signing of the Dayton Accords in 1995. Although successful in stopping the violence, these agreements created an extraordinarily complex state framework that was vulnerable to capture by ethnic elites. In 1998, Dodik became head of the RS government with the explicit backing of Washington and Brussels, projecting himself as a moderate reformer committed to the post-war order; the international community consequently saw him as a suitable partner for consolidating peace (McAdams, 1998).

However, during his second term in office, which began in 2006, he moved from conciliatory rhetoric to openly questioning the constitutional framework, invoking the RS's 'right' to call a referendum on independence and gradually turning this secessionist cause into the pillar of his internal legitimacy(Traynor, 2011).

The strategic shift was formalised in 2015, when Dodik's Alliance of Independent Social Democrats (SNSD) passed a resolution setting 2018 as the deadline for proclaiming independence if the entity considered that Sarajevo continued to restrict its powers (Zuvela, 2015).

Since then, secession has become *de facto* official policy of the ruling party. Just one year later, Dodik organised a referendum—consultative in nature, but symbolically powerful—on the establishment of 'Republika Srpska Day', with 98.81% support (Quesada, 2016). This referendum represented the first direct challenge to the legal authority of the Bosnian state and demonstrated the effectiveness of plebiscites as a tool for mobilising identity.

In 2017, now as president of the RS, Dodik issued a decree banning the teaching of the Srebrenica massacre in public school curricula (Reuters, 2017). This measure, seen by many analysts as an attempt to rewrite collective memory, seeks to reinforce an autonomous Serb-Bosnian national identity and, at the same time, relativise the moral legitimacy of central institutions.

The next milestone came in December 2021, when the RS Assembly voted to gradually withdraw three key pillars of the common state—the judicial system, the army, and the tax administration (Sito-Sucic, 2021). This vote was the first concrete legislative step towards dismantling the federal structure and called into question the practical viability of the Dayton model.

Dodik's rise continued unabated: in November 2022, he was re-elected president of the RS, and in January 2023, he decorated Vladimir Putin during the 'RS Day' celebrations (ApNews, 2023a). The gesture was an unequivocal sign of strategic alignment with oscow and linked the local secessionist agenda with Russian geopolitical interests in the Balkans.

Faced with this dynamic, the High Representative for Bosnia and Herzegovina resorted to his 'Bonn powers' and revoked several laws adopted by the RS on the grounds that they were contrary to the Dayton Agreement (Sito-Sucic, 2021), recalling

that the Constitution does not provide for any mechanism for unilateral secession. In 2024, the Bosnian State Court opened criminal proceedings against Dodik for repeated contempt of central institutions (ApNews, 2023b), thus bringing to trial a conflict that until then had been essentially political.

Tensions reached their peak in April 2025, when RS police units blocked a state operation to execute the arrest warrant against Dodik in the vicinity of Sarajevo (ApNews, 2025). For many observers, this was the moment of greatest risk of direct violence since 1995, as it highlighted the existence of rival security forces within the same sovereign territory. Since then, the stability of the state has been perceived as contingent, subject to the ability of the international community—and the EUFOR mission—to contain possible outbreaks of violence.

The RS conflict is intertwined with the Kosovar question and the formation of a revisionist Belgrade–Budapest axis. Dodik has declared his intention to integrate the entity into the political and, eventually, military convergence between Serbia and Hungary (SwissInfo, 2025c). At the same time, he has strengthened his personal ties with Putin through frequent visits to the Kremlin and public statements hinting that Russia could offer him political asylum if legal action against him is successful (Infobae,2025b). Such links project the idea that the RS acts as a hub in a network of alliances that challenges Euro-Atlantic influence in south-eastern Europe.

Hungary and Serbia have reinforced this support structure. Despite the arrest warrant issued in Bosnia, Hungarian Prime Minister Viktor Orbán sent an official invitation to Dodik to visit Budapest (Hetzmann, 2025), giving him visibility and diplomatic legitimacy. Shortly afterwards, the Bosnian Serb leader appeared at a campaign rally alongside Serbian President Aleksandar Vučić, demonstrating the strategic harmony between the two leaders (ANSA Latina, 2025). This increasingly explicit triple convergence erodes the coherence of the European Union's Common Foreign and Security Policy and exposes Brussels' limitations in imposing unified sanctions on actors who enjoy the protection of a Member State.

The pattern that emerges from Dodik's trajectory is one of calculated escalation: he combines internal regulatory production — capable of stripping federal institutions of their powers — with historical revisionism that shapes the narrative in schools and the media, and with external alliances that provide political, diplomatic and, potentially, financial support. Although secessionist rhetoric began as an electoral tactic, since 2015 it has become a geopolitical tool with three converging functions: consolidating the SNSD's domestic power, keeping Sarajevo in a state of permanent crisis and offering Moscow a vector of influence in the Balkans.

For the Kremlin, the situation offers an asymmetric benefit: without the need to deploy troops, Russia can exploit Bosnia's institutional weakness and divert the attention of NATO and the EU at a time when both are focused on Ukraine and the north-eastern flank. Following the logic applied in Abkhazia and South Ossetia, Moscow supports a local actor who invokes self-determination, denies its own direct interference and reserves the right to provide diplomatic or energy support when it considers it strategic.

At the same time, Hungary acts as an internal spoiler within the Union, blocking sanctions initiatives and projecting a narrative that depicts Dodik as a victim of political persecution. The European Commission has warned, however, that the actions of the RS are hindering Bosnia and Herzegovina's accession process and undermining regional stability (Europa Press, 2025).

In short, the evolution of the Republika Srpska is in line with Russia's strategy of opening up 'micro-fractures' on the Euro-Atlantic periphery, but it also responds to the convergence of interests of local (Dodik), regional (Serbia and Hungary) and external (Russia) actors. Therefore, RS separatism should be interpreted less as a unilateral imposition by the Kremlin and more as the result of a shared geopolitical articulation, the persistence of which threatens to reactivate ethnic fault lines and impose a new focus of military and diplomatic attention on the EU and NATO in the Western Balkans.

4. Conflict scenarios and containment factors

Although there is no open armed conflict in the Balkans today, the region remains immersed in a logic of 'post-military conflict and pre-political conflict', particularly visible in two hotspots: Northern Kosovo and Bosnia-Herzegovina.

4.1 Northern Kosovo

Serbian and Kosovar state structures coexist in Northern Kosovo. Belgrade has never recognised Kosovo's independence and maintains direct influence over the Serb-majority municipalities—Leposavić, Zvečan, Zubin Potok, North Mitrovica, Štrpce, Klokot, Gračanica, Novo Brdo, Ranilug and Parteš—grouped together in the planned Community of Serbian Municipalities (figure 5). Under the 2013 Brussels Agreements, Serbia retains parallel institutions in the area The Goverment of the Republic of Serbia, 2013).

Figure 5. Map of the Community of Serbian Municipalities in Kosovo, according to the 2013 Brussels Agreements, 2025

The overlap of sovereignty is more pronounced in the four municipalities in the far north, adjacent to Serbian territory. There, Belgrade maintains a parallel administration thanks to local support and the reluctance of the Serbian population to fully integrate into the Kosovar system. This institutional duality generates political, identity and security tensions, as discussed in previous sections.

In this context, Serbia has mobilised military contingents on the border on several occasions. Added to this is the presence of nationalist paramilitary groups, such as Civilna Zaštita and Severna Brigada, which are classified as terrorist organisations by the Kosovar authorities (Bytyci, 2023). The resulting situation is a breeding ground for armed incidents between Pristina and pro-Serbian actors, which are likely to provoke further deployments of Serbian troops on the grounds of protecting their compatriots.

The *status quo* is therefore difficult to sustain. Without effective reintegration or formal partition, friction will persist. However, the hypothetical territorial swap—North Kosovo to Serbia and the Albanian-majority Preševo Valley to Kosovo—is unfeasible for economic reasons and due to water and energy security concerns.

Indeed, Lake Gazivoda, located entirely in Northern Kosovo, supplies a significant percentage of the country's drinking water (Sánchez, 2015) and cools the Obilić thermal power plant, which is primarily responsible for national electricity generation (France24, 2018). For this reason, authorities such as Prime Minister Albin Kurti have reiterated that the division of Gazivoda is non-negotiable (Kossev, 2025). Mutual recognition, therefore, seems unlikely in the short term.

4.2 Bosnia and Herzegovina and the Republika Srpska

In Bosnia and Herzegovina, the source of instability is Milorad Dodik's separatist rhetoric. The RS's gradual withdrawal from state military, judicial and fiscal structures, which began in 2021, is eroding the federal framework and could result in Sarajevo losing effective territorial control.

Although regional support for Dodik's project and the European Union's position have been analysed, it is worth considering the role of the United States. As the main player in NATO, Washington led the air campaign against Belgrade and was one of the first to recognise Kosovo's independence. Since then, US diplomacy has systematically leaned towards Albanian positions over Serbian ones. However, the arrival of Donald Trump introduced a degree of ambiguity: his business interests span both Serbia and Albania, and his inner circle exhibits divergent positions.

On 8 March, Secretary of State Marco Rubio condemned Dodik's actions on social media for threatening regional security. In contrast, Rudy Giuliani, a businessman close to Trump, visited Banja Luka and wore a cap with the slogan 'Make Srpska Great Again' during a speech (Rhotert, 2025). The US position is therefore ambivalent.

On the other hand, an institutional contagion effect cannot be ruled out: the Bosnian Croats, who constitute a minority within the Federation of Bosnia and

Herzegovina (figure 6), already proclaimed the Croatian Republic of Herzeg-Bosnia during the war (1992-1995), a self-declared entity that was later dissolved under the Dayton Accords. However, demands for autonomy persist within this community, reactivating secessionist sentiments and calling into question the current federal architecture.

Figure 6. Map of the Federation of Bosnia and Herzegovina 15 January 2023

Bosnian Croat nationalists argue that the Bosniak majority in the Federation marginalises them politically (SwissInfo, 2022). The Croatian National Assembly (HNS) has warned that it will promote its own autonomy if the electoral law is not reformed (Reuters, 2022). Although the Croatian proposal officially aims at greater autonomy and not secession, it shares with the RS strategy the tactic of invoking the creation of a new entity to gain influence or press for reforms, adding instability to the Balkan mosaic.

In short, the two flashpoints—Northern Kosovo and the threat of Bosnian fragmentation—are interconnected by a network of competitive alliances that make the area a veritable grey zone. Serbia projects its power in northern Kosovo and supports Banja Luka to expand its cross-border influence. Hungary, as an internal spoiler within the EU, offers diplomatic cover and blocks sanctions, while Moscow uses the Balkan chessboard as leverage to pressure the EU and NATO.

At the opposite end of the spectrum, Croatia, Albania and Kosovo converge on common interests, tacitly endorsed by KFOR and the EU's civilian dimension. Zagreb could exploit Bosnian Croat discontent to counterbalance Serbian expansion, while Tirana and Pristina seek to avoid a partition that would take Gazivoda away from them and alter the border *status quo*.

Under this scheme of cross-alliances, a localised outbreak—a confrontation in Leposavić or the collapse of the Bosnian judicial system—could trigger reputational commitments. Belgrade would be forced to defend its co-religionists; Zagreb and

Tirana would try to prevent territorial changes; Budapest, a member of the EU and NATO, would complicate a Western consensus.

Thus, latent crises today could metamorphose into interconnected conflict, recalling that in the Balkans a local spark already triggered the First World War. Regional stability will depend on the ability of the European Union and NATO to maintain credible deterrence and channel disputes into negotiating frameworks that prevent the escalation of these opposing alliances, an issue that will be addressed in the following section.

4.3 Containment factors

Although the flashpoints of tension in Northern Kosovo and Bosnia and Herzegovina are approaching critical thresholds, it is worth emphasising the continued existence of a network of containment mechanisms. Stability in the Balkans does not rest solely on the will of local actors, but on a multi-level deterrence architecture that combines European diplomacy, economic interdependence and strategic military presence. Rather than the absence of open hostilities, the region is sustained by a dynamic of 'monitored containment'.

The European Union (EU) has played the role of principal facilitator of dialogue between Serbia and Kosovo since the signing of the Brussels Agreements in 2013. Within this framework, agreement was reached, among other things, on the creation of the Association of Serbian Municipalities (ASM), the incorporation of Serbian police structures in northern Kosovo under the jurisdiction of the Kosovar Ministry of the Interior—with a Serbian regional commander—Serbia's de facto recognition of Kosovar institutions in that region, and a mutual commitment not to block each other's European integration processes (United nations, 2013).

The Brussels Agreement placed Serbia in a more favourable position to advance in the accession negotiations, a process it entered as a candidate country in 2009 (Martínez, 2009). Similarly, the prospect of EU membership is the main normative incentive for Bosnia and Herzegovina, an official candidate since 2016 (Europa Press, 2016), and for Kosovo, which submitted its formal application in 2022 (Zemeno, 2022). It is clear that none of these states will be able to complete the accession process while territorial disputes and political instability persist.

The EU has also played a direct role in crisis containment. Following the shooting in Banjska in September 2023, Brussels sent Special Representative Miroslav Lajčák, whose mediation helped to defuse the warmongering rhetoric in Belgrade and Pristina and re-establish the logic of immediate dialogue (Bajrami and Semini, 2023).

In 2023, a new normalisation agreement, known as the Ohrid Plan, was also reached, whereby the parties agreed to mutually recognise official documents, committed not to block each other in international forums, and agreed to cooperate on energy and telecommunications (Parlamento Europeo, 2023). All these advances were again led under the auspices of the EU.

Finally, the Union complements its diplomatic action with economic incentives: in 2023, it announced a €6 billion package for the Western Balkans, earmarked for Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia (Comisión Europea, 2023b). In short, the EU is not only a mediator; it constitutes the institutional and regulatory framework within which even the most nationalist actors project their expectations of economic modernisation and legitimise their own political agendas.

4.3.1 Role of the European Union as a structural mediator

Unlike ideological discourses or historical loyalties, macroeconomic indicators reveal an indisputable reality: the European Union is by far the main trading partner, investor and financial donor of Serbia, Kosovo and Bosnia and Herzegovina. This interdependence structures local economies and acts as a silent mechanism of containment against possible conflicts.

In Serbia, more than 70% of foreign direct investment comes from EU Member States, with Germany, Austria and Italy leading the way. Notable examples include the Belgrade-Niš railway corridor, financed by a €2.2 billion package of EU loans and grants (Transport Community, 2023), and the more than €800 million allocated to the modernisation of 190 kilometres of the pan-European motorway that will connect the EU-Aegean axis, consolidating Serbia as a regional logistics hub (WBIF, 2025).

Belgrade's deep integration into EU-sponsored assistance, infrastructure and development mechanisms not only modernises its economy, but also anchors it to EU regulatory standards and continental supply chains. Breaking these ties would entail political and macroeconomic costs that would be difficult to bear, even for a nationalist leadership.

From the perspective of complex interdependence, Serbia's ability to resort to force or escalate violence in Kosovo is constrained by the credible threat that Brussels will delay or reschedule aid flows, which are vital for Serbian growth and fiscal stability.

By contrast, ties with the Russian Federation—despite pan-Slavic affinity, shared Orthodoxy, and a history of support in the Kosovo war—lack a comparable structural economic counterweight. Consequently, the incentives provided by the EU function as a pragmatic safety net: Belgrade can exploit its proximity to Moscow rhetorically, but it is unlikely to risk the financial and regulatory anchorage that binds it to Brussels.

4.3.2 Military deterrence and international presence

In a region historically marked by identity conflicts, porous borders and recent memories of violence, the mere expectation of international military intervention alters the strategic calculations of local actors. Unlike other areas of global tension, the Western Balkans maintain a permanent military presence under multilateral mandates, whose objective is not only to prevent the resumption of hostilities, but also to preserve a minimum *status quo* of stability.

In this context, deterrence is not limited to the physical deployment of force, but is based on the credibility of its use. Both NATO and the European Union play a central role as guarantors of security, not only in military terms, but also in political and symbolic dimensions.

In the case of Kosovo, the *Kosovo Force* (KFOR) mission, a NATO-led multinational force, was deployed on 12 June 1999, two days after the adoption of UN Security Council Resolution 1244 (United Nations, 1999). It currently consists of approximately 4,500 troops from thirty-three countries (OTAN, 2025) and its mandate focuses on ensuring a secure environment and freedom of movement for all communities in Kosovo.

The possibility of a Serbian military incursion into Kosovar territory is severely limited by the presence of KFOR and its ability to respond immediately to threats to stability. This has been evident on several occasions, such as during the crisis between 2011 and 2013, when KFOR troops intervened in response to Serb-Kosovar protests in the north (RFERL, 2011), or during the incidents of 2023, when Prime Minister Albin Kurti requested additional reinforcements on the border with Serbia (ApNews, 2023c).

Complementing this international presence, the US base at Camp Bondsteel, located near Ferizaj in Kosovar territory, provides an additional element of strategic deterrence. Established in June 1999 following NATO's intervention, this facility operates as a logistics and command centre within the operational framework of the KFOR mission. In September 2022, troops stationed at the base were deployed in tactical exercises in response to the possibility of a deterioration in security in northern Kosovo (Siebold, 2022).

In May 2025, KFOR conducted joint manoeuvres with the United States National Guard (Wajler, 2025), demonstrating effective interoperability between military and civilian components. Camp Bondsteel thus symbolises a cohesive and functional military presence, reinforcing the message to Belgrade that any attempt at escalation would be met with a forceful response from a coalition organised under NATO mandate.

In Bosnia and Herzegovina, the EUFOR Althea mission acts as guarantor of the implementation of the Dayton Accords. This force originated in 1995 as the Implementation Force (IFOR), established by UN Security Council Resolution 1031 (United Nations, 1995c). During the first months of the post-conflict period, IFOR succeeded in preventing the resumption of hostilities.

In 1996, IFOR was succeeded by the Stabilisation Force (SFOR), created by Resolution 1088 (United Nations, 1996). Its functions included the arrest of war criminals, such as Bosnian Serb General Radislav Krstić, who was detained in December 1998 and handed over to the International Criminal Tribunal for the former Yugoslavia (IRMCT, 1998), as well as the disarmament of militias and the seizure of illegal arsenals, such as in Han Pijesak in October 2001 (OTAN, 2001).

In 2004, SFOR was replaced by EUFOR Althea under Security Council Resolution 1575 (United Nations, 2004). By that date, a unified Bosnian army had

been established and inter-ethnic violence had decreased considerably. The reduction in troop numbers, from sixty thousand in 1996 to seven thousand in 2004, reflected this development. However, EUFOR continues to operate as a stabilising factor, particularly in the face of signs of separatist tension (EUFOR, 2025).

In this regard, following the ruling against Milorad Dodik, the European Union decided to reinforce EUFOR Althea with four hundred additional troops, anticipating a possible attempt at institutional breakdown or localised unrest (Hajdari, 2025). NATO, for its part, has reiterated its support for this mission in the event of an escalation of tensions (Bne Intellinews, 2025).

In conclusion, military deterrence in the Western Balkans is not merely symbolic, but an active risk management tool. The continuity of missions such as KFOR and EUFOR Althea, together with strategic infrastructure such as Camp Bondsteel, form a multinational network of physical presence and immediate response capability. This security architecture prevents unilateral actions and raises the political and strategic cost of any attempt at escalation, thus preserving a still fragile but functional balance in the region.

5. Conclusions

This article has shown that the relative stability of the Western Balkans is not due to the overcoming of historical tensions, but to the existence of multiple containment mechanisms operating at simultaneous levels. From a theoretical perspective, the logic of the balance of power, the concept of the grey zone and complex interdependence allow us to understand the persistence of antagonistic blocs, as well as the fragility of the regional order.

Empirical analysis revealed two emerging coalitions: the Kosovo–Albania–Croatia axis, oriented towards the Atlantic, and the Serbia–Hungary–Republika Srpska axis, with Eurosceptic leanings and links to Moscow. Although these configurations generate risks of escalation, their open confrontation is mitigated by three key factors: the deterrent power of NATO and the EU (KFOR, EUFOR Althea, Camp Bondsteel), normative and economic pressure from Brussels, and the high costs of disrupting the network of regional interdependencies.

In short, the Balkans continue to inhabit a liminal space between peace and conflict. Preventing a new war depends not so much on reconciliation as on maintaining a multi-level architecture of surveillance, deterrence and external engagement, whose resilience will be key in the face of future outbreaks of tension.

In response to the central question of whether the consolidation of these antagonistic blocs increases the risk of armed conflict, this possibility does exist as it reactivates historical fractures and deepens antagonistic geopolitical alignments, especially in Northern Kosovo and the Republika Srpska.

However, this risk remains contained, but not eradicated, thanks to international military deterrence, regional interdependence and economic pressure from the EU.

Therefore, the hypothesis is partially confirmed: the risk exists and is structural, but its immediate realisation is hampered by an external architecture of containment, which, until now, has prevented open escalation.

Precisely in order to strengthen this precarious balance, it is recommended that a dual approach be reinforced, combining greater economic integration with the European Union and credible but proportionate military deterrence. Firstly, it is a priority to accelerate the tangible benefits of the accession process through visible investments in infrastructure, education and youth employment. These initiatives must be widely disseminated at the local level in order to improve public perception of the EU's role as a legitimate mediator. Linking socio-economic development with regional cooperation can weaken the nationalist narrative and foster a logic of transnational co-responsibility.

Secondly, the secessionist rhetoric of leaders such as Milorad Dodik and recent incidents in North Kosovo highlight the need to strengthen international vigilance and presence, in particular through EUFOR and KFOR, with precise mandates and expanded operational capabilities. However, this presence must be projected as a guarantor of stability and not as an occupying force, in order to avoid fuelling perceptions of grievance.

It is also recommended that formal and second-level diplomatic channels be strengthened, promoting dialogue between communities and political elites. European aid must be linked to the fulfilment of peace commitments, without neglecting the economic sustainability of fragile contexts. Finally, economic interdependence should be used as a stabilising mechanism, promoting cross-border projects that generate reciprocal costs in the event of any escalation, thus anchoring local interests to regional stability.

Bibliography

Aljazeera. (2025). Ten of thousands in Hungary defy ban to march at Budapest Pride [online]. *Aljazeera*. [Accessed: 30 June 2025]. Available at: https://www.aljazeera.com/news/2025/6/28/record-attendance-expected-at-budapest-pride-march-despite-orban-warning

ANSA Latina. (2025). El líder serbio-bosnio Dodik en mitin pro-Vucic [online]. *ANSA Latina*. [Accessed: 1 July 2025]. Available at: https://www.ansalatina.com/americalatina/noticia/ultimo_momento/2025/04/12/el-lider-serbio-bosnio-dodik-en-mitin-pro-vucic_530b1014-5df4-4c8f-96a5-21aee7e760f9.html

ApNews. (2023a). Bosnian Serbs award Putin with medal of honor [online]. *AP News*. [Accessed: 1 July 2025]. Available at: https://apnews.com/article/russia-ukraine-putin-politics-government-milorad-dodik-7edc18d0133bbde4c5b84879c0dbe724

—. (2023b). Bosnia: Ratifican acusación contra líder separatista por desafiar a enviado internacional [online]. *AP News*. [Accessed: 1 July 2025]. Available at: https://apnews.com/world-news/general-news-5173b82590b980a51112c82b282eb342

—. (2023c). Kosovo asks for more NATO-led peacekeepers along the border with Serbia [online]. *AP News*. [Accessed: 1 July 2025]. Available at https://apnews.com/article/kosovo-serbia-kfor-nato-tension-border-kurti-bf141c89dfd3a70dfa4a0c9efac9acb9

—. (2025). Tensions rise in Bosnia after reports of failed arrest attempt of Serb separatist leader [online]. *AP News*. [Accessed: 1 July 2025]. Available at: https://apnews.com/article/bosnia-tensions-serbs-arrest-a232ffb9ef8a5abfca061d083a25f9e3

Bayoud, A. (2022). Rusia refuerza su legislación LGBT en su lucha contra la "cultura occidental" [online]. *France24*. [Accessed: 30 June 2025]. Available at: https://www.france24.com/es/europa/20221124-rusia-refuerza-su-legislaci%C3%B3n-anti-lgbti-en-su-lucha-contra-la-cultura-occidental

Bajrami, F. y Semini, L. (2023). EU and US envoys urge Kosovo and Serbia to reasume dialogue in order to defuse tensions [online]. *AP News*. [Accessed: 2 July 2025]. Available at.: https://apnews.com/article/kosovo-serbia-eu-us-tension-diplomacy-08208fd52f4f6a51012259c82c2df4e0 ,

BBC News (RFERL). (2011). Kosovo Serbs stop Nato KFOR bid to dismantle roadblocks [en línea]. *BBC News*. [Accessed: 2 July 2025]. Available at: https://www.rferl.org/a/kfor_dismantling_kosovo_serb_roadblocks/24365352.html

Bickl, T. (2021). Prospects for Judicial Settlement of the Danube Border Dispute Between Croatia and Serbia [online]. *OpinioJuris*. [Accessed: 29 June 2025]. Available at: https://opiniojuris.org/2021/11/26/prospects-for-judicial-settlement-of-the-danube-border-dispute-between-croatia-and-serbia/

Bne Intellinews. (2025). NATO, EUFOR ready to prevent destabilisation of Bosnia after new secession threats [online]. *Bne Intellinews*. [Accessed: 3 July 2025]. Available at: https://www.intellinews.com/nato-eufor-ready-to-prevent-destabilisation-of-bosnia-after-new-secession-threats-368566/

Brezar, A. (2025). El presidente eslovaco, Robert Fico, asistirá al 80 aniversario del Día de la Victoria en Moscú [online]. *Euronews*. [Accessed: 30 June 2025]. Available at: https://es.euronews.com/2025/04/16/el-presidente-eslovaco-asistira-al-80-aniversario-del-dia-de-la-victoria-en-moscu

Bugajski, J. (2025). Poland seeks more effective regional formats as the Visegrad group fractures [online]. *The Jamestown Foundation*. [Accessed: 30 June 2025]. Available at: https://jamestown.org/program/poland-seeks-more-effective-regional-formats-as-the-visegrad-group-fractures/

Bytyci, F. (2023). Kosovo designates two Serb groups as terrorist organisations [online]. *Reuters*. [Accessed: 14 November 2025]. Available at: https://www.reuters.com/world/europe/kosovo-designates-two-serb-groups-terrorist-organisations-2023-06-29/

Comisión Europea. (2023a). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones* [online]. Comisión Europea. [Accessed: 19 November 2025]. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52023DC0690

—. (2023b). *Nuevo plan de crecimiento de 6 000 millones de euros para acercar los Balcanes occidentales al ingreso en la UE* [online]. Comisión Europea. [Accessed: 2 July 2025]. Available at: https://commission.europa.eu/news-and-media/news/new-eu6-billion-growth-plan-bring-western-balkans-closer-joining-eu-2023-11-08_es

Cué Barberena, F. (2023). Serbia moviliza tropas a la frontera con Kosovo [online]. *France24*. [Accessed: 26 June 2025]. Available at: https://www.france24.com/es/europa/20230526-serbia-moviliza-tropas-a-la-frontera-con-kosovo-tras-los-disturbios-por-el-bloqueo-a-alcaldes

Daily News Hungary. (2025a). Orbán y Vucic impulsan lazos energéticos más profundos entre Hungría y Serbia [online]. *Daily News Hungary*. [Accessed: 27 June 2025]. Available at. Disponible en: https://dailynewshungary.com/es/orban-vucic-energy-ties-hungary-serbia/

—. (2025b). Se construirá un nuevo oleoducto desde el país vecino hasta Hungría [online]. *Daily News Hungary*. [Accessed: 30 June 2025]. Available at: https://dailynewshungary.com/es/new-crude-pipeline-to-be-built-to-hungary/

—. (2025c). Hungría, La modernización de la línea ferroviaria Budapest-Belgrado finalizará a finales del 2025 [online]. *Daily News Hungary*. [Accessed: 30 June 2025]. Available at: https://dailynewshungary.com/es/budapest-belgrade-railway-line-end-2025/

DW. (2024). Kosovo cierra dos pasos fronterizos con Serbia [online]. *Deutsche Welle*. [Accessed: 28 June 2025]. Available at: https://www.dw.com/es/kosovo-cierra-dos-pasos-fronterizos-con-serbia/a-70161879

EFE. (2023). Tres muertos y cuatro detenidos entre los atacantes a la policía de Kosovo [online]. *EFE*. [Accessed: 28 June 2025]. Available at: https://efe.com/mundo/2023-09-24/policia-kosovar-muerto-y-otro-herido-tiroteos-gobierno-considera-terrorismo/

El Grand Continent. (2024). Dieciséis años después de la declaración de independencia de Kosovo, sigue la tensión con Serbia [online]. *El Grand Continent*. [Accessed: 26 June 2025]. Available at: https://legrandcontinent.eu/es/2024/02/17/dieciseis-anos-despues-de-la-declaracion-de-independencia-de-kosovo-sigue-la-tension-con-serbia/

EUFOR. (2025). *Common Security and Defence Policy* [online]. EUFOR. [Accessed: 19 November 2025]. Available at.: https://www.euforbih.org/images/pdfs/missionFactsheet.pdf

Europa Press. (2016). Bosnia solicita formalmente su entrada a la Unión Europea [online]. *Público.es*. [Accessed: 2 July 2025]. Available at: https://www.publico.es/internacional/bosnia-solicita-formalmente-entrada-union-europea.html

—. (2025). La UE pide a todos los actores políticos en Bosnia que renuncien a la retórica divisiva tras la condena a Dodik [online]. *Europapress*. [Accessed: 1 July 2025]. Available at: https://www.europapress.es/internacional/noticia-ue-pide-todos-actores-politicos-bosnia-renuncien-retorica-divisiva-condena-dodik-20250227133812.html

France24. (2018). Lake Gazivode, troubled Waters between Kosovo and Serbia, [online]. *France24*. [Accessed: 1 July 2025]. Available at https://www.france24.com/en/20181025-lake-gazivode-troubled-waters-between-kosovo-serbia

Gardner, L. (2025). Emergint military alliances in the Western Balkans [online]. *European Security & Defence*. [Accessed: 30 June 2025]. Available at: https://euro-sd.com/2025/06/articles/44763/emerging-military-alliances-in-the-western-balkans-a-redrawing-of-the-regional-security-map/

Grippo, M. (2024). La reunión que indignó a la UE: Putin y Orban hablando de un acuerdo entre Rusia y Ucrania [online]. *France24*. [Accessed: 30 June 2025]. Available at: https://www.france24.com/es/europa/20240705-la-reuni%C3%B3n-que-indign%C3%B3-a-la-ue-putin-y-orban-hablando-de-un-acuerdo-entre-rusia-y-ucrania

Glenny, M., (2017), *Balkans. Nationalism, War and the Great Powers, 1804-2011.* Granta *Books.*

Hajdari, U. (2025). EU sends more troops to Bosnia as Russia defends Serb leader [online]. *Político*. [Accessed: 3 July 2025]. Available at: https://www.politico.eu/article/eu-sends-troops-to-bosnia-as-russia-defends-serb-leader/

Hetzmann, M. (2025). Orbán invita al controvertido líder serbobosnio a Hungría [online]. *Daily News Hungary.* [Accessed: 1 July 2025]. Available at: https://dailynewshungary.com/es/orban-invites-bosnian-serb-dodik/

Infobae. (2021). Tensión en Kosovo y amenaza de Serbia: advirtió que "reaccionará" para proteger a sus ciudadanos [online]. *Infobae*. [Accessed: 28 June 2025]. Available at: https://www.infobae.com/america/mundo/2021/09/27/tension-en-kosovo-y-amenaza-de-serbia-advirtio-que-reaccionara-si-la-otan-no-lo-hace-antes/

—. (2024). Serbia acusa a la UE de no aceptar su ingreso por negarse a sancionar a Rusia [online]. *Infobae*. [Accessed: 30 June 2025]. Available at: https://www.infobae.com/america/agencias/2024/11/07/serbia-acusa-a-la-ue-de-no-aceptar-su-ingreso-por-negarse-a-sancionar-a-rusia/

—. (2025a). Serbia y Hungría estrechan lazos militares, tras acuerdo entre Croacia, Albania y Kosovo [online]. *Infobae*. [Accessed: 26 June 2025]. Available at: https://www.infobae.com/america/agencias/2025/04/01/serbia-y-hungria-estrechan-lazos-militares-tras-acuerdo-entre-croacia-albania-y-kosovo/

—. (2025b). Putin recibe en el Kremlin a Dodik, perseguido por las autoridades de Bosnia-Herzegovina [online]. *Infobae*. [Accessed: 1 July 2025]. Available at https://www.infobae.com/america/agencias/2025/04/01/putin-recibe-en-el-kremlin-a-dodik-perseguido-por-las-autoridades-de-bosnia-herzegovina/

International Residual Mechanism for Criminal Tribunals (IRMCT). (1998). Statement by the prosecutor regarding the detention of Radislav Krstic [online]. United Nations, International Criminal Tribunal for the former Yugoslavia. [Accessed: 3 July 2025]. Available at: https://www.icty.org/en/press/statement-prosecutor-regarding-detention-radislav-krstic

Keohane, R. O. and Nye, J. S., (1977). *Power and Interdependence: World Politics in Transition*. TBS The Book Service Ltd.

Koha. (2025a). Firma de la declaración de alianza militar entre Kosovo, Albania y Croacia [online]. *Koha*. [Accessed: 26 June 2025]. Available at: https://www.koha.net/es/arberi/kosova-shqiperia-e-kroacia-sot-nenshkruajne-deklaraten-per-aleance-ushtarake

—. (2025b). Ferrocarril Durrës – Pristina, estudio viabilidad presentado [online]. *Koha*. [Accessed: 29 June 2025]. Available at: https://koha.mk/es/hekurudha-kuqezi-durres-prishtine-prezantohet-studimi-i-fizibilitetit-balluku-nje-nyje-strategjike-e-tre-korridoreve-evropiane/

Kossev. (2025). Kurti: ZSO and the divison of Lake Gazivode are not an option [online]. Kossev. [Accessed: 1 July 2025]. Available at: https://kossev.info/en/kosovo-online-najnovije-vesti-kurti-zso-i-podela-jezera-gazivode-nisu-opcija/

Martínez, R. (2009). Serbia solicita la adhesión a la UE [online]. *El País*. [Accessed: 2 July 2025]. Available at: https://elpais.com/internacional/2009/12/22/actualidad/1261436410_850215.html

Mazarr, M. (2015). *Mastering The Gray Zone: Understanding a Changing Era of Conflict*. Lulu.com.

McAdams, L. (1998). Bosnia: New Prime Minister Defies Indifference [online]. *RadioFreeEurope RadioLiberty*. [Accessed: 30 June 2025]. Available at: https://www.rferl.org/a/1087796.html

Miolsevich, M. (2019). ¿Es Posible la reconciliación entre Serbia y la OTAN? [online]. *Real InstitutoElCano*. [Accessed: 26 June 2025]. Available at: https://www.realinstitutoelcano.org/comentarios/es-posible-la-reconciliacion-entre-serbia-y-la-otan/

Mlakar, A. (2025). Vreme Vojnih Saveza Ponovo u modi: da li slovačka postaje deo osovine Beograd – Budimpešta [online]. *Vojnopolitička Osmatračnica*. [Accessed: 14 November 2025]. Available at: https://vojnopolitickaosmatracnica.wordpress.com/2025/04/05/vreme-vojnih-saveza-ponovo-u-modi-da-li-i-slovacka-postaje-deo-osovine-beograd-budimpesta/

Nagy, M. (2025). Orbán sigue el camino de Rusia y veta la marcha del Orgullo LGTB [online]. *EuroEFE*. [Accessed: 30 June 2025]. Available at: https://www.swissinfo.ch/spa/orb%C3%A1n-sigue-el-camino-de-rusia-y-veta-la-marcha-del-orgullo-para-atraer-el-apoyo-de-ultras/89035420

Observatory Economic of Complexity (OEC). (2023a). Serbia [online]. *OEC*. [Accessed: 28 June 2025]. Available at: https://oec.world/en/profile/country/srb?selector343id=Import

—. (2023b). Croacia [online]. *OEC*. [Accessed: 28 June 2025]. Available at: https://oec.world/en/profile/country/hrv?selector343id=Import

—. (2023c). Serbia – Hungría [online]. *OEC*. [Accessed: 2026]. Available at:https://oec.world/en/profile/bilateral-country/srb/partner/hun

OTAN. (2001). *SFOR tropos find illegal arms caches* [online]. nato.int. [Accessed: 3 July 2025]. Available at: https://www.nato.int/cps/en/natohq/news_18514.htm?selectedLocale=en

—. (2024). *Kosovo Air Campaign* [online]. nato.int. [Accessed: 26 June 2025]. Available at: https://www.nato.int/cps/en/natohq/topics_49602.htm

—. (2025). *Nato's role in Kosovo* [online]. nato.int. [Accessed: 14 November 2025]. Available at: https://www.nato.int/en/what-we-do/operations-and-missions/natos-role-in-kosovo

Ozturk, T. (2024). EU Welcomes Kosovo, Serbia decisions to formally recognize each other's vehicle license plates [online]. *Aa.com*. [Accessed: 28 June 2025]. Available at: https://www.aa.com.tr/en/europe/eu-welcomes-kosovo-serbia-decisions-to-formally-recognize-each-other-s-vehicle-license-plates/3102694

—. (2025) Bosnian Serb leader says only solution for country is either a new agreement or separation [online] *Anadolu Ajansi*. [Accessed: 27 June 2025]. Available at: https://www.aa.com.tr/en/europe/bosnian-serb-leader-says-only-solution-for-country-is-either-a-new-agreement-or-separation/3515951

Parlamento Europeo. (2023) *Sobre la Evolución del diálogo entre Serbia y Kosovo* [online]. Parlamento Europeo. [Accessed: 2 July 2025]. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0372_ES.html

Peirano, N. (2025). Serbia y Hungría profundizan su vínculo con un acuerdo de cooperación militar y energía [online]. *DEFOnline.* [Accessed: 30 June 2025]. Available at: https://defonline.com.ar/internacionales/serbia-y-hungria-profundizan-su-vinculo-con-un-acuerdo-de-cooperacion-militar-y-energia/

Peregil, F. (2023). Serbia pone en alerta de combate al ejército tras enfrentamientos en municipio norte de Kosovo [online]. *El País*. [Accessed: 28 June 2025]. Available at: https://elpais.com/internacional/2023-05-26/serbia-pone-en-alerta-de-combate-al-ejercito-tras-enfrentamientos-en-un-municipio-del-norte-de-kosovo.html

Quesada, J. D. (2016). Un polémico referéndum en Bosnia trae viejos odios del pasado [online]. *El País*. [Accessed: 30 June 2025]. Available at: https://elpais.com/internacional/2016/09/24/actualidad/1474728577_740296.html

RadioFreeEurope RadioLiberty (RFERL). (2011). KFOR Dismantles Kosovo Serb Roadblocks [online]. *RadioFreeEurope RadioLiberty*. [Accessed: 2 July 2025]. Available at: https://www.rferl.org/a/kfor_dismantling_kosovo_serb_roadblocks/24365352.html

Reuters. (2017). Serb president bans teaching about Sarajevo siege, Srebrenica genocide [online]. *Reuters*. [Accessed: 30 June 2025]. Available at: https://www.reuters.com/article/world/serb-president-bans-teaching-about-sarajevo-siege-srebrenica-genocide-idUSKBN18X1SD/

—. (2022). Bosnian Croats say may push for own región unless election law changes [online]. *Euronews*. [Accessed: 1 July 2025]. Available at: https://www.euronews.com/2022/02/20/us-bosnia-election-croats

—. (2024). Explosion damages canal feeding Kosovo's main power plants [online]. *Reuters*. [Accessed: 28 June 2025]. Available at: https://www.reuters.com/world/europe/explosion-damages-canal-feeding-power-plants-northern-kosovo-2024-11-29/

Rhotert, A. (2025). ¿Cuál es el plan de Trump para los Balcanes? [online]. *DW*. [Accessed: 1 July 2025]. Available at: https://www.dw.com/es/cu%C3%A1l-es-el-plan-de-trump-para-los-balcanes/a-71882836

Ruíz, J. A., (2010). *Balkans: Europe's Open Wound: Conflict and Reconstruction of Coexistence*. Plaza y Valdes, S.L.

Sánchez, P. (2015). *Kosovo, ¿el camino hacia…? (Parte II). Documento análisis* [online]. Instituto Español de Estudios Estratégicos. Pp. 10-11. [Accessed: 28 June 2025]. Available at: Disponible en: https://www.ieee.es/Galerias/fichero/docs_analisis/2015/DIEEEA22-2015_Kosovo-Camino_hacia_ParteII_PSH.pdf

Santos, J. C. (2022). Albania modernizará con ayuda de la OTAN su base aérea en Kuçovë [online]. *Euronews*. [Accessed: 29 June 2025]. Available at: https://es.euronews.com/2022/03/20/albania-modernizara-con-ayuda-de-la-otan-su-base-aerea-de-kucove

Siebold, S. (2022). NATO brings reserve troops to Kosovo for training amid fears of unrest [online]. *Reuters*. [Accessed: 3 July 2025]. Available at: https://www.reuters.com/world/europe/nato-brings-reserve-troops-kosovo-amid-serb-unrest-2022-09-21/

Sito-Sucic, D. (2021). Serbs vote to start quitting Bosnia's key institutions in secessionist move [online]. *Reuters.* [Accessed: 30 June 2025]. Available at: https://www.reuters.com/world/europe/serbs-vote-start-quitting-bosnias-key-institutions-secessionist-move-2021-12-10/

—. (2023). Bosnia envoy revokes Bosnian Serb Laws defying the state, peace deal [online]. *Reuters*. [Accessed: 1 July 2025]. Available at: https://www.reuters.com/world/europe/bosnia-envoy-revokes-bosnian-serb-laws-defying-state-peace-deal-2023-07-01/

Stojanovic, M. (2025). Can the new document on defence cooperation between Serbia and Hungary be interpreted as "military Alliance"? [online]. *European Western Balkans*. [Accessed: 14 November 2025]. Available at: https://europeanwesternbalkans.com/2025/04/04/can-the-new-document-on-defence-cooperation-between-serbia-and-hungary-be-interpreted-as-a-military-alliance/

SwissInfo. (2022) En una Bosnia fracturada, los croatas también presionan [online]. *SwissInfo*. [Accessed: 1 July 2025]. Available at: https://www.swissinfo.ch/spa/en-una-bosnia-fracturada-los-croatas-tambi%C3%A9n-presionan/47416508?utm_source=chatgpt.com

—. (2025a). Los serbobosnios pedirán unirse al pacto militar con Serbia y Hungría, según Dodik [online]. *SwissInfo*. [Accessed: 26 June 2025]. Available at: https://www.swissinfo.ch/spa/los-serbobosnios-pedir%C3%A1n-unirse-al-pacto-militar-con-serbia-y-hungr%C3%ADa%2C-seg%C3%BAn-dodik/89116546

—. (2025b). Albania, Croacia y Kosovo profundizan cooperación militar en medio de tensiones regionales [online]. *SwissInfo*. [Accessed: 28 June 2025]. Available at: https://www.swissinfo.ch/spa/albania%2C-croacia-y-kosovo-profundizan-cooperaci%C3%B3n-militar-en-medio-de-tensiones-regionales/89028542

—. (2025c). Los serbobosnios pedirán unirse al pacto militar con Serbia y Hungría, según Dodik [online]. *SwissInfo*. [Accessed: 1 July 2025]. Available at: https://www.swissinfo.ch/spa/los-serbobosnios-pedir%C3%A1n-unirse-al-pacto-militar-con-serbia-y-hungr%C3%ADa%2C-seg%C3%BAn-dodik/89116546

The Goverment of the Republic of Serbia. (2013). Brussels Agreement [online]. *srbija.gov.* [Accessed: 1 July 2025]. Available at:https://www.srbija.gov.rs/specijal/en/120394

Traynor, I. (2011). Bosnia in worst crisis since war as Serb leader calls referéndum [online]. *The Guardian*. [Accessed: 30 June 2025]. Available at: https://www.theguardian.com/world/2011/apr/28/bosnia-crisis-serb-leader-referendum

Transport Community. (2023). Modernisation of Corridor X Railway [online]. *Transport Community*. [Accessed: 2 July 2025]. Available at: https://www.transport-community.org/news/modersnisation-of-corridor-x-railway/

Thucydides. (2014). *History of the Peloponnesian War (The Pocket Book – Classics of Greece and Rome*). Alianza Editorial.

TVPWorld. (2024). Hungary, Slovakia and Serbia want more funds to combat ilegal migration [online]. *TVP World*. [Accessed: 30 June 2025]. Available at: https://tvpworld.com/83103303/hungary-slovakia-and-serbia-want-more-funds-to-combat-illegal-migration-

United Nations. (1995a). *Basic Agreement On the Region of Eastern Slavonia, Baranja And Western Sirmium (Erdut Agreement)* [online]. UN Peacemaker. [Accessed: 2026]. Available at: https://peacemaker.un.org/en/node/9387

—. (1995b). *General Framework Agreement for Peace in Bosnia And Herzegovina (Dayton Agreement)* [online]. UN Peacemaker. [Accessed: 2026]. Available at: https://peacemaker.un.org/en/node/9388

—. (1995c). *Resolución 1030 del Consejo de Seguridad de las Naciones Unidas* [online]. Consejo de Seguridad de Naciones Unidas. [Accessed: 3 July 2025]. Available at: https://docs.un.org/es/S/RES/1031(1995)

—. (1996). Resolución 1088 del Consejo de Seguridad de las Naciones Unidas [en línea]. Consejo de Seguridad de Naciones Unidas. [Consulta: 3 julio 2025]. Disponible en: https://docs.un.org/es/S/RES/1088(1996)

—. (1999). *Resolución 1244 del Consejo de Seguridad de las Naciones Unidas* [online]. Consejo de Seguridad de Naciones Unidas. [Accessed: 2 July 2025]. Available at: https://docs.un.org/es/S/RES/1244(1999)

—. (2004). *Resolución 1575 del Consejo de Seguridad de las Naciones Unidas* [online]. Consejo de Seguridad de Naciones Unidas. [Accessed: 3 July 2025]. Available at: https://docs.un.org/es/S/RES/1575(2004)

—. (2013). *First Agreement of Principles Governing The Normalization of Relation (Brussels Agreement)* [online]. UN Peacemaker. [Accessed: 2 July 2025]. Available at: https://peacemaker.un.org/en/node/9756

Vozpópuli. (2025). La UE le recuerda a Kosovo que para entrar en la Unión debe normalizar sus relaciones con Serbia [online]. *Vozpopuli*. [Accessed: 28 June 2025]. Available at: https://www.vozpopuli.com/internacional/la-ue-recuerda-a-kosovo-que-debe-normalizar-relaciones-con-serbia-para-entrar-en-la-union-sg.html

Waltz, K.N., (1979). *Theory of International Politics*. McGraw-Hill

Wajler, G. (2025). Army Guardsmen Conduct Training with Kosovo Search and Rescue Association [online]. *National Guard*. [Accessed: 3 July 2025]. Available at: https://www.nationalguard.mil/News/Article-View/Article/4204358/army-guardsmen-conduct-training-with-kosovo-search-and-rescue-association/

Western Balkans Investment Framework (WBIF). (2025). Corridor X Motorway (E-75 & E-80) in Serbia [online]. *Western Balkans Investment Framework*. [Accessed: 2 July 2025]. Available at: https://www.wbif.eu/project-detail/PRJ-SRB-TRA-005?utm_source=chatgpt.com

Zemeno, A. (2022). Kosovo presenta su solicitud oficial de adhesión a la UE a pesar del conflicto con Serbia [online]. *Euronews*. [Accessed: 2 July 2025]. Available at: https://es.euronews.com/2022/12/15/kosovo-presenta-su-solicitud-oficial-de-adhesion-a-la-ue-a-pesar-del-conflicto-con-serbia

Zuvela, M. (2015). Biggest Serb party in Bosnia threatens 2018 secession [online]. *Reuters*. [Accessed: 30 July 2025]. Available at: https://www.reuters.com/article/world/biggest-serb-party-in-bosnia-threatens-2018-secession-idUSKBN0NG0NB/

Article received: 7 July 2025
Article accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Rouhollah Iran Shahy
Assistant Professor, Doctor and Researcher at the Universidad Politecnica de Madrid

Email: r.iran@upm.es

Sonia Benito Hernández
Full professor and researcher at the Polytechnic University of Madrid

Email: sonia.benito@upm.es

Economic Islamism as a strategy of political legitimation in Iran

Abstract

This paper analyses economic Islamism based on the Iranian experience after the 1979 Revolution, focusing on the theocratic conception of power formulated by Ayatollah Ruhollah Khomeini in his doctrine of Velayat-e Faqih. According to this doctrine, the preservation of the Islamic state takes precedence over any religious duty or moral imperative. The research asks whether the Islamisation of the economy constitutes a viable model of economic organisation or whether, on the contrary, it operates as an ideological strategy aimed at legitimising political power. To this end, the tensions between Islamic economics and modern social sciences are examined. The study is based on a comparative documentary analysis, supported by the analysis of primary and secondary sources. The study concludes that economic Islamisation in Iran does not offer a solid alternative to current economic systems. Instead of promoting inclusive and sustainable development, the model has tended to consolidate structures with authoritarian and exclusionary features, limiting innovation, restricting epistemological pluralism and favouring increasing social fragmentation, which poses serious challenges for the articulation of more just, inclusive and rational economic models.

Keywords

Islam, Economy, Velayat-e Faqih, Taqiyya, Social sciences

Cite this article:

Iran Shahy, R. and Benito Hernández, S. (2025). Economic Islamism as a strategy for political legitimisation in Iran. *Journal of the Spanish Institute for Strategic Studies*. 26, pp. 491-520.

1 Introduction

This research offers an analysis of economic Islamism, focusing on the case study of Iran after the 1979 Revolution. The starting point is the conception of political Islam formulated by Ayatollah Khomeini in *Velayat-e Faqih* (1970). According to this doctrine, the state is one of the fundamental principles of Islam, and this guiding principle prevails over all others (Khomeini, 1999).

Various authors have questioned this Islamisation of the social and economic sciences, from the imposition of religious authorities without academic training in university and administrative spaces to the restriction of critical debate. In the words of Sorush (2010), 'this Islamisation aims to be the last trench against secularisation', as it lacks methodological support by not incorporating modern analytical tools. In this context, the exclusion of dissenting voices favours a discursive monopoly that hinders the advancement of scientific thought. The official perspective, as pointed out by Khamenei (2009)[1] , accuses Western social sciences of being based on materialism and atheism. This position seems to reflect more a fear of political secularisation than a solid epistemological alternative.

Political Islam, as has been the case throughout history with other religions and states in the past, has been linked to expansion by force. According to Zarrinkub (1957), conquered peoples were reduced to conditions of civil and social inferiority, and the Muslim faith determined access to property and basic rights. This logic finds continuity in certain currents of contemporary Islamism, where concepts such as jihad and struggle are interpreted by some groups as legitimate means to achieve spiritual rewards and consolidate political and economic influence.

In this context, the Islamic economy is presented as an alternative to current economic systems, although it has not yet developed its own method based on scientific criteria. The study of economic Islamism is relevant because it proposes a unique model that aims to present itself as an alternative to contemporary economic systems, but which in practice generates profound contradictions between theory and reality. The Iranian experience illustrates how, in certain contexts, the subordination of the economy to religious and political priorities can contribute to the emergence of structural challenges in development, as well as to phenomena of social exclusion and institutional weakness. Furthermore, academic analysis of this model opens up a broader debate on the relationship between religion, politics and economics in contemporary contexts.

In this context, the question guiding this research is: to what extent can the process of Islamisation of the economy in Iran be considered a viable model of economic organisation, or does it mainly respond to an ideological strategy aimed at legitimising and maintaining political power? To answer this question, the work is structured through an analytical progression from the general to the specific.

1 'Many disciplines in the humanities are based on philosophies founded on materialism and disbelief in divine and Islamic teachings. Teaching them causes a lack of faith in divine and Islamic teachings' (Khamenei, 2009).

Following the introduction, the methodological approach used and the criteria for selecting primary and secondary sources are presented. Next, the theoretical and historical framework situates economic Islamism in relation to the classic debates on religion and economics. On this basis, the text develops three blocks of analysis: first, the tension between Islamic economics and modern social sciences; second, concrete economic practice in Iran, with special attention to the financial system, property, and the patronage network; and third, the ideological foundations and their structural consequences, synthesised through comparative tables. Finally, the discussion and conclusions summarise the main findings, contrasting them with alternative models and proposing lines of future research.

2 Methodological approach

This research adopts a comparative and analytical approach to economic Islamism in Iran, contrasting official discourse with its practical application in the post-revolutionary context. This approach allows us to identify the tensions between religious ideology and economic rationality, as well as the structural consequences that derive from this contradiction.

From a methodological point of view, a documentary analysis of primary sources is used, including speeches by religious leaders, the Constitution of the Islamic Republic of Iran, legal texts and institutional communiqués, as well as secondary sources such as specialised academic literature, critical studies and contributions by Iranian and Western authors. This strategy allows for an analysis of economic Islamism as a device for political legitimisation, beyond its doctrinal formulation.

The methodological approach is part of the tradition of ideological and discursive analysis, based on the premise that economic practices are deeply linked to the symbolic and normative frameworks that underpin them (Thompson, 1990). From this perspective, it is argued that economic Islamism is not an economic theory in the strict sense, but rather an ideological construct aimed at normalising the economy from a theological perspective. To address this dimension, tools of critical discourse analysis (Fairclough, 1992) are used to explore how power relations, exclusion and legitimisation are articulated in political-religious language.

A historical-comparative perspective is also incorporated, which allows economic Islamism to be contextualised in relation to other models of economic organisation such as liberalism and centralised planning, as well as experiences of modernisation in other Muslim countries. To this end, analytical criteria have been established that structure the comparison around key thematic axes, such as the conception of property, the principle of scarcity, the role of the state, the inclusion of minorities, the epistemology of knowledge and the instrumentalisation of coercion in processes of political-religious legitimation. These criteria are applied systematically in the comparative tables included in sections 5 and 6, allowing us to visualise the structural differences between the Iranian model, economic liberalism, centralised planning, and other religiously based moral economies such as the Catholic and Protestant models and economic Buddhism.

This methodological strategy not only facilitates the identification of ideological patterns, but also enriches the analysis by placing economic Islamism in a broader framework of normative alternatives. This comparison does not seek to establish normative hierarchies, but rather to highlight the possible structural limitations of the Iranian model in the face of contemporary challenges of inclusion, efficiency and pluralism.

The theoretical framework draws on classical and contemporary authors who have reflected on the relationship between religion, economics and power. Weber (1905) contributes the notion of religious rationalisation, which is useful for understanding how certain doctrines can influence economic organisation. Polanyi (1957) introduces the concept of the 'embeddedness' of the economy in social and cultural structures, which allows us to analyse the subordination of the economic to the religious in Islam. Robbins (1932) defines economics as the science that studies the allocation of scarce resources, which is key to critically evaluating the denial of scarcity in Islamist discourse. Finally, Huerta de Soto (2005) offers a liberal perspective on the role of business, market efficiency and the risks of ideological interventionism, which allows us to understand the practical consequences of the Iranian model.

This methodological approach allows us to analyse economic Islamism not only as a normative doctrine, but also as a system of power that affects economic rationality, social inclusion and institutional viability. The combination of empirical analysis, theoretical reflection and comparative contrast seeks to offer an evaluation of the Iranian model, in dialogue with contemporary social sciences and with the principles of justice, pluralism and rationality that guide modern economies.

In terms of the source selection strategy, priority has been given to those with a direct impact on the institutionalisation of the model after the 1979 revolution. In the case of secondary sources, academic studies published in indexed journals and monographs of recognised prestige, by both Iranian and Western authors, were selected. The validity criteria were based on theoretical relevance, the topicality of the debate and presence in international academic literature. This dual selection sought to ensure a balance between the internal voice of Islamism and external critical perspectives. In the case of Iranian authors, priority was given to intellectuals with a recognised track record in the debate on the Islamisation of knowledge. Likewise, critical voices from within the Iranian system itself have been incorporated, providing access to an internal and nuanced view of the phenomenon under study. This choice seeks to avoid an exclusively exogenous or Westernised reading of economic Islamism and to ensure a balanced analysis that considers both doctrinal justifications and objections raised by contemporary Islamic thought.

3 Theoretical and historical framework

This section develops the theoretical and historical framework within which economic Islamism is situated, in order to place the object of study within the broader academic debates on the relationship between religion and economics. First, it presents the general theoretical foundations that, from sociology, anthropology

and secularisation theory, have enabled us to understand the role of religion in shaping economic life. These classical and contemporary approaches, from Weber and Durkheim to Casanova, Polanyi and Iannaccone, provide an indispensable conceptual background for interpreting the emergence of economic Islamisation projects. Secondly, the specific context of Iranian Islamism is addressed, analysing the ideological formulations that underpin it, in particular the theocratic conception of power defended by Khomeini, the practice of *taqiyya (ketman)*, the logic of religious exclusion and the proposal for a third economic way developed by Al-Sadr (1961). This overview provides an understanding of both the historical roots and the normative nature of the Islamic economy in Iran, paving the way for an examination, in the following sections, of contemporary critiques of its scientific and practical viability.

3.1 General foundations

The relationship between religion and economics has been the subject of reflection since the origins of modern social sciences. The classics of sociology and economics have already emphasised that economic systems cannot be understood in isolation, but are deeply conditioned by the values, beliefs and institutions of each society. In this sense, economic Islamism can be understood as part of a broader debate on the role of religion in shaping social life and, in particular, in organising economic activity.

Weber (2001), in his famous work *The Protestant Ethic and the Spirit of Capitalism*, showed how certain religious values, such as work ethic, asceticism and the moral rationalisation of everyday life, had a decisive influence on the emergence of modern capitalism. For Weber, Calvinist Protestantism contributed to generating an attitude towards work and accumulation that made possible the development of a rationalised, profit-oriented economic system. Although the Islamic case is very different, Weber's approach invites us to consider how religious conceptions can legitimise or condition certain forms of economic organisation. Durkheim (1993), for his part, analysed religion as a total social fact that structures collective life, generating norms, values and solidarity. From this perspective, religion not only influences the economy indirectly, but also constitutes the basis for forms of cooperation and redistribution. The notion of 'mechanical solidarity' (Durkheim, 1893) can help us understand how, in traditional contexts, religion articulates economic practices that reinforce group cohesion. This concept is based on the idea of social cohesion in traditional or primitive societies, where individuals share very similar values, beliefs, customs and roles. Durkheim contrasts mechanical solidarity with organic solidarity, which appears in modern, industrialised societies. In these societies, cohesion is based on the interdependence between individuals with specialised and differentiated functions. Collective consciousness is weaker, but cooperation occurs out of mutual necessity.

Later, Parsons (1966) revisited this line of thinking to propose that economic systems are always embedded in a normative-cultural framework that legitimises institutions and guides social action. According to Parsons, religions offer a system of values that stabilises expectations in economic exchange, reinforcing trust and

cooperation. This is particularly relevant in the case of Iran, where religion acts not only as a moral framework but also as the organising principle of the economic-political system.

The literature on secularisation also provides a useful framework for understanding the Islamisation of the economy. According to Berger (1967), modernity tends to reduce the role of religion in social life, shifting its influence to the private sphere. However, as Casanova (1994) has pointed out, this process is neither linear nor irreversible: in many contexts, religions have responded to modernity through processes of 'deprivatisation', that is, by actively reinserting themselves into public and political life. Islamism can be interpreted as a reaction of this kind: in the face of secular modernisation, it seeks to reinstate religion as the guiding principle of social organisation, including the economy. From this perspective, the Islamisation of the economy in Iran is not an isolated phenomenon, but part of a global dynamic in which religions are reclaiming their ability to order social life in the face of the challenges of modernity.

In parallel, economic anthropology offers tools for understanding the specificity of economic Islamism. Polanyi (1957) argued that in pre-modern societies, the economy was embedded in social, political and religious institutions, and that it was only in modernity that a progressive separation between economy and society took place. Dalton (1976) and other authors expanded on this idea, showing that categories such as 'scarcity', 'market' and 'efficiency' are historical constructs, not universal realities. Islamic economics, being based on normative and religious principles, can be understood as an attempt to maintain this relationship, refusing to accept the autonomy of the economy as a separate sphere.

Another relevant approach is that of the economics of religion, developed in recent decades from rational choice theory. Iannaccone (1998) argues that religious behaviour can be analysed using the same tools as other areas of social action, considering individuals as agents seeking to maximise spiritual and social benefits in relation to costs and constraints. From this perspective, religious institutions can operate strategically to preserve the loyalty of believers, offering symbolic goods in exchange for obedience and material contributions. Applied to the Iranian case, this framework allows us to interpret economic Islamism not only as a moral doctrine, but also as a mechanism for controlling and mobilising resources for the benefit of religious elites.

Contemporary political theory has also addressed the link between religion and economics. Authors such as Habermas (2008) have highlighted the persistence of religion in the public sphere, pointing out that, far from disappearing, religions continue to offer frameworks of meaning that influence social and economic debates. In this context, Islamism represents a particular form of 'public religion' which, beyond contributing values, seeks to directly regulate economic and political organisation.

Taken together, these perspectives allow us to broaden the theoretical framework of economic Islamism in Iran. From Weber to Casanova, via Polanyi and the economics

of religion, we can see that the articulation between religion and economics is not an Islamic anomaly, but a recurring possibility in various historical contexts. What is distinctive about Iranian Islamism is that it takes this articulation to its ultimate conclusion, subordinating the economy to religious principles and using it as a central component in the construction of political legitimacy.

3.2 Foundations of economic Islamism

Economic Islamism, as articulated in Iran since the 1979 revolution, is based on a theocratic conception of power that guides all spheres of social life, including the economy, towards religious principles, subordinating its functioning to religious authority. This vision finds its most influential formulation in the work of Ayatollah Khomeini, particularly in his political-legal treatise *Velayat-e Faqih* (1970). According to Kadivar (2023), the absolute guardianship of the jurist (*velayat-e faqih al-mutlaqa*) maintains that the jurist has broad powers in the administration of society, with the aim of applying the religious principles of Islam. From this perspective, the jurist can even suspend religious, moral or legal norms if he deems it necessary to preserve the interests of the Islamic state. In this model, the government of the religious guardian takes precedence over other normative sources, including religious, moral or constitutional laws. This interpretation of *velayat-e faqih* represents a particular view of Ayatollah Khomeini and some of his disciples, implemented after the Islamic Revolution of 1979 and maintained by his successor in the current Islamic Republic of Iran. Kadivar criticises this conception as incompatible with the principles of justice, rationality and popular sovereignty present in Islamic thought, and for favouring a concentration of religious power with authoritarian features.

The logic of political Islamism is articulated around a series of key concepts that contribute to justifying the subordination of different social spheres to religious power. One of the most relevant is that of *taqiyya (Ketman)*, traditionally understood as 'dissimulation' and deception in defence of Islam, but which in the context of the Iranian regime has been reinterpreted as a tool of governance. This practice, which originally served to protect Shiite minorities from persecution, has evolved into a political strategy that allows tensions between religious discourse and institutional practice to be managed. In the name of preserving Islam, certain discursive ambiguities are tolerated, dissent is restricted and ethical principles are relaxed, raising questions about the normative coherence of the model. As Khomeini (1999) points out, 'when Islam is in danger, everything is permitted', a statement that has been interpreted by some sectors as legitimising the relaxation of certain ethical principles in order to preserve the Islamic order. According to various perspectives, this logic has contributed to the emergence of dynamics that affect institutional transparency, erode social trust, and weaken the economic fabric.

Faith, in this context, is not limited to a spiritual experience, but acquires a political dimension by becoming a criterion for inclusion or exclusion within the political-economic system. Only those who demonstrate loyalty to the regime have preferential access to resources, jobs and rights, while non-Muslims or those considered doctrinally

deviant are treated with restrictions that limit their full participation in public life (Lewis, 2002). In this context, the economy is configured as an instrument of ideological consolidation, geared more towards guaranteeing the hegemony of political Islam than towards social welfare. This contradiction becomes evident when contrasting the promises made by Khomeini himself upon his return from exile in 1979, when he assured that, under the new Islamic order, the most disadvantaged sectors would have free access to water, electricity and transport (IranWire, 2021). These social promises, aimed at garnering popular support, were subsequently displaced by a more restrictive political-religious project. Khomeini's famous phrase, 'We did not make a revolution to lower the price of melons [...]' (Dabashi, 2006), clearly summarises the primacy of ideological objectives over material demands, revealing a conception of economic power subordinate to the consolidation of the theocratic regime.

This subordination of economic power is also reflected in the Iranian Constitution. For example, Article 43 prohibits waste, while Article 49 establishes situations in which property can be confiscated, not only that obtained through procedures considered illegal by Westerners, but also through usury or uncultivated land. Property, in this framework, is not conceived as a right, but as a divine grace (*Farrah-ye Izadi*), a privilege that can be taken away by the political-religious authority. After the 1979 Revolution, this conception served as justification for confiscating not only the property of the Shah's family, but also that of all individuals or legal entities that the new regime considered to have collaborated in some way with the deposed monarch. This conception raises a question about long-term planning: if there are no guarantees of property rights, what is the point of working and accumulating assets to pass on to future generations? Thus, it becomes clear once again how the economy is subordinated to the ideological objectives of the regime, rather than to the material well-being of the population.

The historical roots of this concept date back to an idealisation of the Islamic past, especially the Arabia of the Prophet Muhammad. The ideologues of economic Islamism, such as Al-Sadr, have attempted to construct an Islamic economy based on principles drawn from medieval contracts and the commercial practices of early Islam. In his work *Our Economy*, Al-Sadr (1961) proposes a third way between liberalism and centralised planning, based on social justice, the prohibition of usury (*riba*) and the redistribution of wealth. However, this proposal has methodological limitations with regard to modern economic institutions. As some approaches in economic anthropology point out, pre-modern economies did not know concepts such as competitive markets, productive efficiency or profit maximisation (Polanyi, 1957; Dalton, 1976). Islamic economics, according to its advocates, is based on religious texts and the idealisation of social structures that no longer exist in the contemporary context.

3.3 Contemporary debates on the Islamisation of the economy

Having reviewed the general foundations of the relationship between religion and economics, as well as the ideological basis of economic Islamism in the Iranian case, it is pertinent to address the debate that this model has sparked in academia.

The idea of Islamising the sciences emerged in the 1980s, when Hosseini founded the Academy of Islamic Sciences with the aim of incorporating Islamic principles into various disciplines, from economics to physics. Hosseini argued that the experimental sciences and modern humanities, developed in Western contexts, reflect a worldview centred on human interests rather than the search for universal truth. He therefore considered that Western knowledge is not neutral but oriented towards specific ends, and that it should be reformulated in the light of an epistemology inspired by Islamic values. This proposal poses an epistemological challenge by attempting to reconcile contemporary scientific knowledge with normative frameworks derived from religious tradition (Ladier-Fouladi, 2024).

Amoli Larijani (Jamaran, 2018), current president of the Expediency Discernment Council of the Islamic Republic of Iran, argues that the thesis of the impartiality of science corresponds to an outdated conception, typical of 18th-century Enlightenment thinking. In his opinion, it is unfeasible to separate science from values or ideology, since all forms of knowledge are influenced by the beliefs and cultural conditions in which they are produced. He therefore defends the possibility of Islamising the sciences, arguing that even in the West, currents such as Hans-Georg Gadamer's hermeneutics have questioned the positivist idea of a completely objective or neutral science (Gama, 2021). From this perspective, the Islamisation of knowledge would not be considered a failure, but rather a long-term philosophical and theological project that requires greater investment and academic development.

In contrast, former Iranian President Rouhani takes a critical stance on the division between Islamic and non-Islamic sciences. For him, science is a universal field that does not depend on ideologies or religious beliefs, and he considers it inappropriate to seek the origin of each discipline in the Qur'an or Islamic traditions. Rouhani is ironic about attempts to formulate an 'Islamic physics' or 'Islamic chemistry', pointing out that disciplines such as mathematics, physics and algebra are governed by their own laws that transcend doctrinal differences (Flaquer, 2024).

This debate reflects two opposing views within contemporary Iranian thought: on the one hand, the theological and culturalist position of Amoli Larijani, who defends an epistemology anchored in religious values (Ladier-Fouladi, 2024); and on the other, the rationalist and pragmatic stance of Rouhani, who defends the autonomy of scientific knowledge from ideology. Ultimately, this discussion reveals a structural tension in the Islamic Republic's project: the search for an 'Islamic' scientific identity in a globalised environment marked by Western epistemological paradigms (Flaquer, 2024).

These conflicting views are also reflected in the economic sphere and in public life. On the one hand, traditional fundamentalists and conservatives, who control vast resources through foundations or *bonyads* and contributions from places of worship, are reluctant to embrace any form of market economy. On the other hand, pragmatic conservatives and so-called 'liberals', although dependent on the state, do not exercise the same degree of control over resources, which makes them more inclined towards open-minded positions—within the narrow margins allowed by the Iranian system, of course.

Derakhshan (Hadana, 2015), founder and president of the Faculty of Islamic Sciences and Economics at Imam Sadiq University, argues that the main problem lies not in the Islamisation of the economy, nor in the need to transform Islamic jurisprudence, but in modern economic sciences themselves and the way in which specialists approach these issues. From his perspective, the difficulty lies in economists' lack of adaptation and deep understanding of Islamic principles, rather than in the rigidity of religious law itself. This view argues that, in order to move towards a truly Islamic economy, it is essential for economic experts to develop a more integrated and contextualised knowledge, rather than attempting to modify the theoretical foundations of economics or jurisprudence. Various intellectuals, both inside and outside Iran, have pointed out the epistemological and methodological limitations of the project of Islamising knowledge, as well as its possible effects on scientific and social development. These reflections allow us to put the viability of the Islamic economic model into perspective and understand it not only as a normative proposal, but also as a political device that presents significant internal tensions.

The lack of methodological rigour has been analysed by numerous Iranian intellectuals. For Sorush, an Islamic economy cannot be limited to reproducing formulas inherited from the past, but must be subjected to empirical and analytical evaluation. Otherwise, he warns, it runs the risk of becoming a dogmatic discourse that hinders independent thinking and consolidates a closed ideological vision. Along the same lines, Moghadami (2014) has pointed out that the appointment of religious authorities without academic training to university and administrative positions has 'stifled the social sciences', hindering the construction of a pluralistic and rigorous debate on the country's economic challenges. This reflection is echoed by Ayatollah Alavi Boroujerdi (EcoIran, 2023), who argues that Islamic economics 'is not classified as a science and does not possess scientific characteristics', as it tends to shift 'what is' towards 'what should be', which hinders its empirical evaluation and limits its development as an autonomous discipline. According to Boroujerdi, economics in Islam must be based on reason and the rational behaviour of intellectuals, filtered through the general principles of Sharia law. Although he acknowledges the existence of some religious guidelines (approximately twenty economic principles), he believes that most decisions should be based on experience and practical logic. Boroujerdi also questions the authority of religious leaders in economic matters, emphasising that Islamic jurisprudence can establish ethical standards but cannot generate scientific knowledge in the strict sense. Within this framework, he advocates delegating economic management to experts and proposes moving towards a rational economy based on principles shared by wise minds, beyond ideological labels.

One of the most recurrent observations about Islamic economics focuses on the tension between its rejection of the notion of scarcity and the practice of wealth accumulation by certain privileged sectors. From a doctrinal perspective, Islam maintains that divine creation guarantees abundance and that scarcity is not a real economic problem, but rather an ideological construct of capitalism (Al-Sadr, 1961). This view is reflected in the figure of *Homo Islamicus*, an individual who trusts in providence and directs his economic actions towards the fulfilment of religious

duties rather than the rational maximisation of resources. According to Furqani and Echchabi (2022), this economic agent is defined by his ethical responsibility, his orientation towards collective well-being and his obedience to revealed principles, in contrast to the individualism of *Homo Oeconomicus*. However, as Moghadami (2014) and Kuran (2008) have pointed out, in practice Islamist regimes promote the concentration of wealth in the hands of religious figures and merchants allied with power, generating exclusion and social inequality. Thus, the rejection of scarcity as a scientific category coexists with a system of privileges and wealth accumulation that calls into question the principles of distributive justice proclaimed in official discourse. On the other hand, as Rudnyckyj (2011) warns, neither *Homo Oeconomicus* nor *Homo Islamicus* exist *a priori*; both are effects of specific historical configurations. To claim that one of them represents true human nature may limit the development of a scientific economy.

In short, the theoretical and historical framework of economic Islamism in Iran reveals a deep tension between religious ideology and the demands of the modern economy. Contemporary authors such as Sorush, Alavi Boroujerdi and other reformists have pointed out these contradictions, and in particular Yousefi and Abizadeh, in *An Essay on Economics and Ideology: The Case of Iran*, have analysed how many of the economic problems following the Revolution cannot be explained solely by structural factors, but are conditioned or intensified by an ideology that shapes social and economic orders beyond pragmatic criteria. From this perspective, it can be seen that under ideological influence, principles of efficiency are sacrificed, income distribution is distorted, and collective welfare objectives are subordinated to political-religious goals, to the detriment of more universal scientific and economic approaches. These observations not only highlight the internal tensions of the model, but also open the door to a broader reflection on the need to de-ideologise the economy and recover its scientific, pluralistic and common welfare-oriented dimension.

4 Islamic economics vs. social sciences

The emergence of Islamic economics as an autonomous discipline within political Islam has sought to offer an alternative to existing economic systems. However, this proposal has generated significant tensions with modern social sciences, especially with regard to its methodology, its conception of the economic subject and its relationship with epistemological pluralism. The result has been an ideologised economy with little connection to the fundamental principles of economic science and difficult to reconcile with the analytical frameworks of contemporary social sciences.

According to Al-Sadr (1961), Islam proposes an economic model based on principles of social justice, redistribution of wealth and the prohibition of usury (*riba*). This conception, however, is constructed mainly from a normative interpretation of religious texts, rather than from an empirical theory supported by a systematic methodological apparatus. As Kuran (2008) points out, Islamic economics did not initially emerge as a scientific discipline in the strict sense, but rather as an ideological response aimed at counteracting the cultural and economic influence of

the West and strengthening the role of religious leaders in Muslim societies. In this context, its evolution has been deeply intertwined with political dynamics rather than conventional scientific developments.

By adopting a critical stance towards some of the fundamental tenets of modern economics, Islamic economics occupies a unique position within the spectrum of social sciences. One of the most significant points of tension lies in its rejection of epistemological pluralism. The so-called 'Islamisation of knowledge' tends to privilege a unified worldview based on specific interpretations of Sharia law, which can limit the incorporation of alternative approaches. Sorush (2010) interprets this attitude as a manifestation of concern about the effects of secularisation and critical thinking.

In the case of Iran, the implementation of this vision has had significant implications for the development of the social sciences. Several studies point out that the emphasis on a single ideological perspective has contributed to an environment marked by censorship, self-censorship and restrictions on academic freedom, hindering the production of rigorous and pluralistic knowledge (Rahbari, 2024). This situation has limited the country's ability to generate accurate economic diagnoses, design evidence-based public policies, and establish independent evaluation mechanisms. As a result, academic institutions run the risk of prioritising ideological reproduction over scientific research (Beidollahkhani, 2025).

From a theoretical point of view, Islamic economics faces additional challenges. In many cases, it lacks a systematic theory of value, capital, or the market that would allow it to accurately address contemporary economic phenomena. Its categories tend to be normative or ethical in nature, and its discursive style is closer to a doctrinal exposition than to analytical argumentation. As Polanyi (1957) points out, pre-modern economies did not develop formal economic theories, as they did not face phenomena such as inflation, unemployment or economic growth. In this sense, Islamic economics, based on principles derived from different historical contexts, faces difficulties in responding to the challenges of a globalised, complex and technologically advanced economy.

The divergence between Islamic economics and modern social sciences is also evident in their epistemological foundations. While the latter are based on empirical observation, the formulation and testing of hypotheses, and peer review, Islamic economics relies on the exegesis of sacred texts and the authority of religious scholars. This difference transcends the methodological and reaches the ontological: for certain Islamist approaches, true knowledge is revealed, eternal and sacred, in contrast to the scientific view that conceives it as contingent, revisable and subject to debate. Sorush (2010) summarises this perspective by pointing out that 'Islamisation seeks to deduce the social sciences from Islamic texts, arguing that everything necessary for human beings exists in those texts'. This conception can hinder the development of a critical, open and pluralistic economic science.

The limited scope for epistemological pluralism also has political implications. The Islamisation of the economy is not limited to an intellectual project, but can function as a strategy for legitimising power. By presenting Islamic economics as the only

legitimate form of economic organisation, public debate is restricted and the space for dissent is reduced. As Huerta de Soto (2005) warns, systems that limit free human interaction and entrepreneurial initiative tend to generate dynamics of inefficiency, corruption and repression. The figure of the *Wali Faqih*, or supreme leader, represents a synthesis between religious authority and economic control. According to Namazi (2005), this figure possesses a legitimacy of divine origin that allows him to intervene in all areas of economic life, giving the state a predominant and exclusive role in the management of resources. This concentration of power can hinder the development of competitive markets, innovation and economic autonomy, thus perpetuating a structural dependence on the state apparatus.

Against this backdrop, the social sciences offer an alternative based on empirical analysis, diversity of approaches and the exercise of rational criticism. Economics, as a scientific discipline, cannot be reduced to religious morality or political ideology. Its object of study is human action in contexts of scarcity, and its purpose is to understand the mechanisms that allow for the efficient and equitable allocation of resources. As Robbins (1932) points out, economics does not prescribe ends, but analyses the means to achieve them. Confusing economics with ethics or religion implies ignoring its specificity as a social science.

In this context, Sorush's (2010) position takes on particular relevance. For this author, the Islamisation of knowledge not only represents an epistemological limitation, but also a threat to intellectual freedom. Science, he argues, requires an environment where plurality of ideas and the possibility of dissent are not only allowed, but encouraged. By avoiding dialogue with other schools of thought, Islamic economics runs the risk of becoming a closed system, unreceptive to criticism and interdisciplinary exchange.

This tension between a revealed epistemology, characteristic of political Islamism, and an empirical epistemology, characteristic of modern social sciences, poses significant challenges. As Weber (1905) warned, the rationalisation of social life requires empirical methods and verifiable criteria, which are incompatible with an exclusive dependence on religion. Polanyi (1957) complements this view by pointing out that economics, as an institutionalised activity, must be analysed in its historical and cultural context, which requires an epistemological openness that can hardly coexist with dogmatic approaches. These tensions not only affect the theoretical formulation of Islamic economics, but also have practical implications, as evidenced by Iran's economic experience since the 1979 revolution.

The following section will examine in greater detail the institutional and macroeconomic effects of this approach in Iran, including the banking system, patronage networks and public policies, with the aim of illustrating the empirical consequences of the Islamisation of knowledge.

5 Economic practice in Iran

Based on the logic developed in section 3, we now propose to examine a series of indicators and specific practices that allow us to evaluate the implementation of

Islamic economics in Iran: macroeconomic performance, the structure of the financial system, patronage networks, and regional comparisons.

The economy on which the Islamic Republic of Iran regime is based combines three fundamental pillars: the traditional *bazaar* economy; the powerful economic groups linked to the *bonyads*—some of them inherited from the Shah period, such as the Reza Pahlevi Foundation—; and a strong dependence on revenues from hydrocarbon exports. This hybrid economic structure reinforces the political control of the clergy and conservative elites, while limiting the development of an autonomous and competitive private sector.

The country's economic experience under political Islam reveals significant tension between the normative principles proclaimed by the Islamic Republic and the operational dynamics observed in practice. Although the 1979 Iranian Constitution establishes that the economy should serve as an instrument for the spiritual and social development of human beings, in practice it has tended to play a functional role in institutional consolidation, ideological alignment and the preservation of certain structures of influence. This dissonance between the normative ideal and empirical reality has been analysed by various authors, both nationally and internationally.

The Constitution of the Islamic Republic of Iran defines the economy as a means, not an end. Its preamble states that "the economy is a means to achieve the spiritual objectives of Islam, not an end in itself as in materialistic systems" (Islamic Republic of Iran, 1979). This formulation seeks to distinguish the Islamic economic model from contemporary systems, which, according to various Islamist ideologues, are based on values such as greed, exploitation and materialism (Al-Sadr, 1961). However, this idealised vision does not always translate into a coherent economic architecture or effective public policies. According to World Bank data (2024), Iran's GDP reached USD 436.9 billion, with annual inflation at 32.5% and an unemployment rate of 9.2%. These indicators reflect an economy under significant strain, where growth is insufficient to offset the loss of purchasing power and the deterioration of the labour market. For its part, the International Monetary Fund estimates economic growth of 3.3% for 2024, although it warns of persistent structural imbalances that could limit the sustainability of such growth.

One of the most distinctive features of the Iranian economic system is the historic alliance between the Shia religious authorities and the *Bazaar*. This relationship, which dates back centuries, has intensified since the 1979 revolution, forming a network of influence with significant economic and institutional implications. The *Bazaar*, as a traditional commercial centre, has received preferential treatment from the religious authorities, including tax benefits, priority access to foreign currency and participation in public contracts. This configuration has contributed to slowing down certain processes of economic modernisation, hindering the diversification of the productive fabric and favouring the expansion of an informal economy with a strong presence of actors linked to religious structures. Instead of expanding equitable access to resources, the current economic model has tended to consolidate a clerical elite with a significant presence in strategic sectors of the national economy.

Among the most influential *bonyads* are the Foundation of the Disinherited (*Bonyad-e Mostazafan*) and the Imam Khomeini Foundation, which, together with the economic conglomerate controlled by the *Pasdaran* (Islamic Revolutionary Guard), form a business network that enjoys extensive fiscal and regulatory privileges. This privileged position, underpinned by the alliance between religious and military power, hinders the competitiveness of the private sector and consolidates a clerical and parastatal elite with a dominant presence in strategic sectors of the national economy.

Islamic banking, promoted as an ethical alternative to the excesses of the conventional financial system, has generated significant debate in the Iranian context, especially in relation to the consistency between its founding principles and their practical application. Although the regulatory framework explicitly prohibits the charging of interest (*riba*), various studies have pointed out that, in practice, Islamic financial institutions resort to mechanisms such as commissions, profit margins and penalties which, in certain cases, fulfil equivalent economic functions. According to Sobhani (2013), professor of economics at the University of Tehran, effective interest rates in Iran exceed 25%, which has raised questions about the banking system's fidelity to its proclaimed values. This situation is exacerbated by the fact that such interest is exempt from taxation, which may encourage the accumulation of capital without a direct link to productive investment.

More broadly, some analysts interpret the persistence of challenges such as the financial crisis and unemployment as manifestations of unresolved structural problems in the economic model inspired by political Islamism (Kia, 2016). Added to this is a high rate of bank delinquency, which exceeds 15%, according to the Central Bank of Iran (2023), attributed in part to the granting of loans to individuals or entities linked to political power. This dynamic has hampered the recovery of funds and affected confidence in the financial system.

Hossein-Zadeh (2016) points out that a considerable proportion of Iran's gross domestic product, more than 65%, is concentrated in speculative activities, while the manufacturing sector faces significant restrictions in access to financing. This orientation has favoured the channelling of resources towards assets such as foreign exchange, precious metals and real estate, to the detriment of investment in productive sectors that could contribute more directly to sustainable economic development. In this context, even large manufacturing companies[2] have chosen to establish their own financial institutions. This strategy has raised concerns among some analysts, who warn of a possible diversion of resources from production to financial activities with less structural impact, which could limit the country's industrial dynamism and economic diversification.

This dynamic is accentuated by the Iranian economy's almost exclusive dependence on oil and gas, which constitute the state's main source of income and a central component of the trade balance. This sectoral concentration limits productive diversification, as financial resources, investment and labour are concentrated in the extraction and export

2 As may be the case with Iran Khodro.

of hydrocarbons, to the detriment of other sectors such as manufacturing, agriculture and the service industry. As a result, the economy faces what is known as the 'Dutch disease': the overabundance of liquidity generated by a single sector which, far from strengthening the economy as a whole, causes inflation, makes domestic production more expensive, weakens the competitiveness of other sectors and creates a structural imbalance with regard to a multisectoral and sustainable economy.

This structural vulnerability is compounded by political and institutional tensions. The Leader's long-term orientations, geared towards stability and ideological strategic objectives, often clash with the five-year plans of successive governments, which seek to balance growth, employment and industrial development. These differences are amplified by struggles between power groups—including *bonyads*, *Pasdaran*, *bazaar* actors, and state-owned enterprises—that control key sectors of the economy and defend their own interests. The interaction of these forces hinders the effective implementation of coherent economic policies and limits the consolidation of balanced industrial development, leaving the Iranian economy trapped in a pattern of hydrocarbon dependence and low productive performance in non-oil sectors.

In contrast to the Iranian model, some Muslim-majority countries, such as Turkey and Malaysia, have developed hybrid financial systems that combine Islamic principles with market economy mechanisms. Turkey has promoted participatory banking under state regulation, while Malaysia has implemented a dual financial system that allows for the coexistence of Islamic and conventional banking, thus favouring greater institutional flexibility. Recent studies, such as that by Durán Herrera *et al.* (2023), which analyses a sample of sixteen conventional and sixteen Islamic banks, suggest that these models contribute to balanced competition and more effective regulatory integration. In the case of Turkey, where fifty-four banks operate, six of which are participatory, a functional coexistence between the two systems has been observed, with positive results in terms of attracting investment, promoting entrepreneurship and complying with international transparency standards (Habib, 2021). In this comparative context, Kuran (2008) offers a structural critique of the Iranian model, pointing out that, in certain cases, Islamic banking has been used as a tool for ideological legitimisation rather than as an instrument of economic development. This observation suggests that, rather than orienting the economy towards collective well-being, some approaches have prioritised political consolidation through religious references, which has limited the system's ability to respond to contemporary socio-economic challenges.

TABLE 1. IRAN'S MACROECONOMIC INDICATORS (2024-2025): RECENT DEVELOPMENTS AND OFFICIAL ESTIMATES

Indicator	Value 2024	Value 2025 (estimated)	Source
GDP (USD)	436,900 million	437,000 million	World Bank
Inflation (%)	32.5	42.4	World Bank / Trading Economics
Unemployment (%)	9.2	7.2	World Bank / Trading Economics
Interest rate (%)	22.0	23	FocusEconomics
Trade balance (USD)	-934 million	—	Trading Economics

Source: author's own elaboration.

The explanations offered by various economic schools allow crises to be approached from different analytical frameworks, which contrasts with the limited presence of technical analysis in the economic discourse of political Islamism. The Austrian school, for example, attributes crises to the artificial expansion of credit and the distortion of relative prices, which generates inefficient investments and speculative bubbles (Mises, 1949; Hayek, 1976). The Keynesian school, for its part, identifies the fall in aggregate demand as the main cause of crises, proposing fiscal stimulus policies and public works as corrective mechanisms (Keynes, 1936). From a structural perspective, the Marxist school points to the fall in the rate of profit and the accumulation of capital as central factors in the genesis of crises (Marx, 1867). All these schools of thought offer conceptual tools for understanding economic cycles, formulating public policies and evaluating their results.

In contrast, political Islam tends to interpret economic failures from a moral or religious perspective, linking them to the loss of Islamic values. However, this view does not exhaust Islamic economic thought. In fact, there are theoretical developments within modern Islamic economics that address structural and technical issues, such as redistribution through *zakat*, the prohibition of interest (*riba*) and the promotion of social justice as the cornerstone of economic development (Orozco, 2013; Carrazco, 2024). In addition, some authors have attempted to construct an Islamist school of political economy of development, which interprets underdevelopment as the result of historical, political and economic factors, including colonialism and structural dependence, without renouncing a normative vision based on the Qur'an (Hidalgo-Capitán, 2011). Therefore, although political Islamism has instrumentalised religious elements in its economic discourse, it cannot be said that there is a total absence of analysis. Rather, there is a coexistence of doctrinal and structural approaches with varying degrees of systematisation, which poses the challenge of integrating these frameworks into a broader dialogue with contemporary social sciences.

The Islamisation of the economy has also had significant social implications. In some contexts, the exclusion of non-Muslim citizens from the education system and public employment has generated dynamics of inequality that have been interpreted as the creation of a second-class citizenry. Likewise, the legitimisation of private property based on religious faith rather than work or investment raises tensions with the principles of equality and social justice (Dadgar and Najafi, 2001). On the other hand, some studies have pointed out that the Islamist economic model has, in certain contexts, favoured the concentration of resources in the hands of religious figures, under the theological justification that these assets belong to the hidden Imam. This conception has posed challenges for the implementation of democratic oversight mechanisms by limiting transparency in the management of certain public assets (Mahsuli, 2005). In this context, practices have been documented that tend to link the allocation of privileges to criteria of ideological affinity rather than to principles of merit or efficiency, raising concerns about the consolidation of institutional dynamics that are not aligned with modern governance standards.

The notion of maximisation, understood as the rational pursuit of the best results with the available means, has been questioned by political Islamism, which

interprets it as a manifestation of human selfishness. However, some analysts point out that, in practice, certain Islamist leaders have accumulated wealth and power, reproducing dynamics similar to those they criticise in Western models. This apparent contradiction has led to the suggestion that the Islamist economic approach is not always based on universal ethical principles but, in certain contexts, may adopt an instrumental morality aimed at consolidating political power. In this regard, Huerta de Soto (2005) suggests that systems that restrict free interaction between individuals and limit the exercise of entrepreneurial initiative may face risks associated with inefficiency, concentration of power and lack of institutional transparency.

6 Structural impact of econo[m]ic Islamism

This section addresses four analytical axes interrelated with the structure of economic Islamism: the denial of the principle of scarcity, the relationship between property and inequality, the systematic exclusion of religious minorities, and the legitimisation of the use of coercive mechanisms as an economic instrument. Although each of these aspects poses specific challenges, their articulation reveals a common ideological pattern: the subordination of economic rationality to a theocratic logic, in which religious references are used as a normative framework for the consolidation of political power.

The denial of scarcity, explained above, is directly connected to the logic of property. In Iranian economic Islamism, property is not legitimised by work, investment or merit, but by religious faith. According to Dadgar and Najafi (2001), 'the real reason for giving legitimacy to private property is being Muslim'. This assertion turns property into an ideological privilege, excluding non-Muslims from access to goods, services and economic rights. Scarcity, denied in theory, is reproduced in practice through mechanisms of exclusion that fragment citizenship and reinforce structural inequality.

The exclusion of religious minorities, such as Baha'is, Zoroastrians and Christians, is not only a consequence of the logic of property, but also an expression of the theocratic conception of power. Documents such as the Cairo Declaration (1990) affirm that 'all people are equal in terms of dignity and honour', but add that 'true and solid belief is the only thing that ensures and guarantees the growth of this integrity'. This clause makes faith a criterion for citizenship, legitimising the exclusion of those who do not conform to the official interpretation of Islam. In this context, the economy ceases to be a space for rational interaction and becomes a mechanism of ideological control.

Finally, the legitimisation of coercive mechanisms as an economic tool closes the circle of this ideological articulation. Various studies have pointed out that, in certain contexts, political Islamism has historically resorted to forms of coercion to implement its economic and social model. According to Khomeini (1970), 'to apply Islam to real life, blood must be shed'. The concept of jihad, understood as the struggle for the expansion of Islam, legitimises the appropriation of the property of conquered peoples.

Taken together, these four axes—scarcity, property, exclusion, and coercive action—should not be understood as isolated phenomena, but as components of an articulated ideological structure. The denial of the principle of scarcity weakens economic rationality; property is linked to religious criteria rather than investment or work; exclusion fragments citizenship; and the use of coercive mechanisms contributes to the non-consensual redistribution of resources. Below is a comparative table between three economic models—Islamic, liberal, and centralised planning—with the aim of summarising their ideological foundations, organisational principles, and structural consequences. The comparison allows us to visualise the differences in key aspects such as the conception of property, the role of the state, the inclusion of minorities, the epistemology of economic knowledge, and the use of coercive action as a mechanism of legitimation. This tool complements the analysis developed in sections 2, 3, 4 and 5 of this study and offers a structured view that facilitates the evaluation of economic Islamism in the Iranian context. The selection of comparative axes was based on analytical criteria and a review of specialised literature. Structural dimensions common to the main models of economic organisation were chosen: conception of property, recognition or denial of scarcity, role of the state, inclusion of minorities, epistemology of knowledge and use of coercive action as legitimisation.

TABLE 2. STRUCTURAL COMPARISON BETWEEN ECONOMIC MODELS: ISLAMIC, LIBERAL AND CENTRALISED

Aspect	Islamic Economy	Liberal Economy	Centralised Planning Economy
Main Foundation	Sharia (Islamic law), faith and morality; subordination of the economy to theology.	Free Market, Private Property, Pursuit of Profit (Gain); based on individualism.	Collective Ownership and State Control of the Means of Production; based on collectivism.
Conception of Property	Mixed (private, state, public) and subject to ethical standards. Legitimised by faith (religious privilege).	Predominantly private. Legitimised by work, investment and contract.	Predominantly State or Collective. Private property is limited or non-existent.
Principle of scarcity	Denial of scarcity; it is believed that God provides sufficient resources (Baraka/Rizq).	Recognition of scarcity as an organising principle.	Recognition of scarcity; centralised allocation of resources by the state.
Motivation of the Economic Agent	Homo Islamicus guided by religious values; obedience to the Islamic State and pursuit of Falah (comprehensive well-being).	Rational Homo Oeconomicus who maximises individual utility and profit.	Economic agent subordinate to the state plan and collective objectives.
Role of the State	Absolute interventionism (in theocratic models); the State intervenes to guarantee social justice (Zakat, etc.).	Limited state (minimal); guarantees rights, regulates the market and provides essential public goods.	Total state; directs all production, distribution and consumption.
Resource allocation mechanism	Market regulated by ethical principles and state intervention to guarantee social justice.	Market (supply and demand) and the price system.	Central plan (established by the state) that defines what, how and for whom to produce.
Financial Instruments	Islamic banking; prohibition of riba (interest); based on profit and loss sharing (P&L sharing).	Interest-based banking system; interest is the price of money; financial regulation exists.	State banking system; total control of credit and investment by the government.
Epistemological Pluralism	Rejection of pluralism; religious/ theological reasons, with the imposition of a revealed vision.	Epistemological pluralism; openness to debate, criticism and diverse schools of thought.	Rejection of pluralism; political/ state reasons, where knowledge is subordinate to the state plan and not to religion.

Aspect	Islamic Economy	Liberal Economy	Centralised Planning Economy
Inclusion of minorities	Exclusion of religious minorities (in strict models); hierarchical citizenship.	Inclusion based on universal rights and equality before the law.	Inclusion conditional on ideological loyalty and membership of the dominant group.
Relationship with modernisation	Rejection of Western modernism; attempt to create an economic and social 'third way'.	Modernisation as a process of innovation, technological change and openness.	Modernisation directed and controlled by the state to achieve specific objectives (e.g. industrialisation).
Use of coercive action as legitimisation	Justified as a means of protecting the Islamic State and Divine Law (in certain radical regimes).	Rejection of coercive action as a political instrument; institutional and legal resolution of conflicts.	Use of coercive action as a tool for political control, repression and enforcement of the Plan.

Source: auhor's own elaboration.

7 Beyond the Iranian model: alternative approaches

7.1 Doctrinal comparison of normative economies

To enrich the analysis, it is useful to compare economic Islamism with other models of moral economy developed in other religious traditions. The Catholic social tradition, for example, proposes an economic model based on widely distributed property, the principle of subsidiarity and social justice, as an alternative to both capitalism and socialism. For its part, economic Buddhism, formulated by Schumacher (1973), promotes simplicity, sustainability, and spiritual well-being as guiding principles of economic activity.[3] These models, although also normative, are articulated with universal ethical principles and mechanisms of inclusion, which contrasts with Iranian economic Islamism.

The Catholic model, inspired by the social encyclicals of Leo XIII and Pius XI, approaches property as a natural right that should be widely distributed among citizens. Unlike economic Islamism, which legitimises property through faith, Catholicism promotes family and community property as the basis for social justice. It also recognises scarcity as an organising principle, but proposes mechanisms of subsidiarity to manage resources at the local level, avoiding the concentration of economic power.

For its part, economic Buddhism, formulated by Schumacher (1973), starts from a spiritual conception of scarcity: not as deprivation, but as an opportunity for voluntary simplicity. This model promotes inclusion through the reduction of

3 The choice of Catholic social doctrine and economic Buddhism is due to the fact that both constitute explicitly normative formulations of moral economies which, like economic Islamism, are presented as ethical alternatives to capitalism and socialism. Unlike other religious approaches, such as liberal Protestantism, the aim is not to pass moral judgement on their validity, but to establish a comparative framework between traditions that articulate comprehensive religious responses to the problem of economic justice.

material desire, environmental sustainability and community cooperation. Property is conceived as a means to collective well-being, not as an ideological privilege, and coercive action is excluded as an economic mechanism, in line with the principles of compassion and non-aggression.

In summary, the comparison between economic Islamism, the Catholic model and the Buddhist approach reveals three normative proposals with divergent ethical foundations. While Iranian economic Islamism has been interpreted by some authors as a use of religious references to support exclusionary practices and concentrations of power, the Catholic and Buddhist models tend to link the economy with principles of social justice, sustainability and inclusion. This comparison highlights that not all economies inspired by religious values adopt an authoritarian orientation, and that there are spiritual traditions capable of engaging constructively with democratic values and contemporary development challenges.

The following table summarises the structural differences between three religious models of economic organisation: Iranian economic Islamism, the Catholic model and economic Buddhism. Through the axes of property, scarcity, inclusion and coercive action, it shows how each tradition articulates its vision of the economic order. The selection of these comparative axes was based on analytical criteria and a review of the literature. These axes allow us to observe not only doctrinal differences, but also practical consequences in terms of social inclusion, economic rationality, and modernisation. The comparison is conceived as a heuristic tool, not as an exhaustive classification, with the aim of highlighting key tensions between economic Islamism and other traditions.

TABLE 3. STRUCTURAL COMPARISON BETWEEN RELIGIOUS MODELS OF ECONOMICS: ECONOMIC ISLAMISM, CATHOLIC MODEL AND ECONOMIC BUDDHISM

Model	Property	Scarcity	Inclusion	Coercive action
Economic Islamism	Legitimised by religious faith; ideological privilege	Denied as a structural principle; attributed to human corruption	Exclusion of religious minorities; citizenship conditional on faith	Legitimised as a mechanism of redistribution and conquest (jihad)
Catholic model	Widely distributed natural law; family and community property	Recognised; managed through subsidiarity and local structures	Inclusion based on human dignity; social justice	Rejected as an economic means; emphasis on cooperation
Economic Buddhism	Means for collective well-being; voluntary simplicity	Accepted as an opportunity for sustainability and moderation	Inclusion through reduction of desire and community cooperation	Excluded on grounds of compassion and non-aggression

Source: author's own elaboration.

7.2 Favourable perspectives, international reception and internal diversity of Islam

Although this study takes an analytical perspective on Iranian economic Islamism, it is relevant to incorporate some voices that highlight certain positive aspects of the model, with the aim of enriching the analysis and strengthening its scientific character. In particular, Islamic banking has been presented by various authors as an

ethical alternative to the conventional financial system. According to Chapra (2000), the prohibition of usury (*riba*) and the promotion of fairness in transactions are principles that could contribute to a more just and stable economy. Along the same lines, Siddiqi (2006) argues that Islamic banking, based on profit and loss sharing schemes, fosters a more transparent relationship between lender and borrower, which could reduce systemic risk. While these perspectives are subject to debate in terms of their practical application, they offer normative arguments that deserve to be considered and tested from an empirical perspective.

It is also relevant to briefly explore the international reception of the Iranian economic model. Although economic Islamisation in Iran has been criticised in various quarters, some Islamist movements in countries such as Pakistan, Sudan and Nigeria have shown interest in adopting certain elements of the model, particularly with regard to Islamic banking and redistribution mechanisms inspired by religious principles. This trend responds, in part, to the perception that the economic models promoted by colonialism and globalisation do not fully fit the realities and needs of some Muslim societies, which has prompted the search for alternatives based on their own values (Orozco, 2013).

However, these attempts have faced significant challenges in their implementation due to factors such as lack of institutional infrastructure, doctrinal diversity and social resistance. In contrast, countries such as Malaysia and Turkey have developed hybrid models that combine Islamic principles with market mechanisms, achieving greater international acceptance and more sustainable economic results (Carrazco, 2024).

Finally, it is essential to recognise the internal diversity of Islam in order to avoid identifying the Iranian model with economic Islamism as a whole. Twelver Shi'a Islam of the Jarifite sect, which predominates in Iran, has significant doctrinal differences from Sunni Islam, which constitutes the majority in the Muslim world. However, even within Shiism itself there is considerable theological and political diversity: reformist, spiritualist and rationalist currents coexist, questioning the subordination of the economy to religious power and proposing more pluralistic interpretations of Sharia law. As Sorush (2010) points out, the Islamisation of knowledge should not be confused with Islamic thought as a whole, as there are intellectual traditions that promote pluralism, rationality and social justice. Recognising this diversity makes it possible to avoid generalisations and open up the analysis to a more nuanced understanding of economic Islamism.

Beyond the Iranian case, the Islamic world is home to a remarkable doctrinal diversity that translates into different economic approaches. Sufism, for example, has historically promoted a spiritual vision of the economy centred on self-sufficiency, austerity and community solidarity, rejecting both capitalist materialism and authoritarian forms of religious organisation. For its part, moderate Sunni Islam, predominant in countries such as Indonesia, Malaysia and Jordan, has tended to articulate mixed economic models that combine Islamic principles with market mechanisms and democratic institutional frameworks (Hernando, 2017; El Radar, 2025). These currents, although less visible in the dominant political discourse, offer

viable alternatives that integrate Islamic ethics with the contemporary challenges of development, without resorting to exclusion or the political use of religious references. Recognising this plurality makes it possible to avoid reductionism and understand that Iranian economic Islamism represents a specific interpretation, not the entirety of Islamic economic thought.

8 Conclusions

The Islamisation of the economy in Iran since the 1979 revolution poses significant challenges in terms of viability and sustainability compared to contemporary economic models. This study has shown that economic Islamism, rather than consolidating itself as a scientific discipline or a structured technical proposal, presents itself as an ideological construct that has contributed to the consolidation of political power through reference to religious principles.

The analysis has identified four structural axes that allow us to understand the limitations of the Iranian model: a reinterpretation of the principle of scarcity, a conception of property linked to religious legitimacy, the exclusion of minorities in the economic sphere, and the use of coercive action as a tool of control. These elements are articulated within a theocratic logic that tends to subordinate economic rationality to the interests of religious power. The denial of the principle of scarcity hinders the application of rational choice criteria and limits the formulation of effective public policies. Property, understood as an expression of faith, can restrict equitable access and generate structural inequalities. The exclusion of minorities contributes to social fragmentation and weakens civic cohesion, while the use of coercive actions, legitimised as a defence of the religious order, becomes a mechanism for forced redistribution and ideological consolidation.

This study invites reflection on the challenges facing Iran in its search for an economic model that harmonises religious principles with criteria of efficiency, equity and sustainability in an increasingly interdependent global context. The dimensions analysed in this study suggest that economic Islamism, as it has developed in Iran since 1979, faces serious difficulties in establishing itself as a viable alternative to current economic models. Instead of promoting inclusive and sustainable development, the model has tended to reinforce authoritarian and exclusionary structures that limit innovation, restrict epistemological pluralism and contribute to social fragmentation, corruption and illicit practices. The subordination of the economy to religious ideology has transformed the system into an instrument of control rather than a tool geared towards collective well-being.

Given this situation, there is a need to move towards a reformulation of the economy from an empirical and open perspective, recovering its scientific, empirical and pluralistic dimension. This transformation does not imply renouncing Islamic identity, but rather reformulating it in dialogue with modern social sciences. Modernisation should not be understood as Westernisation, but rather as an epistemological opening that allows cultural values to be integrated with universal principles of justice, rationality and freedom. Islamic societies have a rich philosophical, legal and ethical

tradition that can contribute to the development of their own economic models, provided that they are articulated with empirical methods and verification criteria.

One way forward could be to promote a reformist Islamic economy, based on Islamic ethics but articulated with modern analytical tools. This requires abandoning the claim that all economic knowledge can be derived exclusively from religious texts and adopting a critical and dialogical attitude. As Sorush (2010) points out, the development of sound Islamic social sciences requires a thorough knowledge of contemporary social sciences, promoting rigorous academic training, epistemological openness and respect for intellectual pluralism.

At the same time, moving towards a more participatory economy, based on public deliberation processes and accountability mechanisms, is a fundamental step towards strengthening social cohesion and sustainable development. In this context, excessive concentration of power, limited inclusion of minorities and the use of coercion as an economic tool have proven to be obstacles to achieving these goals.

Economic democratisation is not limited to opening markets, but also involves ensuring that all citizens, regardless of their faith or political affiliation, can actively participate in decisions that affect their well-being. As Huerta de Soto (2005) warns, systems that restrict free interaction between individuals tend to generate inefficient dynamics, prone to mismanagement and institutional weakening.

It is equally important to recognise that modernisation is neither a homogeneous nor a linear process. Each society must find its own path, articulating its cultural values with universal principles. Islamic economics can play a constructive role in this process if it renounces doctrinal exclusivity and opens itself to dialogue with other traditions. Plurality of approaches, constructive criticism and a willingness to learn from experience are necessary conditions for building a truly human economy. In this sense, cultural identity should not be seen as an obstacle, but as a valuable resource. The Islamic intellectual tradition can engage in dialogue with the modern economy, provided that it is reinterpreted from an open and pluralistic perspective. As Warraq (2010) asserts, overcoming fear of the West and recognising the values of democracy and liberalism does not imply a renunciation of identity, but rather an invitation to build a modernity of one's own based on respect for diversity and the pursuit of the common good.

This analysis is supported by theoretical references such as Weber (2001), who emphasised the importance of rationalisation in modern economic organisation, the absence of which in Iran contributes to structural inefficiency. Polanyi's notion of 'embeddedness' helps us understand how the subordination of the economy to social and religious structures limits its institutional autonomy. From Robbins' perspective, the denial of the principle of scarcity contradicts the fundamentals of economic science, while Huerta de Soto's approaches to ideological interventionism help explain the dysfunctions of the Iranian financial system. These references reinforce the conclusion that economic Islamism, in its current formulation, fails to establish itself as a viable alternative to existing models.

Finally, this study opens up relevant avenues for future research, such as the formulation of a reformist Islamic economy compatible with democracy,

epistemological pluralism and scientific methods. It is essential to explore which elements of Islamic tradition can dialogue with principles of social justice and economic rationality without falling into dogmatism, as well as the role of Islamic universities as spaces for scientific research. Two aspects that could enrich the debate are: on the one hand, internal reforms promoted by reformist currents that seek to reinterpret religious texts in contemporary contexts; on the other, comparative studies between Muslim countries with hybrid models (such as Turkey and Malaysia) and those with more rigid theocratic structures. This perspective would make it possible to identify the conditions necessary for building a reformist Islamic economy capable of engaging with modernity without renouncing cultural identity.

References

Al-Sadr, M. B. (1961). Our Economy. Islamic Publishing House.

Beidollahkhani, A. (2025). Policy-Mediated Epistemic Control: How Authoritarian Regimes Repurpose Graduate Political Science Research Agenda – The Case of Islamic Republic of Iran. *Higher Education Policy*.

Berger, P. (1967). *The Sacred Canopy: Elements of a Sociological Theory of Religion*. Anchor Books.

Carrazco Núñez, E. I. (2024). Islamic economics: an alternative for development in the face of the global crisis? [online]. *InterNaciones*. 12(27). [Accessed: 2026]. Available at: https://internaciones.cucsh.udg.mx/index.php/inter/article/download/7277/6525

Casanova, J. (1994). *Public Religions in the Modern World*. University of Chicago Press.

Chapra, M. U. (2000). The future of economics: An Islamic perspective. The Islamic Foundation.

Dabashi, H. (2006). *Theology of Discontent: The Ideological Foundation of the Islamic Revolution in Iran*. Transaction Publishers.

Dadgar, Y., and Najafi, S. M. B. (2001). *Advanced Principles of Islamic Fiqh in Economics*. Razi University, Kermanshah.

Dalton, G. (1976). *Anthropology and Economics*. Anagrama.

Declaration of Human Rights in Islam. (1990). *Cairo Declaration*. Organisation of the Islamic Conference.

Derakhshan, M. (2015). Statements on Islamic economics at the 3rd International Congress of Islamic Humanities. *Hadana.ir* [site currently inaccessible].

—. (2023). Economist challenges existence of Islamic economy on Iranian TV [online]. *IranWire*. [Accessed: 2026]. Available at: https://iranwire.com/en/politics/115965-economist-challenges-existence-of-islamic-economy-on-iranian-tv

Durán Herrera, J. J.; García-López, M. J. and Rienda, J. J. (2023). *The responsible duty of Islamic banking: Different results from conventional banking? Application to the Malaysian case*.

Durkheim, É. (1893). *The Division of Labour in Society*. Paris: Félix Alcan.

—. (1993). *The Elementary Forms of Religious Life*. Alianza Editorial.

EcoIran. (2023). Interview with Ayatollah Alavi Boroujerdi: Jurisprudence does not produce economic science; jurists should leave the work to specialists [Video] [online]. *YouTube*. [Accessed: 2026]. Available at: https://www.youtube.com/watch?v=Tdeg52DWTuI

El Radar. (2025). Saudi Arabia and Indonesia: Opposing views of 'moderate Islam' [online]. El Radar. [Accessed: 2026]. Available at: https://www.elradar.es/arabia-saudi-e-indonesia-visiones-opuestas-del-islam-moderado/

Fairclough, N. (1992). *Discourse and social change*. Polity Press.

Flaquer García, J. (2024). The relationship between Islam and science: from medieval harmony to contemporary concordism [online]. *Journal of the Sociology and Theory of Religion*. 16, pp. 1-28. [Accessed: 2026]. Available at: https://doi.org/10.24197/jstr.1.2024.1-28.

FocusEconomics. (2024). *Iran Economic Outlook* [online]. FocusEconomics.com. [Accessed: 2026]. Available at: https://www.focus-economics.com/es/countries/iran/

Furqani, H., and Echchabi, A. (2022). *The concept of Homo Islamicus and the role of the individual in the economy: An Islamic perspective* [online]. *Econstor*. [Accessed: 2026]. Available at: https://www.econstor.eu/bitstream/10419/302031/1/1818045540.pdf

Gama, L. E. (2021). Hans-Georg Gadamer's hermeneutic method [online]. *Writings - Faculty of Philosophy and Letters, Pontifical Bolivarian University*. 29(62), pp. 29-48. [Accessed: 2026]. Available at: https://doi.org/10.18566/escr.v29n62.a02.

Habermas, J. (2008). *Between naturalism and religion*. Paidós.

Habib, A. (2021). *Turkish banks: overview*. Turkpidya.

Hadana. (2015). *Islamic economics from the perspective of Dr Derakhshan*.

Hayek, F. A. (1976). *Law, legislation and liberty: Volume 2. The mirage of social justice*. University of Chicago Press.

Hernando de Larramendi, M. (2017). Islam and foreign policy: the case of Morocco [online]. UNISCI Discussion Papers. 47. [Accessed: 2026]. Available at: https://www.unisci.es/wp-content/uploads/2018/05/UNISCIDP47-4LARRAMENDI.pdf

Hidalgo-Capitán, A. L. (2011). The Islamist school of political economy of development [online]. *UNISCI Discussion Papers*. 26, pp. 121-150. [Accessed: 2026]. Available at:https://www.redalyc.org/pdf/767/76718800006.pdf

Hossein-Zadeh, I. (2016). How Parasitic Finance Capital Has Turned Iran's Economy Into a Case of Casino Capitalism [online]. *Global Research*. [Accessed: 2026]. Available at: https://www.globalresearch.ca/how-parasitic-finance-capital-has-turned-irans-economy-into-a-case-of-casino-capitalism/5541782

Huerta de Soto, J. (2005). *Socialism, Economic Calculation and the Entrepreneurial Function* (3rd ed.). Unión Editorial.

Iannaccone, L. (1998). Introduction to the Economics of Religion. *Journal of Economic Literature*. 36(3), pp. 1465-1496.

International Monetary Fund (IMF). (2024). *World Economic Outlook: April 2024* [online]. Imf.org. [Accessed: 2026]. Available at: https://www.imf.org/es/Publications/WEO/Issues/2024/04/16/world-economic-outlook-april-2024

IranWire. (2021). Fact-Checking the Islamic Republic: Did Khomeini Promise Free Water and Electricity? [online]. *IranWire.* [Accessed: 2026]. Available at: https://iranwire.com/en/fact-checking/68822/

Islamic Republic of Iran. (1979). Constitution of the Islamic Republic of Iran, Constitutional preamble [online]. [Accessed: 1 October 2025]. Available at: http://www.Islamelsalvador.com/miscelanea/constitucion.pdf

Jamaran. (2018, 26 February). Amoli Larijani: To say that we do not have "religious science" is a stupid argument [Translated title] [online]. *Jamaran.ir.* [Accessed: 2026]. Available at: https://www.jamaran.news/fa/tiny/news-870843

Kadivar, M. (2023). *What does the guardianship of the jurist mean?* [online]. [Accessed: 2026]. Available at: https://kadivar.com/20209/

Keynes, J. M. (1936). *The general theory of employment, interest and money*. London: Macmillan.

Khamenei, A. (2009). University professors are the commanders on the front lines of soft warfare [Speech] [online]. *leader.ir* [Website of the Supreme Leader of Iran]. [Accessed: 2026]. Available at: http://www.leader.ir/langs/fa/?p=contentShowyid=5814

Khomeini, R. (1970). *Velayat-e Faqih: The guardianship of the Islamic jurist. Islamic State*. [n.p.], Beirut.

—. (1989). *The Testament*. Ministry of Islamic Culture.

—. (1999). *Sahife-ye Emam: Collection of Imam Khomeini's speeches*. Institute for the Compilation and Publication of Imam Khomeini's Works.

Kia, S. (2016). Why Can't Iran's Economy Revive? [online]. *American Thinker* [Accessed: 2026]. Available at: https://www.americanthinker.com/articles/2016/03/why_cant_irans_economy_revive.html

Kuran, T. (2008). *The roots of Islamic economics* [translated into Persian]. Tebyan.

Ladier-Fouladi, M. (2024). From the Islamisation of universities to the Islamisation of social sciences in Iran [online]. *Communications.* 114, pp. 29-48. [Accessed: 2026]. Available at: https://doi.org/10.3917/commu.114.0029

Lewis, B. (2002). *What Went Wrong? Western Impact and Middle Eastern Response*. Oxford University Press.

Mahsuli, S. (2005). Statements on wealth as the property of the Imam. *Weekly magazine "La Mirada de Jueves".*

Marx, K. (1867). *Capital: A critique of political economy. Volume 1, The process of capitalist production*. New York, NY: Cosimo.

Mises, L. von. (1949). *Human Action. A Treatise on Economics.* Unión Editorial.

Moghadami, E. (2014). The Islamisation of the social sciences in Iran. *Alef Daily*. 12(4), pp. 1-6. [Accessed: 2026]. Available at: http://old.alef.ir/vdcfxjd0ow6djva.igiw.html?244602

Namazi, H. (2005). *Economic Systems*. Sahami Enteshar Publishing House.

Orozco de la Torre, O. (2013). Development of the Islamic economy and banking: historical evolution and current situation in Europe. En: Orozco de la Torre, O. and Alonso García, G. (eds.). *Cuadernos de la Escuela Diplomática*. 48, pp. 167-187. [Accessed: 2026]. Available at: https://www.awraq.es/storage/2014/01/009-Desarrollo-de-la-economia-y-banca-Islamica-evolucion-historica-y-actualidad-europea.pdf

Parsons, T. (1966). *Societies: Evolutionary and Comparative Perspectives*. Prentice-Hall.

Polanyi, K. (1957). The economy as an institutionalised process. In: Godelier, M. (ed.), Anthropology and economics. Anagrama.

Polanyi, K. (1957). *The Great Transformation*. Beacon Press.

Rahbari, L. (2024). *Academic (Un)freedom in Iran after 1979: (Transnational) State Suppression of Academia and Risks for (Diasporic) Academics*. American Association of University Professors.

Robbins, L. (1932). *Essay on the Nature and Significance of Economic Science*. Fondo de Cultura Económica.

Rudnyckyj, D. (2011). Homo Islamicus and Homo Economicus, Revisited: Islamic Finance and the Limits of Economic Reason. *8th International Conference on Islamic Economics and Finance*. Doha, Qatar.

Schumacher, E. F. (1973). *Small is Beautiful: Economics as if People Mattered*. London: Blond & Briggs.

Siddiqi, M. N. (2006). Islamic banking and finance in theory and practice: A survey of state of the art. *Islamic Economic Studies*. 13(2), pp. 1-48.

Sobhani, H. (2013). Usury, the biggest problem facing the Iranian economy. Tabnak. http://www.tabnak.ir/fa/news/361395

Sorush, A. (2010). *The secret and necessity of social sciences* [online]. [Accessed: 2026]. Available at: https://www.drsoroush.com

Tabnak. (2024). Critique of the ideas of Seyed Monireddin and his successor Seyed Mahdi Mirbagheri [online]. *tabnak.ir.* [Accessed: 2026]. Available at: https://www.tabnak.ir/fa/news/1249366/

Thompson, J. B. (1990). *Ideology and Modern Culture: Critical Social Theory in the Age of Mass Communication* [online]. Autonomous metropolitan University.

Warraq, I. (2010). *Virgins? What Virgins?: And Other Essays*. Prometheus Books.

Weber, M. (2001). *The Protestant Ethic and the Spirit of Capitalism*. Alianza Editorial.

World Bank. (2024). *Iran Economic Monitor: Spring 2024 Sustaining Growth Amid Rising Geopolitical Tensions* [online]. World Bank Group, Open Knowledge Repository.

[Accessed: 2026]. Available at: https://openknowledge.worldbank.org/entities/publication/6790f292-cf7f-4f16-b522-7f35e9d1161f

Yousefi, M. and Abizadeh, S. (1992). An essay on economics and ideology: The case of Iran [online]. *Humanomics. 8*(3), pp. 29-59. [Accessed: 2026]. Available at: https://doi.org/10.1108/eb006132

Zarrinkub, A. (1957). *Two Centuries of Silence.* 2nd ed. Amir Kabir Publishing House.

Appendix I. Glossary of the main Islamic terms used

Term	Translation
Ayatollah	Sign of Allah, the highest rank in the Shia hierarchy
Fatwa (pl. *Fatawaa*)	The legal opinion of specialists in Islamic law
Faqih	Jurist
Fiqh	Jurisprudence
Mujtahid	Jurist
Riba	Usury or interest
Sharia	Islamic law
Wali Faqih	Jurisprudential guardian, spiritual leader, supreme leader
Velayat-e Faqih	Guardianship of a jurist
Jihad	Defending principles, or fighting for the explanation of the Muslim religion in general

Source: author's own work.

Article received: 16 October 2025
Article accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Luis Barragán Márquez
Lieutenant of the Civil Guard and responsible for the area fight against jihadist radicalization of the Jihadi Information Command of the Civil Guard Information Command

Email: luisbarragan@guardiacivil.es

Salvador Berdun Carrion
PhD. In Criminology by the University of Granada

Email: salvadorberdun1@gmail.com

Jihadism in the prison system. The case of Rida B

Abstract

The recent sentence imposed on inmate Rida B. for threatening prison officers and glorifying terrorism has brought the issue of jihadist radicalisation in prisons back into the spotlight. However, this phenomenon has particular characteristics that differentiate it from jihadist radicalisation and its criminal manifestations outside prisons. The fact that convictions for jihadist activities in prisons have been handed down to inmates classified as high risk raises questions about the extent to which the prison system is able to prevent jihadist activity in prisons.

Keywords

Terrorism, Prisons, DAESH, Radicalisation, Glorification.

Cite this article:

Barragán Márquez, L. and Berdun Carrion, S. (2025). 'Jihadism in the prison system. The case of Rida B'. *Journal of the Spanish Institute for Strategic Studies*. 26, pp. 521-546.

1 Introduction

In a ruling dated 25 February 2025, the Fourth Chamber of the National High Court sentenced Rida B., an individual imprisoned for common crimes (La Vanguardia, 2025), to a total of six years for crimes of glorification of terrorism and unconditional threats directed at a professional group, in this case prison officers. This sentence is a departure from previous rulings in other cases of jihadist activity in Spanish prisons. In 2004, Operation Nova[1] resulted in five convictions for membership of a terrorist organisation. In the case of Operation Escribano (2020)[2] , two inmates were convicted of collaborating with a terrorist organisation.

In most cases, the convicted individuals were classified as maximum security prisoners and subject to the strictest regime, with restrictions on their movements and interactions with other individuals. This raises the question of how jihadist activity manages to develop in such a restricted environment.

As Marc Sageman (2004, 2008) pointed out, jihadist radicalisation is not articulated solely through formal hierarchies, but through networks of affinity and personal ties that reinforce ideological cohesion. This approach is particularly useful for understanding how, even in highly restrictive environments, dynamics of socialisation and ideological resistance can be maintained among inmates.

Under the hypothesis that jihadist activity itself is seen as a form of resistance against the prison administration, and that the judicial and prison response to the phenomenon reflects a regulatory adaptation aimed at containing radicalisation in prison, a series of three key questions arise: What strategies do inmates linked to jihadism use to maintain their activity within the prison? How does the prison administration react to these strategies and what mechanisms does it use to detect and contain them? To what extent does the case of Rida B. show a change in judicial or prison practice with regard to the treatment of jihadist activity in prison?

To answer these questions, we will use a dual perspective: prison and legal. The first will focus on explaining how individual resistance develops in maximum security

1 Operation Nova dismantled a group of around thirty prisoners who called themselves "Martyrs for Morocco". The group was formed in Topas prison between 2000 and 2002 under the leadership of inmate Mohamed Achraf, and later spread to other prisons. The main leaders and organisers of this network were convicted under the old Penal Code for membership of a terrorist organisation. It should be noted that until the 2015 reform, there were no criminal offences adapted to the new forms of terrorism adopted by jihadism in the West.

2 Operation Escribano is the largest investigation carried out in Europe in the field of jihadist radicalisation in prisons in favour of the terrorist organisation DAESH. The investigation began in 2017 when graffiti depicting DAESH flags was detected in a prison and was expanded to investigate a large group of inmates who maintained an intense correspondence, both through regulated channels and by circumventing the prison administration's control measures. The investigation concluded at the end of 2020, finding that the main suspects had planned to form a group to unite and reincorporate prisoners convicted of terrorism offences into jihadist militancy and continue terrorist activity upon their release from prison.

prison regimes. The second will focus on the importance of prison regulations and the reasons on which the National Court has based its decision. In terms of structure, the paper is organised according to the three questions posed in the hypothesis. First, we analyse the strategies employed by prisoners linked to jihadism to maintain their activity within the prison environment, understood as a form of resistance to institutional authority. Secondly, it examines the prison administration's response to these strategies, as well as the regulatory and operational mechanisms designed to detect and contain them. Finally, it addresses the case of Rida B. as a representative example of judicial and prison adaptation to jihadist activity in prison, assessing the extent to which it reflects a change in institutional practice and in the application of the current legal framework.

2 The Closed Regime and Challenges to Prison Security

This section aims to contextualise what the closed regime means in terms of security. It also introduces the influence of prison subcultures and the idea that authority and security in the prison environment are not absolute concepts, but are challenged by the prison population with the means available to them.

2.1 Prison regulatory framework

The principle of re-education and reintegration forms the basis of the Spanish prison system. This mandate is enshrined in Article 25.2 of the Spanish Constitution of 1978, which establishes that "custodial sentences and security measures shall be aimed at re-education and social reintegration and may not consist of forced labour".

In compliance with this principle, the General Prison Law (Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria, LOGP) was enacted, which sets out the objectives and foundations of the system. Subsequently, Royal Decree 1201/1981 of 8 May approved the first Prison Regulations, later replaced by Royal Decree 190/1996 of 9 February, which adapted the regulations to the changes introduced by the 1995 Penal Code and to the sociological evolution of the prison population.

The closed regime represents the highest level of control within the Spanish prison system and reflects the practical application of the principle of scientific individualisation provided for in the LOGP. According to Article 72, this system is divided into three levels of classification, the first being the most restrictive and intended for inmates who are particularly dangerous or unsuited to the ordinary or open regime.

The guiding principle of Spanish prison policy—the re-education and social reintegration of prisoners—does not, however, ignore the existence of inmates who are disruptive and resistant to prison treatment. Some of them pose a danger that compromises both the internal order of the establishments and the external security of society, which justifies the existence of a particularly severe regime.

Article 10 of the LOGP specifies the conditions of the closed regime, characterised by limited communal activities and greater control and surveillance of inmates. This

regulation is complemented by Articles 100 and 101 of the Prison Regulations (RP), which define the classification system and the regime applicable to each degree.

In this context, Article 102.5.c of the RP incorporates a criterion of particular relevance to the analysis of the jihadist phenomenon: membership of criminal organisations or armed gangs as an indication of particular dangerousness. This provision is particularly significant in the prison treatment of inmates convicted of jihadist terrorism offences, where institutional concern about proselytism and radicalisation has led to the application of the closed regime and their inclusion in the Special Monitoring File (FIES) as a means of containing radical ideologies.

In this way, Spanish prison regulations show an adaptive evolution in response to new forms of organised crime and the phenomenon of jihadist radicalisation, focusing on the prevention of ideological contagion within prisons.

2.2 Impact of the jihadist phenomenon on prison regulations

The treatment of jihadist terrorism in prison is one of the main security challenges facing the Spanish prison system. As Reinares, García-Calvo and Vicente (2018) point out, Spanish prisons have been areas of jihadist radicalisation, although to a lesser extent than other social or virtual spaces. However, at certain times they have also served as places for jihadist groups to organise and plan criminal activities. This assessment, based on judicial and police data, allows the Spanish prison phenomenon to be placed in a comparative perspective and highlights the need to maintain preventive measures and deradicalisation programmes within prisons.

The Spanish prison system's first contacts with individuals linked to Arab international terrorism date back to the 1970s. During the 1980s, organisations such as Hezbollah, AMAL[3] , and others linked to Palestinian terrorism also operated in Spain. During this period, a total of twelve individuals were imprisoned, which was truly exceptional.

In the mid-1990s, the situation began to change with the establishment of Algerian networks in Spain. In 1995, Ghebrid Massaoud (Sirvent and Duva, 1995) was arrested in Barcelona, marking the beginning of a new cycle in which the number of jihadist prisoners began to grow steadily (Berdún, 2023: pp. 413-414). Since then, jihadist terrorism has brought a significant number of inmates to Spanish prisons. Most of them have been classified as first-degree prisoners.

The closed regime usually involves the inclusion of first-degree inmates in the FIES file. The regulation of the FIES underwent a final transformation with Royal Decree 419/2011 of 25 March, which addressed the problem arising from the annulment of Instruction 21/1996. The reform covered the FIES in the 1996 Prison Regulations.

3 The Amal Movement (in Arabic, حركة أمل Harakat Amal; *amal* means 'hope') is a Lebanese Shia organisation.

In addition, the idea of the prison institution as another part of the state security apparatus was reinforced.

Concerns about the rise of jihadist terrorism influenced the reform of the RP, giving new functions to the prison administration in the fight against terrorism (Berdún, 2023: p. 192). Concepts such as the importance of collaboration between the prison system and the information and intelligence services were introduced, as was the approval of organisational rules for surveillance, control and intervention in response to attempts by prisoners to continue criminal activities in prisons. At this point, it is worth highlighting the capacity for social mobilisation and cohesion of imprisoned ETA militants grouped together in the so-called 'Prison Front'.

The reform expressly regulated the existence of the FIES in Article 6.2 RP, and Article 65.3 established the possibility of creating specialised groups of officials to control prisoners involved in these forms of crime. With this regulation, the FIES transcended the limits of prison security to become part of anti-terrorist policy in its broadest sense.

Analysts from the Civil Guard Information Service in charge of the Rida B. case have highlighted the importance of adapting regulations to the evolving terrorist threat and, in particular, the daily work of prison officers to maintain adequate control over inmates likely to become involved in proselytising networks within prisons, in contrast to the situation in neighbouring countries, which is often described as close to chaos.

However, the regulatory and organisational measures adopted have not succeeded in eliminating the conflict inherent in first-degree regimes. In these contexts, prison authorities continue to be challenged by resistance dynamics which, in some cases, find symbolic legitimacy in jihadist ideology.

2.3 The challenge to authority in maximum security environments

2.3.1 Resistance and disobedience in restrictive environments

Authority is not an immutable concept. Even in maximum security environments, there is room to evade institutional control and challenge established authority. Sykes warns of the imperfection of prison power:

> 'The criminal in prison rarely denies the legitimacy of confinement. At the same time, recognition of the legitimacy of society's substitutes and its body of rules is not accompanied by an obligation to obey, nor is it internalised, and the prisoner thus accepts the fact of his captivity on one level and rejects it on another. If, for one reason, the institution of custody is valuable to a theory of human behaviour, it is because it makes us realise that men do not need to be motivated to conform to a regime they define as legitimate'. (Sykes, 1958: p. 48).

Sykes, referring to the problem of maintaining order in prisons, suggests that only in the case of total or almost total isolation of individuals can one speak of almost absolute control:

> 'If a prisoner confined in solitary confinement bangs his head against the wall, it is individual madness; if he refuses to bathe or eat, his rebellion remains within the confines of his cell. However, in a maximum security prison, maintaining order is much more complex than moderating self-destructive impulses or isolated gestures of protest'. (Sykes, 1958: p. 17)

From these words, it could be deduced that strict confinement prevents any kind of dissent on the part of inmates. However, Foucault (1976) stated in his book *The History of Sexuality* that 'where there is power, there is resistance'. In any space of authority, there is room for confrontation.

There are examples of defiance of authority and the prison regime in high-security spaces. For example, Pelican Bay Prison in California was the scene of collective challenges to authority by inmates housed in the so-called *Security Housing Unit* (SHU). Reiter (2014: p. 579) defines this type of unit as the archetype of *supermax* prisons. The protest spread throughout much of the Californian prison system and was followed by hundreds of inmates. This was a success, considering that these were individuals who had no prior connections and were not part of an organised group.

Recently, in Italy, there was a protest by an inmate linked to anarchism, Alfredo Cospito, who went on hunger strike against the application of Article 41bis of the Italian prison law regulating the application of the high security regime. He was linked to the Informal Anarchist Federation, a decentralised and autonomous network with characteristics typical of insurrectionary and diffuse resistance networks. According to Marone (2023), Cospito had spread propaganda from prison, despite being in a high security regime. The campaign had a profound public impact and led to attacks claimed by anarchists in Italian and European cities. He also maintained contact with inmates linked to the mafia and also subject to Article 41bis. Members of the Italian mafia have repeatedly attempted to oppose both the 41bis regime and the *ergastolo ostativo,* highlighting the legal controversies surrounding this regime. This highlights the potential of prisons as *hubs* for individuals belonging to different types of criminal networks.

These conflicts are not new. The challenge to established authority was constant in the 1970s with the outbreak of social and racial conflicts in American and Western prisons. Some of these conflicts arose from issues of ethnic and religious identity. On other occasions, there are no political or social reasons to be found, but rather they are simply the result of friction between prisoners and guards.

Prison power is susceptible to challenge, even in regimes where individuals face greater limitations. It is possible to confront the system, sometimes through what Garreaud (2014: p. 158) calls the political technologies of the total institution and the 'practices of the prisoners' selves'. This dialectic can escalate, from prisoners' self-mutilation to escapes and riots, but it does not necessarily imply political content.

Sometimes, prisoners in the most restrictive prison regimes seek ideological justifications for their maladjustment to the prison regime. To this end, they seek outside support from anti-system movements. Examples of this narrative can be found in numerous publications by prisoner support groups that focus on such behaviour

as a social or political struggle[4][5][6]. There are numerous cases of prisoners convicted of common crimes who are linked to campaigns against maximum security regimes in different countries: FIES in Spain, 41bis in Italy, and F-type prisons in Turkey.

Figure 1

Figure 2

Figure 3

2.3.2 Jihadist challenge to the prison administration, the Spanish case

Colouring activities in support of terrorism with a social or political struggle became a constant feature of the imprisoned militancy of extreme left-wing ethno-nationalist terrorist groups such as the IRA, ETA and GRAPO. One of the most renowned jihadist leaders in the Spanish prison system, Mohamed Achraf, promoter of the jihadist networks dismantled in the Nova and Escribano operations, was inspired by this type of activity.

In early 2018, Achraf began demanding that the prison administration allow jihadist prisoners to go out into the yard together, identifying them as 'Islamist political prisoners', and gradually increased his demands for their regrouping in the same prison and module. As a means of pressure, in the spring of that year, he began a forty-five-day hunger strike, sending letters to other like-minded prisoners

4 Examples of these narratives can be found in the *Tokata* newsletter, which frequently devotes its pages to criticising the closed regime in Spain and its equivalents in other countries.

5 Graphic archive of the Sancho el Sabio Foundation. Poster with the text "Herriaren borrokarekin gure askatasuna: expetxeak apurtu, amnistia osoa, errefuxiatuek Euskadin bizi behar dute" (With the support of the people, our freedom: open prisons, full amnesty, refugees must live in the Basque Country) produced by the organisation Gestoras Pro-Amnistía, which was banned for being part of the ETA network. Available at: https://www.euskalmemoriadigitala.eus/handle/10357/54134

6 In March 2022, the fifth issue of the publication "O MUJAHIDEEN IN THE WEST", an English-language magazine produced by the Hurras Al-Tawheed (HAT) group, was published on social media under the title "Jihad, the only path to glory", in which two articles containing threats against prisons were published. The first, entitled *"Are we going to let them rot in prison?"*, calls on Muslims in the West to attack prisons and free Muslim prisoners, considering that they have sacrificed their lives to defend true Islam. The second, entitled *"Kill all the Guards!"*, orders the murder of prison officers, specifying that such attacks should be carried out when they arrive home and by stabbing.

proposing that they support his initiative, along with expressions typical of the jihadist imagination[7].

'We are also on strike over the issue of the courtyard. All this until we achieve victory or martyrdom. And until their injustice, aggression and war end. And until they give in and put us together in one wing and allow us to go out into the courtyard together'.

His influence on other inmates led them to reiterate the same request to the prison administration and adopt the idea that they should fight for a 'Prison Front', putting pressure on the authorities to concentrate jihadist prisoners in prisons close to their places of residence, emulating the demands of prisoners belonging to the terrorist organisation ETA. As part of this campaign, in June 2018 Achraf published an article entitled 'Situation of subjugation, control and extermination of prisoners under the "Anti-Jihadist Protocol2 in State Prisons' in the activist newsletter *Tokata*. Achraf had previously published several letters in *Tokata*[8].

Another case in which inmates linked to jihadism used this type of media as a platform for their demands is M.E.H.E.Y., who appeared on websites linked to this type of movement[9]. In all cases, this inmate vehemently declared himself to be an individual linked to the resistance against the closed prison regime. This is a widespread practice among the prison population classified as first degree.

3 Jihad in maximum security prison environments

This section describes the impact of radicalisation in prisons and the influence that prison subculture, the 'prisonisation' of religious sentiment and the adoption of an individual and collective identity conditioned by the jihadist narrative on prisons can have on these processes.

7 The operation was prosecuted by Section 4 of the Criminal Chamber of the National Assembly. The oral and public trial took place between 4 and 21 July 2022, with a total of five trial sessions.

8 On 7 December 2014, Achraf published a letter in *Tokata* entitled "The Prison Inquisition. Reflections by Mohamed Achraf". Available at: https://tokata.info/la-inquisicion-penitenciaria-reflexiones-de-mohamed-achraf/. On 12 November, he also published a letter criticising the FIES regime entitled "From the Isolation of Malaga II, Letter from a prisoner in struggle against state violence and racism". Available at: https://tokata.info/desde-el-aislamiento-de-malaga-ii-carta-de-un-preso-en-lucha-sobre-la-violencia-y-el-racismo-de-estado/

9 This individual sent a letter published in the *Tokata* newsletter entitled: "Collective demand for decent living conditions in the isolation of Villena prison (Alicante II)". Available at: https://tokata.info/reivindicacion-colectiva-de-unas-condiciones-de-vida-dignas-en-el-aislamiento-de-la-carcel-de-villena-alicante-ii/. Another letter in which the same inmate sends greetings to Achraf. Available at: https://www.federacionanarquista.net/companerismo-desde-el-departamento-de-castigo-de-la-carcel-de-picassent-valencia/

3.1 The risk of radicalisation and its impact on the prison environment

Concern about radicalisation and the spread of ideas based on a radical view of Islam has become a priority for security and police authorities and prison services[10]. Prisons can become breeding grounds for jihadist radicalisation. Prisoners may come into contact with extremists and adopt radical views while serving their sentences, in many cases attracted by the promise of redemption.

From an academic point of view, there is consensus that the phenomenon of radicalisation must be addressed, but there is a need to avoid alarmism. Furthermore, there is a significant gap in research that needs to be filled, as Veldhuis and Kessels (2013: p. 3) point out that most studies are based on qualitative evidence, and access to quantitative data is needed to understand the scale of the phenomenon.

3.2 Collective identity in the prison environment. A radical prison subculture?

Political identity has been a fundamental tool in the construction of prison collectives of terrorist organisations such as ETA, GRAPO, the IRA and the RAF. For example, with regard to ETA prisoners, Alcedo Moneo points out that:

> 'Prison is the ETA space par excellence, where militants can express themselves as such. There, they are recognised as ETA members by their fellow villagers, the officials in charge of their custody, and the anonymous masses who see their photos among many others on large posters calling for amnesty for Basque prisoners. Prison, like the street before it, is a place of struggle and resistance, but in prison it is passive. With the struggle, the characteristics that accompany it reappear, for example, clandestinity, although they do have some peculiar characteristics'. (1996: p. 285)

In these cases, we are talking about organised and hierarchical groups. On the contrary, when considering the problem of proselytism and jihadist activity in prisons, the issue presents a different perspective. Prisoners linked to jihadism or who may be vulnerable to radicalisation processes do not constitute an organised and structured group. Therefore, the possibility of creating structures in prisons will depend largely on the interaction of individuals during their imprisonment.

It is interesting to understand how identity and individual awareness influence the greater or lesser risk of radicalisation in maximum security prison environments.

10 Examples of this are the 2021 National Security Strategy (ESN) (p. 57) and the European Council Conclusions on preventing and combating radicalisation in prisons adopted in June 2019. In this regard, EUROPOL, through its Report on the Situation and Trends of Terrorism in the European Union (TE-SAT), continues to highlight, year after year, the large number of terrorist attacks carried out in Member States and perpetrated by individuals who have been totally or partially radicalised in prison. It should be noted, for example, that in 2020 at least five jihadist attacks in Europe involved prisoners or ex-prisoners at the time of the attack.

Liebling and Straub (2012, pp. 15-21) point out that monotheistic religions are prone to being misinterpreted or misused and are attractive in prison, while individuals with communication skills are attractive to other subjects. Liebling and Straub cite Hamm, who concludes that the behaviour and influence of Muslim prisoners vary according to the characteristics and social conditions of the prison. Overcrowded maximum security institutions provide conditions conducive to radicalisation.

In contrast, in prisons with appropriately designed regimes and activities, the risk of radicalisation can be counteracted. The appeal of Islam lies in the fact that it can serve as a justification for the acts that have led the inmate to prison by blaming the 'West' or the 'infidels', allowing bonds of trust to be established or even serving as a mechanism for channelling rebellion against the system. In many cases, religious conversion serves to reinforce their own cultural identity and is expressed as a form of individual and collective resistance against the West in a restrictive environment.

On the other hand, certain charismatic individuals can take on special relevance in a context where individuals experience a deep sense of insecurity. For Marranci (2012: pp. 23-24), Islam in prison is defined on the basis of individual emotions, although that faith may be 'performative' (i.e., expressed more as an external performance or manifestation than as a deep internal conviction).

Misinterpretations of religious concepts that operate in the processes of radicalisation and recruitment in prison are conditioned by the way in which individuals experience their imprisonment and by institutional control. There is a third factor, the prison subculture, which conditions the way in which individuals adapt to the prison environment. It is worth asking whether we can speak of a prison subculture shaped and based on a radical interpretation of Islam. A jihadist subculture in prison that would differentiate its members from the general prison subculture. In this way, they play with the Salafist concept of 'takfirism', classifying as 'good Muslims' those who subscribe to their understanding of Islam and are loyal to their group within the prison wing, while labelling as 'bad Muslims' or apostates those who do not submit to the discipline of their group and do not interpret Islam in those terms.

In prison, many inmates classified as first degree consider this classification a sign of individual status vis-à-vis the rest of the prison population. Often, these types of inmates define themselves as 'warriors' who defy the system[11]. In the case of individuals convicted of jihadism or classified as radicalised for recruitment and leadership activities, Civil Guard investigators point out that inmates with this profile often boast about their classification as a symbol of prestige within the prison. However, their expressions of opposition to the prison regime are very limited thanks to the special supervision given to this type of inmate.

11 Interestingly, until recently, inmates with this profile often had Sun Tzu's *The Art of War* in their cells as a reference book.

For terrorist organisations, maintaining the identity and militancy of their members within prisons is essential to maintaining the cohesion of their organisations. GRAPO member Bittor Dieguez described the group's philosophy in prison as follows:

> 'We are communist prisoners, we have a concept of life and we take it everywhere. We cannot conceive of life in prison without doing anything, with our hands tied, lying around in the courtyards as they have managed to do with common prisoners. It would be unacceptable for us to be subjected to such conditions. Always and in any prison, also depending on the strength we have had, we have tried to maintain these minimum standards, to be able to study collectively, to be able to improve ourselves, to be able to train ourselves better so that tomorrow we can contribute more to the cause' (Dieguez, 1989).

With regard to jihadism, it is necessary to determine the ideological basis of this phenomenon in prison. Above all, because jihadist militancy sometimes arises in prison, unlike what happened with other terrorist groups. Marranci (2020) points out that religion can become a way of reaffirming their personality by confronting their religious identity against an institutional authority they consider unjust or illegitimate. Based on this perception of unjust imprisonment and illegitimate authority, *tawhid*, the principle of the oneness of God, evolves from a theological principle to a survival mechanism that allows prisoners to reinforce their own personality in the face of a system they perceive as hostile.

Officials often report how radical inmates interrupt scheduled activities such as roll calls with prayer. This is a mechanism of identity reaffirmation and resistance, but also a violation of prison regulations masked by the practice of religion to avoid disciplinary sanctions.

Hamm (2009: p. 144) reports the existence of small influential groups of individuals capable of spreading a 'prison' version of Islam (*Prison Islam*). They thus take advantage of the traditional prison dynamics of coercion and the use of pressure groups. In this way, a simplified version of Islam is spread, adapted to respond to the perceptions of incarcerated individuals. With regard to this concept of 'prison Islam', the approach to this unorthodox version of religion is often based on motivations to seek protection and integration into a group that facilitates the stay in prison.

Sometimes, the approach to religion is based on utilitarian reasons such as access to greater social interaction or group protection, even in the most restrictive prison environments. The group dynamics typical of the prison environment facilitate this practical approach, which can precede a recruitment process and is carried out discreetly through direct interaction.

García Martínez (2008: pp. 188-189) mentions this prison religious subculture that defines models of behaviour and can lead to the adoption of attitudes of 'resistance' to the system. Sometimes, prisoners adopt a 'ritualistic' approach to religion focused on their own identity, in which religious expressions are subject to 'prison ritualisation'. In other cases, the 'rebellious' approach serves to justify the behaviour of individuals linked to violent crime.

The propaganda approach of Al Qaeda and DAESH is oriented towards mere religious and ideological conversion through learning, building a prison jihadist subculture in which individuals are told how to be *cool.* This explanation, derived from cultural criminology, allows us to go beyond the traditional justifications of conversion or rebirth to understand certain behaviours (Sunde and Sandberg, 2021: p. 282). Applied to the prison environment, this form of attraction to the individual can take the form of an invitation to challenge the rules. These subcultures constitute an added difficulty in maintaining orderly coexistence and the resocialising aims of punishment.

The fear of radicalisation has contributed to a feeling among incarcerated individuals that the experience of deprivation of liberty has worsened (Liebling, Williams and Lieber, 2020: p. 1664). Maximum security environments provoke greater feelings of aversion to the system and its rules. When collecting testimony from an inmate regarding the risk of radicalisation, he stated: 'I don't need to radicalise anyone here—they're all already anti-authority!' (Williams and Liebling, 2023: p. 98).

Contrary to the perception that these subcultures may contribute to violent radicalisation processes in prisons, other authors believe that they may play a role in counteracting the emergence of radicalisation processes in prisons (Bucerius, Shultz and Haggerty, 2022). Linge, Sandberg and Tutenges (2023: p. 1384) consider that radicalisation processes among criminals are complex and unpredictable, and that exposure to jihadism fuels both radicalisation and resistance to it. It is therefore important to understand that prison can be both a favourable and an unfavourable environment for radicalisation.

The experience accumulated by the Civil Guard in prison investigations also points in this direction. There are many inmates, Muslim or otherwise, who reject jihadist radicalisation and terrorist violence and who, with due caution and confidentiality, denounce jihadists who pressure other inmates for not being 'good Muslims', either because of their sexual orientation or because they do not practise the religion in Salafist terms.

3.3 Prison in the jihadist narrative

Prison is a fundamental pillar of the jihadist narrative. A large part of the ideological developments of political Islam have taken place in prison. Ibn Taymiyyah is a paradigmatic example, very influential in contemporary Islam. A scholar of the Hanbali school of law, characterised as the most rigorous of all, with a literal, inflexible and uncompromising interpretation of the Qur'an and Sunnah, his thinking was based on the belief that Islam was perfect and complete in the time of the companions of the Prophet Muhammad (*al-salaf al-salih*). This led him to reject other variants of Islam, such as Sufism and Shiism, among others, calling for their persecution and declaring their followers *kāfir* (unbelievers). He was imprisoned for seven years for his legal rulings and confrontations with scholars from other schools of jurisprudence. Taymiyyah is a key figure in the jihadist imagination, defining imprisonment as a 'divine' blessing.

More recently, names such as Hassan Al Banna and Sayyid Qutb have become references in the jihadist imagination of martyrdom in prisons. Sayyid Qutb conceived his main work in prison. After the attempted assassination of Nasser, numerous members of the Muslim Brotherhood were imprisoned. During this period, Qutb wrote *Ma'alim fi-l Tariq* (Milestones), which summarises his political thinking, centred on the need to apply Sharia law in all areas of society and human relations.

Qutb's work was decisive in the evolution of later references. This was the case of Shukri Mustafali, a jihadist leader and follower of Qutb and the Muslim Brotherhood. He participated in the assassination of the Egyptian Minister of Religious Affairs and was convicted and executed in 1978. During his time in prison, he radicalised his views, considering the whole of society to be apostate and infidel. He was the main founder of the group or sect Takfir Wal Hijra (Anathema and Exile), a radical organisation that gained followers over time, especially after Shukri's execution. The same can be said of other individuals who were prominent in the rise of jihad. Muhammad abd-al-Salam Faraj, one of the ideologues of the Tanzim al-Jihad organisation, was executed in 1982 after being imprisoned. His political thinking was captured in a pamphlet entitled *Al-Farida al-gha'iba* (*The Forgotten Duty*). Ayman al-Zawahiri, one of the leaders of Al Qaeda, was imprisoned in Egypt. His stay in prison during the 1980s and the torture he suffered sharpened his radicalism and made him a leader among the other inmates.

Zaynab Al-Ghazali deserves special mention. It is important to highlight her role as a woman, given the significance of her story. Al Ghazali recounted her experience in prison in the first person under the title *Ayyam min Hayati* (*Days of My Life*) and is a symbol in that she extends to women the narrative of resistance against 'tyrants' in prisons.

The most recent manifestations of this phenomenon have found an ideal environment in crime and prisons to spread their narrative and attract followers. This is the case with DAESH, whose very origins can be traced back to a prison, as acknowledged by David Petraeus, the general who led the US operation in Iraq, when he admitted that: 'these extremists were basically running a university to train terrorists on our own premises' (BBC, 2015). His statements give us an idea of the important role played by prisons such as Camp Bucca and Abu Ghraib, where the leader of DAESH, Abu Bakr al-Baghdadi, self-proclaimed Caliph and 'leader of all Muslims', was interned, along with a dozen members of his leadership.

The link between crime and terror has been a growing concern in recent years. Basra and Neumann (2017: pp. 1-6) believe that DAESH has skilfully used its narrative to recruit members in these environments. The organisation's magazine, *Rumiyah*, has praised jihadists with criminal pasts and justified the commission of crimes as a means of waging jihad, saying that it is not behaviour that needs to be changed but motivation, which provides moral justification for individuals who feel the need to legitimise their behaviour. DAESH is well aware that people with criminal records have skills and resources that make them very effective in carrying out terrorist plans.

According to Civil Guard investigators, this form of redeeming sins or crimes, which modern DAESH jihadism defends in its propaganda, is attractive to young Muslims in Western prisons because it labels institutions as apostates and the jihadist imagination forgives them for their crimes if they join the jihadist cause. It should be remembered that in the early years of the jihadist group's growth, in order to swell its ranks, it adopted the strategy of the "Breaking the Walls" campaign[12], which succeeded in freeing hundreds of militants from Iraqi prisons between 2012 and 2013. This operation had a profound symbolic impact, presenting prisons as spaces of resistance and redemption. The resulting narrative reinforced the idea that imprisonment does not interrupt jihad, but is part of it, legitimising violence against prison institutions.

Berdún (2024: p. 205) cites several cases in which the jihadist propaganda apparatus has placed special emphasis on directing a promise of redemption to common criminals. For example, a group of British jihadists in Syria, calling themselves *Rayat al-Tawheed*, coined the apt slogan 'sometimes people with the worst pasts create the best futures'. Al Qaeda's magazine, *Inspire*, referred to the prisons of the infidels in 2016 and asked Allah to 'accept the exploits of our mujahideen brothers in the West, double their rewards, and for those who have been imprisoned, make their prison a garden among the gardens of paradise' (Bayliss, 2016). In 2016, in a video on the administrative structure of the caliphate, DAESH announced the existence of the 'Committee for Prisoners and Martyrs', whose mission was to monitor prisoners, rescue them, and help their families. In its magazine *Dabiq*, it mentioned prisons as a place to continue the struggle[13]. In its eighth issue, it interviewed Boubaker al-Hakim[14], who described his seven years in prison[15].

For DAESH, imprisoned members of the organisation are still considered 'soldiers or mujahideen' and important assets to the organisation. They must continue to wage jihad wherever they are and with the means at their disposal, even inside prisons and with the constraints of confinement. Thus, DAESH's strategy in prisons includes threats and attacks on prison officers, both security guards and other staff, as it considers this to be a legitimate and necessary struggle, which is why there are calls to attack prison staff inside and outside prisons.

12 The "Breaking Down the Walls" campaign was announced by the leader of Islamic State of Iraq, Abu Bakr al-Baghdadi, in a speech on 21 July 2012:

"And we bring you good news of the beginning of a new phase in our struggle. We are starting it with a plan we have named 'Breaking Down the Walls' and we remind you of your main priority: to free Muslim captives wherever they may be and to make it your primary goal to prosecute and kill their butchers (judges, investigators and guards)."

Excerpt from Abu Bakr al-Baghdadi's speech: 'And God wants nothing but to perfect His light' 21 July 2012.

13 See: *Inspire Magazine*. Autumn 2016. 1438. Issue 2016.

14 Boubaker Al Hakim had been arrested in Syria. Upon his return to France, he devoted himself to recruiting fighters to send to Iraq. Arrested for these acts, he spent seven years in prison.

15 Interview with Abū Muqātil At-Tūnusī. *Dabiq Magazine*. Issue 8.

3.4 Recruitment of new members

Recruiting members within prisons is one of the fundamental elements of jihadist narrative. This discourse was initially used by Al Qaeda and later by DAESH in a more refined way. Authors such as Yaacoub (2018) highlight the importance of prisons as spaces for radicalisation. Warnes and Hannah (2008: p. 408) also find similarities with the prison structures of terrorist groups such as the IRA and ETA, considering that much of the behaviour of jihadists in European prisons was a 'replica' of the way IRA and ETA prisoners behaved during their incarceration. The passage of time has nuanced this discourse, and although it is true that the problem of radicalisation exists, jihadist structures in prisons have not managed to replicate those of previous, more organised groups.

In France, Khosrokhavar (2013) considers that radicalisation processes in prisons occur between two individuals or small groups. The case of Italy is similar. According to Rhazzali (2017: pp. 261-286), the presence of organised groups that can be conventionally defined as radical Islamists does not seem to be a characteristic of the Italian prison system. In Spain, the phenomenon of radicalisation is described very clearly by Carou García (2019) in his study on jihadist recruitment in prison when he states:

> 'Prison, as a total institution, places the individual in an existential situation of extreme complexity, in which he is forced to develop social relationships – not of his own choosing – and to adapt to a markedly restrictive organisational and architectural structure. In such an environment, radical Islamic ideology, conveniently manipulated and adapted to the personal circumstances of each case, acts at different levels. Faced with the loneliness and uprooting caused by imprisonment, adherence to a fanatical Salafist ideology acts as an element of socialisation, thus preventing the individual from becoming isolated. Jihadist cells surround the individual with a false perception of respect and recognition within the group, so that he perceives a kind of community protection, an aspect that is particularly relevant in a hostile environment such as prison' (Carou-Garcia, 2019: p. 55).

Although the experience accumulated in recent years allows the prison institution to mitigate the phenomenon described by Carou García, the truth is that entering prison is a personal crisis. The impact of a new hostile reality forces the individual first into shock (loss of freedom, truncated projects and dreams, social shame) and then into reflection on the events that have led them to this situation.

Inmates who have additional vulnerabilities, such as the absence of a family support network, not speaking the language, lack of financial resources, or a solid religious upbringing, find themselves in the dichotomy of either advancing alone on their prison journey towards resocialisation or taking refuge in the protection offered by their peer group.

Case studies carried out by the Civil Guard in its investigations highlight that it is within this framework that radicalising agents operate, offering the group protection typical of prison subculture. In this case, under the cultural pretext of joining their

peers, the communal and tribal nature of the *umma*, being a 'good Muslim', and seeking redemption in the practice of the Salafist version of their religion, they are gradually initiated into jihadist indoctrination.

It should be borne in mind that we are dealing with a model of approach, recruitment and radicalisation in a closed and highly exposed environment in which victim and perpetrator coexist, despite the efforts of prison institutions to keep radicalising agents isolated and offer inmates leisure or work options[16]. As a result, vulnerable prisoners are easily integrated into peer groups that offer them a certain degree of protection and social comfort in exchange for following the self-appointed leader of the group.

In the case of young people from non-Western cultures, a profile that is becoming increasingly common in the Spanish prison system and which combines multiple vulnerabilities, other elements typical of youth come into play, such as defiance of authority, adventure, belonging to a subversive group that feeds the feeling of being victims of an unjust system, resentment and hostility. In this environment, individuals gradually shape their perception, justifying any affront or 'stressor' under the argument of 'you vs us' (the West vs the *umma*). Under this mindset, prison is illegitimate, while being united in hatred of the West or the infidels is not only legitimate but also a religious duty and a defence of one's own community that allows one to regain the honour lost in the commission of crimes. It is a path of manipulation that leads new followers towards utopian and destructive thoughts, in which jihad is seen as a redemptive renewal and martyrdom as liberation.

4 The case of Rida B. Threats and glorification of terrorism within the prison system

The importance of this case lies in the novelty of the legal classification of the acts committed by Rida B. (threats and glorification of terrorism) and the lengthy sentence imposed. It is also noteworthy that Rida B's actions must be interpreted in a specific context that has conditioned his activity. The prison environment limited the way in which the protagonist of this case carried out his pro-jihadist activity. It should be noted that his radicalisation process was a long one. According to the investigation, it lasted just over a year (from the first signs to when he swore allegiance to his leader and jihadist role model). This highlights the importance of monitoring by prison institutions, both in detecting his radicalisation process and in following up on it.

4.1 Context and background of the case

As we have seen in previous sections, there is a prison subculture that establishes customary rules outside the institutional framework and a religious subculture shaped

16 Instruction 17/2011, of 8 November, sets out the "protocol for intervention and rules in closed regimes", as Royal Decree 419/2011 of 25 March modified certain regulatory aspects and established the obligation to intervene in closed regimes, as well as the creation of a stable technical team and the implementation of a treatment programme.

by the fact of imprisonment that can condition the behaviour of the individuals who are part of them. Both factors can lead a sector of the prison population, influenced by certain narratives, to seek their own space for protest and confrontation with the administration. This confrontation presents a series of particularities due to the limits that the prison environment, especially in closed regimes, places on disruptive and risky behaviour that threatens the orderly coexistence of a prison establishment. In this context, we can situate the case of Rida B.

In this section, we will describe his process of radicalisation over the years and the difficulties that investigators from the Civil Guard's Information Headquarters encountered in reconstructing his life. We will also analyse the way in which Rida B. carried out his jihadist activity. It is necessary to dwell on the importance of radicalising agents in prison. In addition, attention must be paid to the importance of the glorification of terrorism and the threats made by Rida B. on behalf of DAESH, as well as the operational and legal response by the Prison Service, the Civil Guard and the National Court.

This case study provides us with a profile of prisoners who are vulnerable to radicalisation and who, once they have embraced this ideology, develop their own proselytising activities. Rida B. carried out his activities within the confines of closed prison wings, which greatly limited the resources available to him for carrying out his jihadist activities. Through the study of the radicalisation process, his links with other jihadists and his activity in favour of DAESH, a reality is revealed that often goes more unnoticed than that of those convicted of terrorism, but which does not therefore pose a lesser risk. Rida B. carried out at least two types of activities in support of DAESH, as documented in his sentence: on the one hand, painting flags of the jihadist organisation; on the other hand, threatening prison officials with explicit statements such as [17]: 'you are all going to die under the flag of the Islamic State'; 'I am going to kill you and your families [...] to kill in the name of Allah and the flag of the Islamic State'. In addition, Rida B. also showed signs of behaviour typical of prison life, such as boasting about his dangerousness and anti-establishment character. In many cases, this took the form of uncontrolled outbursts of anger stemming from his own character.

4.2 Limits on jihadist activity in the prison environment

Despite posing a risk to the life and physical integrity of prison staff and inmates, jihadist activity can be encouraged by the physical environment of a closed prison regime. These limits prevent actions carried out in a controlled environment such as a prison from being comparable in terms of means and execution to those that may occur outside. The Civil Guard analysts responsible for the investigation that led to

17 The investigation into Rida B. was conducted by the Sixth Central Investigating Court of the National High Court and tried by the Fourth Section of the Criminal Chamber of the National High Court. The oral and public trial took place on 3 and 4 February 2025. "Moroccan prisoner sentenced to another six years in prison for graffiti in support of Islamic State and threats." (El Debate, 2025)

the conviction of Rida B. emphasise this point. Even this type of activity is confused with events typical of prison dynamics. For example, threats to prison staff or the possession of homemade weapons by inmates may be considered normal in certain environments, despite the extreme danger they pose. An analysis of the operations carried out by the FCSE in prisons leads to the conclusion that the means used to recruit and radicalise other inmates are the same as those traditionally used in prisons: coercion, threats, the use of force, as opposed to the self-serving use of solidarity, group protection or favours.

Control by the administration is circumvented through mechanisms that are nothing new, except for the purpose of jihadist radicalisation. The main tools used for this purpose are intermediaries and chains of 'favours' and friendship that allow news to be passed between individuals. Officials working in closed prisons point out that it is common for inmates classified as first degree, due to rotations between centres, to know each other directly or indirectly. It is also common for this type of practice to be carried out individually or with the participation of two or three people[18]. It should be borne in mind that recruitment or glorification activities in prisons are extremely difficult and persistent. In addition, DAESH uses a series of symbols that can be expressed through gestures or through oral or written forms. Examples include the *tawhid* gesture (extending the arm with the index finger pointing to the sky to express the oneness of God) or the repetition of certain Islamic quotations.

These activities are perfectly suited to the confines of the prison system. As researchers from the Civil Guard point out, prison jihad and the radicalisation of third parties in this closed environment have particular characteristics. The dissemination of ideas is not based on physical media such as books or videos via the Internet. Everything is based on oral transmission through the recitation of certain suras from the Koran or *nasheeds,* messages sent through correspondence which, despite institutional control, flow through parallel channels, especially through what researchers have called "messenger pigeons", i.e. inmates whose correspondence was not subject to any kind of intervention. These letters convey greetings, support, loyalty and radical ideology, accompanied by feelings of opposition to the prison system. The vast majority of these letters include prayers and other religious texts from the Salafist creed and are accompanied by DAESH flags and even slogans used by the terrorist organisation, such as *baqiyah, tatamaddad, takbir,* and *Allahu Akbar.*

4.3 Rida B's radicalisation process

In its ruling 4/25, the National Court considered that Rida B.'s actions were part of the promotion and praise of DAESH. The Civil Guard's investigation has made it possible to reconstruct his radicalisation process, from before he even entered prison

18 Some examples of this type of activity reported in the press (El Mundo, 2015a, 2015b, 2026; El Independiente, 2020; El País, 2021a, 2021b; El Faro de Vigo, 2021; El Correo Gallego, 2021; Europa Press, 2021)

to the moment when he formalised his commitment to DAESH's ideology and objectives while in prison. The court ruling also describes him as a dangerous and disruptive inmate, which is why he was included in the FIES file.

Based on the Civil Guard's investigation, the National Court considered that Rida B.'s activity in prison was motivated by the designs of DAESH, which considers prison to be a suitable place for recruiting militants and spreading its radical ideas, inciting violent attacks against prisons and their staff[19] .

The reconstruction of this process has been meticulous and has been based on the investigation carried out by the Information Headquarters, as well as on reports from the General Secretariat of Penitentiary Institutions, technical eyewitness reports from various Judicial Police units, handwriting expert reports from the Civil Guard's Criminalistics Service, witness statements and other proceedings. All of these refer not only to the period of the criminal investigation, but also to the period prior to Rida B.'s imprisonment.

Sources close to the investigation warn that the convicted man had shown signs of radicalisation during his stay in a juvenile detention centre. At that time, Rida B. had photos of Osama Bin Laden and armed young people in conflict zones in his possession. Later, after entering prison and reaching the age of majority, he began to show signs of increasing radicalisation under the influence of a first radicalising agent. His behaviour became more violent and confrontational, with threats and attacks on prison staff as he continued his radicalisation process. The prison administration detected this incipient radicalisation process, which led to his classification as a FIES.

Gradually, his conflictiveness increased, and he began to maintain contact with inmates linked to jihadist terrorist cells and networks. Among these individuals, he contacted two inmates investigated in Operation Escribano for their high capacity for recruitment and radicalisation, one of whom was linked to two previous jihadist networks. As a result of these contacts, Rida B. declared in a letter his adherence to the ideology of DAESH and his loyalty to one of those investigated for terrorist recruitment and indoctrination in the network dismantled by the Civil Guard in Operation Escribano. It should be noted that Rida B. was investigated in that operation, detecting his level of radicalism and his oath of allegiance to one of the leaders under investigation, even going so far as to paint the DAESH flag in a prison courtyard, but his activity at that time did not result in criminal charges.

His radicalisation process continued with new incidents until he began to be investigated for the activities for which he has been convicted. Over a period of one year, between 2022 and 2023, he engaged in a series of behaviours with the clear aim of glorifying DAESH terrorism and intimidating prison staff in the name of the 'Islamic State'.

19 SAN 955/2025 - ECLI:ES:AN:2025:955. P. 4.

4.4 Graffiti and threats in prison

Rida B.'s activity focused mainly on graffiti and threats to the prison officers responsible for his custody.

As for the graffiti, the ruling considers that it constituted representations of the DAESH flag and its most characteristic slogans. Such graffiti was made with the purpose of spreading this doctrine among other inmates and anyone connected with the prisons[20].

The investigators, and subsequently the ruling, consider that the painted images were a representation of the *shahada* ('There is no God but Allah'), with a shape and distribution that has been adopted as a distinctive sign by the terrorist organisation DAESH, which defines it as the flag of 'unicity or monotheism' and serves to vindicate its actions and propagate its activities[21].

The graffiti was painted using the means and opportunities available to Rida B. in a controlled environment. This meant that the flags and slogans could not be exactly the same as the original or, as the Civil Guard officers explained at the trial, the background of the flag could not be black.

The investigation into Rida B.'s activity of disseminating DAESH symbols has made it possible to attribute the authorship of fourteen DAESH flag graffiti[22], ten of them in public areas such as dining rooms or courtyards where other inmates who are at risk and vulnerable to jihadist recruitment enjoy their leisure time.

Figure 4

Detail of graffiti painted by Rida B. of the DAESH flag on a wall in the common areas of a prison.

According to the ruling, these graffiti created a risky situation in which the display of the DAESH flag was not only a call for ideological affinity with the terrorist

20 SAN 955/2025 - ECLI:ES:AN:2025:955. P. 3.

21 SAN 955/2025 - ECLI:ES:AN:2025:955. P. 4.

22 Some graffiti was up to 3.5 metres high, making it highly visible.

group, but also an explicit call to wage jihad, a call that every person who considers themselves a "good Muslim" must practise jihad to the best of their ability. These were carried out in different prisons. Alongside the DAESH flag, Rida B. painted other slogans such as: 'Always smile, soldier'; 'Resist until you cease to exist'; 'Allahu akbar' ('Allah is the greatest') and 'Religion has never led us to do anything illegal'.

At the hearing, Rida B. stated that the graffiti did not represent a flag and that it was 'a wake-up call, in the sense of saying: gentlemen of the prison system, do something'[23]. In contrast to what happened in the past in the cases of ETA and GRAPO militants, it should be noted that it is common practice during criminal proceedings related to jihadism for individuals to deny their militancy.

As for the threats, these were directed both at prison officers as a group and at some of them in particular: '[...]You will find out because the flag of the Islamic State will soon be spread throughout the world and you will die as infidels'; 'Cowards, torturers, come and get me. I will kill you as commanded by the flag of the Islamic State present throughout the world'; [...] 'You will embrace Islam or die'; 'Allah is the only God, Muhammad his prophet and no one above God'; 'Soon the Islamic State will rule the world'. All of these statements were made for the purpose of making demands and appealing to the 'Islamic State' to reinforce their intimidating effect.

This intimidating effect was evident in the statements made by officials during the trial. The statements made by prison officials and the social worker who wrote the report in which Rida B. expressed his plans to kidnap and murder a prison official were decisive[24].

Rida B.'s aggressive state and his willingness to commit a violent act were demonstrated by the convicted man on numerous occasions with expressions such as 'being willing to do anything' or statements that if he carried out his violent intentions, people from the terrorist milieu would contact his family, as is often the case in suicide attacks.

The theft of razor blades from closed-regime departments is one of the few occasions on which a prison weapon or 'spike' can be made[25]. For investigators, the concealment of the blades constitutes a preparatory act in the context of violent actions that Rida claims to have planned and causes fear and alarm among officials. According to sources close to the investigation, this situation is based on the convergence of five elements: collective and individual threats to certain prison officials; the jihadist ideology embraced by Rida B.; the campaigns against prisons and prison staff promoted by DAESH; the plans to murder expressed by Rida B. in an interview with a social worker; and Rida's intention to obtain a sharp object. The

23 SAN 955/2025 - ECLI:ES:AN:2025:955. P. 9.

24 SAN 955/2025 - ECLI:ES:AN:2025:955. P. 16.

25 Other options include using window panes or trying to get hold of pieces of window hinges or bed fixing screws. Sometimes windows are torn out with the intention of using them as blunt objects against the officers who have to intervene to subdue the inmate.

investigation found that Rida B. managed to obtain blades on three occasions. This means that, considering himself a 'soldier of the Islamic State', he had taken steps to carry out his threats by stealing blades with which he could carry out his plans to attack.

4.5 Conviction and legal basis

Rida B. was convicted of glorifying terrorism and sentenced to three years in prison. He was also convicted of making unconditional threats against a professional group and sentenced to three years in prison. In the case of glorification, the Fourth Section of the Criminal Chamber of the National High Court considered that Rida B.'s conduct was serious enough to pose a risk that his activity could lead to the commission of terrorist acts in the future:

> 'The defendant's acts of public promotion, glorification and justification of the terrorist organisation DAESH, which, with his continuous and insistent acts of propaganda among the prison population of the centres where he painted images of DAESH flags, with their characteristic slogans unified in the *shahada*, created a risk of future acts of a terrorist nature among those who saw and read them, as these were not mere personal acts that did not transcend the confines of the cells in which the accused lived, but rather graffiti painted in common areas that were also used by the prison population not subject to the strict isolation regime applied to the accused. Furthermore, it is implausible and hardly coherent to deny, as the defendant's defence does, that the drawing was the DAESH flag because it lacked the characteristic black colour. Applying the rules of logic, the defendant lacked black paint with which to perfect his graffiti; instead, he drew the square outlines, the phrase about Allah, drew the seal of the prophet and alluded to his status, as depicted on the DAESH flag, which he did to the best of his ability and in accordance with the temporary conditions and availability of materials he had, as the accused himself has maintained, supported by the prison officer witnesses[26]'.

The court ruling is also forceful with regard to the existence of the crime of threats under Article 170.1 of the Criminal Code. The ruling considers that the threats are directed at prison officers as a group and are serious enough to have a frightening effect on their recipients[27]. In a context where threats are frequent, the ruling is innovative, arguing as follows for the conviction:

> 'In the present case, the intimidation referred to in Article 170.1 of the Criminal Code was directed by the accused, first at a prison officer, but later at other members of the prison service, affecting the group as a whole,

26 SAN 955/2025 - ECLI:ES:AN:2025:955 P. 7.

27 SAN 955/2025 - ECLI:ES:AN:2025:955 P. 8.

> not only because of the expressions used by the accused, but also because of the circumstances in which they were uttered, creating a state of fear and intimidation among the victims, since the accused made generalised statements and referred to the families of those who were listening to him, lending credibility to his statements, not only because of the literal meaning of what he said, but also because he implicated the terrorist organisation itself, for which he was promoting among potential new followers through his graffiti. Therefore, we maintain that the content and forcefulness of the terms used constitute serious threats capable of intimidating that group. Threats that do not require the actual instilling of fear in the passive subjects in order to be consummated, as it is sufficient that they come to the knowledge of the recipients, without considering them to be mere individual threats to the four people who are initially considered to be the passive subjects of the crime of threats that they witnessed, since their scope transcends them and encompasses the community of civil servants affected'.

5 Conclusions

The evolution of jihadism in the Spanish prison system shows a progressive institutional adaptation to a changing threat. From the first isolated cases in the 1970s and 1980s to the consolidation of networks linked to international terrorism in the 1990s, the prison administration has redefined its control mechanisms and collaboration with the intelligence services. The creation and subsequent consolidation of the Special Monitoring File (FIES) and the reform of the Prison Regulations in 2011 reflect this evolution, in which prisons have gone from being a marginal space in the phenomenon to occupying a central place in strategies for the prevention and detection of violent radicalisation.

From a prison perspective, the ruling highlights the limits, but also the capabilities, of the system to detect and contain processes of violent radicalisation. Despite the restrictions of the closed regime, the case shows how some individuals maintain significant proselytising activity. It also underlines the value of the prevention and investigation work carried out by prison institutions and the security forces, which are capable of reconstructing the radicalisation process and proving the terrorist intent of the convicted person.

The ruling constitutes an important development in the prevention and prosecution of jihadist activity in Spain. While previous convictions in the prison system had been for membership of a terrorist organisation or for recruitment and indoctrination, this ruling is a milestone in recognising the potential seriousness of certain acts laden with symbolism in a sensitive environment such as a prison.

Furthermore, the ruling considers that glorification poses a risk of radicalisation and polarisation of other inmates exposed to the influence of Rida B. and punishes behaviour, namely threats, that is common in interactions between the prison population and prison staff, considering that the behaviour is serious enough to warrant criminal punishment.

This case demonstrates the importance of consolidating early detection mechanisms and inter-institutional cooperation. The development of these policies will continue to be key to preventing the formation of jihadist groups in prisons.

Bibliography

Alcedo Moneo, M. (1996). *Militar en ETA: historias de vida y muerte.* San Sebastián: Haranburu Editor.

Arribas López, E. (2009). *The closed regime in the Spanish prison system.* [Doctoral thesis: UNED].

Basra, R. and Newmann, P. R. (2017). Crime as Jihad: Developments in the Crime-Terror Nexus in Europe. *CTC Sentinel*, 10(9).

Bayliss, C. (2016). ISIS recruits European criminals by promising redemption if they join heinous terror cult [online]. *Express*. [Accessed: 2026]. Available at: https://www.express.co.uk/news/uk/719727/ISIS-InternationalCentre-Study-Radicalisation-Rayat-Al-Tawheed-Banner-of-God

BBC. (2015). Cómo Estados Unidos contribuyó a la creación de Estado Islámico [online]. *BBC*. [Accessed: 2026]. Available at: https://www.bbc.com/mundo/noticias/2015/04/150422_eeuu_ayuda_crear_estado_islamico_irak_camp_bucca_lv

Berdún Carrión, S. (2023). *The organisational forms of terrorist groups in prison. From classic terrorist organisations to jihadism.* [Doctoral thesis: University of Granada].

—. (2024) *Political violence and the prison system in Spain.* Madrid: Tecnos.

Carou-García, S. (2019). Jihadist recruitment in prison. Analysis of legal instruments aimed at its prevention. *Cuadernos de la Guardia Civil: Revista de seguridad pública*. 59, pp. 47-68.

Dieguez, B. (1989). *Combate.* 485, p. 14.

El Correo Gallego. (2021). Cae en Teixeiro un preso por yihadismo. *El Correo Gallego*.

El Debate. (2025). Condenado un preso marroquí a otros 6 años de cárcel por hacer pintadas a favor del Estado Islámico y amenazar [online]. *El Debate*. [Accessed: 2026]. Available at: https://www.eldebate.com/espana/20250226/condenado-preso-marroqui-otros-6-anos-carcel-hacer-pintadas-favor-estado-islamico-amenazar_274023.html

El Faro de Vigo. (2021). Detenido en Melilla un presunto yihadista tras radicalizarse en la cárcel. *El Faro de Vigo*.

El Independiente. (2020). Detienen a un preso en Las Palmas que planeaba atentados yihadistas tras salir de prisión. *El Independiente*.

El Mundo. (2015a). Dos detenidos por enviar al PP una carta con amenazas de bomba en nombre del Estado Islámico. *El Mundo*.

—. (2015b). La Policía detiene a un preso por captar yihadistas y amenazar con bombas en Madrid y Barcelona. *El Mundo*.

—. (2016). Detenido un preso que avisaba de tramas yihadistas para atentar en España. *El Mundo.*

El País. (2021a). Detenidos tres reclusos yihadistas que dieron una paliza a otro que rechazó unirse a su 'célula'. *El País.*

—. (2021b). Detenido un expreso yihadista dispuesto a atentar que no pudo ser expulsado de España por la pandemia. *El País*.

Europa Press. (2021). Una operación policial frustra la actividad de adoctrinamiento yihadista de un preso en la cárcel de Daroca (Zaragoza). *Europa Press*.

García Martínez, J. M. (2008) Psycho-social functionality of beliefs in prison. *Social actions and research*. (25), pp. 171-200.

Garreaud, A. (2014) '... It was the blood of prison...' Biopolitics, bodies and anarchy behind bars. *Archives: Journal of Philosophy*. (9).

Khosrokhavar, F. (2013). Radicalisation in prison: The French case. *Politics, Religion & Ideology*. 14(2).

La Vanguardia. (2025). Un acusado de la yihad penitenciaria niega que amenazara a funcionarios y condena a Dáesh [online]. *La Vanguardia*. [Accessed: 2026]. Available at: https://www.lavanguardia.com/vida/20250203/10346770/acusado-yihad-penitenciaria-niega-amenazara-funcionarios-condena-daesh-agenciaslv20250203.html?utm_term=botones_sociales

Liebling, A. and Straub, C. (2012). Identity Challenges and the Risks of Radicalisation in High Security Custody. *Prison service journal*. 203(1), pp. 15-22.

Liebling, A.; Williams, R. and Lieber, E. (2020). More Mind Games: How 'the Action' and 'the Odds' Have Changed in Prison. *The British Journal of Criminology*. 60(6), pp. 1648-1666.

Linge, M.; Sandberg, S. and Tutenges, S. (2023) Confluences of street culture and jihadism: The spatial, bodily, and narrative dimensions of radicalisation. *Terrorism and political violence*. 35(6), pp. 1373-1388.

Marone, F. (2023). The Prisoner Dilemma: Insurrectionary Anarchism and the Cospito Affair. *CTC Sentinel*. 16(3), pp. 21-26.

Marranci, G. (2012). From Caged Bodies to Caged Souls: The Case of Former Muslim Prisoners and The Importance of Religious Counselling. *Countering Violent Extremism*. 23.

—. (2020) *Faith, ideology and fear: Muslim identities within and beyond prisons.* Routledge.

Reinares, F.; García-Calvo, C. and Vicente, Á. (2018). *Jihadism and prisons: an analysis of the Spanish case* [online]. ARI 123/2018, Elcano Royal Institute. [Accessed: 2026]. Available at: https://www.realinstitutoelcano.org/analisis/yihadismo-y-prisiones-un-analisis-del-caso-espanol/

Reiter, K. (2014). The Pelican Bay hunger strike: Resistance within the structural constraints of a US supermax prison. *South Atlantic Quarterly*. 113(3), pp. 579-611.

Rhazzali, M. K. (2017). Religious instances and negotiation of difference: Muslims in Italian prisons [translation by Agustina Zaros]. *Society and Religion: Sociology, Anthropology and History of Religion in the Southern Cone*. 27, pp. 261-286.

Sageman, M. (2004). Understanding Terror Networks. University of Pennsylvania Press.

—. (2008). Leaderless Jihad: Terror Networks in the Twenty-First Century. University of Pennsylvania Press.

Sunde, H. M.; Ilan, J. and Sandberg, S. (2021). A cultural criminology of 'new' jihad: Insights from propaganda magazines. *Crime, Media, Culture*. 17(2), pp. 271-287.

Sykes, G. M. (1958). *The Society of Captives: A Study of a Maximum Security Prison.* Princeton: Princeton University Press.

Veldhuis, T. M. and Kessels, E. J. (2013). Thinking before leaping: The need for more and structural data analysis in detention and rehabilitation of extremist offenders. *ICCT Research Paper*.

Warnes, R. and Hannah, G. (2008). Meeting the challenge of extremist and radicalised prisoners: The experiences of the United Kingdom and Spain. *Policing: A Journal of Policy and Practice*. 2(4), pp. 402-411.

Williams, R. and Liebling, A. (2023). 'Do prisons cause radicalisation? Order, leadership, political charge and violence in two maximum security prisons', *The British Journal of Criminology*. 63(1), pp. 97-114.

Yaacoub, S. (2018). British and Lebanese prisons: Are they fertile breeding ground for terrorism?. *Journal of Strategic Security*. 11(3), pp. 79-92.

Article received: 29 May 2025
Article accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Iván Soto Macia
Computer engineer and Master's degree in Intelligence. Expert in cybersecurity, strategy and foresight.

Email: adventt@protonmail.com

Wargames and the future of decision making

Abstract

The ability to make decisions is not only innate, it can be trained, but how to do so has never been a trivial matter: Can a firm and solid decision theory be constructed? Are the skills that make a good decision-maker transferable? Wargames have historically been an effective tool for exploring these questions.

The latest advances in artificial intelligence have given wargames a new lease of life and have substantially facilitated game support functions. However, their application in agents and assistants for choosing a course of action raises difficult questions. Can automatic agents solve some of the problems afflicting current methods of training and evaluating decision-makers—and specifically, wargames?

At the same time, the growing community of civilian players—whether in the field of e-sports or board games—offers collective intelligence and a massive and diverse testing ground, whose dynamics can be exploited. A diversified source of cognitive profiles relevant to the analysis of decision-making performance.

The analysis shows that at the intersection between wargames, artificial intelligence and civilian players, an unprecedented opportunity arises: to rethink how we train, evaluate and expand decision-making capabilities. Likewise, three lines of operational action are proposed: the establishment of comparable metrics between different types of decision-makers, the gradual integration of automatic agents and

the structured incorporation of the civilian community through collaboration mechanisms.

Keywords

Wargames, Tecision-making, E-sports, Civilian players, Automatic agents.

Cite this article:

Soto Macia, I. (2025). Wargames and the future of decision-making. *Journal of the Spanish Institute for Strategic Studies*. 26, pp. 547-568.

1 Introduction

The RAND Corporation defines wargames as analytical games that simulate military aspects at the tactical, operational or strategic level (RAND, n. d.). Their purpose is to examine the effectiveness of doctrines, train military commanders and analysts, explore scenarios, evaluate plans and possible courses of action (CoA), as well as their impact and consequences.

The use of wargaming is as old as war itself, with roots dating back to playful and ritualistic practices in various ancient and classical civilisations. However, its widespread use and formalisation as a systematic tool for training and strategic analysis originated in the military command centres of Prussia in the early 19th century, with the popularisation of Kriegsspiel (Caffrey, 2000).

Since then, wargaming has gone through cycles of boom and innovation—associated with volatile, uncertain, ambiguous and complex environments—and relative neglect – associated with periods of perceived stability. An illustrative example is the use, during the Cold War, of wargames as an essential element in planning nuclear scenarios, assessing deterrence doctrines and escalation processes in the context of a mutually assured destruction environment. In contrast, after the collapse of the Soviet bloc, its use declined in many military structures, displaced by a complete reliance on linear predictive models and established doctrine.

For obvious reasons, the 21st century, and especially the last decade (Work, 2015), has brought them back to the forefront. The growing complexity of today's conflicts—characterised by hybrid domains, asymmetric threats and accelerating change—highlights the need for tools that enable our decision-makers to explore the uncertain, anticipate the improbable and train adaptability. Their return is not simply a revival of past methods, but an adaptive reconfiguration in response to the demands of the present. Wargaming has evolved from an instrument reserved for military use to a versatile tool for navigating the complexity faced by organisations of all kinds, including civilian ones.

2 Methodology and scope

This essay is an analytical-conceptual narrative documentary review aimed at examining the current limitations of wargaming and its interaction with two variables: (i) automatic agents and (ii) civilian gaming communities.

Although not systematic, the selection of sources was made according to criteria of thematic relevance, authority and topicality. It should be noted that, although criteria of institutional diversity were applied, most of the contributions included are of Anglo-Saxon origin. This concentration responds to the objective dominance of research centres, military organisations and universities in the contemporary production of prospective literature on wargaming, and not to a deliberate restriction of the framework of analysis.

This is a flexible process that does not aim to be exhaustive, but rather to identify recurring patterns, structural limitations and opportunities for integrating variables that are in principle external to the world of wargaming. This approach provides an explicit and appropriate methodological framework for achieving the stated objective of the manuscript: to offer a structured synthesis and carry out a prospective exercise together with an action plan for the future.

3 Types of wargames and associated advantages

In 1962, the *United States Army Strategy and Tactics Analysis Group* (STAG, currently part of *the Centre for Army Analysis*) proposed a taxonomy of wargames according to their purpose (Roberts, 1962), which remains fundamentally valid today. They highlighted the following non-exclusive categories:

- Operational or analytical wargames: designed to test both the decision-maker (their skills, problem-solving abilities, analytical thinking, among others) and current doctrines. They are usually modelled on current elements and contexts that can be easily recognised by the player (organisations, equipment, tactics, etc.).
- Training or educational wargames: the objective is to facilitate learning in the decision-making process, understanding of a specific topic, historical event or doctrinal concept. They tend to simplify complex systems to focus on the desired lessons.
- Research or experimental wargames: these aim to analyse or evaluate new concepts, doctrines, alternative courses of action, etc., and are less factual and more speculative in nature.

In this context, as Perla and McGrady (Perla and McGrady, 2011) postulate, the practice of wargames offers multiple advantages. Although the category of wargame will determine the degree to which each of the stated objectives is achieved, the analytical exploration of new courses of action, the identification of opportunities for improvement and deficiencies in current doctrines, the modelling of new processes, and the anticipation of the consequences of certain decisions in safe environments are particularly noteworthy.

However, probably the most controversial aspect is the advantages that wargaming brings to the participants or players themselves. Improving the ability to understand and generate situational awareness, increasing critical and adaptive thinking, and superior decision-making skills are some of the proposed benefits. Unfortunately, these aspects are difficult to verify without a comprehensive and solid theory of decision-making.

Although the academic consensus (Sabin, 2014) suggests that wargaming is far from being a mature theoretical discipline, much has already been written on the subject, as well as on the use of technology and, in particular, Artificial Intelligence (hereinafter AI) in this type of process. This article, however, aims to focus on something more specific: (i) with regard to wargames, on the effects on the decision-maker, (ii) with

regard to the use of AI, exclusively on the role of automatic agents, and (iii) in the prospective field, on the impact that the contrast with the civilian player community would have on both types of players (military and automatic agents).

4 Limitations and problems of wargames

Before exploring how automatic agents and the civilian player community can help overcome some of the main limitations of wargames, it is worth first explaining what set of problems we are referring to. Without attempting to provide an exhaustive list, the main limitations and problems that wargames present today are (Grossman, 2023; Curry, 2020):

– The problem of modelling reality: this can be summarised by the statement that reality is too complex to be modelled and systematised in the form of a game. The process of designing a game abstracts characteristics of reality—like any model—which can result, at best, in an ineffective wargame and, at worst, in a pernicious wargame.

  It could be argued, however, that all decision-makers interpret reality through mental models, which are also subjective and simplified abstractions. The problem, therefore, is not that wargames are simplifications, but how and by what criteria these models are constructed[1].

  On the opposite side of the same problem, a high level of detail and realism reduces the repetitiveness of the game and limits it to a specific context and theatre of operations. This makes it difficult to generalise lessons learned and synthesise conclusions that can be extrapolated to other situations and codified in the form of new doctrines.

– The problem of input quality: as in any other information processing system, the quality of the output depends on the quality of the input. In the case of wargames, this translates into the relevance, diversity and richness of thought of the participants.

  When exercises are restricted to homogeneous player environments—primarily military—the game's ability to generate disruptive ideas, challenge established doctrine, or open up spaces for strategic innovation is also limited. The lack of cognitive diversity impoverishes the results and reproduces biases already present in the organisational structure.

  In this sense, wargaming must take all precautions associated not so much with simulation tools as with deliberative forums, where different perspectives can be confronted and generate novel solutions or creative disruptions.

– The problem of immersion: another fundamental limitation lies in the emotional disconnect between the decision-maker and the consequences of their decisions

1 At this point, it is necessary to consider whether, in the event of misalignment, it is desirable to push the wargame to adequately contain the player's decision-making framework, or to push the player's mental models towards the reality that the *wargame* aims to reflect.

on the field of action during the practice of a wargame. By transferring decision-making to a simulated environment, the impact of incidental emotions, which play a fundamental and recognised role, as described in various studies on general decision-making models (Lerner *et al.*, 2015), is reduced. Numerous authors, such as Rubia (Rubia, 2000) and Damasio (Damasio, 2011), argue that reason, far from being independent, is deeply mediated by emotional processes that systematically influence the assessment of risks and rewards. The rational weighing of alternatives cannot be understood independently of affective processing.

This emotional disconnect does not imply that decisions made in a wargame are qualitatively worse or less rational—one could argue just the opposite—but it does force us to recognise that they can never completely emulate the psychological conditions surrounding real decision-making. This problem profoundly qualifies the usefulness of wargames as educational and learning tools, while it does not significantly impact their use in improving and creating new courses of action.

– The problem of evaluation and feedback on results: a critical and often underestimated limitation is the difficulty of rigorously evaluating the results of a wargame and extracting systematic lessons. Wargames, unlike simulations, are essentially narrative and qualitative in nature, which differentiates them from systematic and purely quantitative tools. Many exercises lack robust ex-post analysis mechanisms to identify what has been learned about the doctrines and courses of action employed by the players or to what extent doctrinal hypotheses have been tested.

  Without clear structures for observation, conclusion and incorporation of lessons learned, wargames can become aesthetically appealing but epistemically sterile events. The lack of objective evaluation criteria makes it difficult to distinguish between valuable insights and mere lucky improvisations by the player. This limits their usefulness for designing new doctrines or improving procedures in operational environments. If we wish to support the legitimacy of wargames as an analytical tool, it will therefore be necessary to provide them with these observation structures, as well as mechanisms for the traceability and replicability of players' actions and their results, without compromising the social elements that make them distinctive and useful.

– The problem of the lack of a decision theory: finally, we must mention a structural deficiency which, although not exclusive to wargames, profoundly conditions our ability to evaluate their effectiveness and impact on the player: the absence of a solid, empirically validated theory of decision-making.

  Today, there is no established standard or scale that allows for the objective measurement of a decision-maker's ability, beyond the subsequent analysis of the consequences of their actions within the narrow framework of *the* wargame played. Without a robust theory, the assessment of the effectiveness of a wargame—and the improvement in the skills of its participants—is subject to informal criteria. Only intuition justifies some of the advantages we highlighted and which are perceived by those who practise the activity.

We refer to a model similar to those used for assessing IQ, for example, the Wechsler scale (Coalson, Raiford, Saklofske and Weiss, 2010). Different scales have been developed to assess specific cognitive elements that are fundamental to the gaming process, such as fluid intelligence, working memory, verbal working memory, social performance, mental flexibility and attention span. However, we do not have any similar element that integrates these abilities into a theory for decision-making in real contexts.

This gap has been pointed out by various experts (Banks, 2024) and represents an active line of research, especially in leading centres dedicated to the study of security or socio-economic decision-making[2]. Some pioneering projects, such as those developed by Carnegie Mellon University[3], have begun to exploit the role of AI in social decision-making (AI-SDM, short for *Artificial Intelligence Social Decision Making*). The growing number of publications and citations in this area in 2024 demonstrates the interest and expansion of this field.

These limitations do not invalidate the value of wargames as an analytical, educational or experimental tool—the three dimensions mentioned above—but they do highlight the need to rethink their design and, in particular, to determine the role that AI or civilian players can play in addressing some of these problems in a novel and effective way.

5 The role of Artificial Intelligence

5.1 Beyond automatic agents: simulations and use cases

One of the most common misconceptions when discussing AI in the context of wargames is its identification with simulation or data modelling systems. Although they share certain structural elements—scenario representation, rules of action, complex variable processing, attribution, etc.—these are tools with essentially different purposes and foundations (see table 1).

Simulations (e.g., those used for logistics prediction, operational planning, or conflict evolution) seek to replicate, with the greatest possible degree of accuracy, the behaviour of real systems: there is no problem with modelling reality; they seek to capture and reproduce it with the highest level of detail. Their logic is that of mathematical approximation, calibrating models with historical data, refining algorithms and equations, and offering probabilistic outputs. They do not aspire to explore decision spaces; the focus is on the result and not on the process, on prediction and not on deliberation, improvement of doctrine or learning by the decision-maker.

2 See: https://www.mors.org/Communities/Communities-of-Practice/Wargaming and https://idm.uni.edu/about-us/overview

3 See: https://www.cmu.edu/ai-sdm/

Compared to the openness and unpredictability of a wargame, simulations are deterministic. Integrating simulations into specific functions of a wargame, such as award processes, can enrich the game, but implementing them in decision-making processes jeopardises the very essence of the wargame (Compton *et al.*, 2025).

In the field of AI, the range of use cases it offers for *wargames* is very broad (Knack and Powell, 2023). In this regard, we can highlight:

Tabla 1: Comparación entre *wargames* y simulaciones

Característica	*Wargames*	Simulaciones
Propósito	Entendimiento de la complejidad y de la toma de decisiones humanas	Generación de datos, predicción de resultados
Competencia	Explora la interacción sistémica y el mecanismo causal	Proporciona probabilidades y simula condiciones
Aproximación	Centrada en el humano, iterativa y con un foco cualitativo	Basada en datos, algorítmico y con foco cuantitativo
Nivel de abstracción	Alto, estratégico o operacional	Bajo, táctico
Foco	Entender el "por qué"	Predecir el "qué"
Validación	Compleja, requiere juicio experto y diseño de escenarios	Complicada, pero susceptible de verificación cuantitativa

Figure 1. *Source*: author's own elaboration, based on Compton et al. (2025)

- Applications in wargame design: content generation, scenario generation, etc.
- Applications in game execution: opponent simulation (red cell), adjudication process, assistants for choosing a course of action, etc.
- Applications in game analysis: identification of key interactions, behaviour modelling, assessment of the decision-maker's accuracy, etc.
- Logistical applications: real-time translation, transcription of player dialogues, etc.

Particularly interesting—and therefore the focus of this article—are advances in agent modelling for game resolution and decision-making. This is what the Alan Turing Institute (Knack and Powell, 2023) describes as high-risk, high-reward applications, or what Davis and Bracken (Davis and Bracken, 2022) call long-term ambitions for AI-enhanced decision-making: assistants for choosing courses of action and simulating opponents[4].

4 We therefore focus on the application of assistants in *wargames*, but it should be noted at this point that it is not necessary to move around a board (and face the problem of modelling reality) in order to take advantage of AI in the decision-making process. In the field that deals with reality without abstraction, indeterminate or of unknown determination, it is called *decision-making under deep uncertainty* (DMDU). The objective, in this case, is not to optimise our CoA, but to find strategies with good results in the wide range of circumstances that an uncertain future represents.

5.2 Automatic agents: what are they and why are they important?

Regarding the first question, what are automatic agents, it should be noted that we are referring primarily to optimisation agents: systems capable of deciding and making inferences with the particularity that they learn from their observations of their environment.

Unlike traditional expert systems[5], which are based on pre-parameterised rules such as 'If A occurs, do Y' or 'If (A and B) occur, do Z', automatic agents do not rely exclusively on their a priori knowledge. Their strength lies in their ability to evaluate the different options available to them and choose a strategy or action not only because the inference rule indicates it, but because they can estimate, using a function (usually called a value or utility function), the degree of proximity of each option to the objectives pursued.

In the case of expert systems, the world is a state machine that is as simple or complex as the number of rules you have been able to parameterise. If the system encounters a situation for which it has no defined rule, it will be unable to decide. Automatic agents, however, do not need to capture reality through a set of rules. On the contrary, the utility function allows us to assess any situation, the possible actions to be taken and the possible states to be transitioned to, without the need to know them exhaustively in advance.

The relevance of utility functions is that they work well with uncertainty, and we can load most of the decision-making process into the state we know for sure, the current state. But how do we know which future states to apply these utility functions to? That is precisely what Markov decision processes do[6].

If we add machine learning engines to reweight our decision-making process, we have achieved a concrete description of a simple system: a reinforcement learning model. And if the learning engine is based on deep learning techniques, the term applied is deep reinforcement learning (see figure 1), one of the most promising fields of research in the world of AI.

Gráfico 1: Modelo esquemático de un sistema *Deep Reinforcement Learning*

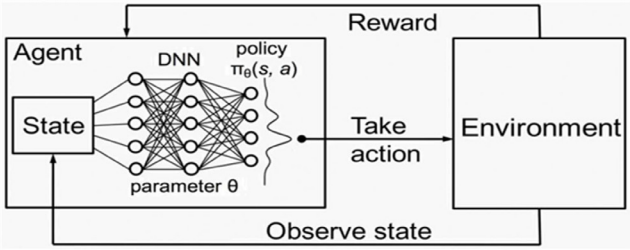


Figure 2. Source: Mao et al. 2016

5 An expert system is a system that aims to simulate human reasoning, in the same way that an expert in a field of specialisation would. They are fundamentally divided into rule-based systems, case-based systems and Bayesian network-based systems.

6 A Markov Decision Process is a procedure that occurs in non-deterministic environments or environments with a certain degree of uncertainty, using a state transition function to calculate the probability of reaching a new state when performing an action on the current state.

The paradigm is simple in its formulation but powerful in its implications: an agent faced with an infinite number of states that make up its environment anticipates the usefulness of the different states it can transition to (reward) based on the available actions, makes decisions (take action) and then adjusts its decision parameters using machine learning mechanisms. Through this continuous cycle of action and feedback, the agent progressively refines its performance.

Regarding the importance of automatic agents in game theory—and, by extension, in wargames—it is relevant to note that the scientific community's efforts to 'solve'[7] games using these agents is not arbitrary, nor is it based solely on a certain competitive component of performing tasks previously considered human using computers. Huge amounts of money are rarely invested for reasons not based on operational objectives and, as shown by Stanford's *Artificial Intelligence Index Report* (Nestor *et al.*, 2024), investment is growing in the private sector and skyrocketing in the public sector, particularly in defence departments. The application of optimisation agents to games is clearly more than just a passing fad.

'Transferability' is the key word. A paradigmatic example is Alphafold, DeepMind's deep reinforcement learning-based AI capable of predicting the protein folding process—with revolutionary implications for biology—which would not have been possible without AlphaGo. Agents that solve games are agents that can be applied to solving other problems, and depending on the characteristics of the games solved (e.g., Go, with a very complex field of action), the range of problems to be addressed will be more or less broad. This is known as the transferability and generalisation property of deep reinforcement learning.

Returning to the nature of games, we highlight three characteristics that will largely determine how simple or complex it will be to produce automatic agents that play at a superhuman level: (i) complexity of the field of action, (ii) real-time play, and (iii) complete/incomplete information play.

In games with complete information and differentiated turns, regardless of the complexity of the field of action, such as chess or Go, agents have long since surpassed the best human players. In real-time environments with high complexity of the field of action and incomplete information, characteristic of many video games such as *Starcraft II*, automatic agents are already at a level similar to that of the best humans. AlphaStar, also from DeepMind's Alpha series, reached the 'Grand Master' level in 2019. OpenAI, for its part, achieved comparable performance in *Dota2*. These achievements show that, under the right conditions, automatic agents not only reach but exceed the human level in strategic decision-making games.

How would an agent specifically designed to play wargames behave? As we have seen, achieving superhuman agents is not a technical issue; we can do it regardless of the characteristics of the game. It is a question of the business case being profitable,

7 When we talk about 'solving', we are really referring to tackling the problem at a superhuman level, not what is technically understood as a 'solved game' in game theory.

which brings us to the contingency of wargames and the absence of a firm decision theory, a clear benchmark for comparing the capacity of decision-makers and, particularly in this case, the usefulness of wargames as a training and competition tool. A search for the aforementioned transferability of capabilities with the aim of closing the gap between the decision-maker in the wargame and the decision-maker in a real theatre of operations. Is it possible to generate automatic agents capable of choosing superior courses of action, outside of traditional doctrine, and with greater speed and consistency?

Kofford, from DARPA, summarises the rationale behind research in this line of work (Freedberg, 2023):

> 'I'm a chess player, and there's a lot to learn from chess AI. Modern chess engines can not only beat human players, but they can also help them by analysing their games, commenting, and advising on better moves. Similar AI tools for warfare help commanders and their staffs to plan a military operation'.

In short, automatic agents can be understood as adaptive decision-making systems, capable of learning from their environment, anticipating consequences, and optimising their actions based on defined objectives. Their value lies not only in outperforming humans in certain games, but in their ability to transfer that performance to broader and more complex domains: from wargames to the theatre of operations. Without forgetting that this is the ultimate goal, these agents are also ideal for addressing several of the limitations and problems of wargames that we have outlined above, from the problem of modelling and diversity of thought to the difficulties of evaluation and the absence of a consolidated theoretical framework for decision-making. Below, we will explore how automatic agents can contribute to mitigating these problems and enhancing wargaming as a tool for learning and strategic analysis.

5.3 Contribution of automatic agents to mitigating the problems of wargames

Based on the limitations and problems of wargames, which we discussed earlier, we propose the following areas for improvement, derived from different ways of integrating automatic agents into the process:

– Support for modelling reality: the use of automatic agents allows the design of wargames with multiple actors/players without proportionally increasing the number of human participants, which makes wargames with more dimensions (economic, social, cybernetic, etc.) viable, reflecting a more complex and richer reality and chain of interdependent decision-making processes. In addition, agents can help mitigate some of the cognitive or institutional biases that contaminate design proposals, such as overconfidence or the tendency towards the *status quo* and a preference for 'acceptable' rather than optimal outcomes in the definition of the rewards associated with each action.

- Generation of cognitive diversity: one of the main limitations of wargames is the homogeneity of participants. Agents can be trained with different heuristics, strategic styles or deliberate biases (e.g., aggressive, conservative, exploratory, etc.), thus simulating a plurality of decision profiles that enriches scenarios and broadens the spectrum of outcomes.
- Design of adaptive and non-deterministic opponents: compared to the predictability of human opponents in simple environments, or doctrine-based scripts, automatic agents introduce dynamic adversaries that learn, adapt and explore new strategies. Unconstrained by cultural, hierarchical or doctrinal inertia, agents can identify and test unconventional strategies, contributing innovative ideas and thus broadening the spectrum of options available for strategic reflection and potential improvement of the decision-making process. Additionally, this increases the uncertainty of the game, enhances the sense of immersion and forces decision-makers to face unexpected dilemmas.
- Exhaustive and transparent tracking of the decision-making process: agents allow each step of their reasoning to be recorded and analysed—actions considered, utility assessments, discards and final choices. This level of traceability provides extremely valuable material for comparing processes, identifying biases and feeding structured feedback, traditionally one of the weaknesses of wargames.
- Unfortunately, when we talk about deep learning as a learning engine, we incorporate into the equation the well-worn problems of explainability, replicability and reliability that affect, in general terms, most AI solutions. The foreseeable rise of 'Causal AI' over the next few years may prove crucial in this regard.
- Comparative evaluation of human performance: agents can serve as a benchmark against which to evaluate the decisions of human participants. This comparison makes it easier to distinguish effective decision-making styles from ineffective ones, identify recurring error patterns and provide more objective feedback, overcoming the reliance on subjective or narrative judgements.
- Contribution to the construction of metrics and decision theory: the use of agents generates large volumes of structured data on decision-making in simulated environments. This data can be used to develop comparable metrics and, potentially, to cement a more robust theory of decision-making, thus filling the current gaps in the field.

Apart from the general problems associated with AI (we have already mentioned some, such as the difficulties posed by the problem of explainability in tracing the decision-making process), there are also specific pitfalls on the horizon for its application to wargames, notably:

- The problem of trust in the agent: overvaluing the courses of action proposed by the agent can cause the human decision-maker to assume as their own decisions that are the product of a hallucination or a poorly modelled situation. In general, the level of scrutiny of automatic decisions may be lower than that of human decisions, particularly if the causal chain is not understood.

- The problem of decision ethics: by definition, automatic agents are utilitarian, as are their utility functions. It is impossible to imbue them with categorical imperatives. Accepting the courses of action proposed by these agents can lead to ethical and moral dilemmas.
- The problem of attribution of responsibility: related to the previous problem, an automatic agent cannot be held responsible for the courses of action it proposes, so these decisions and their consequences are entirely attributable to the human in charge of the process (human-in-the-loop). This problem becomes more apparent when we leave the sandbox of our wargame and try to transfer the doctrine to the real world. To what extent would the decision-maker be willing to take these courses of action if they are unable to fully understand them?
- The problem of behavioural differences between automated and human agents: the learning of human decision-makers—it should be remembered that the effects on the decision-maker are the focus of our analysis—in wargames may not be entirely useful, given that the automated agent may exhibit clear behavioural differences. In the words of Parasuraman and Riley (1997), using automated systems can distort learning: humans are good at interpreting the intentions and patterns of other humans, but we have difficulty anticipating or understanding the behaviour of automated systems (giving rise to what the authors end up calling 'automation surprises'). There is a risk that, instead of acquiring generalisable learning, the human decision-maker will over-adapt to playing against automated agents.
- The training set problem: training these types of agents is very intensive in terms of the need for data and games. Synthetic training sets—generated by the agents themselves—reduce variability and affect the quality of learning.

6 The role of board games and e-sports

6.1 Untapped potential

If automated agents represent the technological side of the effort to overcome the limitations of wargames, there is a second, equally promising dimension: the civilian community. Parallel to advances in artificial intelligence, the growth of the civilian gaming community—from board game enthusiasts to e-sports professionals—has created an ecosystem with as yet largely unexplored potential for research and decision-making training. These environments offer not only a massive and diverse testing ground, but also a living laboratory of playing styles, creativity and coordination in highly competitive contexts. In this sense, analysing the role of board games and e-sports allows us to understand how the collective intelligence and distributed talent of civilian players can complement and enhance what automatic agents bring to wargames.

Any proposal for a comprehensive decision-making theory considers a set of cognitive components that form part of wargaming practice: fluid intelligence, working memory, verbal working memory, social performance, mental flexibility, and attention span, among others. These are exactly the same components involved in board games and e-sports.

With the growth in the practice of these games, interest in knowing what effects they have on cognitive abilities has also increased, and what was intuitively assumed is beginning to be proven: the improvement is real, in the same cognitive components that mediate in wargames. Furthermore, the benefits seem to be more pronounced the more demanding the difficulty factors already described for automatic agents are: real time, complexity of the field of action, and incomplete information. Based on these criteria, e-sports lead the way in cognitive gains (Martinez *et al.,* 2023):

> '[…] the findings demonstrate that play time predicts players' cognitive performance. It seems that video games affect cognitive performance more than board games do, which has never been demonstrated in previous studies. The unique features of this main game type surely explain its specific relationship with cognitive functions. Video games seem to have a greater potential for overall cognitive enhancement because they involve processing various types of information and adapting strategies dynamically and in real time'.

In the same way that speed training strengthens the lower body and in turn partly determines the athlete's overall performance, it is very likely that these cognitive components are not only impacted and improved, but also determine the ultimate quality of the human decision-maker. In short, these are transferable skills: what improves performance in a complex game also has an impact on other decision-making domains.

From this perspective, it is reasonable to expect that a competitive civilian player—whether a professional e-sports player or a board game expert—will perform well as a decision-maker in wargames. The transferability of the skills that make a human decision-maker brilliant remains a field of enormous potential, still largely unexplored and even less exploited.

6.2 Contribution of civilian players to mitigating the problems of wargames

Many of the limitations of the two domains mentioned above (wargaming and the contribution of automated agents to them) seem potentially solvable or, at least, mitigable with other approaches that incorporate civilian players:

- Support for wargame design and modification: tabletop and e-sports players bring practical experience in complex rule environments, emergent dynamics, and interaction systems that is extremely valuable for designing more robust games. They can help identify imbalances, introduce innovative dynamics and improve gameplay without sacrificing realism, thus helping to reduce the problem of static, oversimplified or biased modelling in accordance with current doctrine.
- Contribution to a comprehensive theory of decision-making: the widespread practice of strategic games provides empirical evidence on how the cognitive abilities involved in decision-making are developed and transferred. This wealth of data and experience offers fertile ground for advancing towards a more robust theory of

decision-making, overcoming the current lack of comparable metrics in wargames. Civilian players function as a natural field of experimentation.

– Diversity of thought and playing styles: we have already highlighted the cognitive diversity generated by agents, but in the case of civilian players, we have a human community that is diverse in age, gender, education and cultural background. This heterogeneity introduces variability in strategic styles, risk appetite and sensitivity to different dilemmas. In practice, this enriches wargames, reducing group bias and bringing creativity to decision-making processes, something difficult to replicate with automated agents without large amounts of training.

  As the literature on military innovation points out, many of the most significant doctrinal advances have emerged thanks to perspectives introduced by external actors who question established assumptions, revealing conceptual gaps and opening up new lines of tactical-operational adaptation (Millet y Murray, 1996; Biddle, 2006). Therefore, when civilian players participate in wargames—and often outperform professional military personnel—a very useful creative tension is generated between the old rules and the new tactics, prompting officers to constantly question and refine what they think they know.

– Generation of large volumes of non-synthetic data: both competitive board games and e-sports naturally produce massive databases, full of human decisions in highly competitive contexts. This material is an extraordinarily valuable resource for training, validating and stressing automatic agents, which normally depend on artificial data. In contrast, this data presents the real cognitive variability of human decision-makers, providing behavioural patterns that cannot be reproduced using synthetic data, which allows the behaviour of agents to be brought closer to the real complexity of the decision.

– Bridge between human decision-makers and automatic agents: civilian players, due to their utilitarian and competitive approach, occupy a middle ground. They lack the emotional immersion of military decision-makers, but they introduce human creativity and adaptability that automatic agents do not yet possess (it is impossible not to think of *Ender's Game* here). In this way, they act as a kind of 'missing link' that facilitates both the understanding of how agents learn and the validation of their performance.

– Element of comparison and competition: civilian players allow metrics to be established for comparison with military decision-makers by introducing human rivals with high strategic capacity in controlled game conditions. Competition, as has been demonstrated in other sporting and cognitive fields, acts as a powerful driver of continuous improvement. For wargames, this means providing an environment in which both humans and agents can be measured objectively, stimulating constant improvement.

  Institutions such as the Modern War Institute at West Point (Moran and David, 2022) have long studied the need to improve military decision-making and the potential benefits of contrast and competition with civilian players (gamers), such as improved speed, the incorporation of aseptic or dispassionate approaches, and the prevalence of informed intuition:

'Military officers realised that "their speed of decision-making was lacking compared to gamers with greater intuition and skill". This connects to real military concepts such as the OODA loop (Observe, Orient, Decide, Act), where faster decisions give you a huge advantage'.

7 An action plan for the future

Once both the problems and the potential solutions that automatic agents and civilian players can bring to the state of the art have been outlined, it is easy to sketch out a development roadmap for the future. The goal is to fit the pieces of this 'puzzle' into a roadmap that allows for orderly progress.

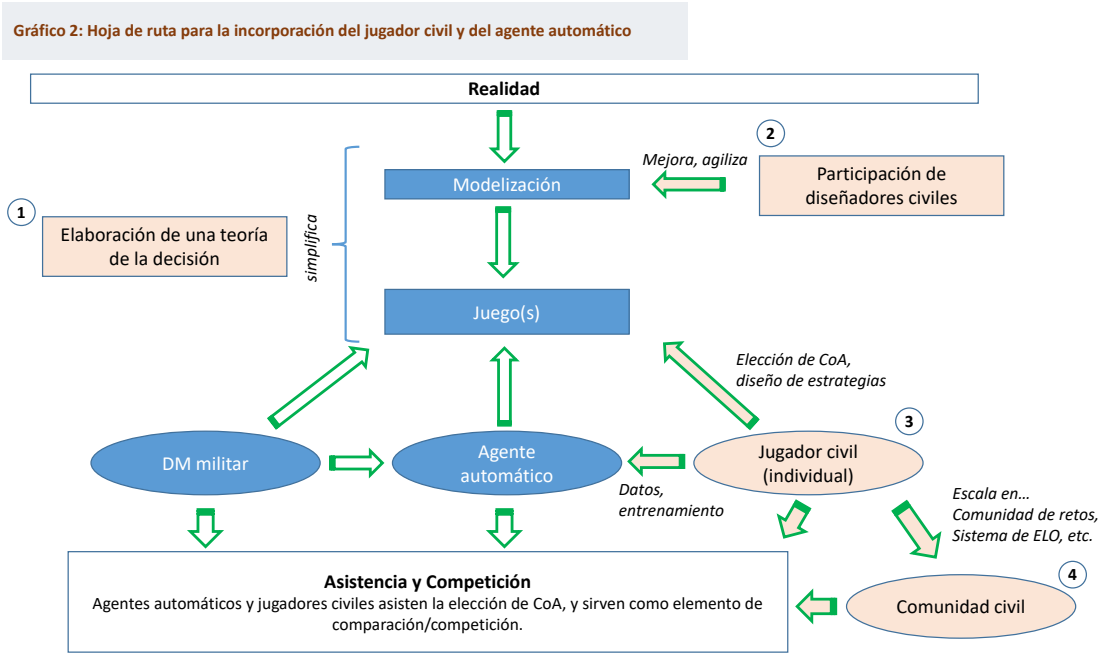


Figure 3. *Source*: author's own elaboration

In view of the above:

1. Development of a decision theory: the first step is to consolidate the foundations on which wargaming is based. The absence of a solid decision theory currently limits the ability of human decision-makers to evaluate and compare. Without attempting to resolve this structural deficiency, it is possible, in the field of wargames, to:
   - Isolate the cognitive abilities that are part of the decision-making process.
   - Weigh their relative importance according to different contexts and levels of uncertainty.
   - Develop comprehensive assessment scales that allow us to measure not only isolated capabilities, but also the overall performance of the human decision-maker as a complex cognitive system.

   This step involves laying the foundations of the intended cathedral, providing wargaming with a more solid conceptual and methodological basis.

2. Participation of civilian designers: at the same time, it is advisable to open the field to designers with experience in board games and *e-sports*. Their expertise in balance, game dynamics and user experience can:
   - Increase the production capacity of wargames, expanding the design pipeline.
   - Improve the quality, appeal, and challenge that these games pose for human decision-makers.
   - Introduce mechanical innovations that help overcome the problem of overly rigid modelling.
3. Civilian player participation: Civilian players—particularly competitive or professional ones—can gradually become part of the wargaming ecosystem, contributing in three key areas:
   - Generation of high-quality training data for automated agents, based on thousands of conveniently recorded human decisions.
   - Comparison and direct competition with military decision-makers, establishing objective metrics that promote continuous improvement.
   - Assistance in choosing courses of action and exploring alternative doctrines.
4. Civilian community participation: in a final stage, the active involvement of the wider community of players can be sought in order to harness their collective intelligence. Some examples are:
   - Open and collaborative challenges: if decision theory remains unconsolidated and wargames remain specific and contingent products, specific challenges open to the community can be designed, following 'Capture the Flag' models.
   - Gamification and professionalisation: if sufficiently abstract and generalisable wargames can be designed, they can be gamified and distributed, creating a competitive scene with ranking systems (dynamic Elo) through prizes and incentives. This would make it possible to identify civilian decision-makers with exceptional talent, amplifying the impact of the third point.

It is easy to draw up highly disruptive scenarios when the three driving forces—(i) decision theory, (ii) AI applied to *wargaming,* and (iii) the incorporation of civilian gaming—advance in a joint and coordinated manner. At that point, wargaming would cease to be solely a military training tool and become a global decision-making laboratory, where human creativity, the power of AI and the diversity of the civilian community would mutually reinforce each other.

8 Atlantic, European and Spanish doctrinal context

As part of NATO, Spain participates in an alliance that is very active in strategic innovation, where wargaming is a central formative and forward-looking element. Of particular note are the contributions of Allied Command Transformation (ACT),

which leads the Audacious Wargaming initiative[8], whose objective is to develop its own capacity within the framework of wargaming to explore strategic futures, stimulate critical thinking and experiment in controlled risk environments. As its name suggests, it is the organisational structure responsible for the most daring aspect of wargaming, which has a long tradition in the alliance and is currently very active[9], also through the Allied Command Operations (ACO).

At the European level, the European Defence Agency (EDA) was a pioneer in organising joint *wargames* in its field, although its efforts now seem to be focused on promoting simulation and modelling programmes such as the Integrated European Joint Training and Simulation Centre (EUROSIM).

In the Spanish context, although there is no visible or structured official doctrine like that of other European countries (UK Ministry of Defence, 2017; Bundeswehr, 2024), we do have a recently created reference point in the EMAD wargaming centre, both in terms of developing the activity and promoting it (for example, with the holding in 2024 and 2025 of wargaming conferences aimed at personnel from the Army, Navy and EMAD agencies). Particularly noteworthy is the involvement of the academic community in the centre's initiatives (Faculty of Education and Psychology of the University of Navarra), which facilitates the alignment of efforts not only towards the design of more effective wargames, but also towards the comparative metrics we propose in this essay.

On the analytical side, CESEDEN actively works on research into both *wargames* and the integration of emerging and disruptive technologies (EDT), particularly AI, and the convergence of these two lines of research is also frequently referenced in the centre's publications (Garat, 2024). In terms of integrating the academic and civil communities, CESEDEN's activities are channelled through collaboration agreements involving the university world, such as the Almirante Juan de Borbón Chair[10].

9 Conclusion

The incorporation of civilian players and the development of automatic agents applied to wargames should not be understood as alternative approaches, but as complementary dimensions of the same problem. While agents provide adversary simulation capabilities, adaptability and systemicity in the exploration of courses of action, civilian players introduce cognitive diversity, creativity and empirical data that enrich the training and validation of models. The convergence between the two approaches opens up the possibility of designing more rigorous and useful wargames and training decision-makers more effectively. An ecosystem where artificial

8 See https://www.act.nato.int/wargaming/ for more information.

9 See https://www.act.nato.int/activities/win24/ for more information.

10 See https://www.ucm.es/catedra_juan_de_borbon/ for more information.

intelligence and collective intelligence—civil and military—mutually reinforce each other, shaping a new horizon for research and practice in decision-making in complex environments.

Throughout this essay, a progressive action plan has been proposed that begins with the consolidation of a decision theory applicable to wargaming, continues with the integration of civilian designers and players, and culminates in the creation of a new strategic learning ecosystem. This roadmap must be translated into concrete operational lines that allow progress towards its implementation, beginning with:

1. Developing a system of metrics to compare decision-makers: regardless of whether they are military, civilian or automated agents. The usefulness of wargaming will increase significantly when it is possible to evaluate the performance of the decision-maker objectively and consistently. To this end, it is necessary to move towards a cross-cutting metric architecture that allows decisions and decision-makers to be compared. These metrics should evaluate aspects such as consistency under uncertainty, exploratory capacity, risk management, adaptation to demanding time frames, pressure situations or different scenarios (games).

   Given that this architecture is the operational dimension of decision theory yet to be developed, it will require institutional collaboration: agreements with universities specialising in cognitive psychology or other related fields such as data science applied to decision-making, as well as joint research programmes.

2. Progressive and controlled integration of automatic agents in wargames: they must be incorporated following a phased roadmap, defined in advance, until opponents are simulated. In the first phase, their role in support functions should be explored in depth: allocation and estimation of consequences, logistics or traceability of the decision-making process to improve *ex post* analysis. From there, agents should be trained in simplified wargames that allow parameters to be adjusted without the cost of operating in a complete environment. The next step could be their gradual introduction as assisted adversaries.

   This may require the creation of an institutional 'sandbox', where collaboration with applied research centres, in this case AI and computational game theory, can take place. Outside the academic world and unlike the operational front line, the technology industry, which has been working with AI for years in the development of adversarial agents for video games, would also have an important role to play here.

3. Structured integration of the civilian community: the incorporation of the civilian community—tabletop gamers, independent designers, wargaming communities, competitive e-sports players—can be articulated through concrete steps and mechanisms designed to generate operational, analytical and training value from the outset.

   First, it would be necessary to map talent, a preliminary 'cognitive catalogue' to guide calls for proposals and pilot programmes. This does not seem a complicated

task, as these groups are identified, segmented and highly motivated to collaborate if we are able to define the incentives appropriately. From this starting point, agreements should be established with clubs and associations to form stable groups that participate in iterative cycles of wargaming and specialised tournaments, with the aim of both collecting training data and identifying high-cognitive-performance players. Some ideas for these tournaments will include not only the confrontation of different types of decision-makers, but also wargames with mixed teams to analyse the tension between innovation and doctrine; or alternative doctrine days led by civilians.

In parallel, it would be desirable to establish a collaboration programme with independent publishers and designers, focusing on mixed design workshops, early validation of game mechanics and the transfer of design methodology from civilian to military.

Many of the skills involved in decision-making are transferable. Recognising this reality means abandoning prejudices and accepting that new generations of players possess, in certain cognitive aspects, a remarkable level of skill. It would be a missed opportunity to ignore this potential; integrating it, on the other hand, opens the door to a future where wargaming becomes a meeting place for technological innovation, human talent and methodological rigour.

Bibliography

Banks, D. E. (2024). The Methodological Machinery of Wargaming: A Path toward Discovering Wargaming's Epistemological Foundations [online]. *International Studies Review*. 26, (1). [Accessed: 2025]. Available at: https://doi.org/10.1093/isr/viae002

Biddle, S. (2006). *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton University Press. P. 20.

Bundeswehr. (2024). Wargaming Handbook [online]. [Accessed: 2025]. Available at: https://www.bundeswehr.de/resource/blob/5834032/9b940ee3d268b1a08b6b205b600bf155/en-handbuch-wargame24-data.pdf

Caffrey Jr., M. (2000). Toward a History-Based Doctrine for Wargaming [online]. *Aerospace Power Journal (Fall 2000)*. Pp. 33-56. [Accessed: 2025]. Available at: https://apps.dtic.mil/sti/pdfs/ADA521381.pdf

Coalson, D. *et al.* (2010). WAIS-IV. Advances in the Assessment of Intelligence. WAIS-IV Clinical Use and Interpretation [online]. *Practical Resources for the Mental Health Professional.* Pp. 3-23. [Accessed: 2025]. Available at: https://doi.org/10.1016/B978-0-12-375035-8.10001-1

Compton, J.; Mroszczyk, J., and Tattar, M. (2025). Too Much Tech Can Ruin Wargames [online]. *War on the Rocks*. [Accessed: 2025]. Available at: https://warontherocks.com/2025/06/too-much-tech-can-ruin-wargames/

Curry, J. (2020). Professional Wargaming: A Flawed but Useful Tool [online]. *Simulation & Gaming*. 51(5), pp. 612-631. [Accessed: 2026]. Available at: https://doi.org/10.1177/1046878120901852

Damasio, A. (2011). *Descartes' Error*. 1st ed. Barcelona: Editorial Destino.

Davis, P. K. and Bracken, P. (2022). Artificial Intelligence for Wargaming and Modelling [online]. *Sage Journals*. EP-68860. [Accessed: 2025]. Available at: https://www.rand.org/pubs/external_publications/EP68860.html

Freedberg, S. J. (2023). 3 ways DARPA aims to tame 'strategic chaos' with AI [online]. *Breaking Defence*. [Accessed: 2025] Available at: https://breakingdefense.com/2023/09/three-ways-darpa-aims-to-tame-strategic-chaos-with-ai/

Garat, J. M. (2024). Artificial intelligence as a factor in the transformation of military operations at the operational level [online]. CESEDEN, Ministerio de Defensa. [Accessed: 2025]. Available at: https://www.defensa.gob.es/ceseden/-/la_inteligencia_artificial_como_factor_de_transformacion_de_las_operaciones_militares_en_el-nivel_operacional-1

Grossman, T. (2023). The Promise and Peril of Wargaming [online]. *CSS Analyses in Security Policy*. 319. [Accessed: 2026]. Available at: https://css.ethz.ch/en/center/CSS-news/2023/03/the-promise-and-peril-of-wargaming.html

Knack, A. and Powell, R. (2023). Artificial Intelligence in Wargaming: An evidence-based assessment of AI applications [online]. *CETaS Research Reports*. [Accessed: 2025]. Available at: https://cetas.turing.ac.uk/publications/artificial-intelligence-wargaming

Lerner J. S. *et al.* (2015). Emotion and decision making [online]. *Rev Psychol*. 3(66): pp. 799-823. [Accessed: 2026]. Available at: https://doi.org/10.1146/annurev-psych-010213-115043

Mao, H. *et al.* (2016). Resource management with deep reinforcement learning [online].

[Accessed: 2025]. Available at: https://people.csail.mit.edu/alizadeh/papers/deeprm-hotnets16.pdf

Martinez, L.; Gimenes, M. and Lambert, E. (2023). Video games and board games: Effects of playing practice on cognition [online]. *PLoS One.* [Accessed: 2025]. DOI: 10.1371/journal.pone.0283654.

Moran, N. and David, A. (2022). Why gamers will win the next war. Modern War Institute [online]. *Modern War Institute.* [Accessed: 2025]. Available at: https://mwi.westpoint.edu/why-gamers-will-win-the-next-war/

Millett, A. R. and Murray, W.R. (1996). *Military Innovation in the Interwar Period*. Cambridge University Press.

Nestor, M. *et al.* (2024). The AI Index 2024 Annual Report [online]. AI Index Steering Committee. Institute for Human-Centered AI, Stanford. [Accessed: 2025]. Available at: https://aiindex.stanford.edu/report/

Parasuraman, R. and Riley, V. (1997). Humans and Automation: Use, Misuse, Disuse, Abuse [online]. *Human Factors*. 39(2), pp. 230-253. [Accessed: 2025]. Available at: https://doi.org/10.1518/001872097778543886

Perla, P. P. and McGrady, E. (2011). Why Wargaming Works [online]. *Naval War College Review*. 64(3), Article 8. [Accessed: 2025]. Available at: https://digital-commons.usnwc.edu/nwc-review/vol64/iss3/8

RAND. (n. d.). Wargaming [online]. RAND. [Accessed: 2025]. Available at: https://www.rand.org/topics/wargaming.html

Roberts, C. R. (1962). Development of Centaur. A computerised wargame (part I, General Considerations) [online]. [Accessed: 2025]. Available at: https://apps.dtic.mil/sti/tr/pdf/AD0296460.pdf

Rubia, F. J. (2000). *The brain deceives us*. 1st ed. Madrid: Temas de hoy.

Sabin, P. (2014). Simulating War: Studying Conflict through Simulation Games. Bloomsbury Publishing Group, London.

UK Ministry of Defence. (2017). Wargaming Handbook [online]. gov.uk. [Accessed: 2025]. Available at: https://www.gov.uk/government/publications/defence-wargaming-handbook

Work, R. (2015). Wargaming and Innovation, Memorandum [online]. US Department of Defence. [Accessed: 2025]. Available at: https://paxsims.wordpress.com/2015/04/02/wargaming-and-innovation/

Article received: 9 September 2025
Article accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Roberto Espinosa Valdes
Researcher in training at the UNED International Doctoral School. PhD Programme in International Security

Email: roberevtraceur@gmail.com

War as a game: strategic 'gamification' in contemporary armed conflicts

Abstract

This article analyses how various armed actors implement video game logic—'gamification'—in current armed conflicts. Using a comparative methodological design of case studies (the Russian-Ukrainian war, jihadist extremism and Latin American organised crime), an operational indicator rubric is applied to assess the degree of formalisation of these practices. The forms, functions and strategic objectives of gamification are identified and its operational, psychological and communicative effects on combatants and civilian audiences are assessed. The results show that 'gamification' acts as a strategic multiplier, enhancing propaganda and recruitment. It is observed that each case presents a different level (structured in Ukraine, symbolic in jihadism and informal in organised crime) and that these dynamics contribute to the transnationalisation of war narratives, trivialising violence and attracting young audiences in particular.

Keywords

Digital propaganda, Jihadism, Organised crime, Video games, Ukraine.

Cite this article:

Espìnosa Valdes, R. (2025). War as a game: strategic gamification in contemporary armed conflicts. *Journal of the Spanish Institute for Strategic Studies*. 26, pp. 569-596.

1 Introduction

War has never been limited to the physical and crude realm; historically, it has also been shaped by informational, symbolic and visual dimensions in which actors construct their own narratives of combat (Huizinga, 2000). This process has evolved over time and, today, a point has been reached where state and non-state actors resort to elements characteristic of video game design and interactive digital culture—such as the assignment of scores, levels, symbols, rewards or missions—to encourage behaviour, reinforce cohesion or maximise communicative impact (Lakhani *et al.*, 2022). This phenomenon is known as 'gamification' and should not be understood as the simple use of games for training, but rather as the systematic adoption of game rules and incentive systems in contexts outside of leisure; in this case, armed conflict. In this article, we take this definition in an operational sense and develop it in greater detail in the theoretical framework, where we reconstruct the academic genealogy of the concept and its transfer from video game design and reinforcement psychology to strategic communication and security studies.

The last two decades have seen exponential growth in the use of globally connected technologies such as smartphones, social media, audiovisual platforms and online video games. Various armed actors have taken advantage of these digital environments to create interactive, visually appealing, easily shareable content structured according to the logic of video game design: rankings of enemies killed, virtual rewards, and narrative episodes organised by levels, among other elements (Hassan and Hamari, 2020; Lakhani *et al.*, 2022; NATO StratCom COE, 2021). This 'gamification' of conflict has enhanced propaganda dissemination capabilities, facilitated recruitment, and boosted combatant morale, enabling competition for digital attention in the context of contemporary hybrid conflicts (Bachmann and Gunneriusson, 2015).

With its advantages and disadvantages, gamification substantially alters the social perception of armed conflict, transforming it into a visual and interactive experience that can contribute to the conversion of violence into spectacle and its trivialisation (Winkler and Dauber, 2014; Pötzsch, 2015). It thus becomes a tool that allows combatants to mobilise emotional support, construct heroic narratives, reinforce collective identities and generate dynamics of involvement similar to those of video games, especially among young people accustomed to such logic (Lakhani *et al.*, 2022; Hassan and Hamari, 2020).

At the same time, its strategic use poses ethical risks related to the glorification and aestheticisation of violence, as well as the possible desensitisation of audiences, whose production mechanisms are analysed in depth in the methodological section and fall within the ethical limitations of this study.

In this sense, 'gamification' is analysed here as a genuine strategic multiplier within the cybernetic and media dimensions of contemporary hybrid conflicts.

The application of video game logic to everyday life—and also to the realm of conflict—has been gradually incorporated, without the world having yet paused to reflect on its implications. Thus, fundamental questions such as what forms

'gamification' takes in contemporary armed conflicts, what strategic objectives armed actors implement it for, or what effects it may have on combatants and civilian audiences, remain largely unaddressed in strategic and security studies.

Addressing the above questions, this article aims to analyse how different armed actors apply gamification logic in the development of current and recent armed conflicts. To this end, the forms, functions and strategic objectives of these practices are identified and an operational rubric of 'gamification' indicators is applied to three case studies—the Russian-Ukrainian war, jihadist extremism and Latin American organised crime—assessing their operational, psychological and communicative effects on combatants and civilian audiences.

The article is structured in five distinct sections. First, a theoretical framework is presented that defines and distinguishes the main concepts of interest in the security context. Next, the methodological approach of the study is outlined. Subsequently, the three case studies are analysed in succession and a systematic comparison is presented. A discussion section links the findings to the specialised literature and public policy implications. Finally, the conclusions of the study are presented and possible lines of future research are proposed.

2 Theoretical Framework

2.1 Conceptual framework on 'gamification'

'Gamification' can be defined as the incorporation of elements of video game design into non-playful contexts in order to induce behaviour, generate engagement or alter the perception of reality. It should not be confused with the simple use of video games for training or simulation, as it involves introducing game structures into a real, non-recreational context, in this case, armed conflict.

The genealogy of the concept of 'gamification' dates back to its initial adoption in the business world in the late 2000s, when it began to be applied in marketing and human resources strategies to boost motivation through game mechanics. From then on, the playful approach quickly spread to sectors such as education, health and experience design, consolidating around 2010 as a wide-ranging strategy. Pioneering authors such as Werbach and Hunter (2012), Deterding *et al.* (2011) and Huotari and Hamari (2012) laid the conceptual foundations for 'gamification', demonstrating its usefulness in increasing participation in non-playful contexts and emphasising that it is not just a matter of adding superficial 'layers' of play, but of designing experiences that take advantage of the motivational potential of play in a structured way.

It is also necessary to distinguish 'gamification' from related concepts such as playification and serious games, as they are often used interchangeably despite referring to different phenomena. Playfulness refers to an attitude or disposition towards reality, usually for expressive, creative or recreational purposes, but without the intention of inducing specific behaviours or the presence of structured rules (Sicart, 2014). In contrast, 'gamification' involves the deliberate and structured adoption of game

mechanics—points, rewards, levels, missions, immediate feedback—within a real-world environment that is not a game, with the explicit purpose of motivating or directing the behaviour of participants (Deterding *et al.*, 2011). Thus, while a drone pilot who plays basketball for entertainment between missions would simply be introducing play into his routine, the score he is assigned for neutralising an enemy tank and which is recorded on a scoreboard is an example of 'gamification' of his warfare, by converting operational effectiveness into a quantified and comparable achievement.

Similarly, a serious game differs from 'gamification' in that it is a complete game created for educational, training or simulation purposes, rather than purely recreational objectives (Michael and Chen, 2006). In a serious game, the playful experience is at the core of the activity (e.g., a military video game designed to train recruits), while 'gamification' consists of inserting fragments or dynamics of play into an existing real activity. A mobile application that awards virtual medals for reporting enemy movements, or that ranks users in tables according to their contributions, constitutes gamification applied to conflict, insofar as it adds a layer of play to a real military practice, without becoming an independent game.

From a methodological perspective, it is important to define which practices will be considered 'gamification' in this study and which will not. Many traditional elements of military culture—insignia, ranks, rituals, honour systems—have existed for centuries and serve organisational, disciplinary, or symbolic functions, but they do not constitute a game in themselves (Frasca, 2007). Therefore, they are not interpreted here as 'gamification' unless there is a structured reinterpretation under a clearly designed game logic; that is, unless these elements are deliberately reused within a 'gamified' dynamic that turns them into components of a 'game system' with defined rules, objectives and rewards. Only under this condition of intentional design is 'gamification' considered to exist. Consequently, conventional military practices, such as awarding real medals for acts of bravery or using rank hierarchies, will not be classified as 'gamification' in our analysis unless they have been explicitly reconfigured as part of a system of 'gamified' points, levels or rewards.

Firstly, from the perspective of motivational psychology, 'gamification' relies heavily on extrinsic incentives that reinforce specific behaviours: points, rewards, rankings and other stimuli that act as 'prizes' for desired behaviour (Skinner, 1953). In this framework, scoring systems, medals, or rankings operate primarily as short-term reinforcements: they increase the likelihood that certain actions will be repeated as long as the incentive remains available and visible to participants. Self-determination theory suggests, however, that for gamification to have more lasting effects, it must also connect with intrinsic motivations, addressing individuals' needs for autonomy, competence, and social belonging (Deci and Ryan, 2000). When this occurs, game mechanics not only 'push' specific behaviours, but also contribute to consolidating a more stable sense of efficacy and belonging.

Secondly, from the perspective of the aesthetics of violence in the media, it should be noted that presenting war in a playful way can trivialise the seriousness of the conflict. Winkler and Dauber (2014) point out that video game-like aesthetics applied to war tend to trivialise violence and turn it into spectacle, diluting the moral barriers

that normally contain it. Pötzsch (2015) adds that interactive media transform combat into a visual product similar to a game, blurring the distinction between reality and playful fiction. Consequently, the 'gamification' of war can contribute to the conversion of violence into spectacle and its trivialisation, both for combatants and spectators, by reframing acts of real violence as if they were surmountable 'challenges' or achievements within a playful progression.

Thirdly, in the field of strategic communication and digital recruitment, gamification is emerging as a contemporary tool for attracting and retaining audiences. Hassan and Hamari (2020) have shown that gamified dynamics can reinforce civic participation in situations of political crisis, suggesting a similar potential for mobilising supporters in extremist contexts. Recent security reports (Dauber *et al.*, 2019; Lakhani *et al.*, 2022) warn that both jihadist organisations and right-wing extremist movements are incorporating gamified elements into their propaganda and online radicalisation activities. The Islamic State, for example, has imitated video game aesthetics and mechanics in some of its materials, presenting missions and symbolic rewards in a narrative reminiscent of franchises such as *Call of Duty*, in order to recruit young people familiar with video game culture and mitigate the perception of cruelty of such actions. In this way, 'gamification' acts as a strategic multiplier for propaganda and recruitment in the digital sphere (NATO StratCom COE, 2021), broadening the reach of war narratives and facilitating the recruitment of new generations of sympathisers and potential combatants.

Finally, the conceptualisation developed here is aligned with the analysis criteria that will be used later in the comparative section of the article. These criteria will make it possible to evaluate the presence and degree of 'gamification' in each case study, systematically distinguishing between fully structured manifestations, predominantly symbolic uses and informal applications of game logic. In this way, the concepts defined in this section establish a common framework that ensures consistency between the theoretical basis and the empirical evaluation of 'gamification' in the conflicts analysed.

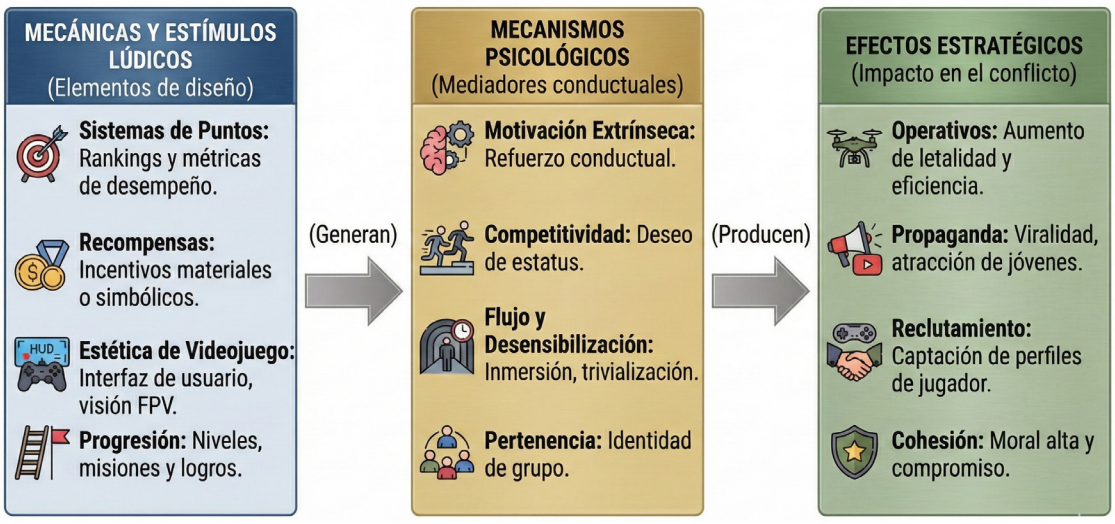


Figure 1 . Model of the strategic cycle of gamification in armed conflict. *Source*: Own elaboration. Shows the relationship between mechanics, psychological mechanisms and effects

2.2 *Common components*

The elements that commonly make up a 'gamified' system —as defined in the previous section— include the assignment of scores as reinforcement of behaviour (e.g. counting enemies killed) (Skinner, 1953), passing levels (which reflect progression and hierarchy), achieving accomplishments or badges (which remain linked to a profile forever), inclusion in leaderboards (which promote competition between participants, even from opposing sides), receiving immediate feedback (made possible today by the hyperconnectivity of the battlefield), completing missions with clear objectives—individual or collective—and, in some cases, the use of avatars or symbolic profiles (Werbach and Hunter, 2012; Deterding *et al.*, 2011; Huotari and Hamari, 2012).

It should be noted that many of these elements—such as hierarchies, badges, missions, or personal emblems—have been present in the military sphere for centuries, fulfilling organisational, identity, or symbolic functions (Frasca, 2007). However, in this paper, they will only be considered indicators of 'gamification' when these components are integrated into an explicitly designed game system with clearly defined rules, objectives and rewards, and not when they function solely as traditional symbols of status or belonging. In this sense, their transposition into the language of video games and their subsequent reimportation into the contemporary battlefield—for example, through scoreboards, digital rewards, or public leaderboards—has given them a new strategic and aesthetic dimension, which will be discussed later in the comparative section applied to the case studies.

2.3 *State of the literature and positioning of the article*

Based on the conceptual framework outlined in section 2.1, this subsection reviews the existing literature on 'gamification' to situate the specific contribution of the article at the intersection of security studies, strategic communication and armed conflict analysis.

The concept of 'gamification' is neither new nor exclusive to the military sphere. In the first instance, authors such as Werbach and Hunter (2012) have explored it in business, educational and healthcare contexts, highlighting how game mechanics facilitate motivation and participation in non-playful environments (Werbach and Hunter, 2012). Deterding *et al.* (2011) approached it from the user experience, analysing how its elements generate playability (Deterding *et al.*, 2011). Huotari and Hamari (2012) have placed it from a user value creation perspective, highlighting the importance of understanding gamification not only as the addition of superficial elements, but as a design process that produces meaningful experiences (Huotari and Hamari, 2012).

Moving into the political and communication arena, Hassan and Hamari (2020) study how gamification reinforces civic participation during political crises; Lakhani *et al.* (2022) analyse it as a form of narrative weapon used by extremist movements online; and the NATO StratCom COE report (2021), while not offering an in-depth analysis, describes the use of video games as an instrument of digital influence and

strategic propaganda. Specialised security reports, such as those published by Dauber *et al.* (2019) and Lakhani *et al.* (2022), have warned about the use of gamified dynamics in recruitment and radicalisation processes, consolidating gamification as an emerging issue in policies for the prevention of violent extremism.

In the purely military sphere, Pötzsch (2015) argues that the media transform war into a visual product with an interactive structure, while Allenby and Garreau (2017) propose conceiving 'digital warfare' itself as a 'gamified' experience. Added to this are works that examine the 'gamified' aestheticisation of violence in jihadist propaganda (Dauber *et al.*, 2019) or in state strategic communication campaigns, as well as journalistic and technical analyses of the 'gamification' of rewards in the Russian-Ukrainian war—for example, point systems associated with the destruction of targets or platforms that advertise rankings of units and operators.

Despite this growing interest, the literature still has several gaps from the perspective of strategic studies. First, most studies focus on a single area (civic participation, online extremism, or video game culture), without developing systematic comparisons between armed actors of different natures. Secondly, studies addressing the 'gamification' of war tend to focus on isolated examples or qualitative descriptions, but rarely operationalise the concept using explicit analytical criteria that allow for case comparisons. Thirdly, the aesthetic and symbolic dimension of 'gamification' has been examined in greater detail than its operational and organisational effects on combatants and military structures.

This article seeks to partially fill these gaps through two main contributions: on the one hand, it proposes a comparative typology that distinguishes between formalised, symbolic and informal 'gamification', applied to three substantially different cases—a modern conventional conflict (the Russian-Ukrainian war), a transnational jihadist actor and Latin American organised crime—which allows patterns and variations in different strategic contexts to be identified; and, on the other, it operationalises 'gamification' through an analytical framework that translates the conceptual framework into concrete indicators (components, functions and strategic objectives), facilitating systematic comparison between cases and dialogue with previous literature on hybrid warfare, propaganda and radicalisation.

3 Methodology

3.1 Type of study and methodological design

This article investigates the phenomenon of 'gamification' in conflicts from a qualitative and exploratory perspective; it does not seek to validate a specific hypothesis, but rather to understand and systematise this emerging phenomenon by developing an analytical typology of 'gamification' and its comparative application to several cases. To this end, a comparative design based on multiple case studies has been chosen, selecting conflicts in which 'gamification' manifests itself in different ways: a modern conventional war such as the Russian-Ukrainian war, the conflict waged by a transnational ideological and irregular actor such as the jihadist, and also

conflicts originated by non-state criminal actors such as Latin American organised crime. This selection responds to the intention to cover a broad spectrum of strategic and operational scenarios. The aim is to analyse how gamification adapts to different strategic, technological and narrative frameworks, identifying both common patterns and relevant variations between them, which are then systematised using a comparative rubric of indicators (table 1) that allows cases to be classified according to a typology of gamification (formalised, symbolic or informal).

3.2 Sources and analysis techniques

This work is based on a combination of academic literature and materials from open sources produced by the armed actors themselves. Although it starts from an analysis of existing academic work on gamification, hybrid warfare, visual propaganda and digital media—such as the work of Allenby and Garreau (2017), who examine digital warfare as a gamified narrative; Lakhani *et al.* (2022), who analyse the use of playful dynamics in the online extremist ecosystem for recruitment and cohesion; Pötzsch (2015), who explores how the media turns war into an interactive visual experience with video game aesthetics; or Werbach and Hunter (2012), who systematise the key elements of 'gamification' and its application outside of gaming—this article seeks to go beyond what has been covered in the academic literature and apply these insights to the systematic comparison of armed actors of different natures.

From an empirical point of view, a distinction is made between primary and secondary sources. Primary sources are considered to be content generated or disseminated directly by armed actors or their support environments (propaganda videos, clips edited with video game aesthetics, social media posts, bots and channels on messaging platforms, mobile applications and other technological resources used in the field). Secondary sources include reports from research centres and specialised agencies, analyses from verification organisations, academic works, and press articles that document, contextualise, or analyse these practices. Where possible, statements based on primary material are cross-checked with at least one independent secondary source in order to mitigate the bias inherent in overtly propagandistic content.

To this end, audiovisual and narrative material disseminated directly by armed actors will be studied, such as propaganda videos, clips edited with video game aesthetics, and content shared on social networks and platforms such as Telegram, YouTube, and TikTok. Mobile applications and technological resources used in the field will also be analysed, such as those designed to report enemy positions in Ukraine or automated jihadist bots and channels. The selection of these materials is based on criteria of theoretical relevance (clear presence of 'gamified' elements), accessibility in open sources and ability to illustrate recurring patterns in each case study.

The thematic content analysis, carried out manually, will identify patterns, structures and recurring elements in these communication products, while a narrative and symbolic analysis will help reveal the origin, intention and projection of the phenomenon of 'gamification'. Both types of analysis are guided by the typology and components defined in the theoretical framework, so that each piece of material can

be classified according to the predominant type of 'gamification' and the strategic functions it fulfils. In particular, the following are coded: (i) the 'gamified' components present (scores, levels, achievements, leaderboards, challenges, avatars, etc.); (ii) the functions they perform (motivational, promotional, organisational, recruitment or cohesion); and (iii) the degree of structuring of the system (formalised, symbolic or informal 'gamification'), which allows the degree and forms of 'gamification' observed to be evaluated in each case study.

To systematise the analysis, an evaluation rubric was designed comprising seven observable indicators corresponding to the main components of gamification (scoring systems, rewards, hierarchies, visual aesthetics, terminology, digital feedback and rankings). Each unit of analysis or fragment of the corpus was evaluated using these indicators on an ordinal scale (0: absence; 1: occasional/symbolic presence; 2: systematic/formalised presence).

This procedure made it possible to determine the degree of structuring of the system in each case (formalised, symbolic or informal) and to qualitatively identify the strategic functions performed by these elements (motivation, propaganda, recruitment or cohesion), the aggregate results of which are summarised in table 1.

Given that the corpus was coded by a single researcher, no inter-coder reliability tests were applied. Instead, to ensure internal consistency and validity of the analysis, an iterative process of category review and systematic triangulation of primary data with secondary sources was used.

3.3 Sampling procedure and delimitation of the corpus

The empirical corpus has been constructed through intentional sampling of materials that, according to previous literature and monitoring of open sources, are particularly relevant for illustrating the use of gamified dynamics in each case study (see the complete inventory in Annex 1). The aim is not to compile an exhaustive list of all the communications produced by the actors analysed, but rather to select a limited but significant set of pieces that clearly concentrate the analytical elements of interest.

In the case of the Russian-Ukrainian conflict, the sampling has focused on examples of platforms and campaigns that introduce scoring systems, rewards or leaderboards applied to military units, volunteers or citizens; as well as audiovisual pieces that present the destruction of enemy targets or participation in certain actions under an aesthetic typical of a video game. For jihadist actors, propaganda products and digital tools (videos, bots, social media channels, instant messaging applications and apps) have been selected that have been documented by specialised organisations and that explicitly incorporate mechanics or references typical of video game design. With regard to Latin American organised crime, the corpus includes videos, social media posts and viral challenges in which criminal organisations showcase their activities or their armed aesthetic in a particularly eye-catching and competitive way.

The selection of materials follows three main criteria: (i) clear presence of 'gamified' elements or playful aestheticisation applied to real conflict practices; (ii) observable relevance in terms of dissemination, repetition, or centrality in each actor's communication campaigns; and (iii) ability to be coded using the analytical framework described in section 3.2 (components, functions, and degree of structuring). Sampling continued until a point of conceptual saturation was reached, at which point new examples added minimal variations to the patterns already identified. Thus, without aspiring to exhaustiveness, the corpus is sufficiently varied and dense to support the comparative analysis presented in the following sections.

3.4 Ethical considerations and limitations of the study

The analysis is based exclusively on material publicly available through open sources (audiovisual platforms, social networks, public reports and academic literature). No closed channels or private communications have been accessed, nor has there been any interaction with online communities linked to the armed or extremist actors under consideration. Likewise, the study has avoided reproducing excessively detailed descriptions of physical violence, focusing instead on gamified structures and their strategic implications.

Given that part of the corpus consists of propaganda material, the study adopts an explicitly critical and contextualising approach. The biases inherent in these pieces are highlighted, and emphasis is placed on the instrumental use of 'gamified' dynamics as a tool for influence, recruitment or legitimisation of violence. The purpose of the article is analytical and preventive: it aims to offer a conceptual framework and observation tools that allow these practices to be recognised and understood, not to provide models that can be replicated or perfected by the armed actors themselves.

As this is a qualitative study based on open sources and the interpretation of a single researcher, the study has clear limitations in terms of exhaustiveness and generalisation. The corpus does not claim to be representative of all the communication produced by the actors analysed, but rather illustrative of certain 'gamified' logics. The results should therefore be understood as typological and analytical proposals that need to be verified and refined, and which may be expanded upon in future research, ideally combining other methods and additional sources.

4 Case studies

Based on the conceptual framework and methodology outlined in the previous sections, this section applies the typology of 'gamification' developed in the article to the comparative analysis of three areas: the Russian-Ukrainian conflict, transnational jihadist actors, and Latin American organised crime. In each case, manifestations of 'gamified' dynamics are identified, distinguishing between more formalised forms (structured systems of scores, rewards and levels), predominantly symbolic expressions (aesthetics and narratives inspired by video games) and partial or unsystematic uses of playful elements, in which some game-specific resources are incorporated

without forming a fully coherent system of rules and rewards. This structure allows for systematic observation of both the specific components of 'gamification' and the strategic functions they fulfil in very different operational and organisational contexts.

4.1 Russian-Ukrainian conflict: gamification in a modern conventional conflict

One case that deserves detailed analysis is the Russian-Ukrainian war, where the Ukrainian Armed Forces have deployed unprecedented strategic digital sophistication. They have integrated various digital platforms, chatbots and FPV (First Person View) drones, incorporating elements typical of video game logic in the midst of a war zone. This technological synergy has made it possible to verify actions on the front line in real time and motivate troops in new ways (Brave1, 2025; Kabachynskyi, 2025).

4.1.1 Promoting competitiveness between units

One of the most innovative mechanisms has been the implementation of a scoring and reward system for drone units. Since August 2025, the 'Army of Drones: Bonus' programme has been awarding e-points for each confirmed enemy kill, emulating the mechanics of a video game (Brave1, 2025; Kabachynskyi, 2025; Shevko, 2025). For example, shooting down a target awards points based on its tactical value: six points for eliminating a Russian soldier, twenty points for damaging a tank or armoured vehicle, forty points for destroying a tank or armoured vehicle, and up to fifty points for neutralising a large-calibre mobile rocket system.

Each point accumulated can then be redeemed on the Brave1 Market platform for military equipment: FPV drones, electronic warfare systems, ammunition, and even autonomous kits[1] (Brave1, 2025). This 'store' integrates its orders with the DOT-Chain Defence logistics network and, crucially, with the Delta situational awareness system. The latter acts as the game's verification engine: by integrating data from drones, satellites and sensors into a digital map, Delta dispels the "fog of war" and allows for real-time validation of destroyed targets (Bondar, 2024). Thanks to this integration, high-performing units have their scores audited instantly and receive new equipment within days.

This points system has encouraged internal competition between units. For example, the Magyar's Birds drone brigade accumulated more than 16,000 points in a few weeks, leading the Brave1 Market leaderboard (Brave1, 2025). That figure is equivalent to redeeming hundreds of additional drones for the unit, demonstrating the effectiveness of the model as a tool for motivation and resource distribution.

As for the use of FPV drones, Ukraine has employed them with an aesthetic clearly typical of video games. Many of its pilots come from the world of video

1 This refers to modules such as Auterion's Skynode, which equip commercial drones with autonomous flight capabilities and electronic warfare resistance through artificial intelligence. See Pokotylo (2025).

games, operating suicide drones equipped with GoPro or Insta360 cameras as if they were playing *Call of Duty*. The documentary Lethal Crysis (2025) shows how these operators use video game terms such as 'headshot' or 'kill streak' to refer to headshots and consecutive enemy eliminations. They even compete to hit difficult targets, creating a competitive gaming atmosphere that boosts both morale and emotional commitment (Lovett and Hinshaw, 2024; The Economist, 2025).

The specific details of how it works and the rewards are reconstructed from public documentation on the Brave1 platform and reports in the specialised press, so they should be understood as approximations based on sources available until mid-2025.

4.1.2 Citizen collaboration

Another key component of this war 'gamification' has been citizen participation through playful dynamics. The government app Diia incorporated the chatbot e-Vorog (literally 'e-enemy') so that any citizen can report Russian troop movements. Each civilian report is integrated into collaborative maps of the intelligence system and, as a symbolic reward, the application rewards each report with a flexed arm icon (an emoji symbolising strength) or other emblems (O'Carroll, 2023). This simple gesture has reinforced the sense of civilian involvement in the war effort, turning citizens into 'players' who compete to provide intelligence from their phones (O'Carroll, 2023).

Taken together, the practices described above allow us to characterise the 'gamification' of the Ukrainian case as predominantly formalised, without excluding symbolic components and specific uses of playful elements. The points system applied to the destruction of targets, the associated material rewards, and the existence of specific platforms that record and display the results of units and remote operators are a clear example of formalised 'gamification': the rules, scoring criteria, and incentives are defined in advance and integrated into the operational logic of war. At the same time, the visual aesthetics associated with drone videos, montages reminiscent of a video game interface, and certain heroic narratives built around specific units reinforce a layer of symbolic 'gamification', which translates real violence into a playful and competitive language. Finally, there are also occasional and unstructured uses of playful elements—references to 'kill streaks', inside jokes, or challenge formats on social media—which do not in themselves constitute a coherent game system, but which contribute to reinforcing the perception of war as a partially 'gamified' experience for combatants and observers.

4.2 Jihadist actors: individualised transnational 'gamification'

Global jihadism reached its peak of notoriety when the self-proclaimed Islamic State (ISIS or Daesh) managed to seize sufficient material resources and territory to combine classic state control with a model of decentralised insurgency. During its heyday between 2014 and 2019, Daesh controlled territories in Syria and Iraq, managed state institutions and, simultaneously, promoted scattered actions by lone wolves and autonomous cells on multiple continents (Winter, 2015).

The persistence of these groups demonstrates that contemporary jihadist warfare transcends physical borders and focuses on ideological conquest, strategically leveraging digital tools to recruit and retain followers. Audiovisual rhetoric plays a crucial role in this dynamic, using highly symbolic terms such as 'soldier of the caliphate', 'hero of the umma', 'sacred mission', or 'martyr level'—which equates death in combat with completing the final stage of a video game—carefully designed to generate aspirations of belonging, prestige, and symbolic status within the organisation (Lakhani *et al.*, 2022).

4.2.1 The narrative of jihad as a process of progression

The journey of the jihadist militant is structured as a path of personal improvement and reward, articulated in phases that are presented as achievable levels or achievements. The process begins with digital recruitment, followed by remote indoctrination, and culminates in various operational outcomes: joining local cells to carry out attacks; travelling to conflict zones to fight; martyrdom (suicide operations); or logistical or cyber defence activities (Lakhani *et al.*, 2022; Winter, 2015).

In all these itineraries, the narrative promotes the idea of overcoming stages until the maximum achievement is reached: personal sacrifice and eternal reward in paradise. Daesh has managed to systematise this journey with symbols, internal hierarchies and posthumous decorations that function as equivalents of achievements or insignia (Winter, 2015).

4.2.2 Audiovisual production with a 'gamified' aesthetic

The rise of Daesh coincided with unprecedented sophistication in its audiovisual propaganda, adopting visual and narrative techniques clearly inspired by video games, particularly those of the genre known as *First Person Shooter* (FPS, in which the weapon is seen in first person). Various academic studies have documented that ISIS propaganda videos reproduce elements such as superimposed scores, subjective perspectives similar to video game viewfinders, replays of highlights, and the use of dramatic music, creating a visual experience for the viewer comparable to that of a realistic combat video game (Dauber *et al.*, 2019).

These audiovisual resources are not merely aesthetic, but serve a crucial strategic function: they represent violence as a playful challenge, reduce empathy towards victims, exalt individual performance, and enhance feelings associated with competition and control (Andrews, 2023).

Jihadist actors have also developed specific digital tools that integrate gamified features to recruit, indoctrinate and retain followers. These include mobile applications and bots that use mechanisms typical of playful logic to encourage constant interaction and ideological adherence.

A clear example is the mobile application Salil al-Sawarim (Clash of Swords). Although not strictly a video game, it is an interactive propaganda product designed

with typical video game elements that seek to ideologically train future combatants and sympathisers (Hunt, 2016; Weimann, 2015).

In addition, jihadist groups have created numerous bots on Telegram that promote interaction through simple religious question-and-answer games, theological knowledge challenges, and virtual rewards that encourage regular participation (Prucha, 2016).

4.2.4 Strategic objectives of gamification in contemporary jihadism

The use of gamified elements by jihadist actors is a strategy designed to achieve specific objectives that strengthen their operational, ideological and communicative capacity:

Firstly, it encourages the recruitment of new followers, especially young people familiar with the dynamics of video games and digital platforms (Lakhani *et al.*, 2022). Secondly, it allows for effective desensitisation to violence, trivialising it by turning it into virtual achievements or challenges, which facilitates the transition to extreme acts (Pötzsch, 2015; Dauber *et al.*, 2019). A third objective is to strengthen internal cohesion by generating friendly competition that boosts morale, ideological adherence and commitment to the organisation (Winter, 2015; Prucha, 2016). Finally, it significantly enhances propaganda effectiveness, achieving greater virality and impact on social networks and audiovisual media, thus expanding its symbolic impact (Winkler and Dauber, 2014; Lakhani *et al.*, 2022).

Gamification is thus consolidating its position as a key multifunctional tool for maintaining the relevance and strategic operability of contemporary Islamist extremism.

Based on the typology proposed in this article, the 'gamified' practices of jihadism combine these strategic objectives with three levels of structuring: At the most formalised end of the spectrum are the applications, bots and platforms that assign 'missions', rewards and scores to sympathisers and combatants, configuring relatively coherent and persistent game systems over time. On a symbolic level, audiovisual production with video game aesthetics and the glorification of 'heroes' or martyrs functions as a 'gamification' of the narrative, turning jihad into a journey of progression and visible achievements. Finally, in a more specific and less structured way, the circulation of memes, inside jokes and playful references in informal channels reinforces the perception of violence as a challenge, without constituting a complete game system, but echoing the formalised and symbolic dynamics described above.

4.3 Latin American criminal violence: 'gamification' and violence as spectacle in illegal economies

4.3.1 Gamer aesthetics and the visual narrative of organised crime

Criminal gangs and groups in Latin America, with particular emphasis on Mexican cartels (Sinaloa, CJNG) and Colombian paramilitary structures (Autodefensas

Gaitanistas de Colombia, Autodefensas Conquistadores de la Sierra Nevada), use visual references and narratives typical of video games to construct their narrative and thus capture the attention of young audiences. These strategies are mainly disseminated on social networks popular among young people (TikTok, Instagram, YouTube, and Telegram). Unlike formalised gamification models with points or reward systems—such as those used in conventional military contexts or in jihadist propaganda—Latin American criminal groups opt for purely aesthetic gamification. There is no explicit scoring system or closed gaming environment; instead, they incorporate visual elements from the world of video games to embellish their messages and displays of power.

This visual approach is particularly effective among young audiences, who crave power, status and social recognition. As Carrillo, the 14-25 age group is particularly susceptible to these narratives, as they offer immediate access to prestige and notoriety that are normally unattainable in their native environment (Carrillo, 2021).

Among the aesthetic resources characteristic of this strategy are: fast-paced electronic music or remixed narco-corridos as the soundtrack to violent clips, graphic overlays in the style of video games such as *Grand Theft Auto* or *Call of Duty*, with superimposed texts such as 'mission accomplished' or 'target eliminated', rapid video cuts that eliminate pauses and focus solely on confrontations and displays of weaponry (this causes continuous cortisol generation in the viewer), and the use of visual symbols (emojis, video game iconography, or violent films such as *Scarface* or *The Inferno*).

In Mexico, the trend known as 'Narco-TikTok' shows young cartel members displaying weapons, armoured vehicles, luxury items and status symbols using filters and aesthetics inspired by video games (Carrillo, 2021; Bonello, 2022). Videos attributed to the Jalisco New Generation Cartel (CJNG) on TikTok show how this audiovisual style makes violence go viral (Bonello, 2022). Meanwhile, in Colombia, videos edited after attacks by the Clan del Golfo circulate on Telegram channels to flaunt their power with video game symbolism (Quevedo Delgado, 2025). These clips transcend the group's immediate circles and reach much wider audiences, normalising violence even among sectors of the population unrelated to crime.

The adoption of 'gamer' aesthetics not only embellishes the criminal narrative, but also trivialises violence, presents membership of the armed group as an attractive and aspirational experience, and projects an image of immediate success with easy recognition. This is a particularly seductive combination for young people with few socio-economic alternatives, as it presents criminal life as a fast track to prestige and gratification.

4.3.2 Symbolic rewards, viral challenges and digital validation

Although these groups do not develop formal 'gamified' applications or systems, they reproduce dynamics typical of video games both in their internal practices and in their online propaganda. These dynamics include public challenges, symbolic rewards and informal competition between members, all aimed at generating status and recognition within the organisation. Unlike traditional military rewards,

contemporary criminal 'prizes' are linked to the digital logic of instant validation, where the public display of achievements and their viralisation on social media are equivalent to 'levels' or 'unlocked achievements' in a game.

One of the most notable practices is the creation of personalised corridos for hitmen and leaders (Carrillo, 2021). Songs have been composed dedicated to figures such as 'El Chino Ántrax', 'La Chapiza' and another dedicated to Alias 'Naín' of the Autodefensas Conquistadores de la Sierra Nevada, broadcast on platforms such as Spotify and YouTube.

Viral challenges on TikTok or Telegram that encourage competition between criminal cells are also proliferating. Challenges to show off the largest convoy or to record oneself dancing with heavy weapons have become popular, generating content that reinforces the culture of violence and its symbolic appeal (Carrillo, 2021; Bonello, 2022).

In this context, violence is not the only way to climb the criminal hierarchy; digital success—measured in views, likes, and other reactions—becomes an additional indicator of status. Fame on social media reinforces criminal identity and fuels internal rivalry, as each member seeks to surpass the viral exploits of others.

4.3.3 Aspirational effects and state weakening

The dissemination of 'gamified' content on social media acts as an aspirational gateway for many young people by promising them quick access to status, luxury and recognition. This effect is particularly powerful among those facing severe socio-economic deprivation, for whom such forms of success were previously unattainable. The viralisation of these messages thus turns criminal activity into a viable and attractive path to social advancement.

The appeal of this playful-criminal narrative transcends the merely economic: criminal networks offer their recruits immediate social prestige, access to material goods and the opportunity to forge a respected identity in the community: the most outstanding members are rewarded with luxury vehicles, exclusive jewellery or ornate weapons, tangible rewards that consolidate individual prestige and highlight their progression in the criminal hierarchy. This encourages other members of the organisation to imitate such behaviour. This symbolic promise of 'being someone' is particularly seductive in environments where the state lacks legitimacy or effective presence (Carrillo, 2021; Marchini, 2023).

Another disturbing effect is the trivialisation of violence: brutal acts are transformed into mass-consumed digital content, which reduces the perceived seriousness of these events and raises the threshold of social tolerance. Constant exposure ends up normalising even the worst atrocities.

Ultimately, this criminal 'gamification' contributes to weakening the legitimacy of the state and poses new challenges for public safety and youth prevention policies, especially in communities exposed to institutional neglect and a lack of socio-economic alternatives.

Based on the typology proposed in this article, manifestations of 'gamification' associated with Latin American organised crime are generally less formalised than in the Ukrainian case, but this does not make them any less relevant. Firstly, forms of symbolic 'gamification' can be identified, in which the display of weapons, vehicles, territories and lifestyles is presented in a competitive aesthetic that invites comparison of the exploits, status and 'brands' of each organisation, bringing their image closer to the world of action video games. Secondly, there are specific and unstructured uses of playful elements, visible in certain viral challenges, internal jokes or informal recognition dynamics (who has participated in more confrontations, who has accumulated more 'feats'), which reinforce the perception of violence as a challenge or personal achievement without crystallising into a coherent game system. Although the degree of formalised 'gamification' observed in other contexts is rarely achieved here, these practices contribute to normalising violence, reinforcing internal hierarchies and maintaining group cohesion, especially among younger members who are familiar with video game culture.

5 Discussion

5.1 'Gamification' as a multiplier in modern warfare

The cases studied show that gamification acts as a multiplier of effectiveness in modern armed conflicts, generating cumulative effects on combatant morale, recruitment capacity, and propaganda, which ultimately has a cross-cutting impact on the different dimensions of the conflict.

Firstly, focusing on the effects on combatant morale, gamification can transform the area of operations into a motivational scenario, where each action becomes a challenge and an achievement if overcome. This increases individuals' psychological resilience and prolongs their commitment to the organisation. A clear example is the case of the Ukrainian conflict, where scores and real material rewards are used to incentivise drone operators; in the case of jihadist terrorism, progression follows an upward logic towards martyr status; and, finally, in Latin American organised crime, immediate recognition is sought, both within the group and in the wider social sphere, especially through social media.

Secondly, gamification builds strong collective identities, fuelled by internal symbols and recognition. Individual action is stimulated not only by the aim of living up to the group's standards, but also by informal competition between members, seeking to stand out or outperform other colleagues. The perceived ease of progressing within these structures also acts as a powerful incentive for recruiting new members.

Finally, 'gamification' helps to turn violence into attractive content for a digital audience. The posts are adapted to the patterns of short, fast-paced videos, similar to those used by social media influencers: vertical clips, less than a minute long, full of visual effects, fast-paced music and fragmented information to maximise their emotional impact. Thus, the target audience is less reluctant to consume this content, normalises it and, in some cases, perceives it as acceptable or even entertaining.

5.2 Differences in gamification models

It has been observed that each case studied presents a very different level of formalisation of gamification. The Ukrainian case is the most formalised, with scoring systems, real material rewards, official government applications and direct interaction between the state and combatants. The jihadist case follows a symbolic model, based on spiritual progression and the narrative of a transcendental mission, without the use of applications or tangible rewards. For its part, gamification in Latin American organised crime is presented as an informal model, geared towards receiving immediate rewards and social status, without a formalised structure or institutionalised systems.

These contrasts are supported by the systematic codification of several observable indicators of 'gamification'. Table 1 summarises the values assigned (0: absence; 1: occasional or symbolic presence; 2: systematic or formalised presence) to each indicator in the three cases analysed.

TABLE I. CODIFICATION OF 'GAMIFICATION' INDICATORS IN THE THREE CASES ANALYSED

Observable indicator	Russian-Ukrainian conflict	Transnational jihadist actors	Latin American organised crime
1. Verifiable scoring system	2 – There is a relatively systematic count of destroyed targets and 'successes' (e.g., panels/statistics in programmes such as Army of Drones, count of targets hit by certain operators or units).	1 – Operations, attacks and 'feats' are mentioned in a quantified manner in propaganda, but without a stable points system or a scoring interface as such.	0 – There is no explicit scoring system: violence or 'reputation' is boasted about, but it is not articulated in the form of points, streaks or visible statistics.
2. Material or redeemable rewards linked to performance	2 – Equipment, drones, financial incentives and other resources are offered to particularly effective operators, in some cases linked to 'bonus' schemes or funding campaigns aimed at rewarding the most successful.	0-1 – Although salaries, loot or material compensation exist, these are not presented as 'gamified' rewards associated with points or achievements (when they do appear, they do so in a very indirect or generic way).	0 – The display of wealth (cars, weapons, parties) is not linked to an explicit 'if you do X, you get Y' system; rather, these are status symbols, not rewards within a structured game.
3. Ranks, levels and cumulative achievements	1 – There are forms of recognition ('star' operators, 'elite' units), but no open and formal system of levels or cumulative achievements equivalent to a video game progression tree.	2 – The militant path is presented as a trajectory of progress (from sympathiser to combatant to martyr), with clear symbolic achievements (status, prestige, promise of transcendent reward) that function as cumulative 'levels'.	1 – There are traditional hierarchies (leaders, hitmen, 'rookies'), and the accumulation of 'feats' reinforces status, but without an explicit 'gamified' level design.
4. Video game-like interface and aesthetics (*overlays*)	2 – Systematic use of FPV drone videos with GoPro/Insta360 cameras, peepholes, game video clip-style editing; the action clearly resembles a first-person combat video game session.	2 – Extensive use of video game-style editing: subjective cameras, visual effects, edited sequences as 'best moments', often with music and rhythm similar to those of a video game recording.	1 – Some content on social media emulates the aesthetics of video games or series (music, editing, visual references), but in a more scattered and less systematic way.
5. Explicit gamer terminology ('headshot', 'kill', 'level up', etc.)	1 – Occasional use of terms such as 'kill', 'frag', 'clip', and comparisons with video games is documented, but they do not constitute the core of the official discourse.	2 – Beyond religious vocabulary, playful expressions and gaming metaphors (missions, challenges, 'levels', rewards) are incorporated to structure the appeal to followers, sometimes even using expressions such as 'headshot' or 'kill streaks'.	1 – Isolated references to video games, '*Call of Duty* mode', challenges or trials appear, but as rhetorical nods on social media, not as systematic language for mobilisation.

Observable indicator	Russian-Ukrainian conflict	Transnational jihadist actors	Latin American organised crime
6. Apps, bots or platforms with feedback	2 – Tools such as the state app Diia and the chatbot eVorog allow users to send information, receive confirmations and, in some cases, messages of recognition or reward, structuring citizen participation as a series of 'missions' with feedback.	1 – Use of channels, bots and groups (e.g. on Telegram) to disseminate tasks and content; they can assign simple missions or give automated responses, but the playful logic is not as developed or visible as in the Ukrainian case.	0 – No apps or bots with 'mission' logic and 'gamified' feedback are identified; coordination is done through messaging channels without their own playful interface.
7. Public rankings and comparison between participants	2 – There are explicit comparisons between units and operators (more drones shot down, more targets destroyed, etc.), sometimes with lists and public recognition that function as de facto rankings.	1 – There are lists of martyrs, exemplary combatants or 'most successful' attacks, but no quantified and updated rankings such as competitive tables.	1 – Symbolic rivalry ('the most feared cartel', 'the most famous hitman'), but based on narratives and reputation, not formal rankings; it can be coded as a rhetorical presence of comparison, without a structured system.

Note. 0: absence; 1: occasional/symbolic presence; 2: systematic/formalised presence.

As can be seen in table 1, the Ukrainian case accumulates most of the indicators at level 2, which justifies talking about formalised 'gamification'; jihadist actors combine indicators at levels 1 and 2, forming a predominantly symbolic model with some semi-formalised elements; while Latin American organised crime is mainly at levels 0-1, associated with informal and unstructured uses of playful repertoires.

Likewise, the ultimate goal of each model also differs considerably: gamification in Ukraine seeks to increase effectiveness on the battlefield, strengthen social resilience and encourage civilian participation; in the case of jihadism, the aim is total surrender through ideological-religious conviction; while in the case of Latin American organised crime, the aim is to improve the recruitment of new members and increase symbolic power at both the territorial and transnational levels.

Finally, the main effects observed in each model are different: in Ukraine, gamification enhances national cohesion and resilience; in jihadism, it encourages the fanaticisation of combatants and a predisposition to total sacrifice; and in organised crime, it promotes an increase in personal status and the glorification of criminal life.

5.3 Transnational projection and global dissemination of gamification

Each model derives specific benefits from the transnationalisation of its narratives. In the Ukrainian case, it generates international sympathy and solidarity, extending the gamer aesthetic to global audiences through social media. The jihadist case is the most pronounced, with effective radicalisation of young people around the world, combining 'gamified' elements that are attractive to this segment and a logic of legitimisation superior to any state or international authority. In the case of Latin American organised crime, the narco-aesthetic has been replicated in Europe and Africa, and not always within migrant communities, demonstrating its growing capacity for cultural penetration.

One of the most visible goals—if not the main one—is to improve recruitment capabilities for each cause. The Ukrainian case favours the targeted recruitment of

young foreigners but, above all, it boosts donations and the generation of logistical support from global sympathisers. The jihadist case encourages the creation of 'lone wolves', radicalised individuals capable of acting even within their local communities or in territories to which they have easy access. For its part, Latin American organised crime mainly targets young people in contexts of exclusion, becoming a model of status and social validation. It should be noted that gamification alone does not explain the dynamics of these conflicts, but interacts with broader social, economic and ideological factors.

5.4 Trivialisation and normalisation of violence

The use of elements from the world of video games turns violent acts into audiovisual content that is entertaining or even motivational. When this content becomes repetitive and banal, it ends up reducing the psychological barriers that have traditionally protected societies. The viralisation of violent content not only facilitates its normalisation through visual repetition, but also reaffirms its social acceptance by perceiving that it enjoys widespread following and digital legitimacy. This effect not only nullifies moral barriers, but also contributes to turning these practices into replicable models for other causes or armed groups.

In certain contexts, this trivialisation is exacerbated by structural impunity. Criminal groups can publish and disseminate violent content without legal consequences, reinforcing their image of power and dominance and projecting the impression that not even the state can impose itself on their informal authority.

The use of 'gamification' and digital aesthetics also contributes to the aesthetic idealisation of violent or aggressive lifestyles. In the case of Latin American organised crime, it is associated with wealth, social status and territorial control; in jihadism, it is linked to religious purity and spiritual transcendence; while in Ukraine it is articulated around a narrative of heroism and collective resistance, where achieving the status of decorated hero or national martyr represents a desirable goal.

Overall, violence is no longer hidden: it is displayed, legitimised and becomes a means of gaining social recognition, aided by interfaces and audiovisual formats that have already been internalised by younger generations.

5.5 Strategic and public policy implications

It is a mistake to consider 'gamification' solely as a narrative or symbolic resource. It should be approached as a tool of power, with tangible effects on recruitment, cohesion and ideological dissemination. Ignoring its potential is therefore a strategic error.

It is essential that defence ministries and national security agencies understand the phenomenon and learn to anticipate its use by hostile actors. In turn, they must develop effective 'gamified' counter-narratives capable of capturing the attention of the same audiences and competing in the digital spaces where battles for perception and social support are fought.

Among the proactive measures, the need to use automated bots capable of amplifying preventive and delegitimising narratives stands out, as well as reinforcing positive content through controlled mass interactions that counteract the bias of viralisation algorithms. Similarly, states could encourage the development of themed video games, apparently neutral or linked to topics of general interest—such as social resilience, cooperation, or national history—with the aim of channelling young people's interest towards narratives aligned with democratic values and respect for human rights. Collaboration with content creators and influencers is another tool that can be used to integrate messages rejecting violence and demystifying crime into the playful and viral formats most consumed by young people, normalising normality in digital spaces.

Given that gamification clearly facilitates the recruitment of younger audiences, it is essential to counteract its effect through public policies aimed at offering attractive alternatives, such as employment, training and social integration options. It is also essential to implement extremism prevention programmes from an early age and to actively combat the social normalisation of violence on social media and in digital environments.

Furthermore, intelligence aimed at preventing radicalisation is becoming a mass phenomenon, supported by digital data analysis and the use of artificial intelligence, which forces states to pay attention not only to external threats, but also to possible recruitment processes within their own societies.

Taken together, a comparison of the three cases allows us to draw some general conclusions about 'gamification' as an emerging way of waging war and narrating it. Firstly, it shows that this is not a marginal phenomenon limited to specific cultural contexts, but rather an adaptable repertoire that cuts across conventional conflicts, jihadist violence and organised crime, with different combinations of formalised, symbolic gamification and specific uses of playful elements. Secondly, it highlights that gamification not only stylises violence, but also introduces incentives and metrics that can influence the behaviour of combatants and sympathisers, affecting target selection, risk appetite and the way 'success' is understood on the battlefield. Thirdly, it suggests that these dynamics open up a new front for security and prevention policies: both the regulation of tools that facilitate the gamification of violence and the development of counter-narratives and communicative responses capable of deactivating the logic of the game around the conflict.

These implications should be interpreted taking into account the methodological limitations outlined in section 3.4, especially the dependence on open sources and the difficulty of measuring the real psychological impact without ethnographic fieldwork.

6 Conclusions

Gamification has established itself as a strategic dimension in contemporary armed conflicts, acting as a multiplier of combatants' morale, recruitment capacity, internal cohesion and propaganda projection. Its flexibility allows it to adapt to contexts as

diverse as those analysed in this study: from a conventional modern warfare scenario such as Ukraine, to transnational and diffuse environments such as jihadism, to Latin American criminal violence, where staging a digital spectacle predominates.

Each model responds to specific needs and objectives: in Ukraine, gamification helps to maximise operational effectiveness and strengthen social resilience; in jihadism, gamification facilitates indoctrination, ideological cohesion and the total dedication of combatants, to the point of encouraging suicidal actions; while in organised crime, it becomes a tool for recruiting young people in contexts of exclusion, offering them immediate prestige and status through the digital display of violence.

The phenomenon is not limited to the local level, but transcends physical and digital borders. The transnational circulation of gamified narratives encourages the imitation of practices and the reinforcement of violent ideologies in distant contexts, thereby increasing the global threat posed by heterogeneous armed actors.

Furthermore, 'gamification' contributes to trivialising violence and idealising criminal or extremist lifestyles, reducing the moral barriers of societies and increasing the risk that young people will normalise violence or even embrace it as a means of prestige and social recognition.

From an analytical point of view, the article has shown that the typology of formalised, symbolic and specific uses of playful elements, together with the comparative rubric applied to the three cases, constitutes a useful tool for organising a phenomenon that, until now, had been described in a fragmentary manner. This proposal makes it possible, on the one hand, to distinguish more precisely between the superficial aestheticisation of conflict and the introduction of structured incentives that affect the behaviour of combatants and sympathisers and, on the other hand, facilitates systematic comparison between armed actors of different natures.

Finally, this study opens up a future research agenda that should address the limitations identified here. It is a priority to extend the analysis to the defensive 'gamification' employed by the Russian Federation, which is absent from this work, in order to contrast authoritarian state models with the Ukrainian model. Likewise, future research should apply quantitative designs that measure the reception of these narratives among young audiences, going beyond the purely sender-based approach of this analysis.

Given this scenario, it is essential that states and international organisations integrate an understanding of gamification into their defence and security strategies, adopting preventive and counter-narrative measures. Anticipating the phenomenon requires not only digital surveillance and artificial intelligence mechanisms capable of detecting patterns of radicalisation, but also cultural, educational and communicative initiatives that challenge armed actors in the field of perceptions.

In short, the gamification of armed conflicts is a strategic challenge that goes beyond the symbolic and requires coordinated, multidimensional responses adapted to the digital reality of the new generations. Only through a comprehensive approach will it be possible to mitigate the effects of this phenomenon and guarantee security in an increasingly interconnected global environment mediated by playful dynamics.

Bibliography

Allenby, B. and Garreau, J. (2017). *Weaponised Narrative: The New Battlespace* [online]. Centre on the Future of War. [Accessed: 2026]. Available at: https://www.defenseone.com/ideas/2017/01/weaponized-narrative-new-battlespace/134284/

Andrews, S. (2023). *First-person propaganda, first-person shooters: A different view* [online]. GNET Research. [Accessed: 2026]. Available at: https://gnet-research.org/2023/06/01/first-person-propaganda-first-person-shooters-and-gamification-a-different-view/

Bachmann, S. and Gunneriusson, H. (2015). Hybrid wars: The 21st-century's new threats to global peace and security [online]. *Scientia Militaria*. 43(1), pp. 77-98. [Accessed: 2026]. Available at: https://doi.org/10.5787/43-1-1110

Bondar, K. (2024). *Does Ukraine already have functional CJADC2 technology?* [online]. Centre for Strategic and International Studies (CSIS). [Accessed: 2026]. Available at: https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology

Bonello, D. (2022). 15-year-old girl kills herself with an Uzi trying to record a TikTok video [online]. *Vice*. [Accessed: 2026]. Available at: https://www.vice.com/en/article/mexico-sinaloa-girl-uzi-tiktok

Brave1. (2025). *Army of Drones: Bonus – Digital reward programme* [online]. Brave1 Platform. [Accessed: 2026]. Available at: https://brave1.gov.ua/en/

Carrillo, L. (2021). How TikTok shows untold truths of communities linked to drug trafficking [online]. *InSight Crime*. [Accessed: 2026]. Available at: https://insightcrime.org/news/how-tiktok-shows-untold-truths-of-communities-linked-to-drug-trafficking/

Dauber, C. *et al.* (2019). Call of Duty: Jihad – How the video game motif has migrated downstream from Islamic State propaganda videos [online]. *Perspectives on Terrorism*. 13(3), pp. 17-31. [Accessed: 2026]. Available at: https://pt.icct.nl/sites/default/files/2023-06/02--dauber-et-al.pdf

Deci, E. L. and Ryan, R. M. (2000). The "what" and "why" of goal pursuits: Human needs and the self-determination of behaviour [online]. *Psychological Inquiry*. 11(4), pp. 227-268. [Accessed: 2026]. Available at: https://doi.org/10.1207/S15327965PLI1104_01

Deterding, S. *et al.* (2011). From game design elements to gamefulness: Defining "gamification" [online]. In: *Proceedings of the 15th International Academic MindTrek Conference.* ACM. Pp. 9-15). [Accessed: 2026]. Available at: https://doi.org/10.1145/2181037.2181040

Frasca, G. (2007). *Play the message: Play, game and videogame rhetoric* [doctoral thesis]. IT University of Copenhagen.

Hassan, L. and Hamari, J. (2020). Gameful civic engagement: A review of the literature on gamification of e-participation [online]. *Government Information Quarterly*, 37(3). [Accessed: 2026]. Available at: https://doi.org/10.1016/j.giq.2020.101461

Huizinga, J. (2000). *Homo ludens*. Alianza Editorial.

Hunt, E. (2016). Islamic State releases children's mobile app 'to teach Arabic' [online]. *The Guardian*. [Accessed: 2026]. Available at: https://www.theguardian.com/world/2016/may/11/islamic-state-children-app-mobile-teach-arabic

Huotari, K. and Hamari, J. (2012). Defining gamification – A service marketing perspective [online]. In: *Proceedings of the 16th International Academic MindTrek Conference*. ACM. Pp. 17-22. [Accessed: 2026]. Available at: https://doi.org/10.1145/2393132.2393137

Kabachynskyi, I. (2025). How Ukraine turned a point-based rewards system into an effective model for war management [online]. *UNITED24 Media*. [Accessed: 2026]. Available at: https://united24media.com/war-in-ukraine/ukraines-new-point-based-rewards-system-for-drone-operators-is-rewriting-war-management-from-the-ground-up-8528

Lakhani, S.; White, J. and Wallner, C. (2022). *The gamification of (violent) extremism* [online]. Radicalisation Awareness Network (RAN). [Accessed: 2026]. Available at: https://home-affairs.ec.europa.eu/system/files/2022-09/RAN%20Policy%20Support-%20gamification%20of%20violent%20extremism_en.pdf

Lethal Crysis. (2025). *Drone pilots: Ukraine #04* [Video] [online]. *YouTube*. [Accessed: 2026]. Available at: https://www.youtube.com/watch?v=JRzJUhvqDR8

Marchini, C. S. (2023). *The digital drug revolution: How online markets are reshaping global illicit trade* [online]. Global Initiative Against Transnational Organised Crime. [Accessed: 2026]. Available at: https://globalinitiative.net/analysis/digital-drug-revolution-online-markets-global-illicit-trade-ocindex/

Marson, J. (2024). The nerdy gamers who became Ukraine's deadliest drone pilots [online]. *The Wall Street Journal*. [Accessed: 2026]. Available at: https://www.wsj.com/world/europe/ukraine-gamers-drone-pilots-russia-85a1af3b

Michael, D. and Chen, S. (2006). *Serious games: Games that educate, train, and inform*. Thomson.

NATO StratCom COE. (2021). *Information Influence1 as a Tool of Hybrid Threats* [online]. NATO Strategic Communications Centre of Excellence. [Accessed: 2026]. Available at: https://stratcomcoe.org/uploads/NATO_StratCom_COE_brief.pdf

O'Carroll, L. (2023). Meet Diia: the Ukrainian app used to do taxes … and report Russian soldiers [online]. *The Guardian*. [Accessed: 2026]. Available at: https://www.theguardian.com/world/2023/may/26/meet-diia-the-ukrainian-app-used-to-do-taxes-and-report-russian-soldiers

Pötzsch, H. (2015). The emergence of iWar: Changing practices and perceptions of military engagement in a digital era [online]. *New Media & Society*. 17(1), pp. 78-95. [Accessed: 2026]. Available at: https://doi.org/10.1177/1461444813516834

Pokotylo, O. (2025). Auterion to supply Ukraine with tens of thousands of AI drone strike kits [online]. *The Defender*. [Accessed: 2026]. Available at: https://thedefender.media/en/2025/07/auterion-to-provide-thousands-aidrones/

Prucha, N. (2016). IS and the jihadist information highway – Projecting influence and religious identity via Telegram [online]. *Perspectives on Terrorism*. 10(6). [Accessed: 2026]. Available at: https://pt.icct.nl/article/and-jihadist-information-highway-projecting-influence-and-religious-identity-telegram

Quevedo Delgado, S. V. (2025). Money, weapons, cocaine and women: the 'hooks' for recruiting minors on TikTok and Facebook [online]. *El Tiempo*. [Accessed: 2026]. Available at: https://www.eltiempo.com/justicia/paz-y-derechos-humanos/plata-armas-coca-y-mujeres-los-anzuelos-para-el-reclutamiento-de-menores-de-edad-en-tik-tok-y-facebook-3448154

Shevko, D. (2025). Ukraine's drone war gets gamified: Why 'Bonus points for kills' is more than a morale booster [online]. *New Voice of Ukraine*. [Accessed: 2026]. Available at: https://english.nv.ua/opinion/ukraine-gamifies-war-with-drone-kill-points-in-army-of-drones-bonus-program-50520526.html

Sicart, M. (2014). *Play matters* [online]. MIT Press. [Accessed: 2026]. Available at: https://mitpress.mit.edu/9780262534512/play-matters/

Skinner, B. F. (1953). *Science and human behaviour*. The Macmillan Company.

The Economist. (2025, 8 July). How drones and video-game techniques are coming together in Ukraine's war [online]. *The Economist*. [Accessed: 2026]. Available at: https://www.economist.com/the-economist-explains/2025/07/08/how-drones-and-video-game-techniques-are-coming-together-in-ukraines-war

Weimann, G. (2015). Terrorist migration to social media. *Georgetown Journal of International Affairs*. 16(1), pp. 180-187. [Accessed: 2026]. Available at: https://archive-yaleglobal.yale.edu/terrorism-cyberspace-next-generation

Werbach, K. and Hunter, D. (2012). *For the win: How game thinking can revolutionise your business*. Wharton Digital Press.

Winkler, C. K. and Dauber, C. E. (eds.). (2014). *Visual propaganda and extremism in the digital environment* [online]. U.S. Army War College Press. [Accessed: 2026]. Available at: https://press.armywarcollege.edu/monographs/946/

Winter, C. (2015). *Documenting the virtual caliphate* [online]. Quilliam Foundation. [Accessed: 2026]. Available at: https://voxpol.eu/file/documenting-the-virtual-caliphate/

Appendix 1: Document corpus analysis matrix

Representative inventory (*N*=50) of the digital artefacts analysed. The selection is based on criteria of relevance, virality and platform diversity, ensuring data triangulation in all three cases.

TABLE A1. CORPUS ANALYSIS MATRIX

ID	Platform/Medium	Description of the artefact	Identified Game Mechanics	Source / Year
U-01	Government app (Diia)	e-Vorog (e-Enemy): Official chatbot for reporting Russian troop movements.	Crowdsourcing / Rewards: Use of civic gamification; immediate feedback and digital validation of the user as a 'virtual defender'.	Ministry of Digital Transformation (2022-2025)
U-02	Website (Brave1)	Army of Drones: Fundraising and training platform.	Points System: Assignment of e-points and rankings for the most effective donors and drone operators.	*United24 / Brave1* (2024)
U-03	YouTube / Telegram	Clips from 'Magyar Birds': videos of drone units with pointers and comical editing.	Interface (HUD): Video game crosshairs overlay, health bars, and *Mario Bros* sound effects upon impact.	Telegram Channels (2023-2025)
U-04	Social Network (Twitter/X)	NAFO (Fellas): Decentralised 'trolling' movement against Russian propaganda.	Avatars/Customisation: Creation of customisable characters (Shiba Inu dogs); memetic warfare structured as clan 'raids'.	Direct observation (2022-2025)
U-05	Simulators	Civilian FPV training: Homemade software for practising kamikaze piloting.	Immersive simulation: Use of console controllers (Xbox/PS) to control real weapons; blurring of the line between game and war.	*The Economist report* (2025)
U-06	Video game	CS:GO Maps: Maps created in Counter-Strike to inform Russians about the war.	Virtual Environment: Use of digital leisure spaces as channels for subversive information ('War in the lobby').	*Helsingin Sanomat* (2023)
Y-01	Video Propaganda	Flames of War series: High-production documentaries by ISIS.	FPS aesthetics: Subjective camera (GoPro on the barrel), slow motion during casualties, 'hero vs. horde' narrative.	*Al-Hayat Media* (Archived)
Y-02	Mobile App	Huroof (Alphabet): App for children of the 'Caliphate'.	Edutainment: Teaching the alphabet using weapons ('T' for Tank, 'B' for Bomb); gamified pedagogy of violence.	*Long War Journal report* (2016)
Y-03	Telegram Bot	Theological Quiz: Automatic bots on encrypted channels.	Trivia/Ranking: Questions and answers about Sharia law with scoring systems and status within the chat group.	MEMRI (2017-2020)
Y-04	Video game (Mod)	ARMA 3 / GTA Mods: Game modifications to recreate ISIS battles.	Roleplay: Simulation of military victories in virtual environments to compensate for real territorial losses.	Forum observation (2018-2022)
Y-05	Social media	Infographics of 'Achievements': Visual posters of battle statistics.	Stats/Metrics: Presentation of enemy casualties and destroyed vehicles with 'end-of-game scoreboard' aesthetics.	Amaq News Agency
C-01	TikTok	#CartelTikTok: Viral trend of hitmen showing off their luxurious lifestyles.	Loot: Display of golden weapons (skins) and 'unlockables' (cars, felines) as level trophies.	TikTok (2021-2025)
C-02	Video game (GTA V)	Grand Theft Auto Online: Roleplay servers controlled by cartels.	Virtual Recruitment: Real recruiters contact skilled players within the game to offer real 'work' (lookouts/mules).	*Forbes / Insight Crime* (2023)

ID	Platform/Medium	Description of the artefact	Identified Game Mechanics	Source / Year
C-03	Instagram/FB	Convoy Challenges: Videos of rows of armoured trucks.	Clan Competition: Demonstration of comparative strength (who has the best 'guild'); paramilitary military parade aesthetic.	Open Networks (2020-2024)
C-04	YouTube Music	Corridos Tumbados / Bélicos: Music videos.	Hero Narrative: Lyrics that narrate the rise of a 'character' from poverty to power (leveling up) through violence.	Peso Pluma / Natanael Cano (2023-2024)
C-05	Messaging	Narco-Culture Emojis and Stickers: Sticker packs on WhatsApp.	Insignia: Use of the 'pizza' (Chapitos) or the 'man in the hat' (Mayo) as badges of belonging to a faction.	Direct observation (2024)
C-06	Twitch	Narco-Streamers: Hitmen broadcasting patrols or parties live.	Streaming: Real-time interaction with the audience, donations and requests for greetings, trivialising criminal activity.	Local press reports (2023)

Note. U = Russian-Ukrainian conflict; Y = Jihadism; C = Organised crime.
Source: author's own elaboration based on data collection from open sources and triangulation with reports from security consultancies.

Article received: 15 September 2025
Article accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Arturo Esteban Ceballos
Association of Spanish security and defence graduates (ADESYD)

Email: aestebanc@alumnos.nebrija.es

Hybrid Threats under Simulation: From Empirical Data to Strategic Modelling. An Empirical and Simulation-Based Approach to the Analysis of Hybrid Strategies

Abstract

Hybrid strategies have become a central focus of contemporary strategic analysis, but their modelling remains a challenge. This article proposes a replicable methodology that integrates empirical analysis, formal classification, statistical modelling and adaptive simulation. Based on the reclassification of events in the GDELT database under the DIMEFL scheme (Diplomatic, Informational, Military, Economic, Financial, and Legal), a quarterly panel of Turkish activity in Libya, Somalia, Mali, and Niger was constructed. This panel was analysed using first-order Markov chains, negative binomial regression and SARIMAX models, which allowed us to identify sequential patterns and long-term trends. As a complement, an agent-based model with reinforcement learning (ABM-RL) was developed, representing Turkey as a strategic actor capable of optimising its influence and reducing reputational costs. The simulation reproduced observed sequences and revealed adaptive logics that are difficult to capture with empirical data alone. Although cognitive processes were not incorporated, cyber-physical-social systems are identified as a promising extension. The proposed architecture constitutes a scalable framework for the study of hybrid threats and provides a solid basis for the development of early warning systems in multi-domain environments.

Keywords

Turkey, Hybrid threats, DIMEFL, ABM-RL, GDELT.

Cite this article:

Esteban Ceballos, A. (2025). Hybrid threats under simulation: from empirical data to strategic modelling. An empirical and simulation approach to the analysis of hybrid strategies. *Journal of the Spanish Institute for Strategic Studies*. 26, pp. 597-628.

Index of acronyms

ABM: Agent-Based Modelling.

ABM-RL: ABM with reinforcement learning.

ACLED: Armed Conflict Location & Event Data Project.

APT: Advanced Persistent Threat (cyber).

ARIMA: AutoRegressive Integrated Moving Average

CAMEO: Conflict and Mediation Event Observations — Event taxonomy (GDELT).

CPSS: Cyber-Physical-Social Systems.

DIMEFL: Diplomatic, Informational, Military, Economic, Financial, and Legal (portfolio of instruments).

DoD: U.S. Department of Defence

EU: European Union.

GDELT: Global Database of Events, Language, and Tone.

GLM NB: Generalised Linear Model — Negative Binomial.

Goldstein (Scale): Metric of 'tone'/valence of events in GDELT used as a reputational proxy.

ICEWS: Integrated Crisis Early Warning System.

MDP: Markov Decision Process — Markov decision process (sequential decision model).

MoU: Memorandum of Understanding — Memorandum of understanding (treaties/agreements).

NATO: North Atlantic Treaty Organisation.

OSINT: Open-Source Intelligence.

CCP: Communist Party of China

PLA: People's Liberation Army (China).

PMESII: Political, Military, Economic, Social, Information, Infrastructure — Strategic domain framework.

Q-learning: Reinforcement learning algorithm (off-policy).

RL: Reinforcement Learning.

SARIMAX: Seasonal ARIMA with exogenous regressors.

SIPRI: Stockholm International Peace Research Institute.

SWP: Stiftung Wissenschaft und Politik — German Institute for International and Security Affairs.

UAV: Unmanned Aerial Vehicle.

UN: United Nations.

ZG: Grey Zone.

1 Introduction

The growing prominence of hybrid threats on the international agenda has been recognised by multilateral organisations such as NATO, which in its recent publications highlights the need to understand how state and non-state actors combine conventional and unconventional instruments to disrupt the international order without triggering open warfare (NATO Public Diplomacy Division, 2024a).

Therefore, the study of hybrid threats is now a central challenge for research in security and international relations. Experience gained in recent conflicts suggests that traditional analytical frameworks, such as game theory or static equilibrium models, are insufficient to explain phenomena characterised by adaptability, multidimensionality and operation on the threshold of open confrontation. Furthermore, many traditional geostrategic analyses have been based on qualitative paradigms or static approaches; however, a more dynamic approach is needed to capture the tactical evolution and learning of revisionist actors.

This approach stems from the fact that hybrid state and non-state actors deploy portfolios of instruments of power—diplomatic, informational, military, economic, financial, and legal—that do not act in isolation but as dynamic combinations that seek to exploit the systemic vulnerabilities of their targets. This logic challenges conventional frameworks for interpreting threats in the traditional sense of the term and requires the development of methodologies capable of capturing the sequencing, interdependence and strategic learning of revisionist actors.

This gives rise to the concept of hybrid modelling, understood as the integration of empirical analysis of large databases with generative simulations of adaptive actors, a methodology that is emerging as a response to this challenge.

Today, we have a wide range of event databases with the necessary traceability and reproducibility, both in open sources and in those available to states or corporations. For this study, we have used the GDELT database, which stands f*or Global Database of Events, Language, and Tone.* This project tracks print, television and digital media in real time in more than 100 languages, enabling in-depth analysis of social, political and emotional dynamics worldwide (Leetaru, n. d.).

Today, GDELT is the most comprehensive and detailed open database on human society, with global coverage from 1979 to the present. Its development involved unprecedented technical and methodological innovations, as well as new partnerships and approaches to monitoring media in multiple languages and formats. With more than 250 million georeferenced records, GDELT not only documents events, actors and emotions on a global scale, but also offers multiple advantages for classifying, refining and analysing the information contained in its databases. The use of this database to inform studies related to security and defence is not new; authors such as Hopp *et. al.* (2019) explored the use of databases such as GDELT to feed automated strategic monitoring systems, reinforcing its applicability in studies applied to hybrid threats.

By exploiting its event coding capabilities, GDELT is the optimal choice for obtaining a systematic empirical representation of the activity of revisionist actors over extended time series.

As for the second pillar of this methodology, the simulation of the adaptive behaviour of these actors, the most current trends contemplate agent-based models with reinforcement learning ABM-RL (agent-based modelling+reinforcement learning). This methodology allows for the possibility of simulating how a hybrid actor experiments with different tactical sequences, adjusting their decisions based on the response of the environment and the target state on which they are acting.

The combination of both approaches (empirical and behavioural) provides an ideal framework for moving beyond mere description towards the inference of causal mechanisms and the exploration of counterintuitive scenarios. In summary, this work proposes an innovative methodological design that integrates an empirical analysis of events coded according to the DIMEFL (Diplomatic, Informational, Military, Economic, Financial and Legal) instruments of power through the global GDELT database with the construction of a generative model based on agents and reinforcement learning ABM-RL. This combination seeks to overcome the limitations of classical models—for example, game theory, which assumes fixed rationality—by incorporating the strategic adaptation and uncertainty inherent in hybrid conflicts. Likewise, the use of geopolitical big data (coded events) allows the model to be based on quantitative evidence, which means we do not have to rely exclusively on subjective estimates or anecdotal cases. In other words, what is required is a combination of open source intelligence (OSINT) methods with large-scale data analysis and advanced computational modelling techniques.

Furthermore, in order to guide the reader on the practical functioning of this methodology, we will present throughout this paper a case study analysing Turkey's hybrid strategies in Africa.

We have chosen Turkey as a case study because it articulates a moderate revisionism that favours hybrid campaigns as we contemplate them in our theoretical framework. The doctrine of the 'Blue Homeland' (*Mavi Vatan*) was conceived by Admiral Cem Gürdeniz and later by Cihat Yaycı. This actor has played a decisive role in Libya's internal processes, obtaining a maritime delimitation agreement that is highly beneficial to his interests. In addition, he pursues an assertive agenda in the eastern Mediterranean; in Africa, he has reached energy and security agreements (Somalia), and analysis of documentary sources reveals synchronised and synergistic actions in the fields of diplomacy, economics, security and information, where this actor does not hesitate to compete with third parties (Gürdeniz, 2006; Denizeau, 2021; United Nations, 2019; Sezer, 2024). Consequently, this pattern of behaviour seems to fit the concept of a revisionist actor as defined by Schweller (1994, 2006).

In just over two decades, Turkey has multiplied its embassies on the African continent, signed trade and financial agreements, deployed troops and built military bases, while developing a cultural and information diplomacy that reinforces its narrative as an emerging power, especially in light of the progressive withdrawal of the military

presence of the European Union and France itself. This is why countries such as Libya, Somalia, Mali and Niger have become priority scenarios for this projection, forming a geopolitical laboratory where hard and soft instruments of power are intertwined.

In conclusion, the choice of Turkey is based on its doctrinal maturation (*Mavi Vatan*) and recent evidence documenting the intensification and systematisation of its actions, typical of a revisionist actor (Arslan, 2025).

In short, the object of study (application of a methodology for modelling hybrid strategies applied to the case study of Turkey in Africa) is relevant both for its geopolitical impact and for the analytical challenges it poses. However, the aim of the work is not simply to describe Turkish influence in Africa, but to demonstrate a replicable procedure for modelling hybrid strategies. To this end, a framework is articulated which, first, theoretically underpins the concept of strategic hybridisation; second, describes a methodological design that integrates empirical data, statistical models and simulation; and third, offers results on the observed and simulated dynamics of Turkish action. Finally, the strategic and methodological implications of the findings are discussed, the limitations of the study are identified, and avenues for future research are suggested.

2 Theoretical framework

The notion of hybrid warfare has been the subject of much criticism due to its conceptual ambiguity and expansive use in strategic discourse. Hoffman (2007) initially introduced the term to describe the combination of conventional and irregular tactics, but its definition has been broadened to the point of losing operational precision. Authors such as Chivvis (2017) have criticised this term, arguing that the notion of hybrid warfare has been instrumentalised in Western strategic discourse, leading to a loss of precision in its empirical application.

Today, the academic community prefers to use the concept of hybrid threat, a concept that has become established in strategic doctrine to describe forms of competition in which military and non-military instruments are intertwined with the aim of destabilising or influencing an adversary. Both the European Union and NATO have emphasised that the distinctive feature of these strategies lies in their multi-domain coordination and in the fact that they operate below the threshold of open warfare (European Commission, 2016; NATO, 2024b). However, academic literature has warned that indiscriminate use of the term 'hybrid' can lead to overgeneralisation, obscuring differences between cases and detracting from the analytical value of the concept, as Galeotti (2016) points out. In their analysis of hybrid conflicts, Renz and Smith (2016) criticise the tendency to use the term as a simplistic label. Instead of offering a useful analytical tool, the concept has become a diffuse framework that groups together conventional, irregular, cyber and psychological tactics without distinguishing their specific dynamics. This ambiguity can lead to ill-founded political and strategic responses, for example, by assuming that Russia operates under a coherent and deliberate model of hybrid warfare, when in reality its actions respond to a more pragmatic and adaptive logic (Renz and Smith, 2016: p. 7).

However, despite these criticisms, there is broad consensus that modern hybrid threats are multi-domain and generally operate below the threshold of conventional warfare. In other words, they combine various tools (diplomatic, economic, informational, cybernetic, etc.) without triggering an open, high-intensity military confrontation. The centrality of the information sphere in most of these scenarios is also recognised: control of the narrative, disinformation and influence on public opinion are as decisive as military coercion.

In this regard, Allied doctrine on hybrid threats has evolved towards a more operational and multi-domain conceptualisation. NATO's *Allied Joint Doctrine for the Military Contribution to Countering Hybrid Threats* (AJP-3.21) (NATO, 2021) states that responses must integrate military, civilian and digital capabilities, articulated in coordinated campaigns operating below the threshold of armed conflict. This doctrinal vision reinforces the need for analytical models that capture the sequentiality and adaptability of hybrid actors.

If we look at frameworks other than NATO doctrine, we see that the concept of 'hybrid' is also considered in academic circles in countries such as Russia and China, among others. In the Russian academic sphere, it is essential to mention the theory of reflexive control put forward by Vladimir A. Lefebvre, who designed a framework according to which decisions can be induced in the adversary by manipulating perceptions, reinforcing the weight of informational dominance and the importance of studying the effects of hybrid actions in the cognitive sphere (Lefebvre, 2001; Thomas, 2004). Another reference point in the Russian view of unconventional conflicts is General Valery Gerasimov, who in a famous speech emphasised the fusion of military and non-military means and the centrality of information in diffuse environments (Gerasimov, 2016).

However, one of the most relevant authors in the study of hybrid threats from a Russian perspective is Andrew Korybko, who emphasises the synergy of political, informational and economic actions as part of the hybrid strategies typical of the so-called 'colour revolutions' (Korybko, 2015).

As for authors from the Chinese sphere, we have both the classic work by Qiao Liang and Wang Xiangsui on 'unrestricted warfare' and the striking doctrine of the 'Three Wars' (public opinion, psychological and legal), in which the authors contextualise the coordinated use of information and the manipulation of legal frameworks as hybrid tools that are extremely useful in times of peace.

Hai Jin, Li-Jun Hou and Zheng-Guo Wang (2018), Chinese military researchers, explore cognitive warfare as a central element of multi-domain conflicts, highlighting the use of artificial intelligence and neuroscience to influence the human brain. They propose that the 'cognitive domain' should act as a new field of operations. They see the West as leaders in cognitive technologies that could manipulate the Chinese population, advocating for the development of national technologies. This perspective connects with broader doctrines, such as the Three Wars, which integrate psychological and perceptual manipulation elements. These works consider the US and its allies as strategic rivals due to their dominance in global narratives, advocating

for an expanded global media presence. This doctrine is integrated with hybrid warfare as an extension of the CCP's political strategy to maintain power, blurring the line between peace and war (peace-war integration). (Qiao and Wang, 1999; Hai *et al.*, 2018; US Department of Defence, 2013).

Therefore, based on this rich cross-disciplinary academic ecosystem, and for the purposes of providing a theoretical framework for our study, we define the term 'hybrid interference' as the intervention of an external actor with revisionist motivations who deliberately, synchronously and synergistically employs their instruments of power in order to provoke cumulative and cognitive effects on a target actor while remaining below the threshold of armed conflict. In other words, it is about how a revisionist actor influences third parties according to Schweller's parameters, without reaching armed conflict, but far exceeding bona fide in international relations. This definition narrows down the phenomenon and sets clear criteria for inclusion and exclusion that guide all subsequent analysis.

Conversely, a hybrid actor is not one that employs isolated single-domain actions, resorts to the open and regular use of force (conventional conflict), engages in bona fide diplomacy without instrumental overlap or the intention to exert pressure, or generates isolated events without recognisable accumulation.

Having established our framework for hybrid interference, it is worth highlighting the need to parameterise these actions in order to frame the debate and obtain a rigorous framework for analysis. One of the classic approaches to this phenomenon has been the DIME model—Diplomatic, Information, Military and Economic—which was later expanded to DIMEFL or more complex models to include other dimensions, such as Intelligence, Financial and Legal (Joint Chiefs of Staff, 2018a, 2018b, 2018c).

> 'The acronym "DIME" (diplomatic, informational, military, and economic) has been used for many years to describe the instruments of national power. Despite how long DIME has been used to describe the instruments of national power, US policy makers and strategists have long understood that there are many more instruments involved in national security policy development and implementation. New acronyms such as MIDFIELD (military, informational, diplomatic, financial, intelligence, economic, law, and development) convey a much broader array of options for the strategic and policymaker to use '.(Joint Chiefs of Staff, 2018b, p. 7)

This taxonomy has served as a common language in strategic planning and facilitates the systematic classification of observable events. However, several authors (Baqués, 2021; Hartley, 2020) have pointed out that DIMEFL, if used rigidly, tends to compartmentalise realities that in practice function interdependently. In hybrid campaigns, diplomacy is reinforced with informational propaganda, economic incentives are accompanied by financial credits, and legal agreements can consolidate the results of military coercion. In other words, the instruments do not act in isolation, but as adaptive portfolios.

In this regard, it is interesting to highlight Hartley's (2020) approach, whose ontological design of modern conflict encompasses both conventional and unconventional warfare. According to this author, it is preferable to formally model actors, relationships, and processes rather than clinging to preconceived lists of instruments. This perspective opens the door to computational representations that transcend fixed taxonomies and focus on causal mechanisms, i.e., how the actions of one actor trigger reactions in another and how the effects propagate across a multi-domain environment. In short, the doctrinal-theoretical debate on hybrid threats oscillates between approaches that privilege organisational clarity (such as DIME) and approaches that seek to reflect the dynamic complexity of hybrid reality.

In addition to DIME models, the academic community has often resorted to game theory as a tool to explain hybrid strategies in the context of strategic studies, allowing for the modelling of deterrence or negotiation dilemmas. However, the weakness of this model lies in its assumption that players have rational logics with fixed preferences and stable time horizons. In this regard, authors such as Padur, Borrion and Hailes (2025) question the usefulness of traditional game theory-based models for analysing hybrid threats, arguing that these approaches tend to assume perfectly rational agents and static decision environments, which limits their ability to capture the adaptability, ambiguity and strategic evolution that characterise contemporary hybrid threats. Instead of relying on predefined equilibria, the authors propose the use of agent-based models with reinforcement learning, which allow for the simulation of emergent and dynamic behaviours in contexts of uncertainty, offering a more realistic representation of how hybrid actors (understood as such according to the theoretical framework we present for this study) adjust their tactics based on feedback from the environment. In other words, the modelled revisionist actor acts as a political-strategic leadership that synchronises and deploys its instruments of power in a reproducible manner.

This approach has given rise to agent-based simulations (ABMs). These models allow heterogeneous actors to be represented with local behavioural rules which, when interacting, generate emergent dynamics. In the field of security, ABMs have demonstrated their ability to explain phenomena such as insurgencies, rumour spreading and social polarisation (Epstein, 2002; Hegselmann and Krause, 2002; *Vosoughi et al.*, 2018). The most recent innovation has been to integrate reinforcement learning (RL) techniques into ABMs, which give agents the ability to adjust their strategies to maximise rewards over time (Sutton and Barto, 2018). This allows for the simulation of adaptive hybrid actors who test combinations of instruments and learn to repeat the most effective sequences.

The work of Padur *et al.* (2025) is a pioneering example: the revisionist hybrid actor does not follow a pre-established plan, but explores tactics such as disinformation, cyberattacks or social manipulation depending on the rewards (gains) obtained by altering the socio-political environment (*status quo*). The environment is composed of social agents representing the victim population, whose opinions, behaviours, and levels of trust are sensitive to the actions of the malicious actor. As the hybrid actor interacts with this environment, the model allows us to observe how cumulative

effects are generated, such as the erosion of social cohesion or the loss of institutional legitimacy. This approach overcomes the limitations of game theory by capturing the non-linearity, adaptability and ambiguity inherent in hybrid threats, offering a more realistic tool that exploits the potential of generative artificial intelligence to anticipate vulnerabilities and design integrated responses. Its findings show that sequencing—for example, launching a cyberattack before a disinformation campaign—can be more effective than isolated actions (i.e., seeking synergy in the use of an actor's instruments of power). These types of results reinforce the idea that hybrid conflicts cannot be understood solely as the sum of actions, but rather as adaptive and synergistic sequential processes. In summary, we propose the hypothesis that the dynamics of hybrid threats respond to the activity of autonomous agents (whether state or sub-state actors) who learn and adapt their strategies through reinforcement learning.

Therefore, this article proposes an integrative approach that combines the descriptive capacity of DIMEFL with the exploratory power of ABM-RL. The aim is not to replace one with the other, but to articulate them in a complementary manner: DIMEFL provides a clear and replicable classification of empirical data (events coded in GDELT), while ABM-RL allows for experimentation with scenarios, validation of hypotheses, and discovery of underlying causal mechanisms. This integration seeks to overcome the dilemma between parsimony and realism, i.e., the aim is to maintain data traceability while capturing the adaptive dynamics that characterise contemporary hybrid threats.

3 Methodological design

The study combines three complementary analytical layers: an empirical base of events obtained from the GDELT database, a strategic mapping of those events in the DIMEFL categories, and a generative Artificial Intelligence model based on agents with reinforcement learning (ABM-RL). This methodological architecture seeks to capture both the observable evidence of hybrid activity and the adaptive mechanisms that explain its dynamics.

3.1 Scope and limitations

We intend to limit the scope and depth of this research within 'laboratory' parameters in order to test and validate our research hypothesis. Our approach adopts a deliberately parsimonious methodology: we isolate a single actor (Turkey) to ensure replicability and control for observer bias; the environment appears observationally through diplomatic, economic, and legal responses, but we do not confront it with its potential competitors (Russia, China, United Arab Emirates), an aspect that remains open to future research of greater depth and scope.

Furthermore, the methodology we propose can be enriched in future research with the contribution of expert judgement that clearly defines the profile of a revisionist actor within a panel or working group and clearly establishes the rules of escalation so that the simulation of agents by AI responds to parameters defined by analysts with

full knowledge of the actors. We do not claim hard causality: our transitions capture patterns from publicly available databases.

3.2 Experimental framework

Our methodological architecture responds to a simple logic: if hybridisation consists of a hybridisation of mechanisms, then we must measure sequences, rhythms and adaptation. We will reclassify GDELT (Global Database of Events, Language and Tone) events in DIMEFL and aggregate the series by quarter to identify multi-instrumental patterns. With Markov chains, we will identify regularities of the type 'what usually follows what'; with the negative binomial (NB) and SARIMAX (Seasonal ARIMA with eXogenous regressors), we will observe persistence and trajectories. The simulation works under controlled laboratory conditions: our Turkey agent learns (reinforcement learning) to choose sequences that maximise influence and minimise reputational, legal and escalation costs. We anchor the exploration in empirical grammar (Markov transitions) and calibrate rewards/penalties with open metrics (e.g., Goldstein tone). The comparison between empirical and simulated matrices converts discrepancies (e.g., Military overestimation followed by Diplomatic) into elements of discussion on those aspects that should be modelled in studies that expand on this one.

In ABM-RL, the reward combines cumulative influence and sequential persistence (DIMEFL) with penalties for reputation (Goldstein), risk of escalation and legal costs, so that the agent optimises below the threshold and adjusts its policy when these signals change.

Going into detail, we will explain the pillars of our methodological framework. The GDELT database codes each event according to the CAMEO (Conflict and Mediation Event Observations) system, which assigns hierarchical codes to actions such as diplomatic agreements, economic sanctions, military acts or legal measures.

The CAMEO system was originally a coding framework developed by Schrodt, Yonamine and Backer (2012) to structure international political events, especially those related to conflict, cooperation and mediation. It uses a hierarchical taxonomy that allows for the classification of more than three hundred types of events, from diplomatic statements to acts of violence, facilitating the automated analysis of geopolitical dynamics. CAMEO is widely used in databases such as GDELT and ICEWS to extract events from global media through natural language processing (Schrodt *et al.*, 2012).

In addition, the GDELT database incorporates the Goldstein parameter. This indicator, originally designed to capture the directionality and severity of political interactions, is widely used in studies of conflict and international cooperation (Goldstein, 1992). It is an index that assigns each event a numerical value between -10 and +10, representing its tone or emotional charge, which is extremely interesting for assessing cognitive aspects.

Negative values indicate hostile or conflictive actions (such as threats or attacks), while positive values reflect cooperative behaviour (such as negotiations or assistance).

This indicator, derived from CAMEO coding, allows the nature of events to be quantified in terms of political intensity and strategic orientation. Although it was not used as a main variable in this analysis, the Goldstein index offers a valuable resource for future models seeking to weigh the qualitative impact of recorded interactions, especially in studies on hybrid dynamics or conflict evolution.

As for the historical series, the period 2002–2025 was selected, allowing us to observe the evolution of Turkey's projection in Africa from the beginning of its opening strategy to the present day. To this end, a search engine was designed using an SQL script that, through Google Cloud's BigQuery tool, downloaded a database of more than fourteen thousand events classified into the six instruments of power that make up the DIMEFL framework: Diplomatic, Informational, Military, Economic, Financial, and Legal. This conversion was carried out using a set of transparent rules for correspondence between CAMEO codes and DIMEFL categories (table I). This step ensures that the empirical evidence can be analysed under a recognised strategic taxonomy, while allowing the procedure to be reproduced and audited.

TABLE I . CAMEO–DIMEFL CORRESPONDENCE

Instrument	Associated CAMEO ranges	Brief description
Diplomatic (D)	01–06	Visits, dialogues, negotiations, multilateral agreements.
Informative/Influential (I)	07 and subcategories in 01–03	Propaganda, media statements, verbal threats.
Military-Security (M)	12, 14–20	Threats of force, deployments, armed conflicts.
Economic (E)	07–11 (except financial)	Trade agreements, investments, economic cooperation.
Financial (F)	Subcodes 08, 10 and 11	Transfers, loans, financial sanctions.
Legal (L)	13, 15–17	Treaties, extraditions, legal/police restrictions.

Source: author's own elaboration based on Schrodt *et al.* (2012) and coding rules developed for this study.

Thirdly, the dataset was organised into a quarterly panel by target country: Libya, Somalia, Mali and Niger. This aggregation made it possible to examine the evolution of Turkey's hybrid strategy in three geopolitical scenarios (Maghreb, Sahel and Horn of Africa). The panel was used both for exploratory analyses (trends, compositions, sequences) and for calibrating the simulation model. To this end, Python code scripts were used to refine the database obtained through SQL searches, represent historical series and map events.

To this end, various mathematical models were used to produce a graphical representation of the DIMEFL empirical model applied to our case study. These models are as follows:

– NB (Negative Binomial) model: count regression that assumes that the variance of the data may be greater than the mean (overdispersion). It is used here to adjust the number of quarterly events based on the instruments used in the previous quarter. The methodological choice is based on the developments of Cameron and Trivedi

(2013), who establish robust criteria for the application of count models in social and economic contexts where the dispersion exceeds the mean. In other words, the Negative Binomial (NB) is a regression technique designed to analyse count data that exhibit overdispersion, i.e. when the variance exceeds the mean, making it more flexible than other models, such as Poisson. In strategic analysis contexts, this model allows the number of events recorded in a given period (e.g., quarterly) to be adjusted based on explanatory variables such as the instruments of national power grouped under the DIMEFL (Diplomatic, Information, Military, Economic, Financial, and Legal) framework, used in the previous period. This approach facilitates the identification of patterns of influence between state actions and the frequency of observable events.

– The SARIMAX (Seasonal AutoRegressive Integrated Moving Average with eXogenous regressors) model is a seasonal ARIMA model with exogenous regressors. It allows us to capture trends and repetitive patterns in aggregate time series, incorporating seasonal effects (quarters) and optional covariates. In this way, we can analyse and predict time series by incorporating autoregressive components, moving averages, integration to address non-stationarity, seasonal patterns and external variables that influence the observed dynamics. Its flexible structure makes it particularly useful in contexts where data exhibit repetitive cycles and are affected by exogenous factors.

– Markov model: a stochastic process in which the probability of moving to a state depends only on the current state. The DIMEFL transition matrix shows which instrument tends to follow which, revealing the typical sequence of Turkey's actions. The Markov model is a stochastic process, i.e., a process that incorporates elements of chance, where the outcome depends on probabilities and is not completely predictable, in which the probability of transition between states depends solely on the current state, without considering the previous trajectory. Applied to strategic analysis, it allows for the construction of a transition matrix between instruments of national power (DIMEFL), revealing sequential patterns in the behaviour of state actors. In the case of Turkey, this approach has been used to identify which instrument—such as diplomatic, military, or financial—tends to follow another, offering a probabilistic representation of its hybrid operations.

Finally, a generative ABM-RL model was constructed in which Turkey was represented as an attacking agent with the ability to select between DIMEFL actions, while African countries were modelled as target agents with probabilistic responses. The Turkish agent was trained to identify sequences that maximise rewards associated with accumulated influence, instrumental persistence and minimisation of reputational costs. In the ABM-RL simulation, the reward combines influence and sequence persistence with penalties for reputation, risk of escalation and legal costs, so that the agent learns under threshold.

Assuming that for future studies it would be ideal to begin with an empirical design of Turkey as an actor based on expert judgement, for the purposes of our research the aim was not to reproduce each real event, but to capture the generative logic that explains why Turkey combines diplomacy, information, economics, finance, legality and, to a lesser extent, military force in the way it does. This modelling

was implemented using a Python script, with a modular architecture that allows parameters to be adjusted and the environment to be extended to other actors.

Although the model is based on classical reinforcement learning (Q-learning), its explanatory power could be expanded in the future by incorporating cognitive dynamics inspired by belief diffusion models. Since strategic decisions are based not only on immediate rewards but also on accumulated perceptions and social dynamics, it is relevant to incorporate belief diffusion models.

DeGroot's (1974) approach proposes that agents update their beliefs as weighted averages of their neighbours' opinions, which allows for the simulation of convergence processes in strategic networks. For their part, Deffuant *et al.* (2000) introduce a logic of tolerance: agents only modify their beliefs if the difference with their interlocutor is within an acceptable threshold, generating patterns of polarisation or consensus. These theories, although developed in the field of sociodynamics, offer useful mechanisms for enriching ABM-RL models with components of social influence, cognitive resistance, and strategic memory.

In future lines of research, these elements could be integrated into parameterised agents operating within the framework of cyber-physical-social systems (CPSS) proposed by Zhou *et al.* (2020). This approach would allow for the simultaneous modelling of physical (observable actions), digital (circulating information) and social (perception and reputation) dimensions, generating more realistic and adaptive simulations. In this sense, an agent calibrated with empirical data and endowed with reputational sensitivity could not only optimise tactics but also evolve strategically based on geopolitical feedback.

Furthermore, this approach could be adapted to cybersecurity scenarios, where agents simulate responses to disinformation campaigns or hybrid digital attacks. Therefore, the proposed architecture not only allows for the representation of observed hybrid sequences, but also opens the door to more complex cognitive simulations, where agents evolve strategically based on their environment, reputation and operational memory.

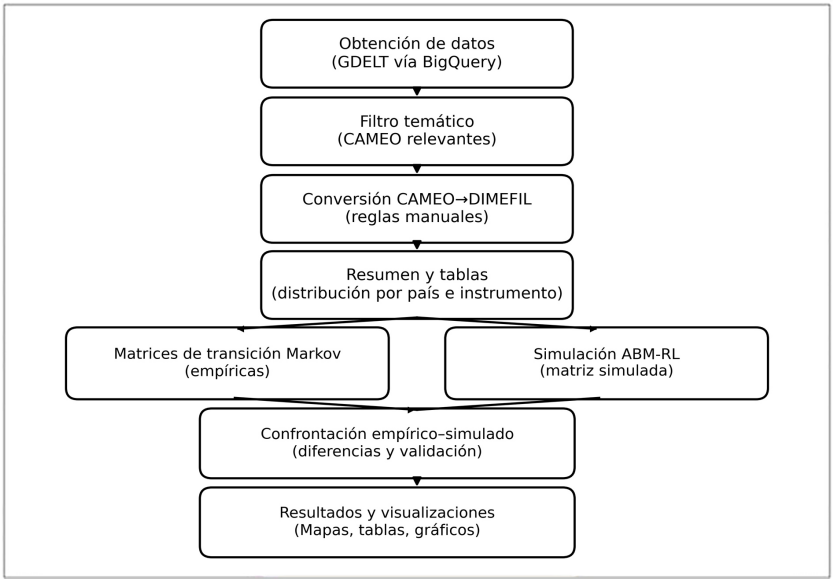


Figure 1 Integrated methodological flow (OSINT+DIMEFL+statistical analysis+ABM-RL simulation). The diagram summarises the stages of the study: (1) extraction of events from GDELT, (2) conversion from CAMEO to DIMEFL, (3) construction of panels and empirical analysis using Markov, NB and SARIMAX models, (4) design of the ABM-RL model and (5) comparison between empirical and simulated patterns. Source: author's own elaboration

This methodological procedure serves a dual purpose: it provides transparency and replicability by relying on open data and explicit rules, while also offering exploratory capacity by combining empirical evidence with adaptive simulation.

4 Results and analysis

4.1 Extraction and mapping of events by DIMEFL (GDELT) categories

The database was accessed through Google BigQuery, which allowed millions of records to be filtered using specific criteria for actors, locations, dates, and event types. Both GDELT 1.0, which provides historical coverage up to 2015, and GDELT 2.0, which updates information in near real time since that year, were integrated. This covered the period 2002–2025, sufficient to capture Turkey's first steps in active policy in Africa through to the consolidation of its presence in the last decade. This interval includes key milestones such as the increase in official visits and the opening of embassies from 2005 onwards, involvement in the Libyan civil war in 2011 and 2019, and the establishment of a military base in Somalia in 2017.

In order to obtain a manageable and representative sample of data, a limit of twenty thousand events in total was set, with no fewer than eight hundred per country. In addition, and in order to focus the study, the dataset was limited to bilateral interactions between Turkey and four African countries: Libya, Mali, Niger and Somalia. This selection is relevant because it represents the three priority geopolitical axes for Turkish projection in Africa: the Maghreb, the Sahel and the Horn of Africa. The inclusion of these countries ensures that the analysis focuses on the scenarios where Turkey's hybrid strategy has been deployed most intensively. Furthermore, the records include both actions initiated by Turkey and those received, allowing for an analysis of the relational dynamics in both directions.

It is clear that what happens in each Turkey–(Libya/Mali/Niger/Somalia) relationship may be influenced by third parties (allies or competitors) or by natural or climatic events. Precisely for this reason, our analysis does not assert causality, but rather describes patterns: we observe what tends to come after what in regular time windows (quarters) and in both directions (initiated and received actions). The sample was designed to be balanced and manageable: an overall cap (twenty thousand events) prevents a single theatre from distorting the whole, a minimum (less than or equal to eight hundred per country) ensures comparable coverage, and the focus on four countries responds to where Turkish activity is most intense and traceable. Furthermore, we compare these sequences with the simulation: when the simulation over- or underestimates a transition, we treat it as an indication of factors not yet modelled (sanctions, reputation, pressure from allies), not as 'proof' of causality.

In line with this caution, the study limits its validity to the current version of the research (single actor and observational environment) and leaves the door open to a more ambitious future simulation that integrates a multi-actor phase, with explicit context variables and additional temporal contrasts, to assess the extent to which these third-party relationships explain (and not just accompany) the sequences we measure here.

Once the data had been extracted, a reclassification procedure was applied to translate the CAMEO codes into the six instruments of power included in the DIMEFL framework: Diplomatic, Informational, Military, Economic, Financial and Legal. The correspondence was defined using transparent and reproducible conversion rules. Diplomatic actions cover codes 01 to 06, which include official visits, negotiations and multilateral agreements. Communication and propaganda events, collected in root code 07 and in certain subcategories of series 01 to 03, were mapped as informational. The military and security sphere was linked to codes 12 and 14 to 20, ranging from threats of force to armed confrontations. Economic actions were identified with codes 07 to 11, excluding those specifically financial, which were treated separately to reflect loans, transfers, sanctions and monetary aid. Finally, legal or judicial actions were associated with codes 13 and 15 to 17, which cover everything from treaties and extraditions to regulatory restrictions.

This extraction and mapping process produced approximately fourteen thousand unique events between 2002 and 2025. Once consolidated and refined using Python code scripting, the records were organised into quarterly panels by country and instrument, allowing trends, sequences and variations in Turkish hybrid activity to be observed. Although the data ultimately reflect media coverage—and are therefore subject to visibility and agenda biases—their breadth, standardised coding, and continuous updating make them a particularly suitable source for identifying patterns of hybridisation on which the statistical analysis and subsequent computer simulation were based.

TABLE II . NUMBER OF TURKEY–AFRICA EVENTS BY COUNTRY AND INSTRUMENT (2002-2025)

Country	Diplomatic	Informative	Military	Economic	Financial	Legal	Total
Libya	4611	2302	847	290	640	427	9117
Mali	318	172	78	11	73	25	677
Niger	130	105	27	5	31	10	308
Somalia	1748	1045	560	87	368	267	4075

Source: author's own elaboration based on GDELT (Google BigQuery).

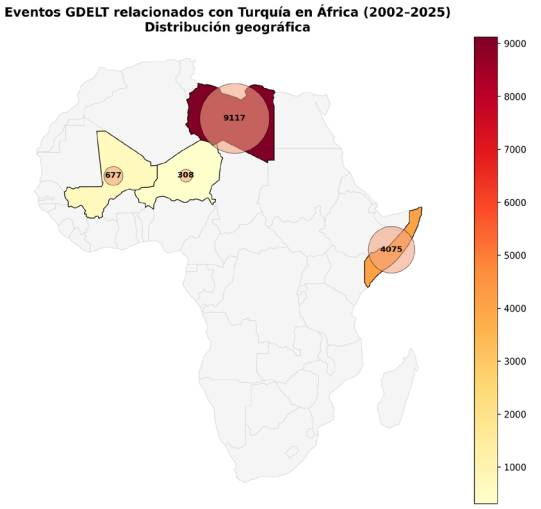


Figure 2. Choropleth map of Turkey–Africa events (2002–2025). The colour intensity reflects the number of events recorded in Libya, Somalia, Mali and Niger. Libya and Somalia account for more than 70% of total events. *Source*: author's own elaboration based on GDELT

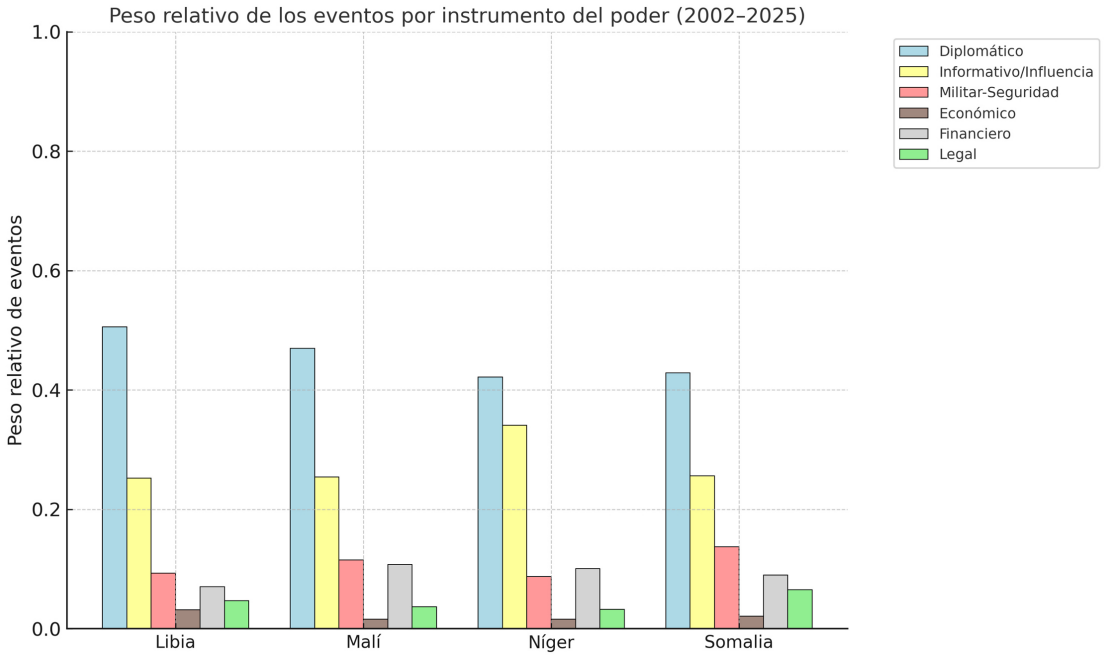


Figure 3. Distribution of DIMEFL instruments by country (2002–2025). Parallel table chart showing the relative proportion of each instrument by target country, with a predominance of diplomatic and informational instruments. *Source*: author's own elaboration

4.2 Empirical transition matrices (Markov model)

The next methodological step was to construct first-order transition matrices from GDELT data, classified according to the DIMEFL scheme. Each cell represents the empirical probability that, after an event linked to a specific instrument of power (e.g., diplomatic), the next observed event will belong to the same instrument or to a different one. This approach is based on Markov processes, which assume that the probability of transition depends solely on the immediately preceding state, allowing strategic sequences to be modelled without the need to reconstruct complete trajectories.

Sequential analysis using Markov chains made it possible to identify the operational grammar of Turkey's hybrid strategy in Africa (Somalia, Libya, Niger and Mali). The matrices reveal high internal persistence, especially in diplomatic and informational instruments, where Turkey repeats consecutive actions (74% and 57% respectively), suggesting prolonged positioning and narrative campaigns. In addition, significant bridge transitions emerge, such as those connecting diplomacy with information (13%) and military with diplomacy (36%), indicating that coercive actions are often followed by institutional or media legitimisation efforts. This pattern can be seen, for example, in Turkey's military intervention in Libya (2020), followed by intense diplomatic efforts and media coverage.

Diplomacy appears to be the dominant structural instrument, while information acts as a narrative reinforcement. Military action, on the other hand, is used in a surgical and contextual manner, almost always followed by a diplomatic-informational offensive that seeks to minimise reputational costs and consolidate influence. As for African responses, the data show a concentration on the diplomatic and legal

levels, probably due to material limitations that prevent a symmetrical military or economic response. This dynamic reveals a structural asymmetry: Turkey deploys complex hybrid sequences, while its counterparts channel the confrontation towards institutional frameworks, such as international law or multilateral diplomacy.

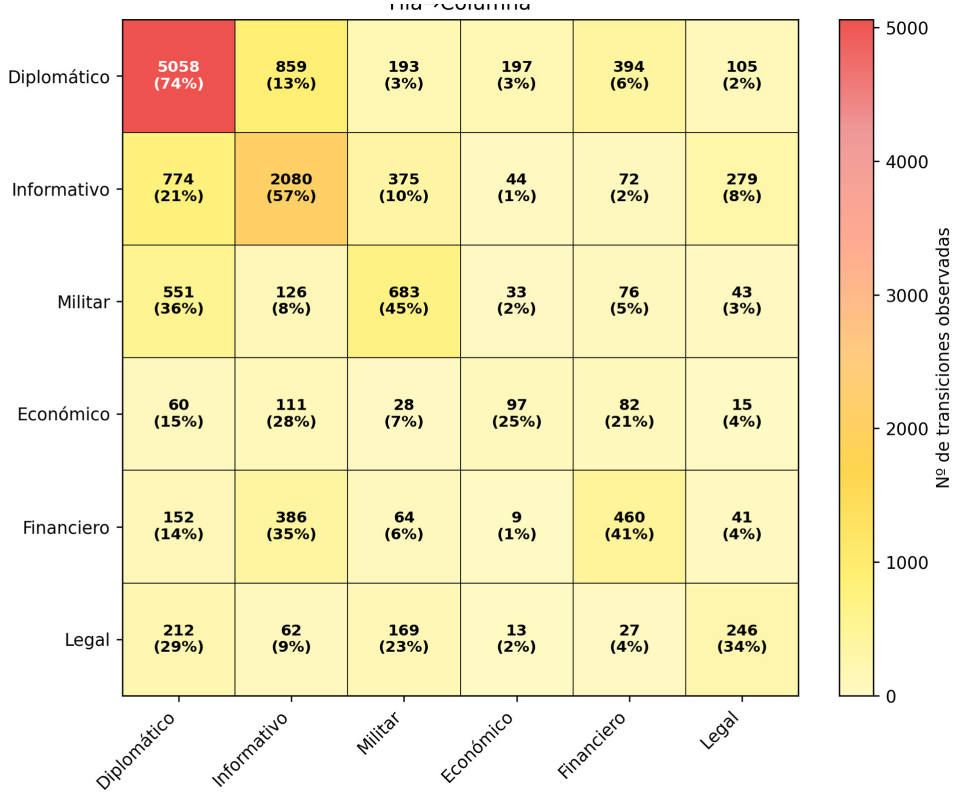


Figure 4. Heatmap of DIMEFL transitions (empirical Markov). Matrix representation of instrument sequences. The diagonal shows persistence (e.g., diplomatic→diplomatic), while the cells outside the diagonal reveal key transitions such as military→informational. *Source*: author's own elaboration

The suitability of this approach to the case study actor and its comparison with the ABM-RL simulation model are explained in the section.

4.3 Dynamic adjustments and temporal trends

The application of statistical models such as Negative Binomial (NB) and SARIMAX complemented the sequential analysis with a more structured reading of temporal dependencies and aggregate trends in historical series. The NB model, designed for count data with overdispersion, showed a robust ability to capture the carry-over effect in diplomatic and informational instruments: quarters with high activity in these domains tend to be followed by new similar episodes, confirming the cumulative nature of hybrid campaigns. This dynamic is particularly evident in Libya and Somalia, where Turkey's projection maintains operational continuity, while in Mali and Niger the behaviour is more erratic and associated with critical junctures such as coups d'état or external interventions. In the Sahel, these disruptions are intertwined with insurgency and local violence, which conditions both Turkey's projection and the predictive capacity of the model (Tollefsen and Buhaug, 2015).

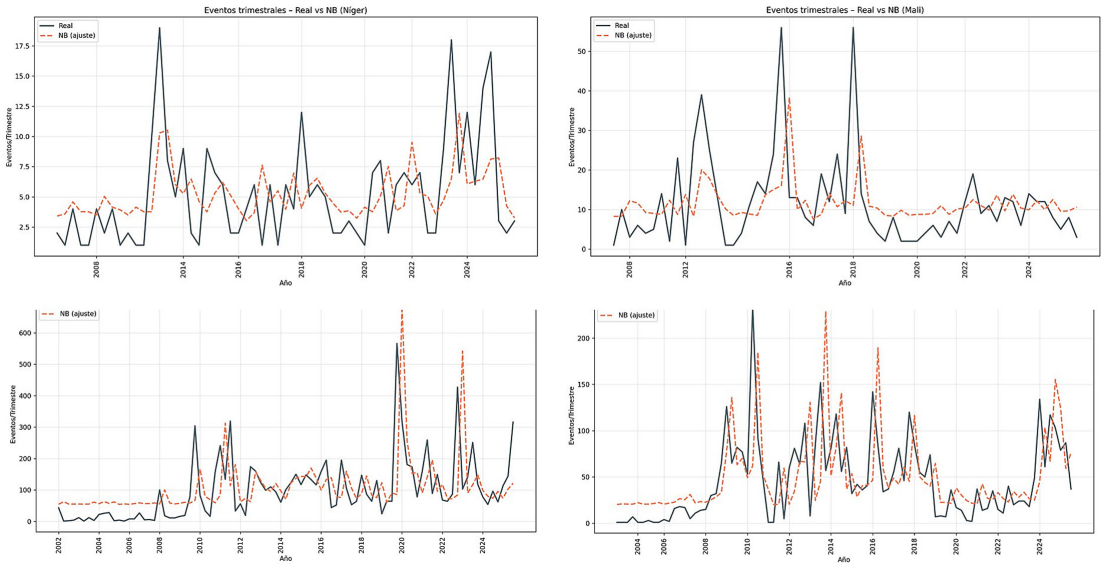


Figure 5. NB adjustment vs. actual data by country. Each graph shows the actual quarterly series (solid line) against the NB model adjustment (dashed line). Libya and Somalia show good predictive capacity; Mali and Niger show greater volatility. *Source*: author's own elaboration

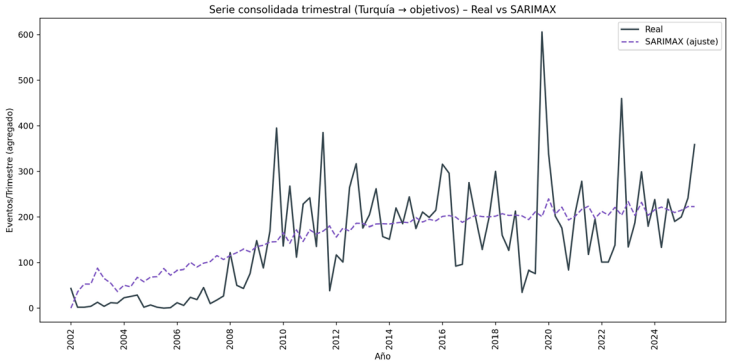


Figure 6. Consolidated series with SARIMAX adjustment (2002-2025). The continuous line reflects observed events and the broken line reflects the SARIMAX adjustment. The upward trend and peaks linked to strategic milestones can be seen. *Source*: author's own elaboration

The adjustment of time series using SARIMAX identified a sustained upward trend in Turkish hybrid activity between 2002 and 2025, with acceleration from 2015 onwards. The most notable peaks coincide with strategic milestones such as the intensification of the conflict in Libya, the opening of the Mogadishu base, and the Turkey-Africa summits. Although no regular seasonality was detected, the model captured structural oscillations linked to these events, reinforcing the idea that Turkey's strategy combines institutional continuity with tactical adaptability in the face of geopolitical opportunities.

The graphs included (figures 5 and 6) illustrate these findings: NB shows greater predictive accuracy in continuity scenarios (Libya and Somalia), while SARIMAX reflects an upward curve with peaks synchronised with moments of high strategic visibility.

The articulation between these dynamic results and the ABM-RL simulation is developed in section 4.4, in order to concentrate the methodological discussion there and avoid redundancies.

4.4 Integration with ABM-RL simulation

The third phase of the analysis consisted of comparing the empirical DIMEFL transition matrix, obtained using first-order Markov chains, with a simulated matrix generated from an agent-based model with reinforcement learning (ABM-RL). The comparison was made for reasons of methodological parsimony: implementing a multi-agent environment, in which African countries would also develop adaptive learning, would have exceeded the scope of this study. Instead, we opted to demonstrate a replicable procedure that contrasts empirical observation and adaptive generation. The ABM-RL matrix does not constitute an 'alternative reality', but rather a virtual laboratory, calibrated with real data, which allows plausible causal mechanisms to be inferred.

In other words, the model is already dynamic in the strict sense: the agent learns over time and adjusts its policy according to signals from the environment observed in the data (e.g., diplomatic-legal responses, variations in reputational tone/Goldstein and context shocks), incorporated as costs and thresholds in the reward function. These signals operate as an adversarial 'proxy' reflex: when the target reacts, the expected cost of certain sequences changes and the agent re-optimises its behaviour. Our objective is to contrast patterns (what tends to follow what) rather than assert hard causality. However, we do not rule out third-party mediations: that is why we treat discrepancies between empirical and simulated matrices as indications of unmodelled constraints. In line with this caution, the work limits its validity to the current version (single actor and observational environment) and opens up a natural extension to a future multi-actor study, with an explicit reaction function and additional context variables.

Turkey was modelled as an attacking agent with the ability to choose between diplomatic, informational, military, economic, financial and legal actions, while African countries were represented as passive targets with probabilistic responses. The Turkish agent was trained to maximise influence, consolidate effective sequences and minimise reputational costs, thus reproducing adaptive strategic decisions. Although the model does not incorporate a complex internal doctrine, the reward function acts as a proxy for Ankara's strategic objectives: the pursuit of influence and the consolidation of presence, balanced with the need to keep reputational costs and escalation risks below a threshold that would trigger open confrontation. This approach, based on the Q-learning method (Watkins and Dayan, 1992), is one of the pillars of adaptive agent modelling.

The comparison between empirical and simulated matrices reveals significant structural consistency. Both confirm diplomatic-informational persistence (D→D, I→I) and the recurrence of bridge transitions (M→D, M→I), reflecting Turkey's tactic of accompanying military interventions with diplomatic offensives or narratives to legitimise its actions. Likewise, the model reproduced economic-financial couplings, indicating that the agent learned to combine these resources to consolidate its presence without directly resorting to force.

The consistency found (D→D, I→I and M→D/M→I bridges) is interpreted within the case of Turkey and not as a universal rule. Future, more extensive studies

could determine whether this is a specific *modus operandi* (e.g., of NATO countries) or a more general grammar of the current international system. In the meantime, our conclusions are limited to the case analysed and are offered as a replicable basis for that comparison.

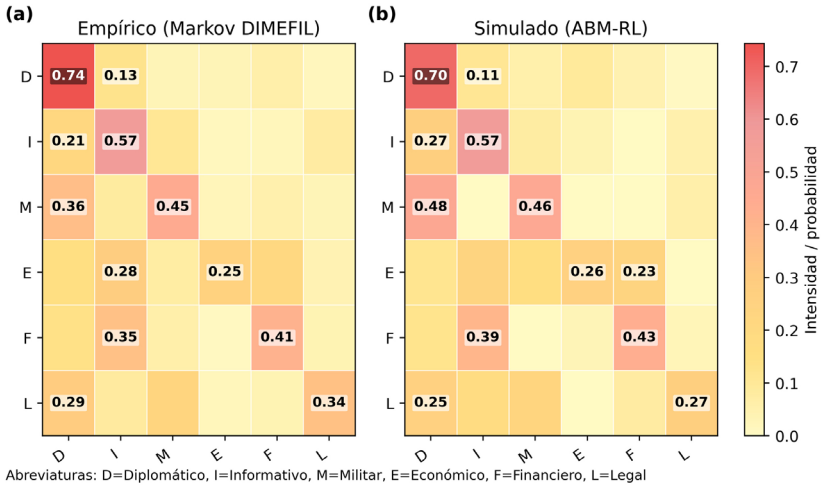


Figure 7 . Transition matrix: empirical (Markov) vs. simulated (ABM-RL). Side-by-side comparison of transition probabilities. The ABM-RL model reproduces the main patterns observed, although it overestimates some military sequences. *Source*: author's own elaboration

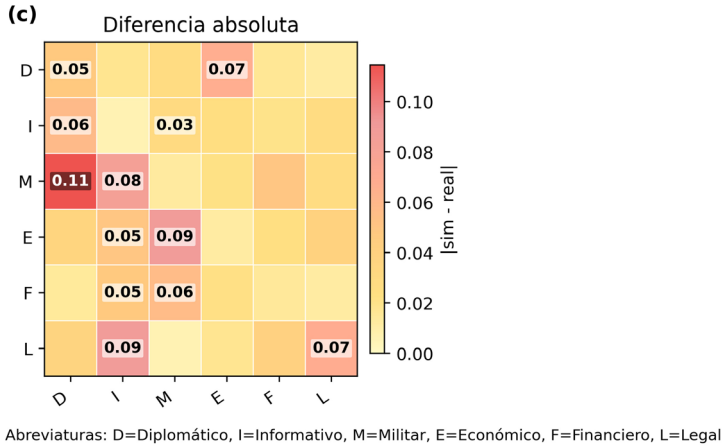


Figure 8. Absolute difference between empirical and simulated matrices. Heatmap of |sim–real|. Low values (yellow) indicate a good fit; high values (orange/red) indicate divergences that point to unmodelled factors, such as reputational costs or interventions by third parties. *Source*: author's own elaboration

However, the absolute difference matrix (figure 8) allows us to identify relevant divergences between the empirical and simulated models, which is key to assessing the limits of the generative approach. The most notable discrepancies are concentrated in transitions involving the military instrument, particularly M→D (military to diplomatic), with an absolute difference of 0.11, indicating that the ABM-RL model predicts this transition with a significantly higher frequency than that observed in the actual data (diplomatic agreements are reached after deploying defence diplomacy or coercive actions, as the case may be). Similarly, the M→I (military to informational) cell shows a difference of 0.08, suggesting that the simulated agent tends to link military actions to media narratives more intensely than empirical patterns reflect.

In addition, other relevant discrepancies emerge in less expected transitions: E→M (economic to military) and L→I (legal to informational), both with differences of 0.09. These values indicate that the simulated model attributes a higher frequency to the conversion of economic or legal instruments towards military coercion dynamics or a rebound in narratives to give visibility to possible agreements, which could reflect a logic of strategic escalation.

These overestimations can be attributed to factors not modelled in the simulated environment. Empirically, transitions from military to diplomatic or informational approaches are conditioned by international reputational costs, such as the risk of sanctions, multilateral condemnation or loss of regional legitimacy. Likewise, the conversion of legal or economic instruments to military or informational ones may be limited by institutional norms, multilateral pressures, or the presence of external actors such as France, the US, or Russia, which introduce operational restrictions that the simulated agent does not face.

In other words, the simulated agent optimises its decisions based on an internal logic of instrumental efficiency, maximising transitions that in theory produce greater strategic impact. However, by not incorporating geopolitical, regulatory or diplomatic constraints, the model tends to overemphasise certain sequences that, in practice, are subject to external costs and structural constraints. This difference between the simulated and the observed does not invalidate the model, but rather reveals its explanatory limitations and points to areas where future simulations could incorporate adaptive penalties or geopolitical counterweights to improve their realism.

4.5 Theoretical discussion and implications

The empirical-simulated comparison allows us to draw several lessons about Turkey's hybrid operations in Africa. First, it confirms that these strategies do not respond to rigid sets of actions, but rather to a sequential and multisectoral design: Turkey combines diplomacy, information, economics and force in a chain, adjusting their deployment to the context. Markov matrices show the structural persistence of diplomacy and information, as well as bridging transitions—especially military→diplomacy and military→information—and economic-financial couplings that illustrate a flexible architecture geared towards consolidating influence.

Secondly, NB models applied to quarterly series confirm that diplomatic and information activity exhibits a carry-over effect, reflecting sustained campaigns in scenarios such as Libya and Somalia. In contrast, volatility in Mali and Niger suggests a more tactical and opportunistic logic, where interventions respond to critical situations rather than prolonged strategies. The SARIMAX model complements this finding by identifying a sustained upward trend since 2015, marked by milestones such as the Libyan civil war, the opening of the Mogadishu base and the Turkey-Africa summits.

Thirdly, the ABM-RL simulation reproduces many of these patterns—persistence in diplomacy and information, military→diplomacy/information sequences,

economic-financial linkages—but also reveals discrepancies. The overestimation of transitions such as M→D or E→M suggests that, in an unrestricted virtual environment, post-coercion legitimisation and economic leaps towards the military would be more frequent. In practice, factors such as international reputational costs, the presence of third parties, or material constraints mitigate these sequences.

Methodologically, the comparison between empirical and simulated matrices demonstrates the complementarity of the approaches: Markov provides descriptive transparency, NB allows for the quantification of persistence, SARIMAX reveals structural trends, and ABM-RL introduces explanatory and exploratory capacity. The decision to limit the simulated model to an attacking agent responds to a criterion of methodological parsimony, which prioritises replicability over complexity.

Taken together, this design not only describes Turkey's hybrid operations, but also offers explanatory hypotheses that enrich the literature on hybrid threats and lay the groundwork for comparative studies in other geopolitical contexts.

4.6 Composite sketch of the hybrid strategy in Africa

The combined analysis of transition matrices, statistical models and adaptive simulation allows us to clearly outline the operational architecture of Turkey's hybrid strategy in Africa. Turkey does not act through isolated interventions, but rather articulates a strategic sequence in which diplomacy constitutes the structural core, reinforced by the information narrative, while military coercion and economic-financial penetration are activated tactically depending on the context. This logic responds less to rigid planning than to tactical adaptability, confirmed by both empirical data and simulated patterns.

Markov chains show high persistence in diplomatic (74%) and informational (57%) instruments, indicating prolonged positioning and legitimisation campaigns. Specific examples include Somalia, where Turkey consolidated its presence with the Mogadishu base in 2017 and the 2024 naval agreement, and Libya, where the 2020 intervention was accompanied by a maritime memorandum and the deployment of advisers and drones. These cases illustrate how the military→diplomacy/information sequence functions as a post-coercion legitimisation mechanism.

For their part, NB models confirm a spillover effect in the diplomatic and information domains, while ABM-RL simulations reproduce these sequences, although they tend to overestimate M→D and M→I transitions. This divergence reflects the absence in the model of factors such as international reputational costs or the intervention of third parties, which in practice limit escalation. In the Sahel, on the other hand, Turkey adopts a more tactical and opportunistic profile: military agreements and the sale of drones to Mali and Niger show a logic of technological penetration, but with greater volatility and dependence on critical situations, such as coups d'état or power vacuums.

Overall, the resulting picture describes a sequential and adaptive hybrid strategy: diplomacy as a structural pillar, information as narrative reinforcement, occasional

military coercion followed by institutional legitimisation, and economic and financial resources as instruments of consolidation. African countries, limited in their symmetrical capabilities, respond mainly at the diplomatic and legal levels, which consolidates a structural asymmetry favourable to Turkey.

This section summarises the findings regarding the 'what' (empirical diagnosis), the 'how' (observed sequences) and the 'why' (logics inferred in the simulation). It thus offers a clear and replicable characterisation of Turkey's hybrid strategy, paving the way for the strategic and methodological implications developed in the conclusions.

4.7 Validation of the hypothesis

The results of the empirical-simulated contrast are consistent with the hypothesis that the dynamics of hybrid threats can be reproduced with autonomous agents that learn and adapt their behaviour. The ABM-RL agent, initialised with the empirical transition grammar, converged towards a stable policy that increases the average return and reduces reputational and escalation penalties throughout the episodes, a sign of learning and not simple random reproduction. The learned policy prioritises the use of instruments of power in the diplomatic and informational spheres and activates connections with security policies and the use of military instruments when the expected cost is low, replicating the patterns observed in the empirical matrices; it also reproduces economic-financial couplings by seeking consolidation without directly resorting to force. Where imbalances appeared (e.g., occasional overestimation of M→D/M→I), the introduction/adjustment of reputational penalties and escalation risk led the agent to re-optimise its sequencing in subsequent iterations, behaviour consistent with strategic adaptation based on feedback.

Overall, the agent's convergent learning and adjustment capacity lend internal validity to the hypothesis and reinforce the value of the model as a virtual laboratory for exploring decision rules. The next logical step—already noted in the scope—is to extend this dynamic to a multi-actor scenario to capture adversarial reflection and third-party mediation, based on a design of our own actor based on expert judgement.

5 Conclusions

This study has addressed a central gap in the analysis of hybrid threats: operationalising the phenomenon with a working definition—hybrid interference as sequential coordination of DIMEFL instruments below the threshold of war, with plausible ambiguity/deniability and cumulative material and cognitive effects—and linking that definition to a replicable pipeline.

To this end, we have worked on three levels, using empirical reclassification (GDELT→DIMEFL) in quarterly panels, dynamic analysis with Markov chains, NB and SARIMAX to identify patterns, persistences and trajectories, and finally an adaptive ABM-RL simulation that transforms the evidence into decision rules under explicit costs and thresholds in 'laboratory' conditions. The result is a transparent

framework that describes observable patterns and, at the same time, explains how an actor can adapt to changing environments.

Applied to the Turkish case in Africa, the approach offers a coherent picture of a hybrid strategy: persistence of diplomatic to informational transitions, bridges from military to diplomatic/informational, so that military intervention is supported by diplomacy or a narrative of legitimisation, and economic-financial reinforcements that consolidate the actor's presence without resorting unnecessarily to force, without this meaning that its use is renounced, as we have seen in the case of Libya.

These findings coincide with and confirm previous research (Arslan, 2025), which already pointed out the following:

> '[…] this study has explained how hybrid warfare and grey zone strategies transformed Turkey's Middle East security policy through multi-level causal mechanisms. Findings have demonstrated with concrete indicators the reciprocal interaction among threat exposure, securitisation discourse, and policy output. The integration of neorealist power balance with Copenhagen School securitisation theory has provided an original theoretical framework explaining both material and discursive dimensions of hybrid strategies'.

The differences between theatres—prolonged campaigns with clear objectives in Libya and Somalia, versus more opportunistic interventions in Mali and Niger—reinforce the idea of sequences that react to the environment. For their part, the empirical response of African countries is concentrated on the diplomatic and legal levels, maintaining the sub-threshold framework and an asymmetry favourable to Ankara.

However, the objective of this work is not specifically the case study itself. What is relevant is that the empirical-simulated comparison validates the working hypothesis: we can model hybrid agents to study how they learn and adapt in order to carry out policies that maximise their influence and minimise reputational and escalation costs. The ABM-RL reproduces the central grammar detected in the data and adjusts its policy when penalties change, which lends internal validity to the approach. Where discrepancies appear (for example, in the occasional overestimation of the military over the diplomatic or informational), they are interpreted as indications of unmodelled constraints (alliances, sanctions, reputational pressure), i.e., they constitute approaches for subsequent multi-actor trials rather than 'failures' of the model.

These conclusions are supported by a deliberately parsimonious scope. Our study has presented one actor (Turkey) and one observational environment to ensure clarity, traceability and replicability; it describes temporal patterns but does not assert structural causality. The sampling of GDELT events (global cap and minimum per country) aims to balance coverage and manageability, reducing biases due to media overexposure and favouring comparability between theatres.

All in all, the main value of the framework we present lies in its portability and its ability to open up and propose future lines of research. The natural extension of

subsequent studies would consist of making an initial design of the actor based on a panel of experts who define and lead the simulations in a multi-actor environment that incorporates adversarial reflection (opponent learning) and explicit context variables and rules of engagement to assess the extent to which the dynamics of opportunistic or competitive actors explain—and not merely accompany—the measured sequences. At the same time, cross-replication of the pipeline in other actors (NATO, non-NATO, non-aligned) and other scenarios will make it possible to determine whether the patterns observed are idiosyncratic to Turkey or correspond to general trends in the ecosystem of international relations in today's world. It should be noted that the analytical framework applied here, based on the DIMEFL scheme and NATO's conceptualisation of hybrid threats, has a Western doctrinal origin. Its application to actors with radically different strategic frameworks (e.g., China or Russia) may require conceptual and methodological adaptations to capture their specific logics of interference (cognitive, legal instruments of power, etc.). Undoubtedly, the analysis of their theoretical frameworks is a starting point for future work in this regard.

In terms of utility, the proposed assembly provides a reproducible basis for early warning and scenario exploration: it integrates open data, transparent rules and a 'virtual laboratory' that converts divergences into research questions. With these pieces, the agenda remains open to richer multi-domain and multi-actor models—without losing sight of the common thread of measuring sequences and patterns and explaining learning below thresholds—moving towards comparative assessments that connect observable tactics with strategic trajectories, always under the guidance of expert judgement, but in an environment that goes beyond simple game theory to take a step further and exploit the potential offered by generative artificial intelligence and agent learning.

Technical Annex: Data extraction, processing and modelling procedure

This annex documents the technical flow followed in the study in order to ensure the reproducibility of the analysis. It details the SQL queries in BigQuery, the mapping of CAMEO codes to DIMEFL, the phases of the Python pipeline, and the statistical and simulation models used.

Data extraction (SQL BigQuery)

The empirical basis was constructed from the GDELT Event Database, combining GDELT 1.0 (2002–2013) and GDELT 2.0 (2015–2025). The SQL script applied the following criteria:

- Actors: Turkey as Actor1 or Actor2.
- Target countries: Libya (LY), Mali (ML), Niger (NG) and Somalia (SO).
- Time interval: 2002-2025.
- Key fields extracted: event identifier, date, actors, CAMEO codes (EventCode, EventBaseCode, EventRootCode), Goldstein, AvgTone, coverage metrics (mentions, sources, articles) and geolocation (ActionGeo_CountryCode, coordinates).

- Preliminary DIMEFL classification: already applied in the query, using explicit rules:
  - Diplomatic: root codes 04–06.
  - Informative/Influence: root 01–03 and any EventCode/EventBaseCode with prefix 07.
  - Legal: root 13, 15–17.
  - Military-Security: root 12, 14, 18–20.
  - Economic: root 08–11, except for financial subcodes.
  - Financial: subcodes 081–087, 101–108, 109–116 (aid, loans, sanctions, transfers).

In addition, to avoid record overload, a maximum of eight hundred events/year and an overall limit of twenty thousand records were established, selecting the most relevant events according to NumMentions, NumSources and NumArticles. The result was a consolidated file with approximately fourteen thousand unique events, exported in CSV for further analysis.

Processing and reclassification (Python pipeline)

The processing was implemented in the pipeline_turquia_hibrida.py script, designed to be reproducible in any environment. The main phases were:

1. Loading and validation: normalisation of dates, cleaning of duplicates, verification of the DIMEFL column and country codes (LY, ML, NG, SO).
2. Geographic visualisation: generation of a choropleth map of Africa with the distribution of events by country.
3. Quarterly panel: aggregation of events by country, quarter and DIMEFL instrument, exporting the quarterly_panel.csv table.
4. Markov transition matrices: calculation of transitions between instruments (empirical) by country and as a whole, with heatmap-type visualisation and export of matrices in CSV.
5. Statistical models:
   - Negative binomial regression (GLM-NB): to estimate the persistence of events based on lagged values[1] for each instrument.
   - SARIMAX: to identify trends and cyclical dynamics in the consolidated quarterly series.
6. Summary by country: table of absolute distribution of events by instrument and country (events_summary_by_country_type.csv).

1 Lagged value: in econometrics and time series analysis, the term *lagged value* is commonly used to refer to the value of a variable in a previous period. Although it is not included in the RAE dictionary, its use is widely standardised in technical manuals and specialised literature (e.g., Greene, 2018).

7. Empirical-simulated comparison: comparison between empirical and simulated Markov matrices (ABM-RL), with graphical outputs in PNG/PDF.

Statistical modelling and simulation

The models applied were:

- Markov chains (order 1): to capture the tactical sequence between instruments.
- Negative binomial GLM: to model overdispersion and temporal persistence.
- SARIMAX: to analyse long-term trends and cycles.
- ABM-RL (Q-learning): to represent Turkey as an adaptive agent that learns to choose between DIMEFL instruments by maximising rewards (accumulated influence, persistence of effective sequences, minimisation of reputational costs).

The comparison between the empirical Markov model and the ABM-RL simulation validated the learning model's ability to reproduce real patterns while exploring informational divergences.

Operational considerations

- Media bias control: limitation of events per country and selection of relevant records.
- Temporal homogeneity: use of quarters as the minimum unit.
- Transparency: all SQL and Python scripts are documented and available for review.
- Scalability: the pipeline can be applied to other actors, countries or periods with minimal modifications.

Bibliography

Arslan, S. (2025). Measuring the impact of hybrid warfare and grey zone strategies on Turkey's Middle East policy: 1991–2024 [online]. *International Journal of Advanced Research*. 13(10), pp. 1041-1058. [Accessed: 2026]. Doi: 10.21474/IJAR01/21995

Baqués, J. (2021). Tell me... mirror, mirror... am I the fairest in the land: analysis of the instruments of power in today's world [online]. *Global Strategy Report*, 29. [Accessed: 2026]. Available at: https://global-strategy.org/analisis-dime

Box, G. E. P. *et al.* (2016). *Time series analysis: Forecasting and control*. 5th ed. Hoboken: Wiley. ISBN 9781118675021.

Butler, D. y Gumrukcu, T. (2019). Turkey signs maritime boundaries deal with Libya amid exploration row [online]. *Reuters*. [Accessed: 2026]. Available at: https://www.reuters.com/article/world/turkey-signs-maritime-boundaries-deal-with-libya-amid-exploration-row-idUSKBN1Y21VL/

Cameron, A. C. and Trivedi, P. K. (2013). *Regression analysis of count data* [online]. 2nd ed. Cambridge: Cambridge University Press. [Accessed: 2026]. Doi: 10.1017/CBO9780511814365

Chivvis, C. S. (2017). *Understanding Russian "Hybrid Warfare" and what can be done about it* [online]. Santa Monica (CA): RAND Corporation. [Accessed: 2026]. Available at: https://www.rand.org/pubs/research_reports/RR1577.html

Deffuant, G. *et al.* (2000). Mixing beliefs among interacting agents [online]. *Advances in Complex Systems*. 3(1-4), pp. 87-98. [Accessed: 2026]. Doi: 10.1142/S0219525900000078

Degroot, M. H. (1974). Reaching a consensus [online]. *Journal of the American Statistical Association*. 69(345), pp. 118-121. Doi: 10.1080/01621459.1974.10480137

Denizeau, A. (2021). *Mavi Vatan, the "Blue Homeland"* [online]. Rabat: Policy Centre for the New South. [Accessed: 2026]. Available at: https://policycenter.ma/publications/mavi-vatan-blue-homeland

Epstein, J. M. (2002). Modelling civil violence: An agent-based computational approach [online]. *Proceedings of the National Academy of Sciences*. 99(Suppl. 3), pp. 7243-7250. Doi: 10.1073/pnas.092080199

—. 2006. *Generative social science: Studies in agent-based computational modelling* [online]. Princeton: Princeton University Press. [Accessed: 2026]. Available at: https://www.jstor.org/stable/j.ctt7rxj1

European Commission. (2016). *Joint framework on countering hybrid threats—A European Union response* (JOIN(2016) 18 final) [online]. EUR-Lex- [Accessed: 2026]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018

Galeotti, M. (2016). *Hybrid war or gibridnaya voina? Getting Russia's non-linear military challenge right* [online]. Mayak Report. Tallinn: ICDS. [Accessed: 2026]. Available at: https://icds.ee/en/hybrid-war-or-gibridnaya-voina

Gdelt Project. (2015). *GDELT event database – Data format codebook v2.0* [online]. [Accessed: 2026]. Available at: https://data.gdeltproject.org/documentation/GDELT-Event_Codebook-V2.0.pdf

Gerasimov, V. (2016). The value of science is in the foresight: New challenges demand rethinking the forms and methods of carrying out combat operations [online]. *Military Review*. [Accessed: 2026]. Available at: https://www.armyupress.army.mil/journals/military-review/archives/2016/january-february/gerasimov

Goldstein, J., (1992). A conflict-cooperation scale for WEIS events data. *Journal of Conflict Resolution*. 36(2), pp. 369-385. [Accessed: 2026] Doi: 10.1177/0022002792036002006

Greene, W. H. (2018). *Econometric analysis*. 8th ed. Harlow: Pearson. ISBN 9780134461366.

Gürdeniz, C. (2006). Mavi Vatan. In: *Turkish Naval Thought* [collection]. [n. p.]: [n. p.].

Hartley, D. S. III. (2020). *An ontology of modern conflict: Including conventional combat and unconventional conflict* [online]. Cham: Springer. [Accessed: 2026]. Doi 10.1007/978-3-030-21820-2.

Hai, J.; Hou, L. and Wang, Z. (2018). Military brain science: How to influence future wars [online]. *Chinese Journal of Traumatology*. 21(6), pp. 321-323. [Accessed: 2026]. Doi: 10.1016/j.cjtee.2018.06.001.

Hegselmann, R. and Krause, U. (2002). Opinion dynamics and bounded confidence: Models, analysis and simulation [online]. *Journal of Artificial Societies and Social Simulation*. 5(3). [Accessed: 2026]. Available at: https://www.jasss.org/5/3/2.html

Hilbe, J. M. (2011). *Negative binomial regression*. 2nd ed. Cambridge: Cambridge University Press. ISBN 9780521198158.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Arlington (VA): Potomac Institute for Policy Studies.

Hopp, F. R. *et al.* (2019). iCoRe: The GDELT interface for the advancement of communication research. *Computational Communication Research*. 1(1), pp. 13-44. Doi: 10.5117/CCR2019.1.002.HOPP

Hyndman, R. J. and Athanasopoulos, G. (2021). *Forecasting: Principles and practice*. 3rd ed. Melbourne: OTexts. [Accessed: 2026]. Available at: https://otexts.com/fpp3/

Joint Chiefs of Staff. (2018a). *Joint concept for integrated campaigning* [online]. Washington, DC: JCS. [Accessed: 2026]. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf

—. (2018b). *Joint publication 3-0: Joint operations* [online]. Washington, DC: JCS. [Accessed: 2026]. Available at: https://irp.fas.org/doddir/dod/jp3_0.pdf

—. (2018c). *Joint doctrine note 1-18: Strategy* [online]. Washington, DC: JCS. [Accessed: 2026]. Available at: https://irp.fas.org/doddir/dod/jdn1_18.pdf

Korybko, A. (2015). *Hybrid wars: The indirect adaptive approach to regime change*. Moscow: RUDN University Press.

Leetaru, K. (n. d.). *The GDELT Project* [online]. [Accessed: 2026]. Available at: https://www.gdeltproject.org/

Leetaru, K. and Schrodt, P. A. (2013). GDELT: Global data on events, location, and tone (1979–2012) [online]. *Harvard Dataverse*. [Accessed: 2026]. Doi: 10.7910/DVN/27427

Lefebvre, V. A.. (2001). *Algebra of conscience*. 2nd ed. Dordrecht: Springer. ISBN 9781402001442.

NATO (2021). *Allied joint doctrine for the military contribution to countering hybrid threats (AJP-3.21)*. Brussels: NATO.

—. 2024a. *Topic: Countering hybrid threats* [online]. [Accessed: 2026]. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm

—. 2024b. *Hybrid threats and hybrid warfare* [online]. Public Diplomacy Division. [Accessed: 2026]. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm

Padur, A.; Borrion, H. and Hailes, S., (2025). Using agent-based modelling and reinforcement learning to study hybrid threats [online]. *Journal of Artificial Societies*

and Social Simulation. 28(1), art. 1. [Accessed: 2026]. Available at: https://www.jasss.org/28/1/1.html

Qiao, L. and Wang, X. (1999). *Unrestricted warfare*. Beijing: PLA Literature and Arts Publishing House.

Renz, B. and Smith, H. (2016). *Russia and hybrid warfare – Going beyond the label* [online]. *Aleksanteri Papers*. 1. Helsinki: University of Helsinki. [Accessed: 2026]. Available at: https://helda.helsinki.fi/server/api/core/bitstreams/9514b166-0249-42a4-a408-9195e7d32292/content

Schrodt, P. A. (2012). *CAMEO: Conflict and mediation event observations—Event and actor codebook* (v1.1b3) [online]. Parus Analytics. [Accessed: 2026]. Available at: https://data.gdeltproject.org/documentation/CAMEO.Manual.1.1b3.pdf

Schweller, R. L. (1994). Bandwagoning for profit: Bringing the revisionist state back in [online]. *International Security*. 19(1), pp. 72-107. [Accessed: 2026]. Doi: 10.2307/2539149

Schweller, R. L., 2006. *Unanswered threats: Political constraints on the balance of power*. Princeton: Princeton University Press. ISBN 9780691120466.

Sezer, C. (2024). Turkey signs energy cooperation deal with Somalia [online]. Reuters. [Accessed: 2026]. Available at: https://www.reuters.com/business/energy/turkey-signs-energy-cooperation-deal-with-somalia-2024-03-07/

Sutton, R. S. and Barto, A. G. (2018). *Reinforcement learning: An introduction* [online]. 2nd ed. Cambridge (MA): MIT Press. [Accessed: 2026]. Available at: https://dl.acm.org/doi/book/10.5555/3312046

Thomas, T. L., (2004). Russia's reflexive control theory and the military [online]. *The Journal of Slavic Military Studies*. 17(2), pp. 237-256. [Accessed: 2026]. Doi: 10.1080/13518040490450529

Tollefsen, A. F. and Buhaug, H. (2015). Insurgency and inaccessibility [online]. *International Studies Review*. 17(1), pp. 6-25. [Accessed: 2026]. Doi: 10.1111/misr.12202

U.S. Department of Defence. (2013). *China: The Three Warfares* [online]. Office of the Secretary of Defence, FOIA Electronic Reading Room. [Accessed: 2026]. Available at: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Litigation_Release/Litigation%20Release%20-%20China-%20The%20Three%20Warfares%20%20201305.pdf

United Nations Treaty Collection. (2019). *Memorandum of Understanding between the Government of the Republic of Turkey and the Government of National Accord–State of Libya on delimitation of the maritime jurisdiction areas in the Mediterranean* [online]. un.org. Istanbul. *Registration No. 56119*. [Consulta: 2026]. Available at: https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280566605a

Vosoughi, S.; Roy, D. and Aral, S. (2018). The spread of true and false news online [online]. *Science*. 359(6380), pp. 1146-1151. [Accessed: 2026]. Doi: 10.1126/science.aap9559.

Watkins, C. J. C. H. and Dayan, P. (1992). Q-learning [online]. *Machine Learning*. 8(3-4), pp. 279-292. [Consulta: 2026]. Doi: 10.1007/BF00992698

Zhou, Y.; Yu, F. R. and Kuo, Y. (2020). Cyber-physical-social systems: A state-of-the-art survey, challenges and opportunities [online]. *IEEE Communications Surveys & Tutorials*. 22(1), pp. 389-425. [Consulta: 2026]. Doi: 10.1109/COMST.2019.2934393

Article received: 7 September 2025
Article accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Daniel Cortés Villanueva
PhD candidate in Law and Social Sciences. UNED International Doctoral School (EIDUNED).

Email: dcortes124@alumno.uned.es

REVIEW

Los servicios de inteligencia al servicio de la sociedad democrática y el orden constitucional

Daniel Sansó-Rubert Pascual

Publisher: Atelier, 2024 (741) pages

ISBN: 978-84-10174-96-2

Daniel Sansó-Rubert Pascual is a prominent academic and criminologist specialising in security, defence and intelligence, with multiple degrees and postgraduate qualifications in Law, Political Science and Criminology. He has had a prolific teaching and research career and is the author of numerous books and articles on organised crime, terrorism and national security. His professional and academic career includes collaborations with institutions such as the Higher Centre for National Defence Studies (CESEDEN) and the Spanish Institute for Strategic Studies (IEEE), establishing himself as a key figure in studies on democratic security.

The book reviewed here belongs to the academic essay genre and was published in 2024 by the legal publishing house Atelier. It consists of 190 pages that address the role of intelligence in modern democracies in the face of current risks and threats, offering a comprehensive and critical analysis of the role played by intelligence services. It is presented as a profound and necessary reflection in a context where constitutional security and the protection of fundamental rights maintain a balance within the space of legality for the achievement and survival of democracy itself in the face of the challenges present in advanced democratic and legal societies.

This work is a socio-legal analysis of intelligence services and their crucial role in defending democracy and constitutional order, in the context of a growing need to respond to new challenges and overcome current classical models, due to the tension between the need for national security and the preservation of civil liberties and fundamental rights. The thesis focuses, within constitutional democratic frameworks, on the necessary evolution to respond effectively to new threats—especially in the areas of hybrid threats, cyberspace, political polarisation strategies and disinformation—while maintaining a balance between security and respect for the law, the operational reinforcement of a solid legal framework and effective democratic control mechanisms, improving their legitimacy and public perception by overcoming negative or preconceived stereotypes, and developing legal intelligence capabilities to counter specific threats such as lawfare and disinformation.

The book is divided into several sections that address different aspects of intelligence services. First, the author takes a historical journey that allows us to understand the evolution of these institutions, from their origins to their development in the current context. This historical perspective is essential to understanding how the functions and public perception of intelligence services have changed over time. A notable aspect is the discussion of the parliamentary and judicial control mechanisms that must exist to oversee the activities of intelligence services. Sansó-Rubert uses examples to illustrate how these mechanisms can be effectively implemented through specific cases, demonstrating that oversight is not only possible but essential to maintaining public confidence in these institutions.

Throughout the work, one of the central themes explored by the author is the need for a balance between security and transparency, arguing that, while intelligence agencies are essential for protecting society from threats, their operations must be subject to a legal framework that guarantees accountability, emphasising that opacity can lead to abuses of power and the erosion of citizens' rights, which is incompatible with democratic principles.

The structure of the book begins with a masterful prologue by Prof. Doc. José Julio Fernández Rodríguez, followed by six chapters with their respective sections—plus the closing bibliography—where the academic approach is probably one of the most notable features given the author's background in research and teaching, suggesting a rigorous and reflective writing style with didactic connotations.

The narrative style is formal and structured, typical of these academic works on security and politics, including well-founded arguments supported by evidence and connections with other authors who are experts in the field, following a clear logic in the presentation of ideas. The narrative is fluid and coherent, characteristic of well-structured academic texts, where arguments are developed in a logical, progressive and forward-looking manner, facilitating the understanding of complex concepts related to intelligence services and their role in democratic society.

It addresses orbital themes such as legal intelligence, disinformation strategies and lawfare, implementing a narrative that connects various aspects in a coherent manner, establishing relationships between these concepts and their impact on the constitutional order. The narrative flow is reinforced by the author's interdisciplinary approach, resulting in a natural discourse between different areas of knowledge, offering a comprehensive view of the subject, alternating theory with practical projections that maintain a balance that favours fluidity in reading and coherence in the presentation of ideas.

The book's argumentation abundantly presents the connotations characteristic of academic rigour, combining perspectives from law, political science and security studies, which allows it to address the topic from multiple angles, lending depth and credibility. The contextualisation within the democratic spectrum emphasises the legitimacy of intelligence agencies and their role in protecting fundamental rights and public freedoms, introducing the culture of intelligence as a mechanism within public policy to raise awareness in society of the relevance of these services. The author's reflections on the institutional control to which these agencies must be subject within the parliamentary and institutional debate stand out, in order to guarantee their transparency and alignment with democratic values and their adaptation, within the legal framework, to contemporary challenges and new threats, such as disinformation and lawfare. Consequently, the book's arguments are solid because they are backed by a proven theoretical basis, clear legal references and a critical approach to the role of intelligence services in a constitutional democracy, demonstrating a deep understanding of current dynamics and contributing significantly to the academic debate on security and democratic governance.

The book incorporates a wealth of sources from various disciplines, reflecting the author's specialised training. As an academic, Sansó-Rubert uses a wide range of sources, including books and research papers in relevant fields, with references to legal frameworks and other influential works on the functioning of intelligence services in democracies.

In terms of originality and innovation, the work analyses emerging concepts such as the globalisation of constitutional law, legal intelligence, disinformation strategies

and lawfare, contributing new perspectives to these fields of study and collaborating in a doctrinal update by addressing the necessary change in the role of intelligence services in the face of risks and threats in modern democratic societies. Consequently, the work is topical and relevant, highlighting the impact of the subject matter addressed due to its importance in the current context, providing a comprehensive analysis, contributing to the academic debate, on new perspectives in these fields of study within the analysis of contemporary challenges. It is worth highlighting the analysis of the balance between security and rights, addressing the tension between the need for security and the protection of fundamental rights in a democratic state. This work is a contribution to the specialised literature, contributing to a growing area of study, offering a specialised contribution on the role of intelligence services within an informed and critical vision.

Consequently, we are presented with a significant contribution to the debate on intelligence and democracy, where the critical and constructive approach invites readers to reflect on how intelligence services can operate ethically and responsibly within a democratic framework. In addressing the complexity of the relationship between security and citizens' rights, the author offers a theoretical and proactive vision and places himself in a context of growing concern for national security and democratic integrity. His analysis is particularly relevant in an era marked by hybrid threats and cyberattacks, offering a unique worldview by combining legal analysis with practical security considerations, reflecting the author's experience in both fields and positioning himself as an important reference for understanding the role of intelligence services in the contemporary democratic context.

In short, the book immerses us in an understanding of the crucial role of intelligence services in modern democracies, tackling the challenges these institutions face in the face of the diversity of current and future risks and threats, all through well-founded reflections on legal intelligence, disinformation strategies and the phenomenon of lawfare. In conclusion, it is essential reading for academics, professionals and anyone interested in understanding the intersection between security, politics and ethics, providing an in-depth analysis that raises crucial questions about the future of intelligence services in an increasingly complex, interconnected and challenging world, where strategies are proposed for improving the control and supervision mechanisms of these operators.

Review received: 8 September 2025
Review accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Abel Romero Junquera
Captain of the Navy. Analyst at the Spanish Institute for Strategic Studies.

Email: abelromero@fn.mde.es

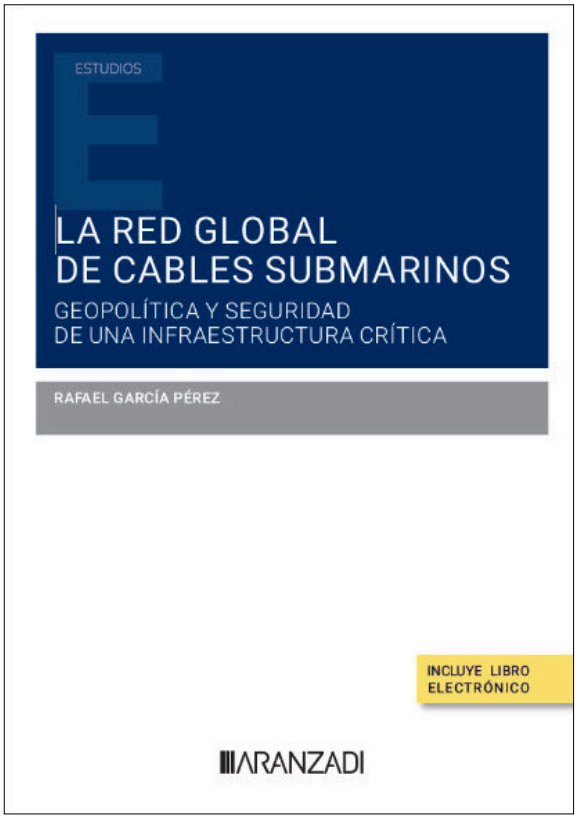
REVIEW

La red global de cables submarinos. Geopolítica y seguridad de una infraestructura crítica

Rafael García Pérez

Publisher: Aranzadi, 2025 (270) pages

ISBN: 978-84-10174-96-2



Rafael García Pérez, in addition to being a professor of International Relations accredited as a university professor, holds a PhD in History, a Diploma in Constitutional Law and Political Science, and a Diploma in National Defence Studies from CESEDEN, among other academic merits.

He is the author of numerous articles and essays on issues related to global trends, security challenges and threats, and although he has extensive knowledge of security and defence issues, his particular concern for maritime affairs and maritime security issues should be highlighted, which has allowed him, for example, to participate as an independent expert in the consultation process carried out by the Department of National Security (DSN) in the recent review of the National Maritime Security Strategy (2023). He is currently part of the team of advisers to the International Legal Advisory Service of the Ministry of Foreign Affairs, European Union and Cooperation, for the extension of the continental shelf before the United Nations Commission on the Limits of the Continental Shelf.

Highly aware of the enormous importance of maritime issues, in this book, *The Global Submarine Cable Network: Geopolitics and Security of Critical Infrastructure*, he transports us to the almost unknown world of the seabed, the ocean floor, emphasising its importance, and in particular that of the submarine telecommunications infrastructure, which is critical for today's society, something of which we are not yet fully aware.

The work begins with a magnificent foreword by Captain Antonio Notario, Head of Political-Strategic Planning at the Department of National Security, and one of the most renowned national experts on maritime security, highlighting the relevance and timeliness of the work in a changing world where the seabed is becoming increasingly important, mentioning the key elements of the submarine cable network that the author will discuss later in the book: the complexity of international law, the technological and industrial implications, geopolitics and national security, all framed within the context of interdependence and the transformative power of economic connections in diplomacy and international relations, in a scenario marked by the long-distance race between China and the US for supremacy in international hegemony.

Regarding the general content of the work, it should be noted that it is not limited to the security of these critical infrastructures, but also addresses the relevance of the global submarine cable network itself, analysing it from various perspectives such as geopolitics, international law, its technological and industrial implications, and national security. This allows the author to identify the main actors in the configuration of the global submarine cable network: states, international organisations and large private corporations. Taking a comprehensive approach, he analyses their role as geostrategic players, acting as major centres of power and influence (they have the will and the capacity to do so). The book opens our eyes to how much is at stake on the seabed: technological supremacy, leadership in the development of artificial intelligence, and above all, who is the protagonist in this new dimension and its relevance in power relations (geopolitics).

Professor García's work invites us to explore all these issues in a systematic and structured way. He begins with a glossary of terms that will allow us to better understand, from a technical perspective, what the submarine cable network is and what its various components are.

He explains that 99% of international data traffic currently travels through the submarine fibre optic cable network, making it the critical infrastructure for digital connectivity between countries, and that the United Nations has described it as the communications infrastructure of paramount importance to the global economy and the national security of states. The cables deployed on the seabed normally follow the same route as traditional shipping lanes, where merchant ships responsible for global maritime trade sail, accounting for approximately 90% of goods transported internationally.

Professor García points out that the global cable network is designed to be redundant, multiplying the number of cables that make the main connections, but the fact that they follow traditional shipping routes means that they are subject to similar geographical constraints. Thus, maritime 'choke points' such as Malacca and Suez are also critical points in the submarine cable network, highlighting the ever-present influence of geography on geopolitics, in this case in its new dimension of competition in cyberspace, where China and the United States are the main players, rivalling each other above all in content generation and in the protection of information transiting the network, which is essentially a struggle for digital hegemony.

The author analyses some of the most salient features of this network, such as the largely private nature of the management, laying and maintenance of submarine cables, and where the global Internet giants, known as GAFAM (Google, Amazon, Facebook, Apple and Meta), are increasingly prominent players. This submarine network is vulnerable to both physical attacks on the cables and cyberattacks (against the systems that manage the network or against the network itself), which is a difficult reality to manage in the absence of an appropriate legal framework. The United Nations Convention on the Law of the Sea (UNCLOS) is very limited, as it is essentially oriented towards states, while non-state actors such as GAFAM are becoming increasingly relevant. In addition, most of the maritime areas where the cables are laid are not subject to the sovereignty of any state.

The book addresses all these issues in a five-chapter structure, which systematically analyses the key elements of the global submarine cable network.

The first chapter analyses the legal dimension of an infrastructure that makes communications possible across the globe, but which does not have a specific international legal regime. After a brief historical review of the most relevant regulations since the 19th century, the current situation is analysed from the perspective of UNCLOS, a legal framework that is essentially limited to the territorial waters of states and does not provide a coherent and adequate regime for their protection. In fact, the author points out that, under international law, submarine cables are legitimate military targets, and he draws on various real-life examples to

emphasise this situation and the need for an adequate regulatory framework for fibre optic cables.

The second chapter seeks to identify the main actors involved in submarine cable networks. Although these are mostly private companies competing with each other, the author questions whether the strategic design of the networks is driven by the interests of these companies, whether it is directed by states, or whether it is actually a combination of both. With regard to security, he points out that knowing the players makes it easier to identify vulnerabilities, either against the network itself or against the information circulating through it.

Although in the early days, the high cost and complexity of managing the cables meant that international consortia (usually centred around a large telecommunications company) had to be used to sell the use of the cable, the new reality is that increased demand in recent decades has led to full ownership, where content companies (GAFAM), the traditional customers, have become owners (of the cable itself and what it transmits), and their financial and technological capacity is allowing them to drive their competitors out of the market, imposing conditions of access and exploitation that are even above the sovereign authority of many states. This forces countries without technological capacity to accept the conditions or give up connectivity, and the states where these large corporations are based (GAFAM are all American) have the political and regulatory capacity to use these companies as vectors in geopolitical competition. Other business actors involved in the manufacture, laying, repair, recycling and removal of submarine cables are also analysed.

Building on the above analysis, the third chapter delves into the geopolitics (power relations explained on the basis of geography) of the global submarine cable network, addressing both its physical dimension (the material structure of the network and the geographical location of the cables) and its virtual dimension (the content that circulates through the network, the exploitation of user data, and, above all, the development and control of a new technology that will be the driving force behind the new production model: Artificial Intelligence (AI). These elements are addressed from the perspective of connectivity and the use that different states make of the Internet (the US uses it as a mechanism for the extraction and economic exploitation of user-generated data; China as a tool for control and surveillance; and Russia as an instrument for subverting other states).

Geopolitical competition (power struggle) for control of the network is becoming increasingly intense; it has gone from being a critical infrastructure in need of protection to an instrument of influence and a threat factor. China and the US, the two main players, are not only competing for control of the network, but also for the data that flows through it, which is indispensable for the development of AI.

Professor García delves into the three main areas of this geopolitical competition: business, security and technical-diplomatic, paying special attention to the latter in this chapter (as in the case of the US veto on Chinese companies, the struggle for the deployment of new large projects, etc.).

The chapter ends with a very interesting view of the geopolitics of cyberspace, concluding that control of the network will allow access (presumably illegitimate) to the information circulating through it, which gives an idea of its strategic importance and why it is therefore the central object of geopolitical competition between the major powers.

The fourth chapter analyses in detail the issue of submarine cable security. It addresses both unintentional threats (natural phenomena, accidents resulting from human activity, etc.) and intentional threats (sabotage of the physical integrity of the network, hostile cyber actions directed at cable management centres either to interrupt data traffic or to extract information transmitted via the cable). The author delves specifically into the protection of submarine cables in the North Atlantic, the actions and initiatives taken by NATO, the European Union, and the states themselves.

The work concludes with a final chapter devoted to the role of Spain, and the Iberian Peninsula in general, in the global submarine cable network, given its excellent geographical position for connectivity between Africa, America and the Middle East. It details the characteristics of the different cables that pass through our waters, how their laying has evolved, and the importance of the main stations and landing points. It argues that in the coming years, 70% of the data reaching Europe will do so via the Iberian Peninsula.

Rafael concludes his work with some final reflections that invite the reader to reflect on the enormous importance of the global submarine cable network, both for its physical size and for the information and data that circulate through it. He points out that although the network initially received little attention from states (different jurisdictions, different companies, insufficient regulation, impossibility of protecting its integrity, etc.), it is now becoming the main focus of geopolitical competition between major powers for control of cyberspace, essentially the US and China, and is characterised by the presence of large technology companies (mostly private, such as GAFAM, in addition to Chinese companies) where governments express their interest in using the network to project power.

Professor García also reflects on the worrying passivity of the EU with regard to the security of information transmitted via cables, which in practice means renouncing European digital sovereignty. Between accepting submission or opting for rupture, he ventures to propose various substantive measures with a view to increasing Europe's role in the geopolitical game for control of cyberspace.

The centrality of the submarine cable network to the international agenda is undeniable, and if the next technological frontier is the development and application of AI, the immense volume of data and the ability to process it almost instantaneously can only be achieved through cables.

Professor Rafael García's book is not only detailed and solidly argued, but also highly relevant at a time of growing geopolitical competition in an increasingly multipolar world, with the United States and China as the main poles, and where data and information, the main fuel for the development of AI, travel through submarine

cables. Despite being a little-known reality, control of the submarine cable network, both in its physical and cybernetic dimensions (the data that travels through the network), has become an essential and priority objective for maintaining (in the case of the US) or achieving (in the case of China) global hegemony in the coming years. The author introduces us to the ins and outs of this new geopolitical reality in a way that is easily understandable for non-experts, but above all entertaining, allowing the reader to take an enjoyable and interesting dive into these submarine matters.

Review received: 3 September 2025
Review accepted: 15 January 2026

Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Gonzalo Vázquez Orbaiceta
Researcher. Naval Thought Centre of the Navy

Email: gvazquezorb@gmail.com

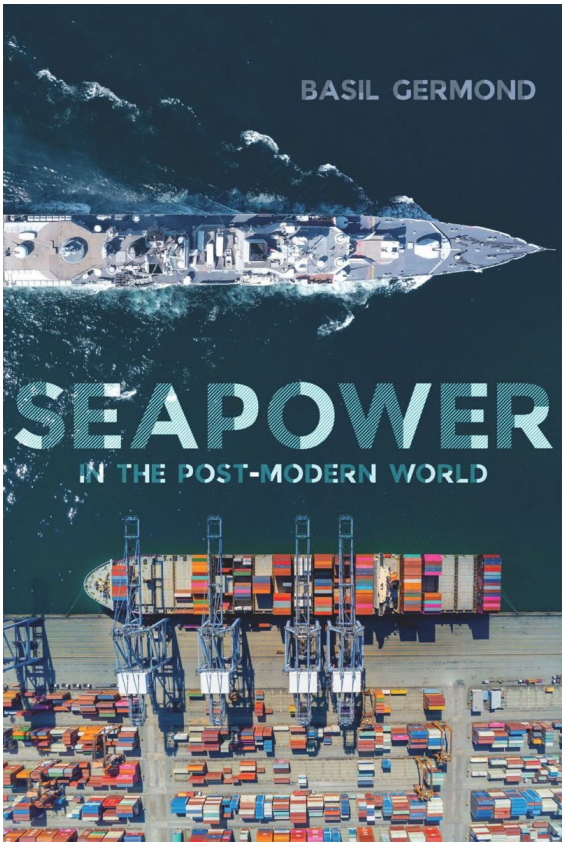
REVIEW

Seapower in the Post-Modern World

Basil Germond

Publisher: McGill-Queen's University Press, 2024 (216) pages

ISBN: 978-0228020882



Basil Germond, co-director of the Security Research Institute at Lancaster University (United Kingdom), is currently one of the most influential voices on maritime power and naval issues. His latest work, *Seapower in the Post-Modern World*, is a true historiography of maritime power from antiquity to the present day, in which the author develops a careful framework for studying the concept, highlighting its importance in today's rapidly changing world. The title of the work, as the author explains in the opening pages, is a tribute to one of the books published just over a century ago by British Admiral Sir Herbert Richmond—one of the most famous disciples of the British historian and strategist par excellence, Julian Corbett—*Seapower in the Modern World* (1934).

The work is divided into seven chapters: A historiography of the concept of maritime power; Maritime power in international relations; Maritime power and post-modernity: A new framework for analysis; From pre-modern to modern maritime power; Solidarity-based and civil maritime power; and The future of maritime power (conclusions). Throughout these chapters, Germond provides a historical review of the existing literature on the subject, efficiently and entertainingly summarising the ideas of the great naval thinkers of the 20th century and identifying the different perspectives (history, culture, strategy, politics, economics) from which this topic has been approached.

The work is also being published at a time when much of the work that has been published in recent years has been limited either to maritime and naval history through biographies of illustrious figures and significant events, or to the exclusive field of maritime security (a field in which figures such as Professor Fernando Ibáñez stand out in our country), leaving aside other issues that shape maritime power as a whole. Germond's work incorporates aspects of all these disciplines to provide a clear and illustrative overview.

The first chapter is essentially a biography of the term 'sea power', originally popularised by the American Alfred T. Mahan in his works published from 1890 onwards. As Germond rightly points out, few works published since then have dared to give a precise definition of the term, which is often treated as a dogma that does not need to be defined. Thus, the different disciplines from which it has been studied and the main figures in the literature of this discipline are reviewed. It also addresses the difference between maritime power and naval power, the latter being the military component of the former, which encompasses many other aspects, and the need for maritime strategy as an instrument to transform maritime power into real influence.

A close example of the importance of clearly defining the differences between the two concepts can be found in the Spanish translations of some of the most representative works in maritime strategic studies. For example, Mahan's seminal work, *The Influence of Sea Power Upon History: 1660-1783*, was translated and published in Spanish as *La Influencia del Poder Naval en la Historia*. This translation often misleads readers unfamiliar with the American author's work, which, far from limiting itself to treating maritime power as the basis of national power from a purely military perspective (naval power), placed special emphasis on the importance of the commercial and economic dimensions of states' maritime activity.

The second chapter focuses on the concept of power and the different perspectives that exist on this concept within international relations, clarifying the concept in relation to the central theme of the work and the field of study in which it is framed. Addressing the different schools of thought within international relations, Germond reviews each one's conception of maritime power and defines the three main axes of analysis that can be used to approach the historical study of maritime power and its influence in today's world: its elements, its articulation or enactment, and its results or objectives.

Based on these three axes or levels of analysis, the third chapter develops the analytical framework that is used throughout the remaining chapters to analyse in detail the main characteristics and particularities of each period. Germond thus defines a theoretical framework for the study of seapower as a historical phenomenon whose development and evolution consist of different stages or eras: pre-modernity, modernity, post-modernity and neo-modernity. This framework is based on a comprehensive conception of the concept of seapower that encompasses all its dimensions. Germond addresses each of these stages through the three axes mentioned above, in order to extract and present to the reader the characteristics of each of these phases or historical moments: the elements and forms of maritime power, the practical exercise of that power, and the ultimate causes or consequences it has for nations and international relations in general.

The fourth chapter focuses on the pre-modern era, covering a period during which entities such as Greece and Carthage dominated the waters of the Mediterranean and laid the foundations for what Alfred Mahan would later call the virtuous circle of maritime power, through which a nation decides to orient all aspects of its existence towards the sea, investing in maritime trade and from whose fruits the resources necessary to protect that trade and defend itself against external threats are born. Germond demonstrates, drawing on the work of historians such as Andrew Lambert (Lambert, 2028), that technological and material factors were what largely limited the expansion of maritime power during this period, rather than cultural and ideological factors.

He then moves on to the modern era (commonly known as the Age of Exploration), studying the process of consolidation of nation states and the development of their maritime power during a period in which the geographical horizons of the known world expanded and what we now call globalisation began to take shape. Germond points out the link between nation states, the construction of empires and the expansion of maritime power, noting that the most immutable and enduring characteristics of maritime power had developed in the pre-modern era rather than the modern era.

He continues his analysis in chapter five by addressing the debate surrounding the characteristics of a post-modern era, considering the extent to which we can recognise that we are currently living in such a period. Here, new characteristics of maritime power emerge, including the compression of time and space, the emphasis on new technologies, the emergence of non-state actors, and the growing influence

of supranational institutions such as the EU and ASEAN in the development and exercise of maritime power. This period also highlights the confrontation between two opposing trends: the growing territorialisation of maritime spaces (represented by aspects such as the United Nations Convention on the Law of the Sea—UNCLOS) versus the deterritorialisation of threats to international security (terrorism being the most notable example of this phenomenon).

The sixth chapter introduces two new concepts developed by the author: collective maritime power and civil maritime power. The first responds to the trend that emerged with the end of the Cold War and the inclination of states with aligned maritime interests to collaborate in order to address the most relevant threats. Germond describes it as a 'solidarity-based society of maritime nations'[1] . The second has to do with the increasing use of maritime spaces for economic purposes through entities such as the merchant navy, large shipping companies, fishing fleets and marine scientific research. The author concludes that the dominance of the Western bloc of nations as an alliance of maritime nations is largely based on this civil-economic vision to exert a dominant influence on the global order, but is increasingly threatened by the emergence of visions from Southeast Asia (primarily China) that challenge this status.

Germond concludes his work with chapter seven and his conclusions, reviewing the general ideas presented throughout the preceding chapters and emphasising the importance of approaching the study of maritime power as a phenomenon that has evolved over the centuries. He argues that continuity rather than change has characterised maritime power as a concept and practice, displaying characteristics that make it universal and not necessarily exclusive to Western nations. He also points to the need to study this phenomenon in greater depth in order to understand more clearly and thoroughly the differences between Western and non-Western nations at a cultural and ideological level.

Broadly speaking, *Seapower in the Post-Modern* World is one of the most comprehensive and succinct works produced to date. As the author points out from the outset, the literature on maritime issues is abundant both in terms of authors and the disciplines from which it is approached. Germond's work therefore succeeds admirably in summarising and organising a significant part of the literature, and in going further thanks to its theoretical framework of analysis. While many other works focus on specific historical periods (as demonstrated, for example, by the literature on Spanish maritime and naval power), Germond provides a linear vision and a clear map for understanding the evolution of the concept as one of the most ancient human experiences.

In this sense, it is a valuable addition to the aforementioned field of study. At the same time, however, the fluidity of the narrative and the author's ability to express

1 This is a highly relevant issue, on which Germond and other authors have occasionally emphasised the importance of a robust commitment to protecting stability and freedom of navigation, fundamental pillars on which globalisation has been based to this day.

the most complex aspects in a simple way make it equally accessible to readers who are unfamiliar with the discipline. Ultimately, it can be conceived as an abridged history of the relationship between human beings and the sea, but also as a guide to understanding the role played by states and non-state entities in the current international order; a role that is set to grow in importance in the coming years and to which special attention should therefore be paid (as China has demonstrated with its ambitious commercial expansion through the Belt and Road Initiative).

Compared to other relevant works in the field, Germond's book is a more than adequate introduction for those new to the field of maritime strategic studies. Today, the global reference work is *Seapower: A Guide for the 21st* Century by British historian and naval expert Geoffrey Till, one of the most illustrious names in this field of study, with whom the author has had the opportunity to share seminars (Till, 2018). His work, the fifth edition of which will be published shortly, is much denser and more overwhelming in content and depth of analysis, resembling more of a manual. In contrast, Germond's work constitutes a first approach to the discipline, providing a remarkably solid knowledge base.

In short, Germond's work is indispensable for academics and professionals in the maritime field, allowing them to reflect on the significance of maritime power for our society, the different ways in which it has been used over the centuries, and, above all, the challenges ahead in an increasingly complex and interconnected world.

Bibliografía

Lambert, A. (2018). *Seapower States: Maritime Culture, Continental Empires and the Conflict that Shaped the Modern World*. Yale University Press.

Till, G. (2018). *Seapower: A Guide for the 21st Century.* 4th ed.. Routledge.

Review received: 8 September 2025
Review accepted: 5 January 2026

DULCINEA
Derechos de explotación y permisos para el auto-archivo de revistas científicas españolas

latindex
BASE DE DATOS ISOC
Dialnet
ieee.es
Instituto Español de Estudios Estratégicos
SHERPA/RoMEO

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL

9 772255 347001 26025