Revista Científica
del Centro Universitario
de la Guardia Civil

Revista
Lógos
Guardia Civil

Version
English

Vol. 3 Núm. 2 (2025)
June

SUMMARY

GOBIERNO DE ESPAÑA · MINISTERIO DEL INTERIOR · GUARDIA CIVIL

Edit:
Ministry of the Interior. General Technical Secretariat. Madrid.

General State Administration Publications Catalogue: https://cpage.mpr.gob.es.

Logos Guardia Civil Magazine
Scientific Magazine of University Centre of Guardia Civil
Edition date: June 2025
NIPO (paper): 126-23-018-2
NIPO (online): 126-23-019-8
Legal Deposit: M-3619-2023
ISSN: 2952-3249
ISSN online: 2952-394X

Responsible entity:
University Centre of Guardia Civil
Research Area
Paseo de la Princesa, s/n
28300 Aranjuez (Madrid)
e-mail: investigacion@cugc.es

Design and layout:
Research Area Office

Official website Logos Guardia Civil Magazine

https://revistacugc.es

CUGC official website

https://www.cugc.es

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

INDEX

III.- CASE LAW REVIEWS

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

INTRODUCTION

Dear reader,

We are pleased to welcome you to the fifth issue of our magazine Logos Guardia Civil, published by the University Centre of the Civil Guard. This new issue brings together a selection of articles that address, from different perspectives and disciplines, some of the most pressing challenges in the field of security, both nationally and internationally.

We open this issue with a contribution from Adriano J. Alfonso Rodríguez, Doctor of Law and Professor of Law and Criminology at the UNED, who offers us a timely reflection on 'Cooperation between security agencies and regional integration processes in Latin America'.

In the research articles section, Juan Francisco Adame Hernández, Director of Strategy, Communication and Promotion at Casa Árabe, presents 'Spain in the face of disinformation: Hybrid challenges and conventional responses', a rigorous study on the risks of disinformation in state security.

Security expert and PhD candidate in Forensic Sciences at the University of Alcalá, Paula Castro Castañer introduces us to 'Intelligence in the spotlight: from Classical Theory to implementation in the Digital Age', a critical approach to the social perception of intelligence services.

The work of Josué Expósito Guisado, sergeant in the Civil Guard and PhD candidate at Pablo de Olavide University, entitled 'Hacktivism: from social protest to state instrumentalisation', analyses the boundaries between digital action and criminal activity.

Alejandro Gómez García, Captain of the Civil Guard and Master's Degree in Operational Security Management, delves into 'International Protection and Sovereignty: the complicated balance between individual rights and national security', a highly sensitive issue in international law.

Don Johannes Luigi Maria Kunz Saporano, a doctoral researcher at the Carlos III University of Madrid, analyses in his article 'Nixon's war on drugs and the rise of virtual border surveillance in the United States' the transformation of security in the US, pointing out how the policies promoted during the "war on drugs" gave way to the development of sophisticated border control systems supported by advanced technology.

The team formed by Francisco Pérez-Fernández, Heriberto Janosch, Enrique López López and Francisco López-Muñoz presents ‘Sexual violence committed by strangers in Madrid and Barcelona: a situational analysis’, a study that provides relevant insights into the geographical distribution and behaviour patterns of urban sexual assaults.

Juan Carlos Rodríguez Bello, First Corporal of the Civil Guard Traffic Group, university expert in road crime and forensic document expert at the UNED, is the author of the article "Drugs and driving: zero tolerance. Methodology of the Synlab laboratory saliva report and approval criteria of the National Accreditation Entity", which addresses scientific and legal standards in the detection of substances.

Mónica Román González is a PhD candidate in the Political Science and Administration and International Relations Programme at the Complutense University of Madrid, and offers us a strategic analysis in ‘The protection of critical underwater infrastructure and the strengthening of security in the Baltic Sea: NATO's Operation Baltic Sentry’, highlighting the importance of international cooperation in maritime scenarios.

Finally, Virginia Belén Subiris Moriel, PhD candidate at the Rey Juan Carlos University, Social and Legal Sciences Programme, closes with ‘Social Economy: The contribution of the Civil Guard Institution through its intellectual capital’, an article that explores the value of shared knowledge and institutional commitment to social development.

On the other hand, the case law review section features a new contribution by Javier Ignacio Reyes López, Senior Magistrate of Alcalá de Henares, who analyses relevant rulings of the Second Chamber of the Supreme Court.

The editorial committee would like to express its sincere gratitude to the authors for their rigour and commitment, and to the external reviewers for their indispensable work. We hope that you find this new edition interesting and that it contributes to knowledge, reflection and continuous improvement in the field of security.

Félix Blázquez González
Director of the CUGC

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

I.- COLLABORATIONS

Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Collaboration

LAW ENFORCEMENT COOPERATION AND CRIMINAL PROSECUTION: PARALLEL CONSTRUCTION?

English translation with AI assistance (DeepL)

Adriano J. Alfonso Rodríguez
Doctor of Law
Professor of Law-Criminology UNED-Lugo. Judge(s)
ajalfonsorodriguez@hotmail.com
ORCID: 0009-0005-2821-4603

Received 14/05/2025
Accepted 14/05/2025
Published 27/06/2025

Recommended citation: Alfonso, A. J. (2025). Cooperation between law enforcement agencies and criminal prosecution: Parallel Construction? *Revista Logos Guardia Civil*, 3(2), p.p. 13-34.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

ORCID: 0009-0005-2821-4603

LAW ENFORCEMENT COOPERATION AND CRIMINAL PROSECUTION: PARALLEL CONSTRUCTION?

Abstract: The existence of two types of security, national and public, has served to empower different bodies to prevent it. The secret services have acquired a prominent role in national security, while public security implies the presence of police bodies. In both cases, surveillance and protection work requires the authorised infringement of fundamental rights. However, the same standard does not exist when the secret services are involved, which is lowered because they are not investigating a criminal act and the problematic communication of the information obtained, when it appears, to the police forces. Is a strategy of concealing the source necessary? In short, is a parallel construction necessary?

Resumen: La existencia de dos tipos de seguridad, la nacional y la pública, ha servido para apoderar a organismos diferentes sobre su prevención. Los servicios secretos han adquirido un protagonismo destacado en lo que respecta a la nacional, mientras que la pública implica la presencia de órganos policiales. Para el trabajo de vigilancia y protección es necesario en ambos casos vulnerar, autorizadamente, los derechos fundamentales. Sin embargo, no existe el mismo estándar cuando participan los servicios secretos que se ve rebajado por no estar investigando un hecho delictivo y la problemática comunicación de la información obtenida, cuando aquel aparece, a las fuerzas policiales ¿Es necesaria una estrategia de ocultación de la fuente? ¿Es precisa, en definitiva, una construcción paralela?

Keywords: Public security, National security, Police, Intelligence service, Procedural safeguards.

Palabras clave: Seguridad pública, Seguridad nacional, Policía, Servicio de inteligencia, Garantías procesales.

ABBREVIATIONS

Art.: Article.

EC: Spanish Constitution.

PC: Penal Code.

CESID: Centro Superior de Información de la Defensa.

CIA: Central Intelligence Agency.

CITCO: Intelligence Centre for Terrorism and Organised Crime.

CNI: National Intelligence Centre.

DEA: Drug Enforcement Agency.

DIA: Defence Intelligence Agency.

MS: Explanatory Memorandum.

FBI: Federal Bureau of Investigation.

FJ: Legal Basis.

LOPJ: Organic Law of the Judiciary.

LOPSC: Organic Law for the Protection and Security of the Citizen.

LSN: National Security Law.

NSA: National Security Agency

SAN: Audiencia Nacional ruling.

SECED: Central Documentation Service.

SED: Secretary of State Director.

SIAM: Senior Staff Information Service.

STC: Ruling of the Constitutional Court.

STS: Supreme Court Judgment.

SC: Supreme Court

1. PREFACE.

Since the attacks on the Twin Towers in New York on 11 September 2001 - with their painful aftershocks on 11 March 2006 in Madrid - we have been facing a convulsive world, where democratic systems are faced with various open fronts, ranging from armed conflicts to transnational organised crime, against the backdrop of persistent terrorist risks, or espionage carried out by hostile countries. Also, less conventionally, we must be alert to cyber-attacks or disinformation campaigns, respond to irregular migration flows, climate catastrophes and global pandemics, or economic insecurity. These facts reflect a world far removed from perpetual peace and expressive of a "Risk Society" which implies confronting a situation of unrest, not provoked by threats but by the individuals who make them manifest (Beck, 2006, p. 107).

Facing the challenges that arise, all of which are very varied, with different roots and complex solutions, places us in the sphere of the so-called protection of "National Security", a concept that has been explained from different perspectives. However, in our country, the regulation of this concept is very recent, barely ten years old, and seeks to provide a regulatory framework for a space which, traditionally, has been in the shadows because it was considered that state action in certain areas should be kept strictly secret, in clear contrast to the idea of "Public Security", whose legislative presence is much earlier, obligatory in democracy, and based on the idea that governing implies a power of containment of police power (Zaffaroni, 2006, p. 165).

In any case, our constitutional text (hereinafter EC) has not addressed the idea of "National Security", nor does it contemplate a definition as such, although it does allude to the concept of "Public Security" in various precepts of our lex superior by establishing the guarantee of "citizen security" by the police forces (art. 104.1 EC) or exclusive state ownership of "public security" (art. 149.1.29 EC).1 CE) or the exclusive state ownership of "public security" (art. 149.1.29ª CE), without forgetting art. 126 CE where it speaks of a "Judicial Police" in a situation of dependence on Judges and Prosecutors in the investigation of crime and the discovery of the offender (*Cfr.* SSTC 175/1999, of 30 September, FJ 7º 86/2014, of 29 May, FJ 4º or 55/1990, of 28 March, FJ 5º). This situation, lacking recognition, has not prevented the idea of "National Security" from emerging as a singular tool for protection, as a policy of its own, although without a ministry to manage it (Herbon Costas, 2021, p. 164). However, this does not prevent us from observing that both "securities" operate in the same spheres, touch on similar aspects and set identical objectives, and although fundamental rights can be violated on both levels, they operate under different criteria, more flexible in their ethical dimension when it comes to matters of national security, and which leave in the air the existence of a bridge to be crossed in cases of collaboration between the different operational bodies responsible for overseeing their fulfilment.

From a regulatory perspective, Article 3 of Law 36/2015 of 28 September on National Security (hereinafter LSN) states that "For the purposes of this law, National Security shall be understood as the action of the State *aimed at protecting the freedom, rights and well-being of citizens, guaranteeing the defence of Spain and its constitutional principles and values*, as well as contributing together with our partners and allies to international security in the fulfilment of the commitments undertaken". In line with this definition, the idea of "Public Security" in the Explanatory Memorandum (EM) of Organic Law 4/2015, of 30 March, on the Protection of Public Security (LOPSC) states

that "The Law, in accordance with constitutional jurisprudence, is based on a material concept of public security understood as an activity *aimed at protecting people and property and maintaining the peace of mind of citizens*, which encompasses a plural and diversified set of actions, different in nature and content, aimed at the same purpose of protecting the legal good thus defined. Within this set of actions are the specific actions of the instrumental organisations destined for this purpose, especially those corresponding to the Security Forces and Corps, to which Article 104 of the Constitution *entrusts the protection of the free exercise of rights and freedoms and the guarantee of public safety...*".

It is easily perceptible, as has been highlighted, the common idea of protection of freedoms and rights that places both concepts in a clear thread of connection, which we can even observe in case law. In this sense, STC 184/2016, of 3 November, the first ruling that has addressed the concept of "National Security", states "*On the other hand, since the State competence is clear, both in matters of defence and public security, it would not make sense that, in an area such as national security, so closely linked to both, to the point of identifying its aims and objectives and the legal assets protected in the manner indicated, the State's competence would become purely residual. In short, national security is not a new competence, **but is integrated** into the state competences of defence and public security*" (FJ 3º). This judgement, which does no more than link the two concepts, does not prevent us from establishing clear differences.

Firstly, the defence of national security against threats, by obtaining information, is a matter for the secret services, specifically, and in our country, the National Intelligence Centre (CNI). In the case of public security, or citizen security, its protection is entrusted to the police services, be they central, regional or local government. Secondly, the secret services, in the surveillance of those activities that could affect national security (espionage, counter-espionage, anti-terrorist work, etc.), operate under a clear criterion of security.), operate under a clear criterion of extreme operational discretion, so that their work remains under the umbrella of classified information, which is not known to the public, and the results of their work are rarely brought before a court, situations that do not affect the work of the security forces, who carry out their activities under the supervision of judicial bodies, with results that are public and publicised, the ultimate aim being to lead, as a rule, to the determination, or not, of criminal liability to be judicially elucidated. Fourthly, the organised violation of fundamental rights requires, both in police work and in the work of the CNI, judicial authorisation, however, while the criminal procedural framework derived from the Criminal Procedure Act (LECRIM) acts as a flange for public security agencies, the secret services operate in a necessarily broader framework where the normative regulation is rather limited, through the only article contained in Law 2/2002, of 6 May, with judicial supervision limited to the authorisation of measures affecting the secrecy of communications and house searches that partially affect art. 18 EC, its purpose being the collection of information whose destination is not, in principle, a trial. However, several questions arise: What is our model of judicial supervision of intelligence activities like? Is it possible for secret services to share information with police agencies? Would it be possible to use it in the framework of criminal investigation and prosecution? Let us look at different aspects suitable for formalising the debate.

2. THE MODEL OF JUDICIAL AUTHORISATION FOR CNI ACTIVITIES.

Traditional intelligence gathering by espionage services has always been based on clandestine techniques and with a necessarily flexible ethical dimension in its development with a rather blurred framework of guarantees for those affected. The greater the threat, the more complex the methods of obtaining information, where evaluation and analysis become precision tools for determining the response, action or decision. In fact, the importance of the secret services in a democracy lies in helping the executive to follow specific lines in defence of national interests, becoming important actors in political decision-making (Pinto Cebrián, 2019, pp. 51 et seq.). They have nothing to do with the investigation of the criminal act, nor of the offender or their procedural prosecution (Sánchez Ferro, 2020, pp. 188-189), without forgetting that it is precisely national security that justifies their functions and enables the violation, albeit ordered, of fundamental rights (Aba Catoira, 2020, p. 228).

In our country, as I anticipated, the CNI, a body of the General State Administration with a unique nature (SAN 2632/2009, 27 May, Sala de lo Contencioso (Rapporteur: Mr Gil Ibáñez, FJ 1º), dependent on the Executive and which *"... is not, nor is* it assimilated to, a body identified with an independent administration, in the sense of that typology of public law entities endowed with the autonomy and functional independence that characterises it: it is an instrumental body of the Government..."*.is not, nor can it be assimilated to a body identified with an independent administration, in the sense that this type of public law entity is endowed with the autonomy and functional independence that characterises it: it is an instrumental body of the Government...*" (STS 1238/2021, of 18 October, Chamber III, (Rapporteur: Mr. Requero Ibáñez) FJ 7º) , which reflects, in its physiognomy, a long evolution in the history of our services. Thus, it became the successor to the High Defence Information Centre (CESID) which, in turn, was created by Royal Decree 1558/1977 of 4 July 1977, a body which brought together the previous information services, the Central Information Service of the Presidency of the Government (CESED) and the Information Service of the High General Staff (SIAM), It has always acted as an intelligence assessment body and, during the different governments, has depended on the Ministry of Defence, except for a period of dependence on the Ministry of the Presidency during the government of Mariano Rajoy Brey. Its initial integration with members of the Armed Forces has ended up evolving with the incorporation of civilian personnel, so that this body can no longer be seen as a mere compiler of military intelligence in the face of a potential military conflict. Its work goes beyond this, as threats are increasingly heterogeneous, with asymmetrical conflicts that develop on invisible battlefields and whose existence and intervention is essential to confront them.

According to article 9 of Law 11/2002 of 6 May 2002, the CNI is headed by a Secretary of State **(**SED**)**, who is the "National Intelligence and Counterintelligence Authority" with the title of "Director", appointed by Royal Decree at the proposal of the Ministry of Defence, and with a five-year mandate that can be successively extended or replaced at any time by the government. Its functions are of "promotion" and "coordination", which can be summarised as "direction" of the body's tasks, appointment of the different management positions, budgetary competence and cooperation "*with the information services of the State Security Forces and Corps*, and the bodies of the civil and military Administration, relevant to intelligence objectives...". He is assisted by a Secretary General, with the rank of Undersecretary, who, among other functions, in

addition to substituting him, is in charge of "Directing the functioning of the common services of the Centre through the corresponding instructions and service orders" (art. 10, Law 11/2002). These are, therefore, the main managers in charge of functions of responsibility in the CNI, with the possible and hypothetical existence of the Foreign Intelligence Division, Counterintelligence Division, Internal Intelligence Division, Economy and Technology Division together with the Sub-Directorate General for Administration and Services and the Sub-Directorate General for Personnel and a Legal Advisory Office, a Technical Office, a Head of Operational Support and a Security Service (arts. 1 and 2 RD 2632/1985). 1 and 2 RD 2632/1985, of 27 December 1985, although later, in RD 266/1996, of 16 February 1996, art. 2 established the existence of intelligence units and operational and technical support units together with a security unit in charge of protection tasks). In any case, it is possible that this internal organisation is very different today.

Among all the issues, there is one that underlies with importance in the face of a history that placed the work of our secret service in the shadows. This is the case of intelligence activities in which searches and wiretapping of targets were carried out, a scenario that was orphaned of any regulation and enormously problematic until Law 2/2002, of 6 May, which in a single precept, with an impact through its transitory law on the Organic Law of the Judiciary 6/1985, of 1 July, (LOPJ), in arts. 125, 127, 135, together with the new art. 125, 127, 135, together with the new art. 342 bis in the same text, decides that a Supreme Court Judge (Second Criminal or Third Administrative Chamber) will be responsible for authorising the CNI to carry out acts affecting the inviolability of the home (art. 18.2 CE) and the interception of communications (art. 18.3 CE). This is an unusual system (Lanz Muniain, 2023, p.27), unparalleled in our neighbouring countries, with the exception, with relative nuances, of the United States, as we shall see, the attribution of jurisdiction to a single judge, and for a temporary period of five years, is not exempt from criticism for departing from the constitutional sense of the ordinary judge predetermined by law (De la Oliva Santos, 2006, p. 154). It is clear that a court of espionage has not been properly created.

The justification for the amendment is provided by the MS of Law 2/2002 which states "For activities that may affect the *inviolability of the home and the secrecy of communications*, the Spanish Constitution requires in its Article 18 judicial authorisation, and Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms requires that this interference be provided for by law and constitute a measure which, in a democratic society, *is necessary for national security, public safety*, the economic well-being of the country, the maintenance of order and the *prevention of crime*, the protection of health or morals, or the *protection of the rights and freedoms of others*". As can be seen, it alludes to the two securities and the aspects that nourish them as an element justifying the violation of Art. 18 EC and against the backdrop of the protection of rights and freedoms, a core element of both.

The authorisation model is extremely peculiar, regulated in the sole article of Law 2/2002, of 6 May, and in synthesis is initiated by the SED, who submits to the SC Magistrate (Chamber II or III), elected by the General Council of the Judiciary (CGPJ) for a period of five years - coinciding with the mandate of the SED - a request for violation of fundamental rights, which must be duly motivated and necessarily contain the

following points: "*(a) Specification of the measures requested. b) The facts on which the request is based, the aims motivating the request and the reasons advising the adoption of the measures requested. c) Identification of the person or persons affected by the measures, if known, and designation of the place where the measures are to be taken. d) Duration of the measures requested, which may not exceed twenty-four hours in the case of the inviolability of the home and three months for the intervention or interception of postal, telegraphic, telephonic or any other type of communications, both periods extendable for successive equal periods in the event of necessity.* Once the petition filed by the SED has been received, the SC Judge has 72 hours (or 24 hours depending on the urgency of the measure) to safeguard its proceedings, which will be secret. The initial judicial decision, possibly an order, and the subsequent ones that extend it, cannot be appealed, nor can they be reviewed, and this is because the only actors in this procedure are the SC Magistrate and the SED, who, on the other hand, "shall order the immediate destruction of the material relating to all information that, obtained by means of the authorisation provided for in this article, is not related to the object or purpose of the authorisation".

It is clear that there are no principles that inspire the request, criteria for granting or refusing it, use or destination of the material obtained, judicial control of the execution of the measures or of the result obtained, with the exception of the extension, the situation of those affected by the immission measure or appeals against the decision issued. In this sense, the justification is, a priori, that the material obtained is neither likely to generate evidence nor will it be used in criminal proceedings (González Cussac, 2015, p.88). However, we cannot rule out, as a first element of nuance, the procedural transcendence of intelligence work, as the use, in the contentious jurisdiction, of CNI reports to deny the nationality of foreign applicants for reasons of "national security" stands out (SSTS 233/2022, 23 February, Chamber III, Speaker: Mr. Menéndez Pérez, FJ 4º; 395/2022, 29 March, of Chamber III, Rapporteur: Mr. Román García FJ 6º; 367/2021, of 17 March, of Chamber III, Rapporteur: Mr. Herrero Pina FJ 2º,; 4376/2015, of 26 October, of Chamber III, Rapporteur: Mr. Del Riego Valledor, FJ 4º; STS 2105/2014, of 26 May, of Chamber III, Rapporteur: Mr Del Riego Valledor, FJ 5º). However, I will return to its use in criminal proceedings later to clarify the issue. In any case, the aim has been to combine relatively antithetical aspects such as supervising something which, by its very nature, could not be supervised, by opening a judicial channel which, on the other hand, does not operationally constrain the agents by keeping them outside the requirements derived from the existence of open criminal proceedings (Alfonso Rodríguez, 2024, p. 132).

The starting point of the request revolves around art. 4 b) of Law 11/2002, of 6 May, which establishes, among others, as the main function of our espionage service that of "*Preventing, detecting and enabling the neutralisation of those activities of foreign services, groups or individuals that put at risk, threaten or threaten the constitutional order, the rights and freedoms of Spanish citizens, the sovereignty, integrity and security of the State, the stability of its institutions, national economic interests and the welfare of the population*". In this sense, this reflects the justifying element of the request for judicial authorisation in the single article, converting the authorising SC judge into the interpreter of non-legal concepts such as "sovereignty" or "integrity", "national economic interests" or the "well-being of the population", which are the ultimate aims of the development of espionage tasks and which, together with respect for rights, freedoms or institutional stability, imply making him the guardian of "national security" that empowers the service to be able to carry out its functions.

The question raised by the judicial empowerment of the CNI to intercept a telephone or enter a home is that it implies a kind of safeguard but distances itself from a function of guaranteeing fundamental rights (Pascual Sarria, 2007, p. 197) which, on the other hand, the Judiciary is attributed by virtue of art. 117.4 EC, and converts the procedure into *a sort of secret file for requesting measures limiting specific fundamental rights, in the framework of intelligence operations for the protection of national security, to a judge of the SC, subject to a temporary mandate and expressly appointed for this purpose* (Alfonso Rodríguez, 2023, p.89).

3. THE AMERICAN MODEL: THE FISA COURT AND A FALLING WALL.

It is not clear whether the United States has been the model for the configuration and physiognomy of our system of control of intelligence activities. However, it is clear that we cannot accept total inspiration, as the procedural system is distant between the two countries, with the adversarial system of North America in which the parties (accuser and accused) are the true "owners" of the American criminal process, and where the principle of the "Due Process of Law", the right to due process with all the guarantees, is shown to be the "motor" of the procedural organisation (Gómez Colomer, 2006, pp. 50-57), in contrast to a model of the Investigating Judge who is blessed by a Trial Judge who is the "owner" of the system (Gómez Colomer, 2006, pp. 50-57), in contrast to the model of the Investigating Judge who is the "owner" of the system. 50-57), in contrast to a model of the examining magistrate that is blessed by a LECRIM of 1882, which is impossible, under any circumstances, in the United States. However, it should be noted that the procedural model of the FISA Court does not respond to this adversarial system.

The US intelligence model is based on a plurality of agencies (CIA, NSA, DIA, FBI in its intelligence branch, Armed Forces and Government Departments with their own services) that are now coordinated by a National Intelligence Director, in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPA) as the Executive's commissioner for the adequate coordination of all organisations, coexisting with intense control by the legislature through parliamentary oversight committees. Given this circumstance, it is necessary to start from a phase of systematic abuses by the FBI or the CIA, highlighted by the Senate *Church* Committee (Arrieta, 2025, p. 122). 122), led to the enactment in 1978 of the *Foreign Intelligence Surveillance Act* (FISA), part of which was the creation of a Federal Court to control the electronic surveillance of foreign agents in the United States, now made up of eleven Federal Judges with public identities but whose work is carried out in secret, and who are appointed by the *Chief Justice of* the Federal Supreme Court of the United States. It is these judges who are in charge of verifying the requests of the Executive, who must prove as "probable cause" - a sensible suspicion that motivates the request - that the target of the listening or surveillance of the electronic devices is a foreign power or agent of a foreign power that is the target of the intelligence-gathering operation, therefore its use was not, a priori, intended to intercept the communications of US citizens. In the absence of a prima facie case of criminal wrongdoing to obtain the FISA Court's warrant, the standard for authorisation is less stringent than the usual standard required by law enforcement to violate fourth amendment rights - privacy (Ruger, 2007, p. 243).

The application is submitted before a judge of the FISA Court in which the government appears with its representation as the only intervening procedural party, where, in addition to proving probable cause, the identity of those involved and the

officials involved, the duration of the electronic surveillance measures, certificates from the intelligence authorities and details of previous applications, among other elements, must be indicated. The fact that it is the executive branch that acts as the sole participant distances the procedure from the adversarial system typical of the US system (Sobel, 2023, p. 15), estimating that one of the reasons, among others put forward at the time by *Attorney General* Griffin Bell during the drafting of the law, which could motivate the lack of other participants, is due to the reluctance of the government itself to declassify information for fear of leaks (Chin, 2021, p.665).

In view of the data provided, the FISA Judge will grant, or deny in detail, the *warrant* for electronic surveillance requested by the Government, identifying the subjects, means, type of information to be obtained and the duration of the warrant, and its denial can be reviewed before the *FISA Court Review*, composed of three judges of the same body, with the possibility of appealing to the *U.S. Supreme Court* if the review is unsuccessful.

However, while until 2001 the FISA mandate served the purpose of intelligence gathering, the 9/11 terrorist attacks in the United States, with the *Patriot Act* of 2001, under section 203, mutated the architecture of the law and thereby broke the *wall* between foreign intelligence gathering and criminal investigations (Donohue, 2021, p. 204), allowing the use of information-sharing by law enforcement agencies (FBI or DEA), obtained for the purpose of foreign intelligence gathering in light of FISA, and in criminal investigations, mixing the use of information-sharing by law enforcement agencies (FBI or DEA), obtained for the purpose of foreign intelligence gathering in light of FISA, and in criminal investigations. 204), allowing the use of information-sharing by law enforcement agencies (FBI or DEA), obtained for the purpose of foreign intelligence gathering under FISA, and in criminal investigations, thus mixing an identical method with different purposes, which prompts several reflections.

Firstly, by virtue of the standards of the request, in that the accreditation of probable cause is different, since in a criminal investigation it was necessary to prove, through that concept, the possible commission of a criminal act, which is not something that occurs in the request for a warrant under the FISA regulation. Secondly, with the common goal of preventing a terrorist attack, the cooperation and transmission of intelligence between spy agencies and law enforcement agencies, whose tasks are different, increased, and thus the boundaries between Intelligence Community and police agency blurred and blended (Stein, Mondale, Fisher, 2016, p. 2266). Third, the possibility of building a criminal case, with information obtained under FISA criteria, became a distinct possibility (think of a federal terrorism or narco-terrorism case in which law enforcement has received information from intelligence agencies as a result of the results obtained under a FISA warrant) so that a clear debate arose regarding the due process rights of those affected and their right to defence against the sharing of intelligence materials between agencies (Reid, 2015, p. 429).

4. PARALLEL CONSTRUCTION" AND INTER-AGENCY INTELLIGENCE COMMUNICATION.

As a result of what was previously observed with respect to the fall of the wall, it is evident that "National Security", a concept that is too ambiguous, was embedded in "Public Security", bearing in mind that the procedural requirements for the violation of

fundamental rights, particularly the privacy of communications, were lowered in the face of the claim of intelligence gathering, intelligence that later, as a result of a change in realities, which led to a mutation of principles, was used for different purposes in a way that bordered on procedural customs and fundamental rights in exercises of interchangeability, either for political decision-making or to form a basis for a criminal case. It is in this scenario that the concept of *"parallel construction"* makes sense, which began with the receipt of intelligence information with relaxed standards for obtaining it, the origin of which cannot be revealed and which, as I pointed out earlier, could well jeopardise procedural guarantees by providing an operational shortcut that could circumvent legal objections and which forces the invention of a parallel channel that diverts attention from the original source (e.g. an artificially created informant). e.g., an artificially created informant concealing intelligence information obtained from a different mandate such as a FISA Court warrant).

If we previously analysed the model for obtaining information by the CNI, the main body of our Intelligence Community, the situation faced by a police agency, be it a state agency such as the National Police, the Civil Guard or the Customs Surveillance Service, or the cases of Autonomous Police, expressive of an integral model (STC 184/2016, of 3 November, FJ 4º) such as Catalonia, Navarre and the Basque Country, each of which has information units and which make up a sort of "Police Intelligence Community" where the Intelligence Centre for Terrorism and Organised Crime (CITCO) intervenes as a body for analysis and coordination between bodies. However, it should be pointed out that, when it comes to gathering intelligence, police forces are subject to procedural constraints, in the context of satisfying public security, which are radically different from those of the intelligence services, and where the judicial authority acts as guarantor of fundamental rights. In this sense, the framework of action provided for in the LECRIM conditions the passage of investigators, subjecting their activity to a set of principles and requirements that establish a standard of procedural guarantees inherent to the rule of law.

A criminal investigation may affect various fundamental rights such as personal freedom (art. 17 EC), privacy (art. 18.1 EC), inviolability of the home (art. 18.2 EC), secrecy of communications (art. 18.3 EC) and also freedom of movement (art. 19 EC), with the judicial authority determining under the assumptions of the law the possible adoption of any measure that affects the above, therefore, although there must be a legal authorisation that allows its adoption, this, however, is not sufficient. It is necessary for the infringing measure to be sufficiently motivated in such a way that it expresses the factual and legal argumentation that determines its adoption in accordance with the principles of speciality, suitability, exceptionality, necessity and proportionality. In other words, a criminal offence must be under investigation (speciality) which in any case must be sufficiently serious to justify the adoption of such a measure, which serves the purpose of the investigation (suitability; SSTC 85/1994, 14th March, FJ 3°; 181/1995, 11th December, FJ 5°; 49/1996, 26th March, FJ 3°; 54/1996, 26th March, FJ 7° and 8°; 123/1997, 1st July, FJ 4°) as the results cannot be achieved by means of other measures that are less burdensome with respect to the fundamental rights of the person under investigation, being essential from the perspective of the specific case (exceptionality and necessity) and finally, only serious, socially transcendent facts with strong indications justify the sacrifice of key fundamental rights at the risk of seeing a situation of criminal impunity (proportionality, STC 49/1999, 5th April, FJ 7°).

It is clear that the request limiting fundamental rights that the police unit instigates

to investigate is subject to the aforementioned justifying requirements, in such a way that, faced with a criminal act that is being investigated in progress, there is a "wall" that needs to be overcome by judicial authorisation in order to be able to continue with the investigation. Under no circumstances can a police request be made for prospective purposes (STS 822/2022, 18 October, Chamber II (Rapporteur: Mr. Palomo del Arco) , FJ 1º.3. a)), i.e., without a prior crime that is indiciously justified, it is not even conceivable to carry out a request aimed at obtaining a judicial decision that violates a fundamental right. Therefore, it is clear that the police forces are there to investigate under precise parameters and clear limitations, and although the clandestinity of the investigation is precise, its final destination is to emerge in a public trial with full respect for the right of defence and with the clear objective of satisfying the demands of "public security" (STC 175/1999 of 30 September, FJ 7º or STC 86/2014, of 29 May FJ 4º), something that contrasts with the task of the secret services where, in the interests of protecting "national security", information is gathered from natural or legal persons, national or foreign, information which is classified and which is certainly not intended to be publicly aired before a prosecuting body to deduce criminal liability and without ideas such as "contradiction", "defence", "suspect" or "defendant" having any substance of their own, given that their work has nothing to do with criminal investigation.

However, despite the above, the fields of action of police forces and secret services are common. Organised crime, terrorism, illegal immigration...are a simultaneous threat to "public security" and "national security" in such a way that:

Organised crime is a security threat characterised by its essentially economic purpose, its undermining effect on political and social institutions, its transnational nature and its opacity. Criminal groups and criminal organisations disguise their illegal operations as legitimate business and increasingly rely on digital technologies, such as crypto-currencies and the dark web. In addition to its economic dimension, organised crime has a relevant destabilising potential. Its structures adapt to the geostrategic environment and have an impact on governance, social peace and the normal functioning of institutions. In terms of serious crime, activities such as the exploitation of children or trafficking for sexual exploitation target vulnerable groups and seriously violate human rights. Smuggling, cybercrime, trafficking in drugs, arms and wildlife, and corruption are tangible threats to national security. The convergence between terrorist groups and organised crime networks is increasing. The increasingly decentralised organisational patterns of these criminal actors favour their cooperation and facilitate terrorist financing (National Security Strategy (2021), pp. 64-65).

It goes without saying that, in view of the above, it is necessary for our secret service and the police forces to collaborate in an activity that could materially coincide in terms of facts and subjects, hence its clearly concentric nature when it comes to, among other issues, terrorism, organised crime or both. At this point, a clear doubt arises: what happens when the CNI, as a result of its eavesdropping, becomes aware of a criminal act that could be investigated due to its imminence?

It is clear that there is no legally regulated system of communicating vessels to formalise the transmission of information when the CNI becomes aware of the commission of criminal acts (Sánchez Barrilao, 2011, p. 61), as there are hardly any references in Law 11/2002, of 6 May, regarding cooperation with the Security Forces, except for specific aspects such as art. 9.2 d), which attributes to the SED the maintenance

and development of "collaboration with the information services of the State Security Forces and Corps, and the bodies of the civil and military administration, relevant to intelligence objectives". It is here where what we previously pointed out as *"parallel construction"* comes into play as an expression of the configuration of a criminal case by a police force concealing the origin of the source that drives it (Reid, 2015, p. 427) and which could necessarily be connected to information obtained by an intelligence agency, having to construct parallel circumstantial evidence elements intended to be the cloak that hides the genesis of the original information, which forces us to see how we should treat intelligence material as the initiator or driver of a criminal police investigation.

In principle, it is necessary to start from what is stated in STS 746/2022, of 21 July, Chamber II, (Rapporteur: Ms. Polo García) which points out:

"As we have said in the judgment cited by the Chamber - 312/2021, of 13 April - there is no right for the accused to disclose the content and scope of international police collaborations. *The investigated persons subject to criminal proceedings do not have a right to disclose the points of police postings, or the identity of the informants, or the information gathered through criminalistic techniques that would lose their effectiveness if they were massively disclosed. There is no right to know the specific tools and materials that were available to the police for the investigation and which could be rendered ineffective for future interventions.* Nor is there a right to know about the investigations into other crimes that could be attributed to the same suspects but which are still in the process of police confirmation, even less so if we consider that, where appropriate, they should be the subject of a separate criminal prosecution procedure (art. 17.1 LECRIM). It is also unacceptable that investigations which do not even affect those being prosecuted and which could ruin other police actions of obligatory prosecution of criminality should be known". (FJ 3.3).

The origin of the previous ruling was due to the refusal of the judicial body in charge of the prosecution to accept the testimony of American DEA agents who provided information to the National Police who carried out a drug investigation that culminated in a conviction. It should be noted that the previous ruling was not new; our High Court had already made it clear quite previously that "...when foreign intelligence services provide data to the Spanish security forces and bodies, *the requirement that the source of knowledge also needs its own sources of knowledge does not form part of the content of the right to a trial with all the guarantees...*" (STS 445/2014, of 29 May, Chamber II, Rapporteur: Ms. Ferrer García FJ 2º ; STS 884/2012, of 12 November, of Chamber II, Speaker: Mr Marchena Gómez FJ 8). Therefore, we obtain a first partial solution: foreign intelligence services can provide our police forces with their sources without any problem in order to start investigating. Their origin, in short, is not relevant and therefore the DEA (or the FBI, or any other foreign police force) could receive information from its own intelligence agency (CIA, NSA... or its intelligence service) and transmit it to police agencies to initiate a criminal case in our country, without entering into the debate on the relaxation of the legal standards for obtaining it, since there is no right to debate the sources of the information, given that it is not required to know them in order to set up due process.

The question of the transmission to the security forces by the CNI of information it

has been able to obtain as a result of its wiretapping or house searches requires further clarification and is in fact a matter addressed in case law denying that its functions have anything to do with criminal investigation (SSTS 1140/2010, of 29 December, of Chamber II (Rapporteur: Mr Berdugo Gómez de la Torre); 1094/2010, of 10 December, of Chamber II (Rapporteur: Mr Marchena Gómez)). And on this point, once again, the different procedural methodology required for a telephone interception, for example, depending on whether it is requested by the CNI or by a police agency, is that they only have in common the need for judicial authorisation, nothing more.

There is no shortage of arguments in favour of the fact that information obtained by the CNI in violation of a fundamental right, and under its own procedural - not procedural - conditions, with judicial authorisation, can serve as a source for initiating a criminal case with the possible communication to the police forces.

Firstly, there is *a principle of unity of action between police and intelligence agencies*, which is imposed by the National Security Strategies that are dictated as a framework for action (art. 4.3 LSN). Thus:

In traditional areas of security, adapting to the changing nature of threats - armed conflict, terrorism, organised crime, proliferation, irregular migration flows, intelligence activities - is a constant feature of the *actions of the various actors of national security.* As these phenomena become increasingly transnational, *the need for concerted action* at all levels *intensifies*. The close links that often exist between several of these threats make it necessary to address them from broad strategic and operational frameworks, under *the premise of the principle of unity of action.* This Report shows that this approach is already fully valid in Spain's response to classic security challenges (Estrategia de Seguridad Nacional, 2013, p. 145).

It is difficult, at the risk of endangering the community, to admit work configured in watertight compartments, and thus the LSN imposes this "unity of action" (art. 4.2), recalling in art. 9.2 that "The *State Intelligence and Information Services*, in accordance with the scope of their competences, will permanently support the National Security System, providing elements of judgement, information, analysis, studies and proposals necessary to prevent and detect risks and threats *and contribute to their neutralisation*". Therefore, the requirement of a convergent sense necessarily takes the form of cooperation between agencies ("Services") in order to meet the requirements aimed at averting risks ("contributing to their neutralisation"). In short, the communication of information is a key element in helping to neutralise the risks that arise.

Secondly, a justification for the communication could be given by *the obligation to report the criminal acts or their imminent commission* by anyone who witnesses them in accordance with art. 262 LECRIM (De la Oliva Santos 2006, p. 164), starting with the SC Magistrate who authorised the interception of communications or the entry into the CNI's home (López Alafranca, 2014, p. 135). 164) starting with the SC Magistrate who authorised the interception of communications or the entry into the CNI's home (López Alafranca, 2014, p. 135) and also by virtue of the requirement of criminal liability (407 and 408 CP) when we are talking about police officers who may provide services to the CNI. The judge's knowledge of the development of the authorised measure must necessarily derive from the need to extend the measures limiting fundamental rights that the CNI may be interested in, as there is no possibility of the authorising body not

knowing the facts, unless a "blind" authorisation is admitted as a "blank cheque" and without successive control, which is not possible as the law provides for such an extension "in case of necessity" (art. 2 d) Law 2/2002), a necessity that would have to be justified, with the facts resulting from the initially agreed measure, in order to continue with the restrictive measures.

The thesis cannot be accepted, without prejudice to its validity, that the lack of consideration of CNI agents as authorities (art. 5.4 Law 11/2002) prevents the obligation to report crimes (Lanz Muniain, 2023, p. 34), however, the obligation imposed by art. 262 LECRIM on those who "by reason of their positions, professions or trades" have knowledge of the criminal act determines that it makes no difference whether or not they are an authority or its agent, as they know of the act through their profession and must report it. However, this communication has been endorsed by the SC itself when it states that "Therefore, the legal function of this Service is not the investigation of specific crimes, without prejudice to the fact that if in the course of their work *they discover* or have indications of criminal actions *they inform the competent police and judicial bodies*, but - it is insisted - their activity is not directly aimed at the discovery of crimes, nor is it conditioned by the prior commission of any" (STS 1140/2010, of 29 December, of Chamber II (Rapporteur: Mr. Berdugo Gómez Gómez). Berdugo Gómez de la Torre) FJ 9º) .

Thirdly, *a hypothetical secret classification cannot cover the impunity of criminal acts* (López Alafranca, 2014, p. 136), which, on the other hand, must necessarily be prevented. Likewise, even in the case of classified information ("internal organisation and structure, means and procedures, personnel, facilities, databases and data centres, sources of information and information or data that may lead to knowledge of the aforementioned matters..." ex art. 5.1 Law 11/2002), nothing hinders a procedure of declassification of information at a procedural level, but this is an issue unrelated to the communication itself which, precisely, has as a limit that information transmitted in which material that must be declassified is not disclosed (Pascual Sarria, 2007 p. 214).

Fourthly, it is precisely the collection of information by the CNI if it implies a violation of the privacy of communications or an entry into the home *that is backed by a judicial decision necessarily motivated by its harmful effect* (SSTC 126/1995, 25 July, FJ 2; 139/1999, 22 July, FJ 2; in the same sense, SSTC 290/1994, 27 October, FJ 31; 50/1995, 23 February, FJ 5; 41/1998, 23 February, FJ 34; 171/1999, 23 September, FJ 10; 8/2000, 8 January, FJ 4); 41/1998, of 24 February, FJ 34; 171/1999, of 27 September, FJ 10; 8/2000, of 17 January, FJ 4), therefore such measures have not been agreed outside a procedural scheme or on a whim in accordance with their operational needs, so that there is no illegality in their obtaining and therefore, neither in their communication for the initiation of a criminal investigation, an investigation that is not contaminated.

In this respect, the evidentiary aspect must be distinguished from the actual issue of communication for the initiation of criminal proceedings. They are different issues. The material obtained by the CNI is not intended to be evidence in criminal proceedings, and this is because it is the police investigation itself which is intended to fulfil this function, recalling that "unlawful evidence" (art. 11 LOPJ) only exists "when the means used to obtain it are constitutionally illegitimate" (STC 49/1999, 5 April, FJ 12). In this sense, STS 1094/2010, of 10 December, in its FJ 2 A reminds us that ".... But what is beyond doubt *is that the existence of a subsequent criminal proceeding in which the notitia*

criminis is not alien to the security file processed by the CNI does not imply the transmutation of the functionality of that file, which would cease to be what it is, distancing itself from its regulatory principles, to become a procedural act sine qua non of the real process and, therefore, subject to the general rules governing the principle of publicity".

And it is precisely the authorising judicial decision that prevents us from speaking of a sort of illegal "ledge" along which our intelligence service would riskily travel. However, although we have said that intelligence material is not destined for criminal proceedings as an element of evidence, it should not be forgotten that "And with regard to the incorporation into proceedings of evidence obtained by the intelligence services and which refers to declassified material, it can be assessed from two different perspectives. Either it acts in criminal proceedings as documentary evidence, when it is evidence of these characteristics, or it serves to conduct the criminal investigation through the witness statement of the perpetrators" (STS 1140/2010, of 29 December, Chamber II (Rapporteur: Mr. Berdugo Gómez de la Torre) FJ 9º).

However, there is no lack of objections to the system, starting with the complexities that the presence of secret services in criminal proceedings could entail (Hassemer, 2000, p. 114), so that there could be a confusion, almost a mixture, that would make police and intelligence gathering functions indistinguishable (Orgis, 2011, p. 162). It would not be good for the police forces, it would not be good for the secret services, and this by virtue of the different parameters of action. On the other hand, obtaining a wiretap or house entry by our secret services is subject to a different standard where one has to justify one's own extremes of danger to national security that may have nothing to do with the commission of a criminal act. In short, it is one thing if in the course of an intelligence operation a serious criminal act is discovered, or one whose commission is imminent, something that must necessarily be communicated or reported to the police forces, and quite another if the procedure of requesting and obtaining a wiretap or house entry by the secret services serves, as a procedural shortcut, to search for the crime itself, which would lead to the irrelevance of the system of constitutional procedural guarantees with regard to the limitation and violation of fundamental rights.

Finally, we noted earlier that not all information can be known, which could lead, in the context of criminal proceedings, to the right of defence being put to the test (art. 24.2 EC), as access to the file in the case of the CNI is subject to restrictions and a situation of classification that contrasts with the availability to the parties involved of all the elements of the criminal investigation. In other words, the presence of the secret services and the information obtained by them in the framework of criminal proceedings cannot emerge as naturally as in a police investigation. In short, not everyone can have access to all the information, with the result that there are elements that are not subject to a hypothetical defence strategy, either of a defendant or of third parties outside the proceedings whose communications or addresses could be affected, that will remain hidden, which may serve to question the purity of the proceedings and of the decision on criminal liability.

5. CONCLUSIONS.

There is a concentric relationship between national security and public security insofar as both work on the assumption of the existence of threats to the rule of law. However, the actors empowered to protect them are different, with the secret services having jurisdiction over the former and the police over the latter. In this sense, tools have been put in place to avert the aforementioned risks through the attribution of measures limiting fundamental rights. In the case of public security agencies (state, regional or local police), their powers are framed within the scope of criminal procedure with very rigorous guidelines for the violation of rights through the need for judicial authorisation to authorise invasive but orderly activities by the security forces within the framework of the LECRIM. The intelligence service (CNI) has only relatively recently been empowered to intercept communications and enter homes by means of a law of judicial control in 2002, but we cannot affirm that its requirements coincide with those of the LECRIM when it comes to granting them, so that we find ourselves with a system of double standards depending on the subject acting.

The concept of *parallel construction* results from a way of acting with respect to police forces who receive intelligence information which, on the one hand, allows them to build criminal cases but, on the other, bearing in mind that there is a lower standard for obtaining intelligence information, they are obliged to conceal its origin, seeking alternative procedures to prevent the original source from surfacing and allowing the investigated person to question its acquisition by violating due process. This issue has come to the fore primarily in North America as a result of the breakdown of the "wall" between police and intelligence activities with the attacks of 11 September 2001, which has led to doubts about the use of information obtained from the Foreign Intelligence Surveillance Court (FISA Court) whose surveillance warrants to an intelligence agency provide information that can then be used by police forces who have been able to avoid having to justify probable cause before a judicial body in order to carry out their investigations. That is to say, it seems to be a sort of operational shortcut that generates doubts, doubts that also affect us about the possible use of information resulting from an authorisation from the SC Judge to the CNI outside a wiretap, outside an entry into a home. In this sense, there are a series of requirements that would motivate the communication of a criminal act resulting from the practice of a procedure restricting fundamental rights by our secret service to police agencies, which could well be the general obligation to report under art. 262 LECRIM. But an elementary unity of action in the prevention of threats that jointly affect public and national security requires cooperation between services and the sharing of information. Think of the imminence of a terrorist attack that comes to light by chance through a secret service wiretap. No one doubts the need for communication and alert, regardless of the possible secret classification of the information, a classification that cannot cover silence in the face of a criminal act or allow it to go unpunished. There is also a declassification process for this purpose.

Our SC has said that when a foreign intelligence service sends a confidence that serves to open a criminal case, there is no right to know the source of the source, therefore, it is not necessary, nor appropriate, to conceal the origin or source of knowledge by the police agency. In the case of communication by the CNI to a public security force, our High Court also endorses, albeit in isolation, the communication of a criminal act without going into the question of whether or not the information is classified as secret, which

means that neither concealment nor the development of alternative strategies, which could compromise the criminal proceedings, seems to make sense. Therefore, there is no room for *parallel construction*, without prejudice to the fact that the presence of secret services in criminal proceedings raises questions which, if they are to be resolved, will require a reform of the system designed by Law 2/2002 of 6 May.

6. BIBLIOGRAPHICAL REFERENCES.

Aba Catoira, A. (2020). Accountability and intelligence services. In J. J. Fernández Rodríguez (Ed.), *Seguridad y libertad en el sistema democrático* (pp. 209-237). Tirant lo Blanch.

Alfonso Rodríguez, A. J. (2023). Democratic governance and accountability: Judicial control of intelligence activities (SDG 16.6). *Revista de Derecho UNED*, (31).

Alfonso Rodríguez, A. J. (2024). Interception of telephone communications, security(s) and procedural guarantees. *Revista Ciencia Policial*, (182).

Arrieta, G. (2025). Balancing the scales: Amici curiae as special masters in the shadow of FISA. *California Western Law Review, 61*(1), Article 6. https://scholarlycommons.law.cwsl.edu/cwlr/vol61/iss1/6

Beck, U. (2006). *La sociedad del riesgo: Hacia una nueva modernidad*. Paidós Ibérica.

Chin, S. (2021). Introducing independence to the Foreign Intelligence Surveillance Court. *The Yale Law Journal, 131*(2). http://www.yalelawjournal.org/author/simon-chin

De la Oliva Santos, A. (2006). *Writings on law, justice and freedom*. Editorial UNAM, Instituto de Investigaciones Jurídicas.

Donohue, L. K. (2021). The evolution and jurisprudence of the Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review. *Harvard National Security Journal, 12*.

Gómez Colomer, J. L. (2006). Adversarial system, accusatory process and accusatory principle: A reflection on the criminal prosecution model applied in the United States of America. *Revista Poder Judicial*, (Special XIX).

Hassemer, W. (2000), Criminal proceedings without data protection? In C. M. Romeo Casabona (Ed.), *La insostenible situación del derecho penal (*pp. 103-128). Comares.

Herbón Costas, J. J. (2021). La gestión de las crisis en el marco de la Ley de Seguridad Nacional: La pandemia por covid-19 y la necesidad de una urgente reforma. *Revista Española de Derecho Constitucional, 121*. https://doi.org/10.18042/cepc/redc.121.05

Lanz Muniain, V. (2023). El CNI un servicio de inteligencia y seguridad: Panorama normativo. *Revista Española de Derecho Militar, (*119).

López Alafranca, M. (2014). But who will watch the watchmen? *Revista Cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales,* (92).

Orgis, M. (2011). Intelligence-led and intelligence-guided operations: The best option for combating pre-eminent threats. In J. Fernández Rodríguez, D. Sanso-Rubert

Pascual, J. Pulido Grajera, and R. Monsalve (Eds.), *Intelligence issues in contemporary society (*pp. 143-166). Ministry of Defence.

Pascual Sarria, F. (2007). El control judicial a la interceptación de las comunicaciones: Especial referencia al control judicial previo a las intervenciones del Centro Nacional de Inteligencia. *Revista Española de Derecho Militar, (*89).

Pinto Cebrián, F. (2019). *Manual of intelligence and counterintelligence (terrorism and counterterrorism)*. Amabar.

Reid, L. (2015). NSA and DEA intelligence sharing: Why it is legal and why Reuters and the Good Wife got it wrong. *SMU Law Review, 68*(2), Article 5.

Ruger, T. W. (2007). Chief Justice Rehnquist's appointments to the FISA Court: An empirical perspective. *Northwestern University Law Review, 101*(1).

Sánchez Barrilao, J. F. (2011). Prevention and intelligence: National Intelligence Centre and the intelligence community in the face of terrorism, organised crime and illegal immigration. *Revista Ejército,* (846).

Sánchez Ferro, S. (2020). Mission impossible? An attempt at a legal understanding of the world of espionage in Spain. In J. J. Fernández Rodríguez (Ed.), *Seguridad y libertad en el sistema democrático* (pp. 159-207). Tirant lo Blanch.

Sobel, A. X. (2023). Procedural protections in a secret court: FISA amici and expanding appellate review of FISA decisions. *University of Pennsylvania Law Review, 172.* [Note: Corrected "Pennsylvania" to "Pennsylvania". Missing page numbers or article number].

Stein, R., Mondale, W., & Fisher, C. (2016). No longer a neutral magistrate: The Foreign Intelligence Surveillance Court in the wake of the war on terror. *Minnesota Law Review, 100.* https://scholarship.law.umn.edu/faculty_articles/564

Zaffaroni, E. R. (2006). *El enemigo en el Derecho Penal*. Dykinson.

ORCID: 0009-0005-2821-4603

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

II.- RESEARCH WORK

Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Research Article

SPAIN IN THE FACE OF DISINFORMATION: HYBRID CHALLENGES AND CONVENTIONAL RESPONSES

English translation with AI assistance (DeepL)

Juan Francisco Adame Hernández
Casa Árabe's Director of Strategy, Communication and Promotion
Master's Degree in International Security Senior Management
Master's Degree in Advanced Studies in Political Communication

Received 08/04/2025
Accepted 03/06/2025
Published 27/06/2025

Recommended citation: Adame, J. F. (2025). Spain in the face of disinformation: hybrid challenges and conventional responses. *Revista Logos Guardia Civil*, 3(2), pp. 37-70.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

SPAIN IN THE FACE OF DISINFORMATION: HYBRID CHALLENGES AND CONVENTIONAL RESPONSES

Abstract: In the current geopolitical environment, characterised by the proliferation of information technologies and global interconnectedness, **disinformation has established itself as a multidimensional threat** that compromises national security structures and the social cohesion of states. This article analyses **Spain's institutional and strategic response to disinformation**, framing it within the broader context of hybrid strategies and **foreign information interference and manipulation (FIMI)**.

The study addresses key concepts such as *disinformation*, *post-truth* and *grey zone*, linking them to the **doctrinal evolution of hybrid strategies within the European Union**. Particular attention is paid to the **cognitive domain** and the mechanisms of narrative construction and interpretative frameworks used to shape and distort public perception. The final section offers a **critical evaluation of the main measures adopted by Spain to counter disinformation**, assessing their coherence, implementation and effectiveness in an ever-changing threat landscape.

Resumen: En el actual entorno geopolítico, caracterizado por la proliferación de tecnologías de la información y la interconexión global, **la desinformación se ha consolidado como una amenaza multidimensional** que compromete las estructuras de seguridad nacional y la cohesión social de los Estados. Este artículo analiza **la respuesta institucional y estratégica de España frente a la desinformación**, enmarcándola dentro del contexto más amplio de las estrategias híbridas y de la **interferencia y manipulación informativa extranjera (FIMI)**.

El estudio aborda conceptos clave como *desinformación*, *posverdad* y *zona gris*, vinculándolos con la **evolución doctrinal de las estrategias híbridas en el seno de la Unión Europea**. Se presta especial atención al **dominio cognitivo** y a los mecanismos de construcción de narrativas y marcos interpretativos empleados para moldear y distorsionar la percepción pública. La última sección ofrece una **evaluación crítica de las principales medidas adoptadas por España para contrarrestar la desinformación**, valorando su coherencia, aplicación y eficacia en un panorama de amenazas en constante transformación.

Keywords: Disinformation, *Fake news*, Hybrid strategies, Cognitive domain, Narratives.

Palabras clave: Desinformación, *Fake news*, Estrategias híbridas, Dominio cognitivo, Narrativas.

ABBREVIATIONS

CIS: Centro de Investigaciones Sociológicas

CNI: National Intelligence Centre

DESI: Digital Economy and Society Index

DHS: Department of Homeland Security

EEAS/SEAE: European External Action Service

ELISA: Simplified Open Source Study

for **ENISA**: European Union for Cyber Security

ESN: National Security Strategy

EU/EU: European Union

FIMI: Foreign Information Manipulation and Interference

IFJ: International Federation of Journalists

INCIBE: Instituto Nacional de Ciberseguridad is cybersecurity.

MAEUEC: Ministry of Foreign Affairs, European Union and Cooperation

MPJRC: Ministry of the Presidency, Justice and Courts Relations

WHO: World Health Organisation

NATO/NATO: North Atlantic Treaty Organisation/North Atlantic Treaty Organisation

1. INTRODUCTION

In today's digital age, marked by the rapid dissemination of information through social media and communication technologies, disinformation has become a major strategic threat. This phenomenon, which includes *fake news* and post-truth, has acquired unprecedented relevance in the geopolitical sphere, affecting both the stability of political systems and public perception and national security. Spain has not been immune to these challenges, facing disinformation campaigns that, in many cases, have been used as tools within broader hybrid strategies.

Disinformation is often interpreted as a phenomenon in itself or addressed in an isolated or decontextualised manner (Lazer et al., 2018). The strategies in which disinformation is embedded are relativised, abstracted or ignored (MAEUEC, 2021). Obviating the necessary multidisciplinary approach (Wardle and Derakhshan, 2017) or the need to identify the strategic objectives that these actions or disinformation campaigns pursue (Terán, 2019). Even when there is a reference to hybrid strategies and/or the grey zone, it is usually not addressed in depth, being relegated to mere mention (DSN, 2021). Disinformation, far from being an isolated phenomenon, is part of a broader strategic framework, including hybrid strategies and the so-called 'grey zone' (NATO, 2024) and especially *Foreign Information Manipulation and Interference* (FIMI).

2. DISINFORMATION, POST-TRUTH AND FAKE NEWS

Disinformation is not a recent phenomenon (Allcott and Gentzkow, 2017; Tandoc, Lim & Ling, 2018). Since societies began to organise themselves into hierarchical structures, humans have deliberately fabricated and disseminated incorrect and misleading stories (Burkhardt, 2017). From political smear tactics in Ancient Rome to propaganda strategies during the First and Second World Wars (Posetti and Matthews, 2018), disinformation has been used to manipulate and convince others. Disinformation has reached unprecedented levels, altering not only public perception, but also directly influencing political and social processes globally. However, as Julie Posetti and Alice Matthews review in their compilation "*A Short Guide to History of Fake News and Disinformation*" (2018), the fabrication and manipulation of information is not a new phenomenon.

In recent years, the media, political campaigns or sporting (or non-sporting) debates on social networks have been filled with new concepts such as *fake* news (Tandoc, Lim & Ling, 2018), post-truth (McIntyre, 2018) or *disinformation/misinformation* (European Commission, 2022). It has gained public relevance due to a series of international events, such as what happened with the World Cup in Qatar (Newtral, 2022), the Cambridge Analytica scandal (Chan, 2020) or what happened in the US presidential elections (BBC World, 2018); which has reignited the debate on its implications for democratic systems, public perception and the geopolitical interests of certain countries. It is a recurrent debate, where the role of social networks, traditional media, verifiers or cybersecurity are often highlighted. This polysemic, confusing and often ambiguous reality brings together different concepts that attempt to name, explain or allude to different realities.

2.1. CONCEPTS AND DEFINITIONS

Disinformation, *fake news* or post-truth are terms, words and concepts that have become very popular, becoming part of colloquial speech and often used as synonyms in an

attempt to reflect a reality that is usually different and complex. However, although these terms are often used interchangeably, each has specific nuances and characteristics that distinguish them, which is crucial for a deeper understanding of the phenomenon (DSN, 2022).

Table 1

Concept	Definition	Relationship with the truth
Fake News	Made-up news with no basis in fact	Completely false
Post-truth	When emotions matter more than facts	The emotional takes precedence over the real
Disinformation	False or manipulated information deliberately disseminated for strategic purposes	It mixes truths and falsehoods to generate a concrete effect.

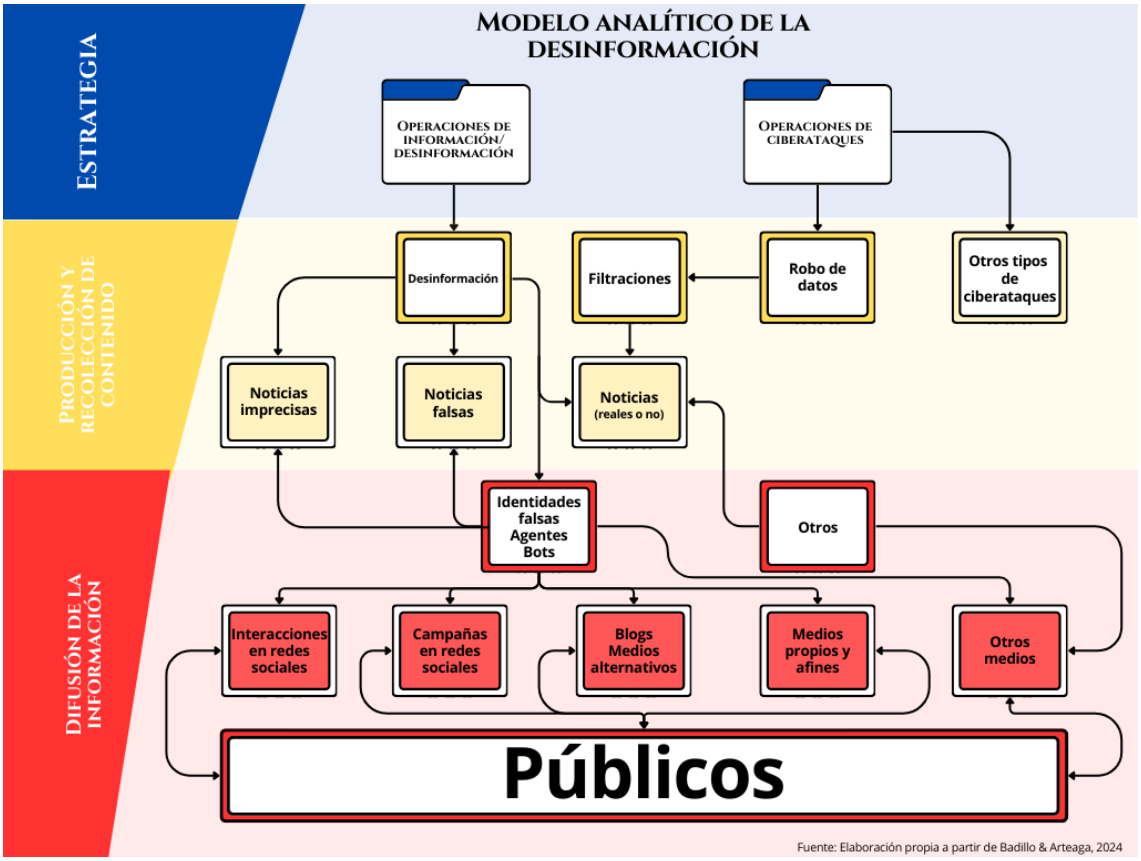
Source: Own elaboration

Let's start by unravelling this complex mishmash of topics by the simplest aspect, *fake news*. We understand *fake news* as false and fabricated news[1] (Gelfert, 2018). These news stories are not only fabricated without any basis in reality, but are often designed to appear plausible and manipulate the audience, exploiting emotions and biases to maximise their impact (DSN, 2022)[2] . They are supposedly news stories created out of fantasy (since they have no relation to reality). Based on Table 1, it is perhaps easier to define them by opposition: they are neither real but decontextualised news, nor exaggerated news (again, real) nor inaccurate news (with real elements) (DSN, 2023a). It is crucial to differentiate *fake news* from other types of misinformation, such as decontextualised or exaggerated news, as the latter, although potentially misleading, are based on real facts, which distinguishes them from completely fabricated news (DSN, 2022). Particularly useful is the analytical model of misinformation proposed by Badillo and Arteaga (2024) shown in Figure 1.

[1] However, it is not a pacified term (Carson, 2018), and although an evolution towards conceptual differentiation can be seen, there are authors (Flores, 2022) and especially in the journalistic world (IFJ, 2018), where "arguments" such as the mere fact that something is false invalidates it to be news (Mayoral, Parratt & Morata, 2019).

[2] The use of artificial intelligence has amplified this capability, enabling the creation of *deepfakes* and other types of manipulated content that can be massively distributed with great speed and reach (DSN, 2023a).

Figure 1



Post-truth[3] is a multifaceted phenomenon (Caridad-Sebastián et al, 2018), where verisimilitude (Rodrigo Alsina, 2005) is more relevant (Rodrigo Alsina, 2005), that is credible, regardless of true or real facts (Dahlgren, 2018). In post-truth, emotions and personal beliefs prevail over objective facts, which has profound implications for democracy and social cohesion, as it allows emotive and often misleading narratives to prevail in public discourse (DSN, 2022; DSN, 2024). This phenomenon not only alters individual perception, but also facilitates the creation of 'echo chambers'[4] in which people are repeatedly exposed to the same ideas, reinforcing their beliefs and isolating them from other perspectives (DSN, 2023a).

There are also multiple definitions of disinformation, which have mutated over time and depending on the sector or field where they are used or outlined (Arteaga, 2020). This term encompasses not only the intentional dissemination of false information, but also the subtle manipulation of facts to distort reality and confuse the public (DSN, 2022). The DSN, in line with EU postulates, defines it as "*Disinformation is verifiably false or*

[3] There is no single position, but unlike the previous (and nuanced) concept, there is a majority consensus on the central element of "wanting to believe" over facts or reality (Olmo, 2019). The phenomenon, "It's a lie, but it might be true" https://twitter.com/hematocritico/status/1241797239779069952?lang=es

[4] An *echo chamber* is a phenomenon in which information, opinions and beliefs are reinforced and amplified within a closed group or community, limiting exposure to different perspectives (Jamieson and Cappella, 2008). For more information on echo chambers see: *The echo chamber is overstated* (Dubois and Blank, 2018). https://www.tandfonline.com/doi/full/10.1080/1369118X.2018.1428656#abstract

misleading information that is created, presented and disseminated for profit or to deliberately mislead the public, and is likely to cause public harm" (DSN, 2022, p.253).

Although adequate, this definition restricts or minimises some of the elements that do feature in the National Security Strategy[5] , such as the reference to the cognitive domain (DSN, 2021) or the emphasis on the intentionality and objectives of those who carry out disinformation campaigns (thus providing it with a context). The cognitive impact of disinformation is crucial, as it is not only about spreading false information, but also about altering public perception and judgement, eroding trust in institutions and fostering social polarisation (DSN, 2022; DSN, 2023a). This opinion coincides with other authors such as Artega and Olmo, who point out that "disinformation makes it possible to fragment, isolate and manipulate infected public opinions, discredit and question objective facts and accredit virtual emotions and induced perceptions as real" (Artega, 2020) and "when the falsehood becomes more subtle, more complex, has been created with tactical intentionality, responds to a strategy and pursues objectives, that is when we can speak of disinformation" (Olmo, 2019).

3. HYBRID STRATEGIES AND GREY ZONE

Hybrid strategies are defined as an approach to conflict that combines conventional and unconventional elements, using a variety of tools - military, economic, diplomatic, cyber and information - to achieve strategic objectives (Colom, 2018). These tools include not only the direct manipulation of information, but also the creation of narratives that alter public perception over the long term, a central feature of both influence operations and disinformation (Torres Soriano, 2022). The use of these strategies is justified by their ability to exploit vulnerabilities through an approach that integrates the military with other domains, such as the cognitive and informational, creating a synergy that multiplies their effectiveness in low-intensity contexts (Walker, 1998).

The grey zone, meanwhile, is characterised by the application of tactics designed to remain below the threshold that would trigger open warfare. This concept is fundamental to understanding how state and non-state actors challenge the international order without crossing the red lines that would lead to armed conflict (Martín Renedo, 2022). In practice, grey zone operations range from economic coercion and the use of disinformation to the employment of special forces in covert missions, which are designed to be difficult to attribute directly to a state (McCuen 2008). The overlap between the physical, virtual and cognitive planes in the grey zone allows these strategies to be executed more effectively, as the perception of conflict is manipulated to disorientate target populations and weaken their ability to respond (Lupiáñez Lupiáñez, 2023).

Hybrid strategies[6] and the 'grey zone' is an evolution of historical tactics and strategies of irregular warfare, now enhanced by modern technology and information networks, allowing for more effective and less detectable influence in a global context (Hafen, 2024). Disinformation, propaganda and influence operations are essential

[5] Although this definition is precise, it is important to consider that disinformation can also be motivated by non-political or non-ideological objectives, such as organised crime or the profit-seeking of non-state actors (DSN, 2023a; Marchal González, 2023).

[6] Although the concept of 'hybrid warfare' has been the subject of multiple definitions and debates, there is still a lack of consensus on its precise characterisation, which complicates its study and application in contemporary strategic analysis (Colom, 2018b).

components of these strategies, which are deployed in an increasingly complex and globalised environment (Hoffman, 2009).

Modern propaganda goes beyond the simple dissemination of messages; it is a sophisticated manipulation of information to shape perceptions and behaviour in line with the strategic interests of those who promote it (Calvo Albero, 2017). Propaganda[7] can be seen as an extension of psychological operations, where the aim is not only to influence public opinion, but also to demoralise the adversary and alter their decision-making capacity (Rid, 2021)[8] . Since 2023, such operations have intensified, especially in the context of global conflicts such as those in Ukraine and Gaza, where propaganda has played a crucial role in polarising public opinion and manipulating information on an international scale (DSN, 2024).

In this context, disinformation not only acts as a tool of influence, but also facilitates other hybrid operations by weakening social cohesion and trust in institutions, creating an environment conducive to the implementation of more aggressive tactics without the need for open military confrontation (Alastuey Rivas et al., 2024). It is crucial to understand that hybrid strategies are not a new phenomenon, but rather an evolution of irregular warfare tactics that have been employed throughout history, although social changes and the advance of technology have greatly expanded the tools available for these strategies, allowing their application on a global scale and with a significant impact on international stability (Calvo, 2023). This can be seen clearly in the Russian Primakov/Gerasimov Doctrine, in China's 'Three War' conception or in the Western 'New Grey Zone Conceptualisation' (Adame Hernández, 2024).

3.1. FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI)

The concept of *Foreign Information Manipulation and Interference* (FIMI) refers to deliberate activities carried out by foreign actors with the aim of distorting information, manipulating public perception and influencing political and social processes in other countries. According to the joint report by the European Union Agency for Cybersecurity (ENISA) and the European External Action Service (EEAS), FIMI encompasses a variety of actions including the dissemination of disinformation, propaganda and psychological operations that seek to sow discord and destabilise democratic societies (ENISA & EEAS, 2022). FIMI can also involve the manipulation of cultural and historical narratives to stoke internal conflicts and destabilise social order by exploiting sensitive issues that resonate with existing prejudices or fears in a society (Buvarp, 2021). The sophistication of these operations lies in their ability to exploit pre-existing rifts within target societies, exacerbating divisions and provoking reactions that undermine social and political cohesion (Allenby and Garreau, 2017). These activities can have profound consequences for the stability of democratic institutions, as they focus on exploiting social and political vulnerabilities (ENISA & SEAE, 2022).

In the context of FIMI, it is essential to recognise that these operations do not always involve the dissemination of completely false information. Often, they rely on subtle

[7] Specifically, propaganda is defined as a "set of techniques used, in a systematic way, to spread partial or biased opinions or ideas among the masses, with a proper, often political, intention" (Donoso Rodríguez, 2020, p. 30), which makes it a key tool in psychological operations.

distortions of real facts, employing techniques such as information saturation or the creation of information bubbles (Rid, 2021); making detection and response difficult. These strategies, referred to as "subtle manipulation of the truth", are particularly dangerous as they play with public perception and the credibility of information sources (Castro Torres, 2021). Moreover, the manipulation of information through non-traditional channels, such as social media and instant messaging platforms, allows foreign actors to maximise the impact of their campaigns by taking advantage of the viral characteristics and global reach of these tools (EEAS, 2024).

FIMI is framed within hybrid strategies. Propaganda and influence actions are key tools within the FIMI framework. Propaganda is employed to promote narratives that favour the interests of the foreign actor, using controlled or like-minded media to disseminate specific messages. These narratives are carefully designed to appear legitimate and often rely on biased or biased sources that lend credibility to the messages disseminated (Maggioni and Magri 2015). Narratives devised to generate distrust towards democratic institutions and polarise society (Bennett & Livingston, 2020). In addition, influence actions are aimed at shaping public opinion or influencing political decisions, which can include anything from manipulation of social networks to covert funding of political or media actors in the target country (EEAS, 2023). A recent example of this has been observed in the Romanian presidential elections (European Commission, 2024). The anonymity provided by digital platforms and the possibility of operating through intermediaries or *proxies* adds a layer of complexity to tracking and identifying the real perpetrators of these campaigns, making it difficult to implement effective countermeasures (Castro Torres, 2021). The use of these methods has allowed foreign actors to operate with an additional layer of anonymity and deniability, complicating efforts to identify and counter these activities (DSN, 2024).

4. COGNITIVE DOMINANCE AND DISINFORMATION

Although the conceptualisation of the cognitive domain is relatively modern, strategies to operate on it such as propaganda (Calvo, 2023), influence (Jordán, 2018) and destabilisation (Quiñones de la Iglesia, 2021) are not. These tactics have historically been used in diverse geopolitical contexts, evolving over time to adapt to new information technologies and changing social dynamics. For example, propaganda, which once relied exclusively on traditional media such as print and radio, is now dispersed through digital platforms and social media, allowing for greater penetration and speed in the dissemination of messages. These tools have acquired unprecedented sophistication, taking advantage of the speed and reach of the Internet and social networks to amplify their effects, as seen in the tactics employed by groups such as Al Qaeda and the Islamic State, which have used these technologies to influence global public opinion and legitimise their actions (Astorga González, 2020). The influence of digital platforms is such that they allow malicious actors to segment audiences and personalise messages, creating echo chambers that reinforce pre-existing beliefs and hinder the dissemination of contrary information. This is enhanced by the use of algorithms that favour polarisation by prioritising sensationalist and emotionally charged content, which, in turn, facilitates the manipulation of the cognitive domain on a large scale (DSN, 2023b).

Louis Althusser's structuralist theory of ideological construction, where the media play a central role in the creation and maintenance of ideologies that dominate public perception, reinforces the understanding of how disinformation tactics are embedded in

the cognitive domain[9] (Althusser, 1971). In line with this, the manipulation of the cognitive domain involves the creation of perceived realities which, although they do not necessarily reflect objective reality, become the basis on which political and social decisions are made (Lupiáñez Lupiáñez, 2023). As various authors such as Foucault point out, language not only describes the world, but also acts upon it (Foucault, 1972), which reinforces the idea that the cognitive domain can be manipulated through the construction of narratives that reconfigure perceived reality.

In relation to disinformation, the grey zone will focus mainly on establishing the context, using strategies such as propaganda or disinformation, with the aim of gradually gaining a strategic advantage over the opponent, which would facilitate improving the effectiveness of future interventions (Hernández-García, 2022). Libicki reinforces this idea by explaining how cognitive operations do not always seek immediate results, but may be designed to sow doubt and confusion, affecting an adversary's ability to make effective decisions in the long run (Libicki, 2021). This approach underlines the importance of gradualism in disinformation strategy, where small changes in perception and narrative can culminate in a significant alteration of the perceived reality, causing the opponent to lose initiative and control over the situation. In this approach, the concurrence between objectives, strategic vision and gradualism should be emphasised.

The relationship between cognitive manipulation and political conflict can also be analysed from a Clausewitzian perspective. Clausewitz argues that war is a rational political act where one seeks to demoralise the adversary not only through direct conflict, but also by manipulating the passions of the population and the perception of reality (Clausewitz, 1976). Through disinformation it is possible to erode the morale of both an enemy army and, even more significantly, its population, with the aim of persuading its political decision-makers to stop their belligerent attitude, to bring about a negotiation or to obtain benefits in an already planned one (Rodríguez Lorenzo et al, 2023).

A fundamental factor to be considered, and one that is often only collaterally addressed, is the political relationship and impact. This aspect, though crucial, is often underestimated in analyses of disinformation, where greater emphasis is placed on the technical or tactical aspects, leaving aside the broader implications for governance and political stability. In a Clausewitzian logic, 'if war is political in nature, it is clear that the main target is not the enemy's armed forces, but the political leadership' (Calvo Albero, 2017).

It is the intersection between the disinformation used in hybrid and grey zone strategies; with the objectives pursued (especially political affectation) where they connect with society, the agenda and public opinion (Sartori, 2007). In this context, the manipulation of information and the creation of alternative narratives not only have an impact at the state or military level, but also have profound implications for the social and

[9] Spanish military doctrine underlines the relevance of STRATCOM (*Strategic Communications*) as a managerial function that integrates INFOOPS (*Information Operations*) and PSYOPS (*Psychological Operations*), applying social engineering and strategic communication techniques to shape the informational and cognitive environment. These capabilities enable the Armed Forces to achieve objectives that transcend conventional means, operating in an intangible realm that permeates all other domains (PDC-01, 2018).

cultural fabric. The construction of these narratives, which use film and media[10] as tools of emotional manipulation, remains central to understanding how malicious narratives can divide and confuse society (Davis, 2005). The ability of these strategies to alter public perception is not only due to the sophistication of the tactics employed, but also to the way in which these narratives align with existing concerns and fears in society, amplifying and redirecting them against specific targets (Castro Torres, 2021).

The construction of malicious narratives, which seek to divide and confuse society, becomes a powerful tool to destabilise not only governments, but also communities and social cohesion as a whole. The need to create a malicious narrative that can be exploited to one's own advantage (Rodríguez Lorenzo et al, 2023), an attractive narrative that sustains the hybrid strategy (Torres, 2022) and the inescapable generation of a narrative that sponsors, covers, strengthens and protects the grey zone (Hernández-García, 2022), give a great role to cognitive frameworks (Goffman, 2006), persuasive communication (Candelas, 2023) and public opinion (Sartori 2007). These elements, although underestimated in many analyses, are fundamental to understanding how disinformation inserts itself into the social fabric and becomes a force for change, eroding trust in institutions and altering the perception of reality. Understanding the relationship between cognitive manipulation and social change is crucial because, as described by Berger and Luckmann (2003), the social construction of reality is a dynamic process (externalisation, objectification and internalisation) that can be easily influenced by actors with control over media (social interaction) and narratives (language).

5. BUILDING NARRATIVES AND FRAMEWORKS

Narratives are structured narratives that seek to make sense of events and shape public perception. Since ancient times, propaganda has been based on the construction of narratives that shape public perception. It has been described how "necessary illusions" are created[11] in order for certain power groups to maintain their influence over society (Herman & Chomsky, 1988). In the context of modern disinformation, narratives are designed not only to convince, but to ingrain beliefs that are difficult to eradicate even when exposed as false[12] . Flynn, Nyhan and Reifler (2017) identify that political misperceptions are not simple information failures, but are due to misperceptions (false or unfounded beliefs held with confidence and resistance to correction), individual factors (such as cognitive biases or partisan or ideological identities) and resistance to change (passive to false information ascertainment or fact-checking processes); but also media and political environments (facilitating selective exposure to sources).

[10] A very eloquent example is the use of more traditional communication (such as cinema) and digital communication (high quality and high production quality videos disseminated *online*) in the communication strategies of organisations as un 'Western' as *Daesh*. With the use, in addition to technical aspects, of emotional tactics and the exploitation of cognitive biases such as anchoring, they have become key components in shaping the perception of the conflict (Astorga González, 2020).

[11] In Manufacturing Consent: The Political Economy of the Mass Media (Herman & Chomsky, 1988), the expression "necessary illusions" is not found as a textual quotation. However, the concept is developed throughout the book. The concept "*necessary illusions*" comes from the later work of Necessary Illusions (Chomsky, 1992).

[12] According to recent research, susceptibility to misinformation is not only driven by partisanship, but also by a lack of careful reasoning and the use of heuristics, such as familiarity with the information and credibility of the source (Pennycook et al, 2021).

These narratives, once in place, can continue to exert a lasting effect due to cognitive inertia and resistance to changing established beliefs (Libicki, 2021; Flynn, Nyhan, & Reifler, 2017). False and highly misleading narratives tend to prevail due to their ability to exploit human emotions, such as fear and moral outrage, which increases their impact and dissemination in social networks (Pennycook & Rand, 2021).

The concept of *framing* refers to the cognitive structures that determine how we interpret and understand information. These frames act as mental shortcuts that organise information and allow us to interpret events according to prior schemes of meaning. Cognitive frame theory highlights how the interpretative structures that society uses to make sense of events can be manipulated through persuasive communication (Goffman, 2006). The dispute for the control of these frames has become a central element in the fight against disinformation; *framing* not only seeks to combat falsehoods, but also to establish alternative frames that reconfigure public debate (Tuñón Navarro, Oleart, & Bouza García, 2019). In the context of hybrid strategies, and by extension the cognitive domain, frames are used to focus public attention on certain aspects of reality while hiding or distorting others[13] . This process allows certain narratives to prevail, not because of their veracity, but because of the way they are presented and contextualised. This process is key to maintaining narrative control and preventing the fundamental premises of the actions undertaken in a conflict from being questioned (Colom, 2018).

In modern practice, *framing* has become a key tool not only to shape the interpretation of events, but also to influence the emotions of the audience, exploiting cognitive biases that hinder critical reflection (Astorga González, 2020).

5.1. IMPLEMENTATION

The construction of narratives and frames in the context of misinformation involves a complex process of creating narratives and cognitive structures designed to influence public perception in a deep and lasting way. This process is based on an advanced understanding of behavioural science, where cognitive biases such as anchoring, availability and confirmation are exploited to ensure that the narratives constructed are resistant to change (Astorga González, 2020). Sophistication in the construction of these narratives employs the ability to combine real facts with subtle distortions, making them harder to discredit and easier for the audience to accept (Rid, 2021). In this way, narratives, which exploit the cognitive and emotional biases of the audience, are structured to be simplified and emotional, which increases their effectiveness in media manipulation (Herman & Chomsky, 1988). These narratives seek not only to convince, but also to establish a perception of reality that is resistant to correction, even when its falsity is exposed[14] . Repeated exposure to fake news increases its perceived credibility, even when it is initially plausible. This effect, known as the 'illusion of truth', plays a crucial role in the permanence and acceptance of false narratives (Pennycook et al, 2021).

[13] Research suggests that the interaction between social networks and human psychology, in particular the tendency to use mental shortcuts and rely on familiarity, contributes significantly to the spread and persistence of fake news (Pennycook et al, 2021).

[14] Another example would be "memetic warfare", which uses memes and other forms of viral disinformation, seeks to create and disseminate narratives that alter the perceptions and emotions of the target audience, achieving a lasting impact that is difficult to counter, especially when it involves parody content and civilian sources (Arias Gil, 2019).

Moreover, *microtargeting* or segmentation of the population according to their beliefs and values has allowed messages to be tailored specifically to each group, coupled with the proliferation of alternative media and channels (and sometimes opaque to the majority of the population and public opinion) has amplified the ability of these frameworks to influence public perception, increasing the effectiveness of manipulation (Astorga González, 2020). This personalised approach to disinformation dissemination maximises the impact on different segments of society, fostering polarisation and reinforcing pre-existing beliefs while making detection more difficult (Maggioni and Magri, 2015).

The impact of these narratives and frames is such that, even when discredited, they can continue to influence public opinion due to cognitive inertia, a phenomenon in which previously established beliefs are resistant to change (Libicki, 2021). This is particularly evident in the way certain narrative frames persist in public discourse long after they have been proven false, continuing to influence social perception and action (Juurvee and Mattiisen, 2020). In this way, the construction of narratives and frames becomes a powerful tool for shaping public perception and maintaining control over the interpretation of reality.

5.2. IMPACT OF NARRATIVES AND FRAMEWORKS IN THE COGNITIVE DOMAIN

Narratives and frames have a profound impact on the cognitive domain, shaping not only how events are perceived, but also how they are understood and remembered. It has been noted that the creation of a malicious narrative can be exploited to the benefit of those who control the narrative, giving great power to cognitive frames and persuasive communication (Rodríguez Lorenzo et al, 2023; Torres, 2022). These elements are fundamental to understanding how disinformation becomes embedded in the social fabric and becomes a force for change, eroding trust in institutions and altering perceptions of reality. Moreover, these frames not only influence individual perception, but also affect collective memory, conditioning the way societies remember and learn from historical events, which can have long-term repercussions on social cohesion and the formation of national identities (Aznar Fernández-Montesinos, 2021). Propaganda and disinformation not only operate through direct messages, but also shape the cognitive environment in which these messages are interpreted, creating an environment of uncertainty and mistrust that facilitates the manipulation of public opinion (Lupiáñez Lupiáñez, 2023).

Cognitive manipulation has proven capable of altering not only the immediate perception of reality, but also of shaping long-term patterns of thought and behaviour (Astorga González, 2020). The impact of these narratives in the cognitive domain is amplified by the use of information technologies that allow for rapid and massive dissemination, which makes the effects of disinformation more lasting and difficult to counteract (Lupiáñez Lupiáñez, 2023).

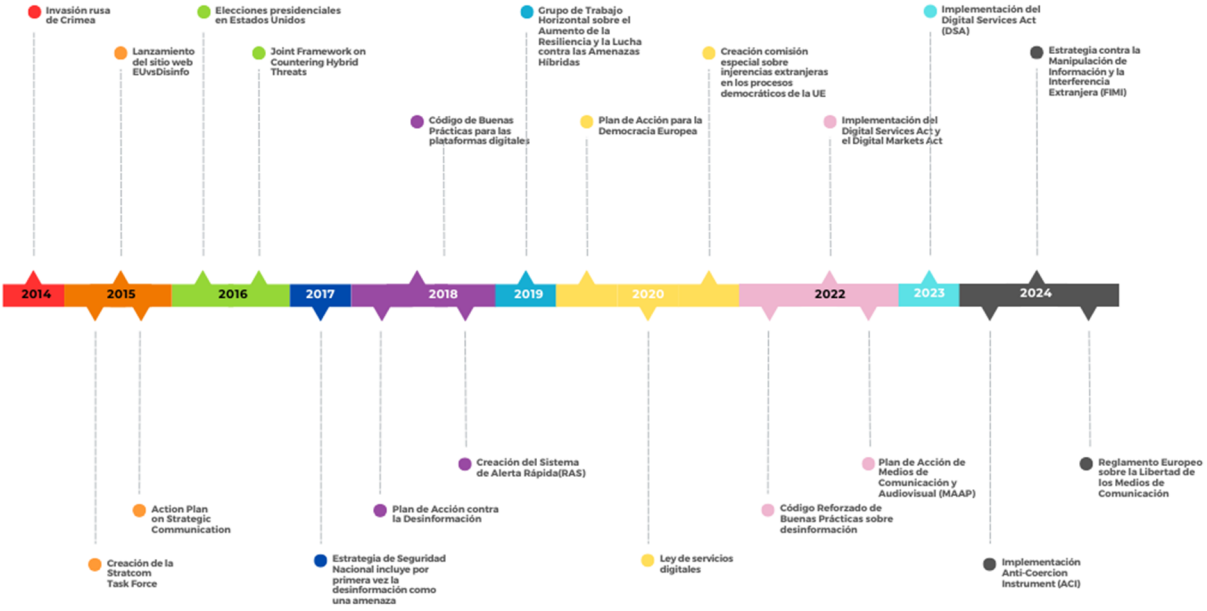
6. EVOLUTION OF DISINFORMATION

The EU has implemented a set of coordinated policies and actions to combat disinformation, recognising its significant impact on the democratic stability and security of member states. The relevance of this threat intensified after events such as the Russian invasion of Crimea in 2014 and the 2016 US presidential election, which highlighted how

disinformation could be used as an effective tool in hybrid conflicts and electoral interference (EEAS, 2015). The main milestones can be seen in Figure 2 .[15]

Figure 2

LAS POLÍTICAS DE LA UNIÓN EUROPEA EN LA LUCHA CONTRA LA DESINFORMACIÓN



Source: Own elaboration.

In Spain, the perception of misinformation has evolved significantly in recent decades, starting in the second half of the 2010s, marked by a growing recognition of the risks associated with the circulation of false and manipulated information, both nationally and internationally (Badillo and Arteaga, 2024).

Political polarisation in Spain, accentuated by the conflict in Catalonia and the growing fragmentation of the political spectrum, has been a relevant factor in the perception of disinformation (Badillo and Arteaga, 2024). Sixty per cent of Spaniards perceived a great political division in the country, and more than 70 per cent considered that disinformation was contributing significantly to this division (CIS, 2021).

Spaniards' trust in the media remains low (below 5 out of 10)[16] , while the influence of social networks is increasing[17] (CIS, 2024). The Media Trust Index, elaborated by Eurobarometer, shows a significant lack of trust among Spaniards. Forty percent of those surveyed in Spain did not trust the traditional media, 12 points higher than the European

[15] For more information on the evolution of EU actions, see *Spain in the face of disinformation: Hybrid challenges and conventional responses (*Adame Hernández, 2024).

[16] On a scale of 1 to 10 on the trust they have in the media, trust has gone from 4.3 in 2021 to 4.2 in 2022 and 4.1 in 2023 and 2024. The trend is more pronounced as it decreases with age: the 25-34 age group rates it at 2.88 and the 18-24 age group at 3.45 (CIS, 2024).

[1717] The percentage of Spaniards influenced by social networks and the internet when making political decisions has increased from 8.6% in 2021, to 9.4% in 2022, 10.3% in 2023 and 16.2% in 2024 (CIS, 2024).

average, and 58% believe that the media provide information subject to political or commercial pressures, 15 points higher than the European average (Eurobarometer, 2024).

Digitalisation and the penetration of social media have played a crucial role in the evolution of the perception of misinformation. According to the Digital Economy and Society Index (DESI) 2024, Spain has experienced a steady increase in the use of the internet and social media. DESI indicates that, in 2024, 96.45% of Spanish households had access to the internet, 88.23% of the population has higher digital skills[18] and 34.4% of companies use several social networks (compared to 28.5% of the European average (DESI, 2020). This high level of connectivity has increased the population's exposure to disinformation campaigns. The growing importance of social media as the main channel for accessing information[19] , especially among young people[20] , suggests a move away from traditional news formats and a preference for visual and brief content (Reuters Institute for the Study of Journalism, 2024).

Finally, the global context has also influenced the perception of misinformation in Spain. The COVID-19 pandemic, for example, triggered an "infodemic", a term coined by the World Health Organisation to describe the overabundance of information, both accurate and inaccurate, which made it difficult for people to find reliable sources (WHO, 2020). During the pandemic, the Latam Chequea network verified more than 1,000 COVID-19-related fake news stories in Spain, many of which were widely spread on social media and messaging apps (Latam Chequea, 2022). This phenomenon exacerbated public distrust and further destabilised the information ecosystem, underscoring the need to strengthen national capacities to effectively detect and counter disinformation (OECD (2024). Amid a growing distrust of traditional media, affecting almost 70% of the population (Novoa-Jaso, Sierra, Labiano, & Vara-Miguel, 2024). Moreover, 37% of Spaniards actively avoid the news, a behaviour that seems to be motivated by the saturation of negative or controversial content that dominates current media narratives (Reuters Institute for the Study of Journalism, 2024).

Spain's institutional response to disinformation has evolved significantly since 2017, when the problem was first recognised in the National Security Strategy, to the implementation of more robust and coordinated policies in the following years. However, this evolution has been marked by both notable advances and some shortcomings in integrating more holistic approaches that include narrative management (Adame Hernández, 2024). .[21]

[18] These include sending/receiving emails; Making telephone or video calls over the Internet; Instant messaging; Participating in social networking; Expressing opinions on civic or political issues on websites or social networks; Participating in online consultations or voting on civic or political issues.

[19] WhatsApp has overtaken Facebook as the main source of information in Spain, with 36% of users using WhatsApp to access news, compared to 29% using Facebook. This transition highlights a shift towards more private, messaging-centric platforms (Reuters Institute for the Study of Journalism, 2024).

[20] TikTok and Instagram are growing rapidly among the under-25s. TikTok is used by 30% of this age group for information, while Instagram reaches 25%, surpassing more traditional platforms such as YouTube, which stands at 15% (Reuters Institute for the Study of Journalism, 2024).

[21] For more information on the evolution of Spain's policies against disinformation, see *España frente a la desinformación: Desafíos híbridos y respuestas convencionales (*Adame Hernández, 2024).

7. CURRENT MEASURES AND TOOLS TO COMBAT DISINFORMATION IN SPAIN

The core of Spain's infrastructure for combating disinformation centres on the Permanent Commission against Disinformation, which coordinates the operational response to disinformation campaigns. This commission acts under the supervision of the Secretary of State for Communication, which leads the government's strategic communication policy. In crisis situations, the Disinformation Coordination Cell manages the response, ensuring that the government's actions are swift and effective (ORDEN PCM/1030/2020, 2020).

The Forum against Disinformation Campaigns in the Sphere of National Security has been one of the main pillars of Spain's strategy against disinformation. In 2023, seven papers were presented that address various facets of the problem, from verification and prevention methodologies (such as *prebunking* and the inoculation theory[22]) to the analysis of Russian disinformation in the context of the war in Ukraine (DSN, 2023b). At the end of 2024, they presented the second edition of the Forum's work, advancing on aspects such as the role of the media and the communications departments of public and private institutions, FIMI, the link between disinformation and hate speech, and working hypotheses on the Spanish media ecosystem and public opinion in relation to disinformation (DSN, 2024b). The Forum channels public-private and public-social cooperation, articulating a strategic and multi-sectoral approach. The depth of its analyses, as well as its efforts to address a complex reality, are clearly evidenced in the evolution of its respective publications.

Or other initiatives such as the positive communication campaigns of the Ministry of Foreign Affairs, European Union and Cooperation to combat disinformation through verifiable narratives[23] , the development of technological tools such as ELISA[24] (Simplified Study of Open Sources) or the DANGER project (INCIBE. (2024), the Action Plan for Democracy[25] (MPJRC, 2024) or the order establishing the elaboration of the National Strategy against Disinformation Campaigns (Order PJC/248/2025, 2025). It is worth noting the lack of studies, reports or analyses on the impact of institutional measures against disinformation.

7.1. ACTION PROCEDURE AGAINST DISINFORMATION

The Procedure for action against disinformation regulated by Order PCM/1030/2020, has as its fundamental purpose the creation of a coordinated framework to detect, analyse and

[22] *Prebunking* is a preventive communication technique that consists of exposing people to a weakened version of disinformation before they encounter it, in order to increase their resistance and critical capacity against future attempts at manipulation. This strategy is similar to psychological 'inoculation', which seeks to generate cognitive immunity against false narratives (Maldita.es, 2023; Roozenbeek et al., 2022).

[23] Highlighting the campaigns "Voto exterior", "Tu Consulado", "Viaja Seguro" and information on the Ley de Memoria Democrática (DSN, 2024. p. 103).

[24] ELISA monitors websites suspected of fostering disinformation campaigns, enabling early detection and a more agile response by authorities (CCN-CERT, 2019). In 2023, it increased its capabilities, integrating artificial intelligence algorithms that allow it to identify disinformation patterns more accurately (DSN, 2024).

[25] Which provides, inter alia, for the implementation of Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Regulation on Freedom of the Media).

respond to disinformation in Spain (ORDER PCM/1030/2020, 2020), particularly in situations affecting national security. This procedure was approved by the National Security Council and falls within the context of European strategies to combat disinformation, particularly those set out in the 2018 EU Disinformation Action Plan.

The procedure is articulated in four fundamental axes: detection, analysis, response and evaluation; and in four levels of activation. The Secretariat of State for Communication is in charge of general coordination, acting in close collaboration with other ministries, the National Security Council Situation Centre and the Working Group against Disinformation. This inter-ministerial group is responsible for advising and proposing actions to the National Security Council, ensuring an integrated and coherent response . [26]

The implementation of the procedure provoked public controversy and led several organisations to file appeals and complaints before the Contentious-Administrative Court[27] . It has also been criticised for its lack of clarity in the definition of competences and fields of action of the different authorities involved (Gómez, 2020; Garrós Font & Santos Silva, 2021) or the lack of specialised resources (Badillo & Arteaga, 2024).

The Supreme Court established very clear limits on the work and scope of the "Procedure for Action against Disinformation" and the bodies it creates by stating that it does not create or grant new competences and cannot affect fundamental rights (Supreme Court, 2021). Thus restricting the protocol to an internal action plan limited to establishing coordination criteria. It also establishes a legal definition of disinformation[28] , something that the procedure does not do.

[26] Annex II sets out the functioning and mode of action of the permanent commission against disinformation (ORDER PCM/1030/2020, 2020).

[27] For more information on the Disinformation Action Procedure, see *Spain in the Face of Disinformation: Hybrid Challenges and Conventional Responses (*Adame Hernández, 2024).

[28] According to the ruling, disinformation is understood as "verifiably false or misleading information which is created, presented and disseminated for profit or to deliberately mislead the public, and which is likely to cause public harm" (Supreme Court, 2021). This definition is taken from the Disinformation Action Procedure (ORDER PCM/1030/2020, 2020) which in turn is taken from the European Commission's Communication COM (2018). The Disinformation Action Procedure limited itself in its point 1. Context to reproducing the European Commission's definition.

8. CONCLUSIONS

Throughout the article, we have analysed how disinformation is embedded in a broader context of geopolitical tactics and strategies, highlighting its role in FIMI. This broader context is enriched by the consideration of how narrative frameworks are strategically employed to steer public debate towards specific narratives that favour the interests of those who construct them, minimising or distorting aspects of reality that might contradict these interests (Tuñón Navarro, Oleart, & Bouza García, 2019; Astorga González, 2020). It has been argued that disinformation does not act as an isolated tool, but is part of a coordinated set of actions designed to influence public perception, manipulate the narrative and create uncertainty in political and social processes (Hoffman, 2009; McCuen, 2008).

Disinformation has had a critical impact on key events over the last decade, impacting both institutional stability and social cohesion. Analyses have revealed that public policies in Spain, while attempting to respond to these threats, have been insufficient due to their fragmented and predominantly reactive nature (Badillo and Arteaga, 2024). This has placed Spanish institutions in a vulnerable position in the face of increasingly sophisticated disinformation campaigns, which have exploited weaknesses in inter-institutional coordination and the lack of a comprehensive preventive approach (Bennett & Livingston, 2020).

The institutional response to disinformation has been limited by the lack of integration between cybersecurity and cognitive defence. The anonymity provided by digital platforms and the possibility of operating through intermediaries or 'proxies' adds a layer of complexity that makes it difficult to identify the real perpetrators of these campaigns (Castro Torres, 2021), fostering the need for a more proactive and forward-looking strategy (Arias Gil, 2019). While significant efforts have been made to improve surveillance and response to disinformation, these have been fragmented and lack the coherence needed to effectively address threats. An example is the absence of a proposed National Strategy to Combat Disinformation Campaigns since 2022 (DSN, 2022). This is clearly exemplified by the activation of Level 1 of the Disinformation Action Procedure. The lowest level of activation of the Procedure involves the concurrence of high-level State bodies such as the Secretary of State for Communication, the DSN, the CNI and the Secretary of State for Digital Transformation and Artificial Intelligence, among others (ORDEN PCM/1030/2020, 2020). It also assigns a predominantly reactive role, which reinforces the limited institutional response and scope.

Another example, the construction of narratives and frames by malicious actors has proven to be a formidable challenge, as these tactics not only distort reality, but also undermine trust in democratic institutions (Berger & Luckmann, 2003; Candelas, 2023), an element that has been little addressed in the Spanish institutional response, and where bets such as digital literacy or fact-checkers (DSN, 2021) yield very limited results. Luckmann, 2003; Candelas, 2023) an element little addressed in the Spanish institutional response, and where bets such as digital literacy or *fact-checkers* (DSN, 2021) yield very limited results (Pennycook, Bear, Collins, & Rand, 2020; Flynn, Nyhan, & Reifler, 2017). In fact, false and highly misleading narratives tend to prevail due to their ability to exploit human emotions, such as fear and moral outrage, which increases their impact and diffusion in social networks (Pennycook & Rand, 2021).

Analysis of the effectiveness of the proposed strategies suggests that a comprehensive approach combining technical and cognitive measures is essential to develop an effective response to misinformation. Current strategies, although necessary, have failed to anticipate and respond to emerging threats due to their reactive (Badillo and Arteaga, 2024) and partial approach that does not address key elements of the problem such as narratives. There is a clear need to adopt a more proactive and prospective stance, allowing institutions not only to respond to current threats, but also to anticipate and neutralise future disinformation campaigns (Libicki, 2021).

One of the initiatives proposed by the main actors is the implementation of advanced technologies, such as artificial intelligence and machine learning, which can play a crucial role in the early identification of disinformation patterns (NATO, 2021; INCIBE, 2024; DSN, 2024b; European Commission, 2025). These technologies enable real-time analysis of large volumes of data, facilitating the detection of anomalies that could indicate the presence of coordinated disinformation campaigns (Rodríguez Lorenzo et al., 2023). However, as discussed throughout this article, for these tools to be effective, it is essential that they are integrated into a broader framework of institutional defence, including both cybersecurity and cognitive defence.

In addition to technological measures, research underlines the importance of strengthening both society and its institutions, increasing their strategic depth and capabilities. The fight against disinformation requires greater investment in economic, institutional and human resources (Rodríguez Lorenzo et al., 2023), commensurate with the magnitude of the threat. Incorporating the logic of the hybrid society into strategic and tactical proposals can increase their effectiveness and reduce the costs of investing in the response (Arias Gil, 2020). This logic allows for greater adaptation to emerging threats and a more efficient response. It is essential for Spain to develop robust national capabilities, especially given that FIMI involves not only major powers such as Russia and China, but also a variety of actors (Badillo & Arteaga, 2024), for which the response cannot rely exclusively on international bodies such as NATO or the EU.

It is necessary to overcome the paradigm that focuses on fostering critical thinking and media literacy and move towards the concept similar to the one proposed by Arias Gil of "strategic citizen" (2020). This new approach implies transforming the logic of individual responsibility, which is passive, atomised, partial and of medium/long-term development, into a more proactive, collective and coordinated social response. Rather than relying solely on individual training in critical skills, the strategic citizen is a collective, proactive, decentralised (but coordinated) resource that can act quickly in the face of disinformation threats. This shift in approach could enable a more dynamic and effective response, addressing threats in the short term and facilitating greater adaptability to the changing tactics of disinformation actors.

A key recommendation is the need for specific training, simulations and manoeuvres in the area of disinformation, similar to those carried out in other areas of security and defence. This proposal is absent from all the documentation analysed above. These activities would enable institutions to be better prepared to identify and neutralise disinformation campaigns before they cause significant damage. In addition, a shift towards a more proactive (use of strategic communication) and forward-looking posture is proposed, allowing potential attack vectors to be identified and preventive measures to be taken to minimise, neutralise or mitigate them before they become real threats. This

includes incorporating the asymmetric logic of the hybrid society, where tactical and strategic responses can be more effective and less costly (Arias Gil, 2020).

Finally, the creation of more dense and coordinated structures in the fight against disinformation is presented as an essential measure. This includes the training of middle management in public administration, the private sector and civil society, especially in areas related to communication, foresight and socio-political analysis. Such training is crucial to ensure that all sectors of society are aligned and prepared to face the complex threats posed by disinformation (DSN, 2022). In this sense, the dispute for the control of narrative frames has become a central element in the fight against disinformation, where the aim is not only to combat falsehoods, but also to establish alternative frames that reconfigure public debate (Tuñón Navarro, Oleart, & Bouza García, 2019). Similarly, knowing, eliminating, mitigating or neutralising one's own cultural, political or social vulnerabilities is key to eliminating attack vectors, reducing vulnerabilities and increasing residency.

In conclusion, there is a need for a significant change in the way Spain deals with disinformation. It is not enough to implement technical or reactive measures; it is essential to develop a comprehensive strategy that strengthens social, cognitive and technological aspects, promoting a more coordinated, proactive and adaptive defence against disinformation threats in an increasingly dynamic and complex global hybrid environment.

9. BIBLIOGRAPHICAL REFERENCES

Adame Hernández, J. F. (2024). España frente a la desinformación: Desafíos híbridos y respuestas convencionales (Master's thesis, Centro Universitario de la Guardia Civil).

Alastuey Rivas, J., García López, M. I., García Vizcaíno, F., Garrido López, A., Mora Moret, F., Pedrazo Majarrez, J. M., & Pérez-Tejada García, S. (2024). Disinformation as a weapon of war. IEEE Opinion Paper 26/2024. Spanish Institute for Strategic Studies (IEEE). Retrieved from https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO26_2024_VVAA_Desinforma (accessed 06/04/2025).

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31(2), 211-236. https://doi.org/10.1257/jep.31.2.211(accessed 06/04/2025).

Allenby, B., & Garreau, J. (2017, January 3). Weaponized narrative is the new battlespace. Defence One. Retrieved from http://bit.ly/3XyiwB2 (accessed 14/08/2024).

Althusser, L. (1971). Ideology and Ideological State Apparatuses. Medellín: La Oveja Negra. Retrieved from https://lobosuelto.com/wp-content/uploads/2018/10/Althusser-L.-Ideolog%C3%ADa-y-aparatos-ideol%C3%B3gicos-de-estado.-Freud-y-Lacan-1970-ed.-Nueva-Visi%C3%B3n-1974.pdf (accessed 14/08/2024).

Arias Gil, E. (2020). Low-cost insurgency: an emerging asymmetric threat. Retrieved from https://canal.uned.es/video/5f6b02325578f274ac7a0632 (accessed 06/04/2025).

Arias Gil, E. (2021). The emerging dimension of fake news: Network-centric warfare and memetic warfare. Retrieved from LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Report. Institute for the Development of Intelligence in the Field of Terrorism, Security and Defence (IDITESDE). https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf (accessed 14/08/2024).

Arteaga, Félix (2020). La lucha contra la desinformación: cambio de modelo. Real Instituto Elcano. https://www.realinstitutoelcano.org/comentarios/la-lucha-contra-la-desinformacion-cambio-de-modelo (accessed 06/04/2025).

Astorga González, L. (2020). Cognitive manipulation in the 21st century. Revista del Instituto Español de Estudios Estratégicos, 16, 15-44. Retrieved from https://revista.ieee.es/article/view/2208 (accessed 06/04/2025).

Aznar Fernández-Montesinos, F. (2021). The battle of the narratives. Retrieved from LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Report. Instituto para el Desarrollo de la Inteligencia en el Ámbito del Terrorismo, Seguridad y Defensa (IDITESDE). https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf (accessed 14/08/2024).

Badillo, Á. M., & Arteaga, F. (2024). The strategic impact of disinformation in Spain. Iberifier report. Retrieved from https://media.realinstitutoelcano.org/wp-content/uploads/2024/04/informe-iberifier-el-impacto-estratagico-de-la-desinformacion-en-espana.pdf (accessed 06/04/2025).

BBC World (16 February 2018). US Justice Department charges 13 Russian nationals with interfering in 2016 presidential election. https://www.bbc.com/mundo/noticias-internacional-43092239 (accessed 04/04/2025).

Bennett, W. L., & Livingston, S. (2020). The disinformation order: Disruptive communication and the decline of democratic institutions. European Journal of Communication. Retrieved from https://iddp.gwu.edu/sites/g/files/zaxdzs5791/files/downloads/The%20Disinformation%20Order%3B%20Livingston.pdf (accessed 14/08/2024).

Berger, P. L., & Luckmann, T. (1966). The social construction of reality. Buenos Aires. Retrieved from https://redmovimientos.mx/wp-content/uploads/2020/07/La-Construcci%C3%B3n-Social-de-la-Realidad-Berger-y-Luckmann.pdf (accessed 06/04/2025).

Burkhardt, J. M. (2017). History of fake news. Library Technology Reports, 53(8), 5-9. https://journals.ala.org/index.php/ltr/article/view/6497/8631 (accessed 06/04/2025).

Buvarp, P. M. H. (2021). The space of influence: Developing a new method to conceptualise foreign information manipulation and interference on social media. The Norwegian Defence Research Establishment (FFI). Retrieved from https://www.ffi.no/en/publications-archive/the-space-of-influence-developing-a-new-method-to-conceptualise-foreign-information-manipulation-and-interference-on-social-media (accessed 02/06/2025).

Calvo Albero, J. L. (18 December 2017). Disinformation: old ideas in new formats. Global Strategy. https://global-strategy.org/desinformacion-viejas-ideas-en-nuevos-formatos (accessed 06/04/2025).

Calvo, J. L. (April, 2023). From silent war to hybrid war. Revista Española de Defensa. https://www.defensa.gob.es/Galerias/gabinete/red/2023/04/p-54-57-red-404-desinformacion.pdf (accessed 06/04/2025).

Candelas, M. (2023). Propaganda in geopolitical conflicts: from psychological warfare to war beyond boundaries. IEEE Opinion Paper 02/2023. https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO02_2023_MIGCAN_Propaganda.pdf (accessed 06/04/2025).

Caridad-Sebastián, M, Morales-García, A. M., Martínez-Cardama, S, & García López, F (2018). Infomediation and post-truth: The role of libraries. https://e-archivo.uc3m.es/bitstream/handle/10016/28096/Infomediacion_EPI_2018.pdf?sequence=1&isAllowed=y (accessed 20/08/2024).

Castro Torres, J. I. (2021). The disinformation environment and the construction of narratives. Retrieved from LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Report. Instituto para el Desarrollo de la Inteligencia en el Ámbito del Terrorismo, Seguridad y Defensa (IDITESDE). https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf [URL not available] (accessed 14/08/2024).

CCN-CERT. (2019, November 11). ELISA: New cyber-surveillance tool from CCN-CERT. Retrieved from https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Noviembre/Noticia-2019-11-11-ELISA-nueva-herramienta-de-cibervigilancia-del-CCN-CERT.html?idioma=es (accessed 06/04/2025).

Centro de Investigaciones Sociológicas (CIS) (2021). Barómetro CIS de febrero-julio de 2022. Madrid, Spain. Retrieved from https://www.cis.es/documents/d/cis/es3351marpdf (accessed 14/08/2024).

Centro de Investigaciones Sociológicas (CIS) (Sociological Research Centre) (2023). Study 3424: Social perception of scientific aspects of genetic manipulation and biotechnology. Retrieved from https://www.cis.es/es/detalle-ficha-estudio?origen=estudio&codEstudio=3424 (accessed 14/08/2024).

Centro de Investigaciones Sociológicas (CIS) (Sociological Research Centre) (2024). Study 3486: Survey on Social Trends (IV). Retrieved from https://www.cis.es/visor?migrado=false&fichero=cru3486_enlace (accessed 01/06/2025).

Chan, R. (2020). The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections. https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10 (accessed 06/04/2025).

Chomsky, N. (1992). *Necessary illusions*. Retrieved from https://resistir.info/livros/chomsky_ilusiones_necesarias.pdf (accessed 06/04/2025)

Clausewitz, C. von. (1976). On war. Sphere of Books. Retrieved from https://www.esferalibros.com/wp-content/uploads/2022/09/De-la-guerra-primeras.pdf (accessed 14/08/2024).

Colom, G. (2018). Hybrid wars. When context is everything. Army Magazine. Retrieved from https://www.ugr.es/~gesi/Guerras-hibridas.pdf (accessed 20/08/2024).

Colom, G. (2018b). The Gerasimov doctrine and contemporary Russian strategic thinking. Army Review. Retrieved from https://www.thiber.org/2019/05/11/la-doctrina-gerasimov-y-el-pensamiento-estrategico-ruso-contemporaneo (accessed 06/04/2025).

European Commission (2022). The Strengthened Code of Practice on Disinformation. Retrieved from https://ec.europa.eu/newsroom/dae/redirection/document/87585 (accessed 20/08/2024).

European Commission (2024, 17 December). Commission initiates formal proceedings against TikTok over election risks under the Digital Services Act Retrieved from https://ec.europa.eu/commission/presscorner/detail/es/ip_24_6487 (accessed 22/03/2025).

European Commission (2025, 15 April). Commission invests €140 million to deploy key digital technologies. Retrieved from https://spain.representation.ec.europa.eu/noticias-eventos/noticias-0/la-comision-invierte-140-millones-de-euros-para-desplegar-tecnologias-digitales-clave-2025-04-15_es#:~:text=La%20Comisi%C3%B3n%20ha%20lanzado%20cuatro,y%20luchar%20contra%20la%20desinformaci%C3%B3n (accessed 22/03/2025).

Dahlgren, P. (2018). *Media, knowledge and trust: The deepening epistemic crisis of democracy*. Javnost - The Public, 25(1-2), 20-27. Retrieved from https://doi.org/10.1080/13183222.2018.1418819 (accessed 06/04/2025).

Davis, G. (2005). The ideology of the visual. In M. Rampley (Ed.), Exploring visual culture: Definitions, concepts, contexts (pp. 163-178). Edinburgh University Press.

DESI dashboard for the Digital Decade (2024). DESI dashboard for the Digital Decade. European Commission. Retrieved from https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts (accessed 06/04/2025).

DSN (2021). National Security Strategy. Department of Homeland Security (2021).

DHS (2022). Department of Homeland Security (2022). Retrieved from https://www.dsn.gob.es/sites/default/files/documents/LibroDesinfoSN.pdf (accessed 14/08/2024).

DSN (2023a). Forum against Disinformation Campaigns in the field of National Security - Jobs 2023. Retrieved from https://www.dsn.gob.es/sites/dsn/files/Foro%20Campa%C3%B1as%20Desinfo%20GT%202023%20Accesible.pdf (accessed 14/08/2024).

DSN (2023b). Presentation of work 2023: Forum against disinformation campaigns in the field of national security. Retrieved from https://www.dsn.gob.es/es/actualidad/sala-prensa/presentaci%C3%B3n-trabajos-2023-foro-contra-campa%C3%B1as-desinformaci%C3%B3n-%C3%A1mbito (accessed 14/08/2024).

DHS. Department of Homeland Security (2024). Annual National Security Report 2023. Government of Spain. Retrieved from https://www.newtral.es/wp-content/uploads/2024/03/IASN2023_0.pdf (accessed 14/08/2024).

DHS. Department of Homeland Security (2024b). Work of the Forum Against Disinformation Campaigns - Initiatives 2024. Retrieved from https://www.dsn.gob.es/es/publicaciones/otras-publicaciones/trabajos-foro-contra-campanas-desinformacion-iniciativas-2024#:~:text=medios%20de%20comunicaci%C3%B3n.-,Trabajos%20del%20Foro%20contra%20las%20Campa%C3%B1as%20de%20Desinformaci%C3%B3n%20%2D%20Iniciativas%202024,-Accesible (accessed 14/08/2024).

Donoso Rodríguez, D. (2020). *Implications of the cognitive domain in military operations*. *IEEE Magazine, 01/2020*. Retrieved from https://emad.defensa.gob.es/Galerias/CCDC/files/IMPLICACIONES_DEL_AMBITO_COGNITIVO_EN_LAS_OPERACIONES_MILITARES.pdf (accessed 01/06/2025).

Dubois, E., & Blank, G. (2018). The echo chamber is overstated: the moderating effect of political interest and diverse media. Information, Communication & Society. Retrieved from https://www.tandfonline.com/doi/full/10.1080/1369118X.2018.1428656#abstract (accessed 06/04/2025).

EEAS (European External Action Service) (2024). 2nd report on FIMI threats - January 2024. Retrieved from https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf (accessed 14/08/2024).

EEAS, European External Action Service (2015). Tackling disinformation, foreign information manipulation & interference. https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en (accessed 14/08/2024).

ENISA & SEAE. (2022). Foreign Information Manipulation and Interference (FIMI) and Cybersecurity - Threat Landscape. Retrieved from https://www.cde.ual.es/wp-content/uploads/2022/12/EEAS-ENISA-Disinformation_Misinformation.pdf (accessed 14/08/2024).

Eurobarometer (2024). EUROBAROMETER STANDARD 102 Public Opinion in the European Union. European Commission. Retrieved from https://europa.eu/eurobarometer/surveys/detail/3215 (accessed 14/08/2024).

IFJ, International Federation of Journalists (2018). What is fake news? A guide to combating disinformation in the post-truth era. Retrieved from https://www.ifj.org/fileadmin/user_upload/Fake_News_-_FIP_AmLat.pdf (accessed 06/04/2025).

Flores, J. M. (2022). "Fake news has always existed, but today it has been catapulted by social networks". Retrieved from https://www.ucm.es/otri/noticias-las-fake-news-siempre-han-existido-pero-hoy-en-dia-se-han-visto-catapultadas-por-las-redes-sociales (accessed 20/08/2024).

Flynn, D., Nyhan, B., & Reifler, J. (2017). The nature and origins of misperceptions: understanding false and unfounded beliefs about politics. Political Psychology, 38(6), 1053-1077. https://doi.org/10.1111/pops.12394 (accessed 06/04/2025).

Foucault, M. (1972). The archaeology of knowledge. Siglo XXI Editores. Retrieved from https://monoskop.org/images/b/b2/Foucault_Michel_La_arqueologia_del_saber.pdf

(accessed 14/08/2024).

Garrós Font, I., & Santos Silva, M. F. (2021). The fight against infodemia: Analysis of the procedure for action against disinformation. Journal of Communication and Health, 11(2), 75-89. https://doi.org/10.35669/rcys.2021.11(2).75-89

Gelfert, Axel (2018). Fake News: A Definition. Informal Logic, 38. Retrieved from https://informallogic.ca/index.php/informal_logic/article/view/5068 (accessed 06/04/2025).

Goffman, E. (2006). Frame analysis: The frames of experience. Centre for Sociological Research.

Gómez, A. (2020, 19 November). The new procedure for action against disinformation: The controversy is served. Blog de Propiedad Intelectual y NNTT Garrigues. Retrieved from https://blogip.garrigues.com/publicidad/el-nuevo-procedimiento-de-actuacion-contra-la-desinformacion-la-polemica-esta-servida (accessed 06/04/2025).

Hafen, R. (2024). Chinese operational art: The primacy of the human dimension. Military Review. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/Q2-2024/Hafen-SPA-Q2-2024/Hafen-SPA-Q2-2024-UA.pdf (accessed 14/08/2024).

Herman, E. S., & Chomsky, N. (1988). The guardians of freedom. Retrieved from https://www.labiblioteca.mx/llyfrgell/1783.pdf (accessed 06/04/2025).

Hernández-García, L. A. (2022). The grey zone: a conceptual approach from the FAS. Retrieved from https://www.atalayar.com/opinion/luis-hernandez-garcia-ieee/la-zona-gris-una-aproximacion-conceptual-desde-las-fas/20220412121331136376.html (accessed 06/04/2025).

Hoffman, F. (2009). Hybrid warfare and challenges. Small Wars Journal. Retrieved from https://smallwarsjournal.com/documents/jfqhoffman.pdf (accessed 06/04/2025).

INCIBE (2024). DANGER: Cybersecurity for detection, analysis and filtering of fake or malicious content in hyper-connected environments. Retrieved from https://www.incibe.es/node/521663 (accessed 06/04/2025).

Jamieson, K. H., & Cappella, J. N. (2008). *Echo chamber: Rush Limbaugh and the conservative media establishment.* Oxford University Press.

Jordán, J. (2018). International conflict in the grey zone: a theoretical proposal from the perspective of offensive realism. Revista Española de Ciencia Política, No. 48. Retrieved from https://www.ugr.es/~jjordan/Conflicto-zona-gris.pdf

(accessed 20/08/2024).

Juurvee, I., & Mattiisen, M. (August 2020). The bronze soldier crisis of 2007: Revisiting an early case of hybrid conflict. International Centre for Defence and Security. Retrieved from https://bit.ly/3iRyeZe (accessed 06/04/2025).

Latam Chequea (2022). Fake news about COVID-19 verified by Latam Chequea network. Retrieved from https://chequeado.com/investigaciones/como-la-desinformacion-sobre-covid-19-infecto-a-america-latina (accessed 14/08/2024).

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... & Rothschild, D. (2018). The science of fake news: A research agenda. Science, 359(6380), 1094-1096. Retrieved from https://doi.org/10.1126/science.aao2998 (accessed 14/08/2024).

Libicki, M. C. (2021). Cyberspace in Peace and War. Naval Institute Press. Retrieved from https://www.researchgate.net/publication/343399173_Military_Operations_in_Cyberspace (accessed 06/04/2025).

Lupiáñez Lupiáñez, M. (2023). How to deal with a cognitive attack: Prototype detection of propaganda and manipulation in psychological operations targeting civilians during a conflict. Revista del Instituto Español de Estudios Estratégicos, (22), 61-93. Retrieved from https://revista.ieee.es/article/view/6058 (accessed 14/08/2024).

MAEUEC, Ministry of Foreign Affairs, European Union and Cooperation (2021). External Action Strategy 2021-2024. Retrieved from https://www.exteriores.gob.es/estrategia2021-2024.pdf (accessed 14/08/2024).

Maggioni, M., & Magri, P. (2018). Twitter and Jihad: The Communication Strategy of ISIS. Journal of Cyberspace Studies, 2(2), 239-241. Retrieved from https://doi.org/10.22059/jcss.2018.66728 (accessed 14/08/2024).

Maldita.es (2023). What is prebunking? This is how this technique works against disinformation before it spreads. Retrieved from https://maldita.es/nosotros/20230323/prebunking-que-es-antes-desmentido (accessed 06/04/2025).

Marchal González, A. N. (2023). The need for a new type of crime: Disinformation as a threat to public order. Boletín Criminológico, 1(2023), 1-14. Retrieved from https://revistas.uma.es/index.php/boletin-criminologico/article/view/17222/17250 (accessed 06/04/2025).

Martín Renedo, S. (2022). Grey Zones on the ground: the end of conventional wars? IEEE Opinion Paper 93/2022. Retrieved from https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO93_2022_SAUMAR_Zonas.pdf (accessed 06/04/2025).

Mayoral, J, Parratt, S, & Morata, M. (2019). Journalistic disinformation, manipulation and credibility: a historical perspective. History and Social Communication, 24(2), 395-409. Retrieved from https://revistas.ucm.es/index.php/HICS/article/view/66267 (accessed 06/04/2025).

McCuen, J. (2008). Hybrid Wars. Military Review, 88(2), 107-113. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20080430_art017.pdf (accessed 06/04/2025).

McIntyre, L. (2018). Posverdad. Madrid: Cátedra.

MPJRC. Ministry of the Presidency, Justice and Relations with the Courts (2024). Action plan for democracy. Retrieved from https://www.mpr.gob.es/prencom/notas/Documents/2024/2024-3002_Plan_de_accion.pdf (accessed 06/04/2025).

Newtral (2022). Qatar World Cup, a showcase for hoaxes and misinformation. Retrieved from https://www.newtral.es/bulos-mundial-catar/20221203 (accessed 06/04/2025).

Novoa-Jaso, M. F., Sierra, A., Labiano, R., & Vara-Miguel, A. (2024). Digital News Report Spain 2024. Journalistic quality and plurality: Keys to news trust in the age of artificial intelligence (AI). Servicio de Publicaciones de la Universidad de Navarra. Retrieved from https://www.unav.edu/documents/98033082/0/DNR_2024.pdf (accessed 14/08/2024).

OECD (2024), Facts versus falsehoods: Strengthening democracy through information integrity, OECD. Publishing, Paris. Retrieved from https://doi.org/10.1787/06f8ca41-es (accessed 14/08/2024).

Olmo, J. A. (2019). Disinformation: concept and perspectives. Real Instituto Elcano. Retrieved from https://www.realinstitutoelcano.org/analisis/desinformacion-concepto-y-perspectivas (accessed 06/04/2025).

WHO, World Health Organization (2020). Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation. Retrieved from https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation (accessed 14/08/2024).

Order PCM/1030/2020, of 30 October, which publishes the Procedure for action against disinformation approved by the National Security Council (2020). *Official State Gazette*. Retrieved from https://www.boe.es/buscar/doc.php?id=BOE-A-2020-13663 (accessed 14/08/2024).

Order PJC/248/2025, of 13 March, publishing the Agreement of the National Security Council of 28 January 2025, approving the procedure for the preparation of the National Strategy against Disinformation Campaigns (2025). Official State Gazette. Retrieved from https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-5151

NATO (2021, 12 August). Countering disinformation: improving the Alliance's digital resilience. Retrieved from https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html (accessed 14/08/2024).

NATO, Headquarters (2024). Hybrid threats and hybrid warfare: Reference curriculum. Retrieved from

https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf (accessed 14/08/2024).

PDC-01. Joint Doctrinal Publication PDC-01 (A) Doctrine for the employment of the Armed Forces. Defence Staff, 2018. Retrieved from https://publicaciones.defensa.gob.es/pdc-01-a-doctrina-para-el-empleo-de-las-fas-libros-papel.html (accessed 14/08/2024).

Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. Trends in Cognitive Sciences, 25(5), 388-402. Retrieved from https://www.cell.com/trends/cognitive-sciences/fulltext/S1364-6613(21)00051-6 (accessed 06/04/2025).

Pennycook, G., Bear, A., Collins, E. T., & Rand, D. G. (2020). Fighting misinformation on social media using crowdsourced judgments of news source quality. Proceedings of the National Academy of Sciences, 117(7), 2775-2785. https://www.pnas.org/doi/abs/10.1073/pnas.1806781116 (accessed 02/06/2025).

Posetti, J., & Matthews, A. (2018). A short guide to the history of 'fake news' and disinformation. International Center for Journalists. Retrieved from https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf (accessed 06/04/2025).

Quiñones de la Iglesia, F. J. (2021). Disinformation and subversion (2.0): Cold War techniques reappear in the 21st century information domain. IEEE Framework Document 12/2021. Retrieved from https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM12_2021_FRAQUI_Desinformacion.pdf (accessed 06/04/2025).

Reuters Institute for the Study of Journalism (2024). Digital News Report 2024. Oxford University. Retrieved from https://reutersinstitute.politics.ox.ac.uk/es/digital-news-report/2024 (accessed 06/04/2025).

Rid, T. (2021). Disinformation and political warfare. Barcelona: Crítica.

Rodrigo Alsina, M. (2005). La construcción de la noticia. Retrieved from https://www.um.es/tic/LIBROS%20FCI-I/La%20produccion%20de%20la%20noticia.pdf (accessed 20/08/2024).

Rodríguez Lorenzo, E, Morales, R, Crescente, D, Cabello, M. I, & Paz, I. (2023). Artificial intelligence in hybrid warfare as a weapon of disinformation. IEEE Opinion Paper. Retrieved from https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO61_2023_EDUROD_Inteligencia.pdf (accessed 06/04/2025).

Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S., & Lewandowsky, S. (2022). Psychological inoculation improves resilience against misinformation on social media. *Science Advances, 8.* Retrieved from https://www.science.org/doi/10.1126/sciadv.abo6254 (accessed 06/04/2025).

Sartori, G. (2007). Politics. Lógica y métodos en las ciencias sociales. Fondo de Cultura Económica. Retrieved from https://maestriainap.diputados.gob.mx/documentos/materia1/sem1/02.pdf (accessed 06/04/2025).

EEAS. (2023). Tackling disinformation: Foreign Information Manipulation and Interference (FIMI). Retrieved from https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en (accessed 14/08/2024).

Tandoc, E. C., Jr., Lim, Z. W., & Ling, R. (2018). Defining fake news: A typology of scholarly definitions. Digital Journalism, 6(2), 137-153. Retrieved from https://doi.org/10.1080/21670811.2017.1360143 (accessed 06/04/2025).

Terán, E. (2019). Disinformation in the EU: Hybrid threat or communicative phenomenon? Evolution of EU strategy since 2015 https://www.idee.ceu.es/Portals/0/Desinformaci%C3%B3n%20en%20la%20UE..pdf (accessed 06/04/2025).

Torres, C. M. (2021). Fake news: the influence of post-truth and disinformation in contemporary politics. Communication and Society, 18(2), 199-217. Retrieved from https://revistas.javeriana.edu.co/index.php/comunicacionysociedad/article/view/31487 (accessed 14/08/2024).

Torres-Soriano, M. R. (2022). Influence operations vs. disinformation: differences and points of connection. Retrieved from https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO64_2022_MANTOR_Operaciones.pdf (accessed 01/06/2025).

Supreme Court (2021, 18 October). Sentencia STS 1238/2021. Retrieved from https://vlex.es/vid/877507365 (accessed 14/08/2024).

Tuñón Navarro, J., Oleart, Á., & Bouza García, L. (2019). European Actors and Disinformation: the dispute between fact-checking, alternative agendas and geopolitics. Journal of Communication and Digital Citizenship, 8(1), 223-238. Retrieved from https://www.redalyc.org/journal/5894/589466348012 (accessed 06/04/2025).

Walker, R. G. (1998). Spec Fi: The United States Marine Corps and Special Operations. Monterey, Naval Postgraduate School. Retrieved from https://apps.dtic.mil/sti/pdfs/ADA359694.pdf (accessed 14/08/2024).

Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe. Retrieved from https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-resear/168076277c (accessed 14/08/2024).

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Research Article

INTELLIGENCE IN THE SPOTLIGHT: FROM CLASSICAL THEORY TO A NEW APPROACH TO IMPLEMENTATION IN THE DIGITAL AGE

English translation with AI assistance (DeepL)

Paula Castro Castañer
Security expert at Telefónica S.A.
PhD candidate in Forensic Sciences at the University of Alcalá
Master in Cybersecurity and Privacy by the Universitat Oberta de Catalunya (UOC)
paula.castroc@edu.uah.es
ORCID: 0009-0008-0315-8387

Received 14/02/2025
Accepted 16/06/2025
Published 27/06/2025

Recommended citation: Castro P. (2025). Intelligence in the spotlight: From classical theory to a new approach to implementation in the digital age. *Logos Guardia Civil Magazine*, 3(2), p.p. 71-100.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

ORCID: **0009-0008-0315-8387**

DEDICATION

To my tutor, Hilario, for trusting me and supporting me in all my projects.

ORCID: **0009-0008-0315-8387**

INTELLIGENCE IN THE SPOTLIGHT: FROM CLASSICAL THEORY TO A NEW APPROACH TO IMPLEMENTATION IN THE DIGITAL AGE

Abstract: This article addresses the evolution of intelligence in the field of Defence and Security, from traditional approaches to its adaptation to the digital era, establishing a proposal that responds to some of the limitations pointed out in the literature on the classic intelligence cycle. To this end, key concepts are explored, such as the definition of the concept of intelligence, the different types of intelligence and even the traditional intelligence cycle and its phases. In addition, a review of the evolution and the different approaches that have been adopted throughout history in the field of intelligence is presented. Finally, it proposes an intelligence model, called IDEM, with flexible phases and combining human analyst talent and automated big data processing to ensure proactive, adaptive and quality intelligence in the face of complex transnational cyber threats.

Resumen: Este artículo aborda la evolución de la inteligencia en el ámbito de la Defensa y Seguridad, desde los enfoques tradicionales hasta su adaptación a la era digital, estableciendo una propuesta que responda a algunas de las limitaciones señaladas en la literatura sobre el ciclo clásico de inteligencia. Para ello se exploran conceptos clave como la definición del concepto de inteligencia, los diferentes tipos de inteligencia e incluso el tradicional ciclo de inteligencia y sus fases. Además, se presenta una revisión de la evolución y de los diferentes enfoques que se han ido adoptando a lo largo de la historia en materia de inteligencia. Por último, se propone un modelo de inteligencia, denominado IDEM, con fases flexibles y que combine el talento del analista humano y el procesamiento automatizado de grandes volúmenes de datos para garantizar una inteligencia proactiva, adaptativa y de calidad ante las complejas amenazas cibernéticas transnacionales.

Keywords: cyber threats, cyber intelligence, intelligence cycle, IDEM model, networked approach.

Palabras clave: Amenazas cibernéticas, ciberinteligencia, ciclo de inteligencia, modelo IDEM, enfoque en red .

ORCID: **0009-0008-0315-8387**

ABBREVIATIONS

ABI: *Activity-based Intelligence*

CCN-CERT: National Cryptologic Centre - *Computer Emergency Response* Team

CESID: Centro Superior de Información de la Defensa (High Defence Information Centre)

CIA: *Central Intelligence Agency*, Central *Intelligence Agency*

CIFAS: Centre of Intelligence of the Armed Forces

CNI: National Intelligence Centre

COMINT: *Communications Intelligence*

COP*: Community Policing*, *Community-oriented* policing

CTI: *Cyber Threat Intelligence*, Cyber Threat *Intelligence*

CYBINT: *Cyber-Intelligence*, Cyberintelligence

ELINT: *Electronic intelligence*

FISINT: *Foreign* instrumentation *signals intelligence*

GEOINT: *Geospatial Intelligence*, Geospatial *Intelligence*

HUMINT: *Human Intelligence*

IDEM: Enhanced Dynamic Intelligence Enrichment and Enhancement

IDS: *Intrusion Detection System*, *Intrusion Detection* System

ILP*: Intelligence-Led Policing*, *Intelligence-led Policing*

IMINT: *Imagery Intelligence*

ISR: *Intelligence Surveillance and Reconnnaissance)*, *Intelligence*, *Surveillance* and *Reconnaissance*

JISR: *Joint Intelligence Surveillance and Reconnnaissance)*, *Joint Intelligence*, Surve*illance* and *Reconnaissance*

MASINT: Measurement and *Signature Intelligence*

ML: *Machine Learning*, Machine Learning

NLP: *Natural Language Processing*

OSCE: *Organisation for Security and Co-operation in Europe*, Organisation *for Security and Co-operation* in Europe

OSINT: *Open-Source Intelligence*

SCADA: *Supervisory Control* and *Data Acquisition*

SECED: Central Documentation Service

SIEM: *Security Information* and *Event Management*

SIGINT: Signal *Intelligence*

SOCMINT: *Social Media Intelligence,* Social Media Intelligence

TCPED: *Tasking, Collection, Processing, Exploitation, Dissemination,* Approach, Collection, Processing, Exploitation*, Dissemination*

TTPs: *Threats, Techniques and Procedures*

ORCID: **0009-0008-0315-8387**

1. INTRODUCTION

In a world where Artificial Intelligence seems to dominate much of the public attention and concern, where does intelligence in all its other guises take a back seat? The omnipresence of Artificial Intelligence in contemporary debates often overshadows the importance of other types of intelligence that are fundamental to human progress and development.

Human intelligence, in its many manifestations, remains an irreplaceable pillar for the prosperity of society, even more so in the complex and changing contexts of this Digital Age. One of these manifestations is competitive intelligence, which makes it possible to obtain actionable recommendations by processing information about the external environment in search of opportunities or developments that could impact the competitive position of a company or country (Lee, 2023). Or prospective intelligence, which, based on past and present information, as well as future speculations, attempts to "draw" a cognitive map to determine different options and reduce the level of uncertainty that accompanies any decision (Montero Gómez, 2006).

It is true that the exponential growth of digitisation, exposure and globalisation is driving the origin and evolution of new forms of intelligence in response to new technologies and data collection methods, giving birth to intelligences such as open source intelligence (OSINT) or geospatial intelligence (GEOINT), among others. These disciplines take advantage of the vast amount of information available to provide a comprehensive, integrated and detailed view of various phenomena. However, intelligence should not be limited to data collection and analysis, but should also integrate ethical considerations and assess the potential long-term consequences of decisions.

Today, information and technology are vital to almost every aspect of life, and intelligence plays a crucial role especially in the field of cyber security, as the ability to anticipate, identify and mitigate threats is essential to preserve the integrity, confidentiality and availability of systems.

However, the question arises: is this capability a reality in today's government and private agencies, is intelligence effective in anticipating and mitigating the growing risks in cyberspace, and is the intelligence cycle up to date to meet the demands of the Digital Age? This paper sets out to conduct a theoretical analysis to address these questions and assess the effectiveness of intelligence in the current context.

1.1. METHODOLOGICAL NOTE

For the development of this work, a narrative review of the academic and technical literature related to intelligence in the fields of defence and security, as well as its adaptation to the digital environment, has been carried out. This review has served as a basis for contextualising the evolution of the concept, critically analysing the classic intelligence cycle and providing the basis for the proposal of the IDEM model.

The search was conducted in academic databases such as Scopus, Google Scholar and Dialnet, as well as national and international institutional sources. Keywords in Spanish and English were used, such as "intelligence cycle", "cyber intelligence", "cyber threat intelligence" or "cyber threats". Priority was given to recent publications (2000-

2024) that offered theoretical approaches, methodological models or critical analyses of the intelligence process. Occasionally, due to the lack of open source literature, reputable websites or websites written by technical specialists in the field were consulted.

Documents without academic or institutional support were excluded, as well as texts that did not specifically address the structural or process dimension of intelligence. The selected literature was organised around five thematic axes: (1) definition of the concept of intelligence, (2) classification of types of intelligence, (3) historical and organisational evolution of intelligence services, (4) critical review of the traditional cycle and (5) contemporary proposals for its adaptation to the digital era.

This methodological approach has made it possible to detect relevant theoretical gaps and serve as a basis for the development of an updated model that integrates both the human dimension and the technological capabilities of intelligence today.

2. CONCEPT AND EVOLUTION OF INTELLIGENCE

The term intelligence is an abstract and complex concept to delimit due to the multitude of approaches under which it can be studied. This difficulty not only responds to the diversity of areas that analyse it, but also to the challenges within the same context to establish a single definition.

In the field of defence and security, most authors link the birth of intelligence to the emergence of states and inter-state relations. However, there is no consensus on the definition of intelligence, largely due to the different approaches adopted in practice by different countries (Andric & Terzic, 2023). This disparity hinders both the theoretical progress of its study and an in-depth understanding of the various dimensions and factors that affect its practice (Payá-Santos, 2023).

In this context, one of the first fundamental classifications, the trinity, was established by Sherman Kent, defining three realities for this concept: intelligence as an organisation, as a process and as an outcome (Díaz Fernández, 2013).

- **Intelligence as an organisation:** refers to intelligence services mainly under the umbrella of the public administration, as in the case of the National Intelligence Centre (CNI) and the Armed Forces Intelligence Centre (CIFAS) in Spain. The functions of these institutions include obtaining, evaluating, interpreting and disseminating intelligence to protect and promote Spain's interests, both inside and outside the country; preventing, detecting and neutralising threats to the constitution, rights and freedoms, sovereignty, state security, institutional stability and the welfare of the population; promoting cooperation with foreign intelligence services and international organisations; interpreting strategic signal traffic; coordinating the use of encryption means; guaranteeing the security of classified information; and protecting its own facilities, information and resources (Jefatura del Estado, 2002).
- **Intelligence as a process**: comprises all activities, generally encompassed in the so-called intelligence cycle (discussed in greater depth in later sections), that are necessary to meet the demands of leaders and that interpret an environment, context or problem. These activities are considered a continuous cyclical process and range from the collection of information from various sources, continuing

with its subsequent analysis and processing, to the dissemination of the data of interest to end users (Chainey & Chapman, 2013).

- **Intelligence as a product:** refers to the result and/or knowledge obtained, in any format, after the intelligence cycle. This product should influence decision-making and impact the interpreted context (Chainey & Chapman, 2013).

Recently, a fourth dimension has also been proposed: **intelligence as culture,** defined by Navarro as "the set of initiatives and resources that promote awareness of its necessity and provide civic understanding of its reality" (Payá-Santos, 2023).

Regardless of the interpretation adopted, intelligence aims to reduce the uncertainty intrinsic to the human condition and the complexity of the contemporary world in decision-making to prevent and avoid any danger or threat (Jordan, 2015).

To achieve this, intelligence draws on theoretical knowledge related to politics, economics, international relations, security, sociology, technology, psychology and so on. Hence, it is essential to present high-quality teams of experts in the different subject areas in order to address problems from multiple perspectives and find more effective solutions with a cross-cutting approach.

The recent multidisciplinary aspect of intelligence is a consequence of the broadening of the concept of security and the growing complexity of the societal context where asymmetric threats and cyber warfare are increasingly common.

In contrast, one of the oldest qualities of intelligence is the secrecy of its activities and information obtained. However, the growing use of open source (OSINT) is changing this perspective. In addition, globalisation and the expansion of internet use also affect conflicts, which are increasingly transnational and require international intelligence cooperation. Still, the protection of sources, especially human sources (HUMINT) remains a fundamental principle, as does the need to preserve discretion in the handling of information to avoid countermeasures, disinformation or breach of sensitive operations.

In short, it could be established that intelligence encompasses the process, the product and the institution that carries out the collection, evaluation and processing of information (Knight, 2024) as a decision-making tool, in order to identify, warn and prevent risks and threats, reducing uncertainty (Francisco & Barrilao, 2019). To achieve this, these tasks must be performed in an intentional, timely, planned, "secret" and organised manner (Andric & Terzic, 2023).

2.1. TYPES OF INTELLIGENCE

There are various classifications of intelligence, but one of the most common is according to the medium in which the information is found, establishing the following types (Kamiński, 2019):

- **SIGINT** (*Signal Intelligence*): is derived from intercepts of signals regardless of how they are transmitted. There are three subcategories: communications intelligence (COMINT), electronic intelligence (ELINT) and foreign

instrumentation signals intelligence (FISINT). It is particularly relevant in monitoring digital threats and hybrid conflicts.

- **MASINT** *(Measurement and Signature Intelligence)*: based on the measurement of physical attributes, such as electromagnetic emissions, chemical properties or acoustic characteristics. It is used in advanced military operations and weapons detection for the purpose of characterising, locating and identifying targets.
- **HUMINT** (*Human Intelligence)*: is the oldest method of gathering information from human sources, whether through interviews, direct observation, infiltration or collaboration with local actors. It is essential in contexts where technologies cannot access it.
- **GEOINT** *(Geospatial Intelligence)* and **IMINT** *(Imagery Intelligence):* geospatial and imagery intelligence. The former combines maps, geographic data and remote sensing information, while the latter focuses on visual analysis of satellite, aerial or drone imagery.
- **OSINT** *(Open-Source Intelligence)*: intelligence derived from publicly available information in physical, analogue or digital format in different media, such as radio, television, newspapers, magazines, the Internet, commercial databases, videos, graphics, drawings, social networks, etc. open or public reports. Their volume, accessibility and usefulness have increased exponentially with the Internet (Stewart Bertram, 2015).
- **SOCMINT** *(Social Media Intelligence*): sometimes also referred to as a subcategory of OSINT, focusing on social media. It is used to monitor trends, detect emerging threats, analyse perceptions and track specific actors (Mahood, 2015).

However, another very common typification is according to their purpose: strategic, tactical and operational (Gruszczak, 2018).

- **Strategic intelligence:** focuses on identifying risks, threats and opportunities to support the definition of objectives and decision making, considering the environment, relevant actors, and possible evolutions.
- **Tactical intelligence**: focuses on the planning and execution of specific operations to achieve an objective of limited scope, derived from the broad objectives of strategic intelligence.
- **Operational intelligence**: also known as operational intelligence in the military sphere, its purpose is to enable the organisation and execution of activities to fulfil a specific mission (Jiménez Villalonga, 2018).

The coexistence and complementarity between these categories makes it possible to build a comprehensive intelligence, adapted to different levels of decision-making.

2.2. EVOLUTION OF INTELLIGENCE APPROACHES AND STRATEGIES

Numerous authors maintain that intelligence is as old as the history of mankind, given that hiding confidential information and discovering that of adversaries has always been a tool for achieving and maintaining power. This is evidenced by civilisations such as ancient China with the millenary wisdom of the master Sun Tzu (Navarro Bonilla, 2005) or classical Greece with the secret information transmission procedures of Aeneas the Tactician (Vela Tejada, 1993).

Originally, intelligence was a tool at the service of political power, with an eminently military focus: to know the enemy's strength, location and capabilities in order to facilitate the leader's decision-making. However, as societies became more complex, so did their threats, which led to the progressive expansion of intelligence towards social, economic or political aspects. Thus, intelligence activities took on a crucial role with the birth of states and the relations between them, with the aim of defending and protecting national interests (Andric & Terzic, 2023).

However, it was not until the mid-20th century, especially after the two world wars and the Cold War, that the global powers began to formally organise their intelligence services (the United States with the CIA, the United Kingdom with MI6 and Israel with the Mossad).

Spain, although less prominent internationally in this field, also made the first attempt to establish an intelligence service around this time. In 1972 the Central Documentation Service (SECED) was created and in 1977 the Higher Defence Information Centre (CESID), but it was not until 2002 that the current CNI (National Intelligence Centre, 2023) was founded.

From that point onwards, the technological revolution and the explosion in the volume of information available marked a radical change: intelligence ceased to be a closed and exclusively state-centric domain and became a cross-cutting, dynamic activity with implications beyond the political-military sphere. Although the essence of intelligence remains the same, the methods, timing and objectives have undergone profound transformations. Massive access to data through open sources, the acceleration of information flows and the globalisation of threats have reduced the life cycle of information and called into question the central role previously occupied by secrecy (Payá-Santos, 2023).

This new context was compounded by the 9/11 attacks, which marked a turning point, highlighting the need to identify and prevent asymmetric and transnational threats, blurring the classic distinction between internal and external intelligence, and pushing police institutions to adopt more analytical, preventive and collaborative models (Knight, 2024).

With the progressive extension of intelligence into other strategic areas, such as policing, which had historically operated with a reactive logic, police functions began to evolve significantly. Its classic approach, focused on responding to completed crimes or responding to requests for service, was challenged as social changes and the increasing complexity of crime demanded new forms of intervention (Organisation for Security and Cooperation in Europe, 2017). Thereafter, various philosophical currents influenced policing such as (Gkougkoudis et al., 2022):

- ***Community Policing*** **or** ***Community-oriented policing*** **(COP):** prioritises cooperation between citizens and law enforcement agencies, fostering trust and prevention (Carter & Fox, 2019).
- ***Problem Solving*** **Policing**: aimed at identifying and analysing the problems underlying crime from a broader, cross-cutting perspective and seeking structural and sustainable solutions (Organisation for Security and Cooperation in Europe, 2017).

- ***Zero Tolerance Policing*:** strict response to even minor offences, based on ideas developed by two American criminologists, James Q. Wilson and George Kelling, who in 1982 published an article entitled "Broken Windows" (Grabosky, 1999).

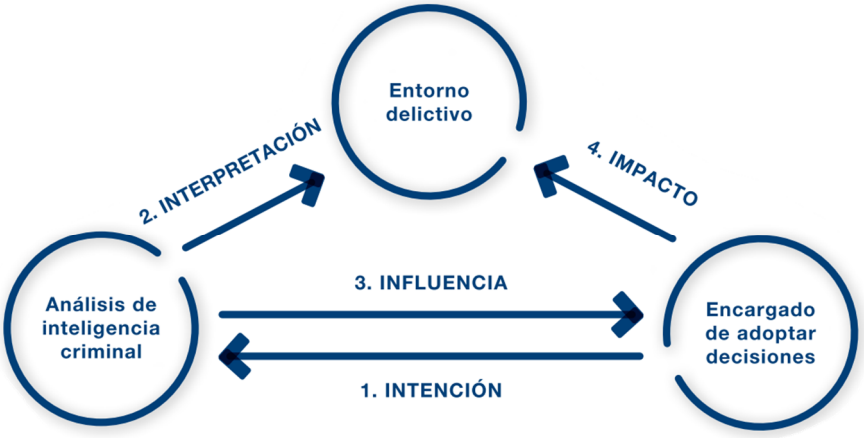
However, in recent decades, due to the complexity of threats and risks, many academics and practitioners have pointed out that the most successful holistic approach to combating the globalisation of crime is *Intelligence-Led Policing* (ILP), which translates as intelligence-led policing. This approach emerged in the 1990s in the UK as a strategy to improve the fiscal efficiency of police services, i.e. to optimise resource allocation, operational productivity and the quality of policing outcomes. Initially implemented primarily to combat serious and organised crime, it has since evolved globally as a proactive model, driven by data analytics and focused on preventing, reducing and disrupting all types of crime. In the United States, it was the events of 11 September 2001 that finally prompted its adoption, focusing its approach on more complex forms of criminality (Summers & Rossmo, 2019).

ILP is a proactive philosophy to identify and prevent criminal problems using raw data and mixed (quantitative and qualitative) analysis, but it is not a point tactic, but a flexible, adaptive and sustainable framework based on objective data (Carter & Fox, 2019). However, its implementation faces challenges in terms of terminological clarity and data integration, as well as the need to ensure respect for human rights in intelligence management.

In parallel, the Activity-Based Intelligence (ABI) model has expanded analytical capabilities, especially in the face of emerging threats. With antecedents in the Cold War, its development has been driven by the need to manage and analyse huge volumes of data generated by modern technologies, such as drones and social media, especially in the context of counter-terrorism. Traditional methods of analysis have proven inadequate in this new environment, as analysts spend too much time searching for information and monitoring known targets, limiting their ability to uncover the unknown. ABI enhances this process by enabling real-time correlation of data from a variety of sources, overcoming the limitations of traditional intelligence, surveillance and reconnaissance (ISR) methods (Atwood, 2015).

Another relevant approach is the 3i model proposed by Ratcliffe in 2006 based on three fundamental pillars: 'interpreting', 'influencing' and 'impacting' the criminal environment. Analysts must actively interpret the environment, influence decision-makers who, in turn, use that intelligence to design strategies that affect the criminal environment (Budhram, 2015). In 2016 he added a further i, that of intent, as can be seen in Figure 1, highlighting the need for clarity and understanding of the objectives set (Organisation for Security and Cooperation in Europe, 2017).

Figure 1
Ratcliffe's 4-i model: intention, interpretation, influence and impact



Note: Adapted from *OSCE Guidance on Intelligence-led Policing (p. 24),* by *OSCE, 2017, OSCE. Intelligence-led Policing* (p. 24), by OSCE, 2017, OSCE

In short, intelligence has evolved from a highly secretive and centralised activity to a cross-cutting, interdisciplinary, distributed and technologically supported process. This evolution justifies the need for new models such as IDEM, which integrate human analysis with automated processing to address modern threats, especially in cyberspace. Moreover, this trajectory allows us to observe a growing convergence between security, defence and technology logics, positioning intelligence as a key component of digital sovereignty and institutional resilience.

3. THE INTELLIGENCE CYCLE

Although Sherman Kent is often credited with the scientific formulation of the intelligence method, subsequent research has shown that a rigorous methodology and a comprehensive set of operations (what later became known as the intelligence cycle) were already outlined, for example, during the Spanish Civil War (Navarro Bonilla, 2004).

The intelligence cycle brings together all the activities that enable the transformation of raw information into intelligence and, as its name suggests, is cyclical in nature. The classic intelligence cycle has four phases, but in some countries different phases or differentiated sub-phases are added. For example, in Spain, the CCN-CERT establishes six phases for the intelligence cycle: direction and planning; collection; transformation; analysis and production; dissemination and, finally, evaluation (National Cryptologic Centre, 2015).

- The first phase, called **direction and planning**, establishes the what and the how, i.e. the requirements of the intelligence product to be produced and the actions to be taken to obtain it. The subject of the study, scope, objectives, deadline and type of report should be clear so that the work in the remaining phases is efficient and results in higher quality and in line with national and international legal standards (Organisation for Security and Cooperation in Europe, 2017).

- In the next stage, **collection,** raw data are collected, e.g. from the sources mentioned above (SIGINT, MASINT, HUMINT, GEOINT, IMINT, OSINT). This process is complex, as analysts must strike the right balance between collecting all necessary and sufficient data without falling into redundant information overload. To do so, they must be aware of the existence, relevance, accessibility and reliability of the selected sources, as well as legal constraints and authorisation requirements (Organisation for Security and Cooperation in Europe, 2017). In addition, the validity and accuracy of the information should be assessed before proceeding with the remaining steps of the intelligence cycle.
- In the **transformation** phase, the raw data collected in the previous stage is converted into structured sets such as databases, bibliographic references, etc., transforming the information into those formats necessary to continue the cycle and obtain intelligence. This stage involves cataloguing, prioritising and referencing the information collected.
- The fourth phase, **analysis and production**, is composed of the activities through which the transformed information is integrated, evaluated, analysed and prepared in order to obtain the final product. Within this stage, two sub-phases can be established: the first involves integrating data obtained from different sources to establish hypotheses and identify a pattern of intelligence; the second involves interpreting the data, i.e. going beyond the information obtained, refuting or supporting the pre-established hypotheses (Organisation for Security and Cooperation in Europe, 2017). Generally, this phase results in what is called *actionable intelligence, an* intelligence product that meets the requirements defined in the steering and planning phase and thus the needs of the consumer. This product in turn can be of many types, such as a trend analysis, a long-term assessment, a current intelligence, an estimation or warning intelligence, etc. (National Cryptologic Centre, 2015).
- In the **dissemination** stage, the final product is delivered to the consumer who has requested it and if necessary, and legally admissible, it will also be shared with other stakeholders.
- The last phase corresponds to the **evaluation** which allows for continuous feedback of all previous phases of the intelligence cycle with the results obtained, allowing for adjustment and refinement of both the individual activities and the cycle as a whole. This is particularly useful in order to meet changing intelligence needs in an optimal way.

However, many experts question this traditional model of intelligence and one of the criticisms voiced is the oversimplification of this model compared to the great complexity of the actual process of gaining intelligence. Robert Clark points out that this term "has become a theological concept: no one questions its validity", even though it does not set out the precise steps to be followed (Phythian et al., 2013).

Furthermore, Arthur Hulnick points out that the notion that intelligence customers guide producers at the beginning of the cycle is incorrect, as customers often expect to be alerted by the intelligence system, so the collection process is mostly driven by the need to fill data gaps and not by policy guidance (Pothoven et al., 2023).

On the other hand, it is not always the case that data collection bodies are approached; often existing databases that have been fed for years are consulted directly

to prepare a report. Or new raw data may be requested from the teams that collect it, but a new demand for intelligence is not usually made at the client level (Jordán, 2011).

As for the analysis phase, its definition within the intelligence cycle is not criticised in itself, but it is stated that it is the stage in which most mistakes are made, not due to a lack of information, but rather the opposite, due to data overload that leads to relevant information being ignored or inadequately interpreted by analysts (Jordán, 2016). Analysts need to be aware of their own mental processes and potential errors, avoiding unintentional cognitive simplifications and, of course, biases. Moreover, in some cases, such as in crisis situations, raw data arrives directly without going through this phase.

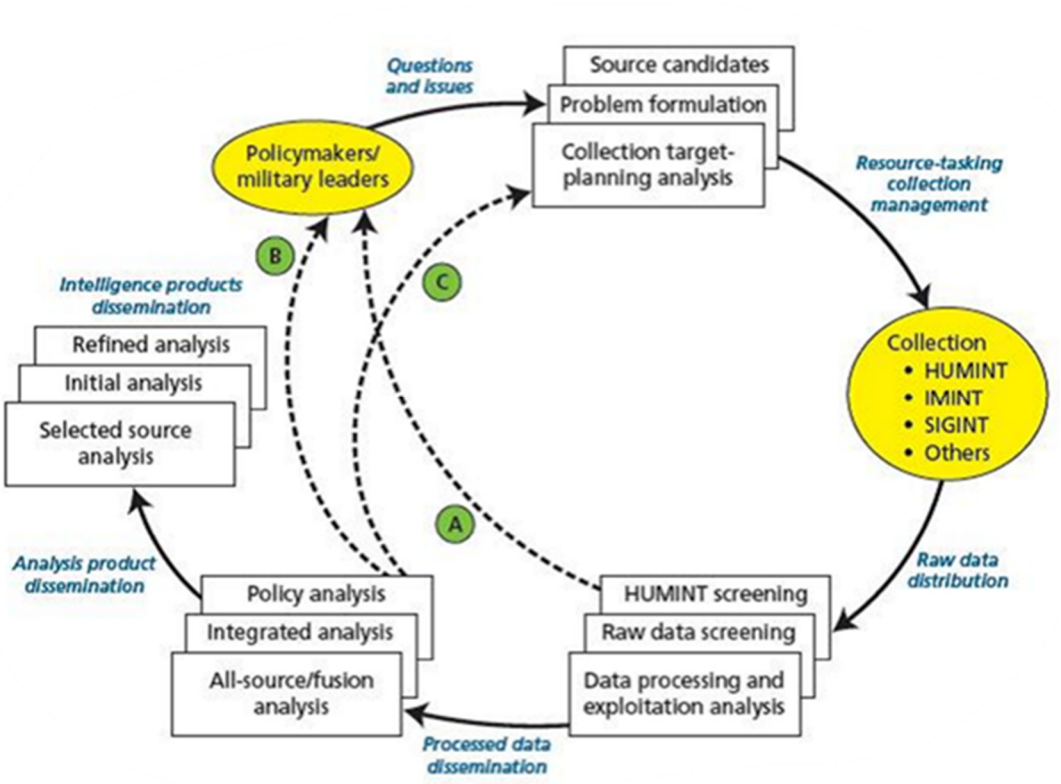
With regard to the dissemination phase, this is sometimes not passed through either, as not all the analyses produced reach the consumers. Many are not read by the recipients and are stored directly in the internal database. In other cases, customers often have already made their decisions and ignore the intelligence that does not support them.

Also, in relation to the intelligence cycle in general, its definition as a sequence of phases that is finally arranged in a circular fashion is criticised, when it is a more dynamic process, where all the phases feed back on each other, and can move forward and backward in any direction within the cycle. It also points to organisational, command and information flow problems that lead to a lack of flexibility in action and communication, slowing down decision-making processes (Organisation for Security and Cooperation in Europe, 2017).

Commentators such as Peter Gill and Mark Phythian argue that the concept of the intelligence cycle has been rendered obsolete by technological advances, the information revolution and changes in threats and targets. They propose replacing it with an 'intelligence network' that better reflects the complex interactions between targeting, collection and analysis, and highlights the contextual factors that influence the process and can be affected by its outcomes (Pothoven et al., 2023).

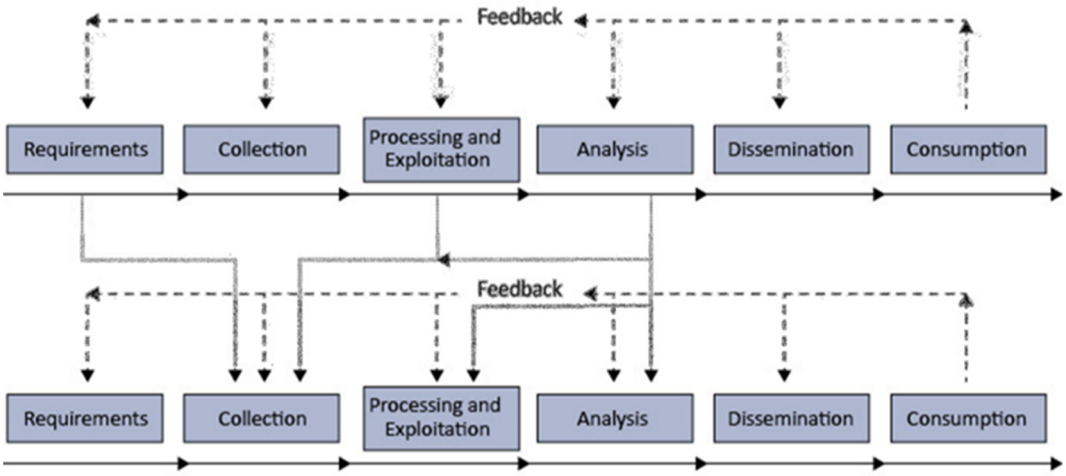
On the other hand, several authors have tried to capture the complexity of the intelligence cycle in alternative schemes to the traditional one. As can be seen inFigure2 , Treverton and Gabbard propose a more realistic approach that includes shortcuts between phases, showing that there are steps that are sometimes missed, for example that unanalysed information may reach decision-makers directly. Mark Lowenthal presents a cycle composed of constant feedbacks, where new needs and ambiguities reactivate the process, making it more dynamic and multi-layered, as can be seen inFigure3 . And Robert M. Clark introduces the *Target-Centric Intelligence* concept, a collaborative and target-oriented model, where all participants build together a shared picture of the intelligence issue of interest, represented in theFigure 4 (Jordan, 2016).

Figure2
Treverton and Gabbard's approach



Note: Taken from *A Review of the Intelligence Cycle* (p. 4) by J. Jordán, 2016, *GESI Analysis (Grupo de Estudios En Seguridad Internacional),* 2.

Figure3
Multi-strata process Mark Lowenthal



Note: Taken from *A Review of the Intelligence Cycle* (p. 5) by J. Jordán, 2016, *GESI Analysis (Grupo de Estudios En Seguridad Internacional),* 2.

Figure 4
Target-Centric Intelligence by Robert M. Clark

Note: Taken from *A Review of the Intelligence Cycle* (p. 6) by J. Jordán, 2016, *GESI Analysis (Grupo de Estudios En Seguridad Internacional),* 2.

Finally, proposals such as NATO's JISR (Joint Intelligence, Surveillance and Reconnaissance) concept have also emerged. This term refers to the integrated set of intelligence and operations capabilities that synchronises and integrates the planning and execution of all intelligence gathering capabilities with their processing, exploitation and dissemination. This concept arises from the need to improve information and intelligence sharing to prevent crises, terrorist threats, transnational criminal activities and cyber threats (Gruszczak, 2018). Intelligence, surveillance and reconnaissance (ISR) have

always been essential activities of military operations, but they were divided according to levels of command (strategic, operational and tactical), or according to the various intelligence disciplines, depending on the type and complexity of the information sources involved. In the current context this division limits the optimal use of intelligence specialists, agencies, sources and activities. Therefore, the JISR model is proposed where intelligence, surveillance and reconnaissance activities function as a single unit, integrating across all levels and domains (Ministry of Defence, 2023).

However, the JISR model presents the same process as the ISR, which is made up of 5 phases: planning, collection, processing, exploitation and dissemination (TCPED). The main difference with the traditional intelligence cycle is that this process is neither linear nor circular, but the different stages are executed dynamically, sequentially, simultaneously or independently, depending on the required result. However, in this model, the ISR process is usually aligned with the collection phase of the intelligence cycle, and the results of this collection are incorporated into the processing stage, as well as supporting the decision cycle.

However, this approach also faces several limitations. First, there may be a lack of sufficient resources to meet all requirements, especially due to the high demand and low availability of certain collection capabilities. There are also technical problems such as limitations in computational power and bandwidth, which affect the ability to process and disseminate results. Adversaries can interfere through attacks on ISR capabilities, camouflage, concealment and disinformation. In addition, access to ISR may be limited by physical, cognitive, virtual, legal and political barriers (Ministry of Defence, 2023).

Intelligence as a process today should therefore move away from traditional linear and cyclical models to more fluid and networked structures, able to respond nimbly to emerging threats and take advantage of the vast volume of available data (Jiménez Villalonga, 2018).

4. PROPOSAL FOR UPDATING THE INTELLIGENCE CYCLE IN THE DIGITAL AGE: THE IDEM MODEL

The classical intelligence cycle has for decades been the backbone of intelligence as a process. At the time, this sequential representation made sense, as it facilitated standardisation, analyst training and operations management. However, the model has significant limitations when transposed to today's contexts of complexity, uncertainty and rapid pace of change, especially in domains such as cyberspace.

In this highly dynamic environment, intelligence has become critically important as a tool for understanding and anticipating threats, particularly in the digital realm. As organisations expand their presence in cyberspace to maximise their visibility and reach, they also increase their exposure to potential attacks. This transformation requires rethinking the role of intelligence beyond its classic formulation, adapting it to the particularities of a decentralised, interconnected and constantly evolving environment.

However, this adaptation is not straightforward. The proliferation of terms and approaches reflects both the youth of the field and its rapid expansion. In some conceptual frameworks, the term cyber intelligence or CYBINT is used as a subtype of COMINT (Jiménez Villalonga, 2018), but it could also be considered as a type of higher intelligence

that encompasses and coordinates OSINT, SIGMINT, SOCMINT and even HUMINT activities (Portillo, 2019).

In the European context, it is more common to speak of cyber threat intelligence (CTI), which refers to the systematic application of intelligence to identify, analyse and mitigate threats affecting cyberspace. According to Gartner (Lee, 2023), CTI is based on evidence-based knowledge that provides context, mechanisms, indicators and practical advice on emerging or existing threats.

That is why CTI plays a crucial role in helping organisations develop a proactive security strategy that enables them to understand and anticipate adversaries' tactics, techniques *and* procedures (TTPs*)*. It also facilitates the identification of threats at their source and the effective response to incidents before they can cause significant damage.

However, when it comes to implementing research or working systems in this field, there is still an absence of specific and widely accepted methodological cycles to structure the process of cyber intelligence collection and analysis. Consequently, there is a tendency to fall back on the traditional intelligence cycle or one of the existing alternative approaches. But as noted, all of them have significant limitations for their effective application in digital environments.

The **classical model** is rigid and sequential; the **model proposed by Treverton and Gabbard** allows some flexibility, but lacks clear feedback; the **Target-Centric model** proposes a continuous cycle closer to the target, but without a really flexible structure between phases; and **Lowenthal's multilevel approach** introduces dynamism, but maintains a certain linearity and the bidirectional connections between phases are not fully understood.

Table 1
Comparative table of different models for representing intelligence as a process

	Classic model	Treverton and Gabbard model	Model by Mark Lowenthal	Target-Centric Model
Structure	Linear or cyclical (successive phases in a circle)	Semi-linear (with possible "short cuts")	Multi-level (with active layers as needed)	Cyclical (target focused)
Start of the process	At the request of the consumer	Similar to classic, but supports restarting from intermediate phases.	From new needs to reactivate previous phases	From target analysis (from previous analysis or from new needs and information)
Main phases	Steering and planning, collection, processing, analysis and production, dissemination, evaluation	Similar to the classical model, but without strict order or mention of feedback.	Same as classic, layered with internal cycles and continuous *feedback*.	Requirements and *gaps*, collection, analysis and dissemination are intertwined around the goal of
Interaction between phases	Limited (feedback at the end)	Medium (linear with shortcuts)	Discharge (continuous and simultaneous)	Average (cycles connected by the target)
Flexibility and adaptability	Low (rigid and sequential model)	Medium (some fluidity, but maintains defined phases)	High (oriented to continually reformulate the process)	Medium: (dynamism around the target)
Dissemination of intelligence	At the end of the process	Can be omitted or brought forward if the product requires it.	It can occur at different levels and times, depending on the internal cycle activated.	End of the process, after the production phase
Feedback	At the end of the process	Not explicitly referenced	At all stages	Not explicitly referenced

This is why this work proposes the IDEM (Enhanced Dynamic Enriched Intelligence) intelligence model with a networked, non-linear and highly adaptive approach, in which the phases of the intelligence process do not follow each other sequentially, but interact in a dynamic, flexible and continuous way, allowing constant feedback between phases and work teams.

While the traditional model starts with **direction and planning,** where intelligence requirements are established according to the decision-maker's needs, the IDEM model proposes to start with a real-time **threat identification and prioritisation** phase. One of the most repeated criticisms of the traditional cycle is its lack of flexibility, as once the objectives have been defined, the process tends to follow a fixed trajectory, which is ineffective in the current context, where threats evolve rapidly and are not always aligned with previously established needs. Therefore, the objective of this phase should be to detect and prioritise emerging threats proactively, without relying solely on initial guidelines from consumers, which often do not arrive in time or are not formulated at all. This phase would become a dynamic and continuous process of its own, fuelled by constant monitoring, real-time recognition of emerging threat patterns and the ability to quickly redirect intelligence efforts as new threats or changes in conditions emerge (Dahj, 2022).

The next phase, **collection**, remains fundamental to intelligence as a process, as without data and information, actionable knowledge cannot be obtained. In the classical model, one of the biggest challenges has been to effectively filter large volumes of data to avoid both information saturation and the loss of critical information. In the Digital Age, this task has become even more complex due to the exponential increase in the amount of available sources and data, driven by new technologies, globalisation, and the short shelf life of information. IDEM addresses this complexity through the use of advanced technologies such as *machine learning* (ML) and artificial intelligence, which enable automated continuous and comprehensive collection. Despite handling significantly larger volumes, these tools make it possible to filter, prioritise and enrich information in real time, ensuring its relevance and usefulness.

In this approach, it does not make sense to establish a specific phase for data **transformation** as in the classical model. Thanks to advanced technologies, such as natural language processing (NLP*)* and *big data* analytics tools, the conversion of raw data into relevant and contextualised information can occur at multiple stages of the process simultaneously. This allows data to be processed, structured and analysed in parallel, facilitating an agile response to new information or changes in the environment.

Furthermore, the separation between **transformation** and **analysis** can lead to a lack of integration and a loss of context during the transition. For this reason, IDEM replaces these two phases of the classical model with a single stage of **contextualisation and enrichment** that focuses on placing the data in context, interpreting its relevance and understanding the connection to other events and patterns. In this way the analysis can be continuously updated and adjusted as new data emerge and new questions arise, developing a capacity for continuous adaptation. It is also essential to process and integrate information from multiple data sources as they facilitate deeper and more efficient interpretation, especially in today's context of hybrid threats. Unlike the traditional approach, and also classical ISR systems, which establishes an individual process for each type of source (OSINT, HUMINT, SIGINT, COMINT, etc.) (Ministry of Defence, 2023), IDEM proposes an interconnected, multi-sensor model, more effective in the detection and analysis of complex phenomena, as suggested by the JISR doctrine of the US Department of Defence, discussed in the section 2.2

In contrast, the IDEM model maintains a specific stage for the **production of** actionable intelligence. While, in the traditional cycle, analysis and production focus on generating reports and recommendations that help decision-making, IDEM advocates products that are not only reactive, but also predictive, allowing for the anticipation of events and trends or the evaluation of impacts that facilitate the adjustment of strategies and decisions in real time. The emphasis here is on intelligence as dynamic decision support, not as a closed product.

Parallel to the development of all these phases, the **feedback** phase defined in the traditional intelligence cycle is indispensable, but reinterpreted as a cross-cutting process. To ensure continuous improvement and a more efficient process, it is crucial that points of improvement or weaknesses are brought out throughout each of the phases. This will allow these observations to be considered not only in the next steps, but also in future research, rather than waiting until the final intelligence product is obtained, as is the case in the traditional model.

Finally, in the traditional cycle, **dissemination** is reserved for the end of the process, once the intelligence report has been produced. IDEM breaks with this logic, proposing a modular and progressive dissemination, not only sharing intelligence as such, but also those threats recognised and classified in the identification and prioritisation phase, or data collected from the different available sources or even those data contextualised and enriched in different formats. Obviously, this early dissemination must be carefully managed, ensuring the protection of sources to avoid countermeasures and disinformation from targets and to protect human sources (HUMINT). However, the transnational nature of today's crimes requires international cooperation of different intelligence services and thus timely and not delayed sharing of information between them for more effective results.

However, despite the technical capabilities offered by automation, the role of the human analyst remains essential at each of the stages described above. Automated tools operate within parameters and algorithms defined by their programmers, who are truly capable of interpreting information in a broader context, taking into account cultural, political and situational factors. Moreover, predictive models lack the cognitive flexibility to handle ambiguities, contradictions or exceptions and may fail in the face of erroneous inputs, biased data or unforeseen situations.

Analysts, by contrast, are able to adapt, innovate and readjust their approaches in response to new paradigms, whereas artificial intelligence models need a large amount of training data to be able to develop new analysis methodologies and are not able to apply creative approaches if new issues arise. This ability of humans to collaborate across teams, to discuss interpretations, to restructure strategies based on *feedback* received is essential for the successful implementation of intelligence strategies (Jordan, 2011).

Table 2
Comparative table of the classical model and the proposed IDEM model

	Classic model	IDEM model (own proposal)
Structure	Linear or cyclical (successive phases in a circle)	Modular, dynamic and networked (concentric, interconnected circles)
Start of the process	At the request of the consumer	Proactive, without prior request
Main phases	Steering and planning, collection, processing, analysis and production, dissemination, evaluation	Identification and prioritisation, collection, contextualisation and enrichment, intelligence production, feedback and dissemination
Interaction between phases	Limited (feedback at the end)	Discharge: interactive and bidirectional phases
Flexibility and adaptability	Low (rigid and sequential model)	Very high (simultaneous and resettable phases)
Dissemination of intelligence	At the end of the process	Cross-cutting and continuous from early stages of the process
Feedback	At the end of the process	Constant: at all stages
Applied technology	Not explicitly covered	Integration of advanced technologies (AI, ML, NLP, *big data*)
Human participation	Central, but hierarchical	Synergistic combination of human analyst and automated tools
Applicability in digital environments	Limited	High (oriented to cyber threats and complex scenarios)

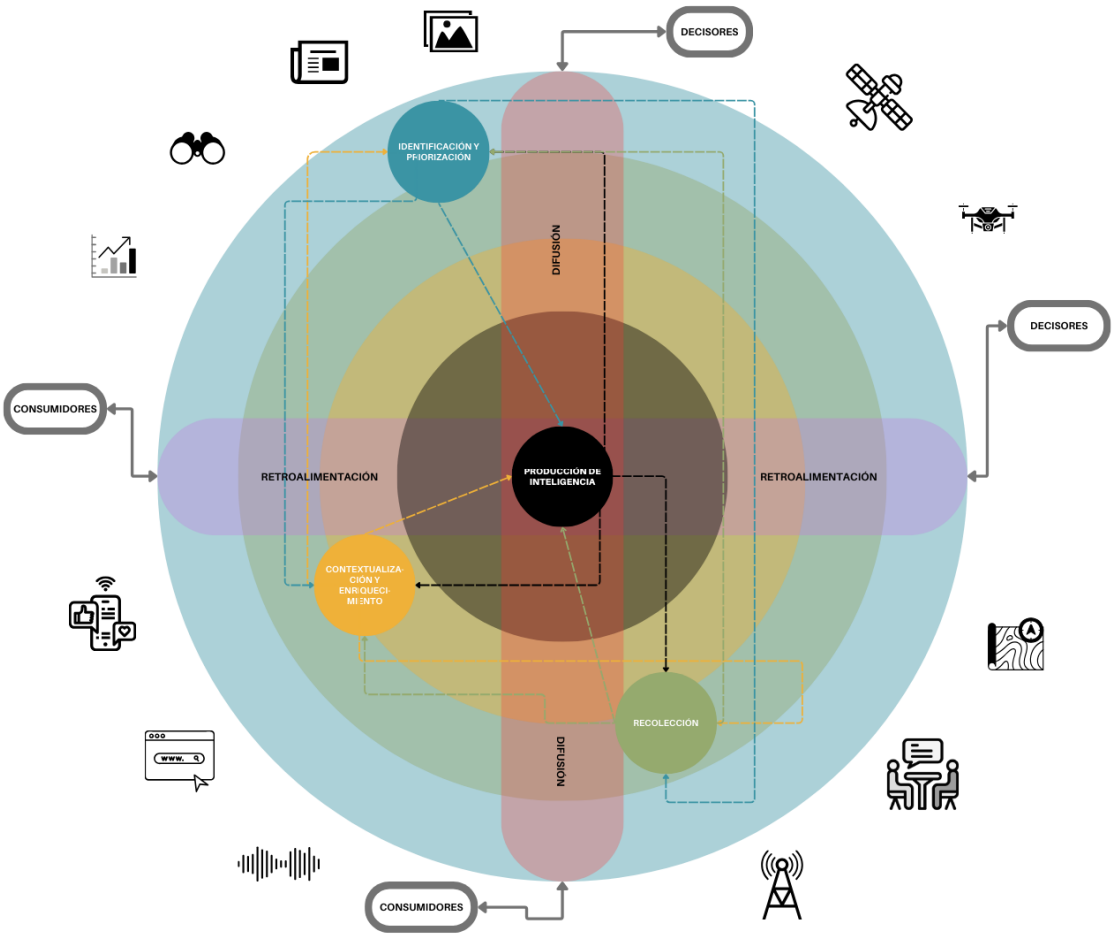
Below is a representative schematic of the IDEM model, in which the different phases are arranged as concentric circles. This arrangement reflects, on the one hand, the increasing proximity to the final intelligence product as one moves towards the centre, and on the other hand, the constant nature of all the stages, as the innermost phases are contained within the outer ones. However, the model does not establish a linear path, it is not necessary to go through all the stages in order to reach the centre. This dynamic character is represented by arrows indicating the possible flows in and out between the different stages, allowing for direct and bidirectional transitions according to the needs of the context.

Perpendicular to these circles and perpendicular to each other, two key elements are integrated, represented as transversal rectangles. The first represents the feedback phase, transversal to all the phases and opportune for the continuous improvement of the whole cycle. The second symbolises the dissemination phase, also collateral to all the stages and essential to obtain more complete products and more effective results.

On the outside of the scheme are the consumers and decision-makers. Their number and relevance will depend both on the intelligence needs required and the expected impact of the analysis conducted. These figures are represented by bidirectional arrows, which indicate their dual function of establishing the intelligence target and criteria, while at the same time receiving feedback or intelligence products to facilitate their decision-making.

Icons from different sources of information are also incorporated, thus supporting the strategy of collecting, contextualising and enriching data from different sources for a more comprehensive, cross-cutting and effective intelligence process.

Figure 5
IDEM intelligence model



Note: Own elaboration, Paula Castro Castañer, 2024.

The combination of adaptability, experience, critical judgement and human talent with the ability of machines to process large volumes of data creates a synergy that guarantees more effective, multidisciplinary, informed and flexible decision-making, ensuring greater quality and relevance of the intelligence generated.

4.1. PRACTICAL EXAMPLE OF THE IMPLEMENTATION OF THE IDEM MODEL

A practical example that would illustrate the usefulness of applying this intelligence model is in case a national energy supplier detects an anomaly in its SCADA control systems. In this situation, there is not yet a confirmed incident or an explicit request from the decision-makers (as they are probably not yet aware of this situation), which implies that the activation of the intelligence process originates proactively and autonomously, based on signals identified in the operational environment. However, the internal

intelligence team activates the IDEM model to anticipate whether it is a real threat or a false alarm.

An automatic alert of anomalous traffic to backup servers comes from the IDS, which initiates the identification and prioritisation phase. This alert, although preliminary, is sufficient for the internal intelligence team to classify the threat as a priority, considering the potential impact that a compromise of this nature could have on the country's critical infrastructure. As a consequence, it is decided to temporarily de-prioritise open investigations into hacktivist campaigns and low-impact geopolitical surveillance, as well as other routine monitoring tasks in dark forums and channels. This reorientation allows to concentrate human and technological efforts on a single working hypothesis: a possible advanced targeted intrusion.

Collection is triggered simultaneously from multiple internal (logs, SIEM, authentication records) and external sources (cyber intelligence feeds, indicators of compromise databases, alerts from cooperating entities or intelligence providers). During this stage, when indications emerge that suggest economic motivations behind the possible attack, such as, for example, the extraction of market data instead of operational information, the process briefly returns to the identification phase in order to reformulate the initial hypothesis. This return allows the analysis to now focus on the possibility of a developing case of industrial economic espionage, thereby shifting the focus of the remaining activities in the intelligence process.

In the contextualisation and enrichment phase, the data collected is integrated with historical information from previous incidents and trend analysis in the energy sector. Behavioural analysis, TTP attribution and historical data mining techniques are used. These methodologies facilitate the detection of patterns and coincidences with campaigns previously attributed to state actors or intermediary groups, i.e. entities operating as proxies or indirect agents of other actors with geopolitical or economic interests.

The intelligence output is distributed in different formats tailored to the specific needs of each type of recipient. This would include tactical alerts targeted at cyber security teams responsible for immediate response, strategic reports targeted at senior energy system managers, and preventative recommendations aimed at other sector operators to strengthen their defence posture.

It is important to note that this production and dissemination of intelligence is done continuously and in parallel with the development of the investigation, without waiting for a "definitive conclusion". This approach allows for an early and dynamic response to emerging threats, since other relevant actors in the energy sector could report similar incidents in their networks upon receiving these products, which would allow reopening cycles of analysis and readjusting threat prioritisation on a national scale.

In addition to external feedback from relevant actors to adjust assumptions and priorities based on signals from the environment, there is also a continuous internal feedback phase aimed at improving the intelligence process itself. For example, during the contextualisation phase, the intelligence team detects that certain key indicators of compromise (IoCs) were not initially prioritised by the automated warning systems. This observation is documented and channelled to the team responsible for adjusting the SIEM's sensitivity thresholds, which allows for refining the detection criteria for future

similar cases. Finally, at the end of the cycle, an internal review of the performance of the IDEM model in this specific case is carried out, evaluating metrics such as response time, accuracy of the initial hypotheses and the usefulness of the products generated. This evaluation feeds an internal knowledge base that allows the adjustment of methodologies, tools and workflows, ensuring that the model evolves adaptively and based on accumulated experience.

This dynamic of backtracking, reformulation and simultaneous action enabled by the IDEM model would be impractical in the classical model of the intelligence cycle, nor in many of the models proposed in the literature reviewed, where processes are more rigid, linear and dependent on the initiative of decision-makers.

5. CONCLUSIONS

Intelligence, understood as organisation, process, product and even culture, plays a key role in managing uncertainty in volatile, interconnected and increasingly hybrid threat environments. Its multidisciplinary nature and the diversity of approaches used by different countries and disciplines make a single definition and a closed classification of its types difficult, but also reflect its conceptual richness and the need for cooperation and constant adaptation.

The classical intelligence cycle, while valuable at the time for providing structure and standardisation, has significant limitations in meeting contemporary challenges, especially in the digital domain. The dynamic and decentralised nature of cyberspace, as well as the volume and velocity of data, require more flexible and adaptive models. The IDEM model proposed in this paper responds to this need by means of a modular, non-linear and networked structure, where phases interact simultaneously and constantly feed back into each other.

This new approach reorganises the stages of the traditional cycle and adds key elements such as proactive threat identification, contextualisation integrated with analytics, early and cross-cutting intelligence dissemination, and systematic incorporation of feedback. It also integrates advanced technologies such as artificial intelligence and machine learning to optimise the management of large volumes of data and improve predictive capabilities.

However, technology alone is not enough. Human judgement, critical capacity, analytical creativity and contextual knowledge remain essential. The synergy between analysts and automated systems ensures more efficient, accurate and useful intelligence for decision-making.

In short, 21st century intelligence must be agile, multidisciplinary and collaborative. Only through hybrid approaches, open to learning and continuous improvement, will it be possible to effectively anticipate and mitigate emerging threats. The IDEM model is a step in that direction: an adaptive and realistic proposal to meet the challenges that the digital era imposes on contemporary intelligence systems.

The reality of the current context continues to present significant challenges and difficulties in effectively anticipating and mitigating contemporary threats, especially those that manifest themselves in cyberspace, as it is difficult to keep up with and ahead

of cyber criminals. It is therefore necessary for the intelligence community to continue to research and develop strategies that diminish current weaknesses, promote intelligence culture awareness, information dissemination and international cooperation.

6. BIBLIOGRAPHICAL REFERENCES

Andric, J., & Terzic, M. (2023). Intelligence cycle in the fight against terrorism with usage of OSINT data. Journal of Information Systems & Operations Management, 17(1). https://doi.org/10.1080/2158379X.2021.1879572

Atwood, C. P. (2015). Activity-Based Intelligence Revolutionizing Military Intelligence Analysis. Joint Force Quarterly, 77. https://ndupress.ndu.edu/Media/News/Article/581866/activity-based-intelligence-revolutionizing-military-intelligence-analysis/

Budhram, T. (2015). Intelligence-led policing: A proactive approach to combating corruption. South African Crime Quarterly, 52. https://doi.org/10.17159/2413-3108/2015/i52a30

Carter, J. G., & Fox, B. (2019). Community policing and intelligence-led policing: An examination of convergent or discriminant validity. Policing: An International Journal, 42(1), 43-58. https://doi.org/10.1108/PIJPSM-07-2018-0105

National Cryptologic Centre (2015). CCN-STIC-425 Cycle of Intelligence and Intrusion Analysis.

National Intelligence Centre (2023). Origins of the Intelligence Services. https://www.cni.es/sobre-el-cni/nuestra-historia

Chainey, S., & Chapman, J. (2013). A problem-oriented approach to the production of strategic intelligence assessments. Policing: An International Journal of Police Strategies & Management, 36(3), 474-490. https://doi.org/10.1108/PIJPSM-02-2012-0012

Dahj, J. N. M. (2022). Mastering Cyber Intelligence. Packt Publishing Ltd.

Díaz Fernández, A. M. (2013). The role of strategic intelligence in today's world. Cuadernos de Estrategia, 162, 35-66. https://dialnet.unirioja.es/servlet/articulo?codigo=4275959

Francisco, J., & Barrilao, S. (2019). Intelligence services, secrecy and judicial guarantee of rights. Teoría y Realidad Constitucional, 309-340.

Gkougkoudis, G., Pissanidis, D., & Demertzis, K. (2022). Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police. Digital, 2, 143-163. https://doi.org/10.3390/digital2020009

Grabosky, P. N. (1999). Zero tolerance policing. Australian Institute of Criminology, 102(Trends & issues in crime and criminal justice).

Gruszczak, A. (2018). NATO's intelligence adaptation challenge. https://www.globsec.org/what-we-do/publications/natos-intelligence-adaptation-challenge

Jefatura del Estado (2002). Law 11/2002, of 6 May, Regulating the National Intelligence Centre.

Jiménez Villalonga, R. (2018, November 26). Types of Intelligence. https://global-strategy.org/tipos-de-inteligencia/

Jordán, J. (2011). Introduction to intelligence analysis. 2340-8421, 2, Art. 2. https://www.seguridadinternacional.es/resi/index.php/revista

Jordán, J. (2015). Introducción a la Inteligencia en el ámbito de Seguridad y Defensa. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 26, Art. 26. https://www.seguridadinternacional.es/resi/index.php/revista

Jordán, J. (2016). A review of the Intelligence Cycle. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 2. https://www.seguridadinternacional.es/resi/index.php/revista

Kamiński, M. A. (2019). Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community. Security Dimensions, 32(32), 82-105. https://doi.org/10.5604/01.3001.0014.0988

Knight, T. C. (2024). Five Thousand Candles: Optimizing Information Sharing Policies for Homeland Security A dissertation. American Public University System.

Lee, M. (2023). Cyber Threat Intelligence (1st ed.), John Wiley & Sons, Inc.

Mahood, L. M. E. K. (2015). SOCMINT: following and liking social media intelligence [Canadian Forces College]. https://www.cfc.forces.gc.ca/254-eng.html

Ministry of Defence (2023). Intelligence, Surveillance and Reconnaissance.

Montero Gómez, A. (2006). Inteligencia Prospectiva de Seguridad (24; Area: Security and Defence). https://www.realinstitutoelcano.org/publicaciones/

Navarro Bonilla, D. (2004). El Ciclo de Inteligencia y sus límites. Cuadernos Constitucionales de La Cátedra Fadrique Furió Ceriol, 48, 51-66. https://dialnet.unirioja.es/servlet/articulo?codigo=2270935

Navarro Bonilla, D. (2005). Information, espionage and intelligence in the Hispanic monarchy (16th-17th centuries). Revista de Historia Militar, Extraordinario, 13-40. https://bibliotecavirtual.defensa.gob.es/BVMDefensa/es/catalogo_imagenes/grupo.do?path=309075

Organization for Security and Co-operation in Europe (2017). OSCE Guide on Intelligence-led Policing (Transnational Threats Department Strategic Police Matters Unit, Ed.; Vol. 13).

Payá-Santos, C. A. (2023). The performance of intelligence in Spain in the public, business and academic spheres. Revista Científica General José María Córdova, 21(44), 1029-1047. https://doi.org/10.21830/19006586.1222

Phythian, M., Warner, M., Gill, P., Richards, J., Davier, P. H. J., Gustafson, K., Ridgen, I., Brantly, A., Sheptycki, J., Strachan-Morris, D., Omand, D., & Hulnick, A. S. (2013). Understanding the Intelligence Cycle (M. Phythian, Ed.).

Portillo, I. (2019). Knowing what is Cyber Intelligence and Cyber Threat Intelligence. https://www.ginseg.com/ciberinteligencia/conociendo-que-es-la-ciberinteligencia-y-el-cyber-threat-intelligence/

Pothoven, S., Rietjens, S., & de Werd, P. (2023). Producer-client paradigms for defense intelligence. Defence Studies, 23(1), 68-85. https://doi.org/10.1080/14702436.2022.2089658

Stewart Bertram (2015). The Tao of Open Source Intelligence. IT Governance Publishing.

Summers, L., & Rossmo, D. K. (2019). Offender interviews: implications for intelligence-led policing. Policing, 42(1), 31-42. https://doi.org/10.1108/PIJPSM-07-2018-0096

Vela Tejada, J. (1993). Tradition and originality in the work of Aeneas the Tactician: The genesis of military historiography. Minerva. Revista de Filología Clásica, 7, 79-92. https://doi.org/https://doi.org/10.24197/mrfc.7.1993

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Research Article

HACKTIVISM: FROM SOCIAL PROTEST TO THE INSTRUMENTALISATION OF THE STATE

English translation with AI assistance (DeepL)

Josué Expósito Guisado
Sergeant of the Guardia Civil
PhD student at the University Pablo de Olavide
Master's degree in Peace, Security and Defence by the Gutiérrez Mellado University Institute (UNED)
jexpgui@gmail.com
ORCID: 0009-0003-4977-3899

Received 18/03/2025
Accepted 05/05/2025
Published 27/06/2025

Recommended citation: Expósito, J. (2025). Hacktivism: from social protest to state instrumentalisation. *Logos Guardia Civil Magazine*, 3(2), pp. 101-122.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

ORCID: 0009-0003-4977-3899

HACKTIVISM: FROM SOCIAL PROTEST TO THE INSTRUMENTALISATION OF THE STATE

Abstract: Hacktivism has evolved from an initial form of digital protest to become a key tool in contemporary geopolitical conflicts. What began as a decentralised movement in defence of freedom of expression and social justice has been progressively instrumentalised by states to execute cyber-attacks, manipulate public opinion and deploy disinformation operations. This phenomenon has been particularly accentuated in the context of the war in Ukraine, where the convergence between Advanced Persistent Threat (APT) groups and patriotic hacktivists has allowed the execution of cyber operations coordinated with state interests. In parallel, the internationalisation of hacktivism has led to the formation of alliances between groups in different regions, broadening its impact beyond the Russian-Ukrainian conflict. Cyberspace has established itself as an ideal arena for confrontation between states in a controlled environment. However, the growing sophistication of attacks and increasingly strategic targeting pose serious challenges to international stability and the security of Western states.

Resumen: El hacktivismo ha evolucionado desde una forma inicial de protesta digital hasta convertirse en una herramienta clave en los conflictos geopolíticos contemporáneos. Lo que comenzó como un movimiento descentralizado en defensa de la libertad de expresión y la justicia social, ha sido progresivamente instrumentalizado por los Estados para ejecutar ciberataques, manipular la opinión pública y desplegar operaciones de desinformación. Un fenómeno que se ha visto especialmente acentuado en el marco de la guerra de Ucrania, donde la convergencia entre grupos de Amenaza Persistente Avanzada (APT) y hacktivistas patrióticos ha permitido la ejecución de operaciones cibernéticas coordinadas con los intereses estatales. Paralelamente, la internacionalización del hacktivismo ha llevado a la formación de alianzas entre grupos de distintas regiones, ampliando su impacto más allá del conflicto ruso-ucraniano. El ciberespacio se ha consolidado como un escenario idóneo para la confrontación entre Estados en un entorno controlado. Sin embargo, la creciente sofisticación de los ataques y la selección de objetivos cada vez más estratégicos plantean serios desafíos a la estabilidad internacional y la seguridad de los Estados occidentales.

Keywords: Hacktivism, APTs, cyberproxies, cyberconflict, cyberattacks.

Palabras clave: Hacktivismo, APT, ciberproxies, ciberconflicto, ciberataques.

ABBREVIATIONS

APT: *Advanced Persistent Threat.*

DDoS: *Distributed Denial of Service* attack.

DOJ: US *Department of Justice*.

FBI: *Federal Bureau of Investigation*.

GRU: Main Intelligence Directorate of Russia (*Glavnoe Razvedyvatel'noe Upravlenie*).

ICS: *Industrial Control Systems.*

IRGC: Iran's *Islamic Revolutionary Guard Corps.*

IT Army of Ukraine: IT Army of Ukraine.

NSA: US National *Security Agency*.

PMC: *Private Military Company*.

PSOA: *Private Sector Offensive Actor*.

SCADA: *Supervisory Control And Data Acquisition.*

Stuxnet: Name of the *malware* used in the "Olympic Games" operation.

1. INTRODUCTION

The war in Ukraine has meant that the Western world has once again been confronted with the impact of political realism. Prior to the invasion of 2022, the vast majority of Western analysts were unable to envision a conventional conflict on the international scene such as the one that continues to occur on Europe's doorstep. Blinded by soft-power doctrines and following the liberal paradigms of capitalist peace or commercial peace theory, European leaders willfully ignored the fact that in some parts of the world, political realism still reigns supreme.

In an increasingly digitised world, where there is virtual interconnection between the intangible plane of information technology and physical space itself, it is not surprising that Europe's current enemy poses a security challenge. As states have become increasingly dependent on information technologies, so have the opportunities for hostile actors (state and non-state) to influence the political and geopolitical environment by deploying actions in cyberspace.

The war in Ukraine has not only marked not only the beginning of an operation of harassment and cyber disruption by cyberthreats linked to the Kremlin, but has also brought about a change in the global hacktivist landscape: what until not so many years ago was the bastion of the defence of freedom of expression, privacy, social justice and human rights, is now a tool with strategic implications and, in many cases, linked directly or indirectly to governments and intelligence services.

The ideological and protest-oriented digital activism that Anonymous once represented is evolving into a phenomenon made up of a myriad of nationalist groups that repeatedly use distributed denial of service (DDoS) attacks to create a climate of tension and persistent harassment of Western enemies.

Hacktivism has become a double-edged tool. On the one hand, it represents a form of expression and struggle for social justice, transparency and human rights. On the other, it has become a weapon used by states to deploy political destabilisation and disinformation campaigns.

The use of cyberattacks for geopolitical purposes has highlighted the fine line between activism and state-sponsored cybercrime. This article seeks to analyse the evolution of hacktivism and its relationship with governments, as well as the role of Advanced Persistent Threat (APT) groups in the use of cyberspace for political and military purposes . [1]

Through a review of concrete cases, it will explore the collaboration (or instrumentalisation) of hacktivists by states, the implications of this practice and its impact on current geopolitics. Finally, a reflection will be offered on the future of

[1] Groups of cyber-attackers often associated with nation states or large criminal organisations, highly sophisticated and persistent, who infiltrate networks for long periods of time for espionage or sabotage and who have abundant resources (technical, economic) to attack high-value targets (governments, large companies) with premeditation and stealth.

hacktivism in an increasingly interconnected world, where artificial intelligence and other emerging technologies could redefine the role of these actors in cyberspace.

Hacktivism is no longer just a marginal phenomenon of digital protest, but a potential security risk for states. Understanding its evolution and implications is fundamental to analysing the future of Spanish cybersecurity.

2. FROM SOCIAL PROTEST TO CYBERWARFARE

Hacktivism has undergone a remarkable transformation since its origins, going from being a form of social protest to a tool used by governments to support a political agenda. If we think about it carefully, this transformation betrays the origins and the very essence of activism, which is why, before analysing the role played by hacktivism as a tool at the service of the state, we believe it is necessary to look at how this phenomenon has evolved since its origins.

In certain contemporary approaches, particularly those oriented towards terminological systematisation, there is a tendency to establish a hierarchical relationship between cyberactivism and hacktivism, understanding the former as a broader phenomenon and necessarily encompassing the latter as a specific manifestation or radicalised variant. This reading, present in both popular literature and some normative analytical frameworks, considers cyberactivism to represent the use of digital technologies for the promotion of social, political or cultural causes through awareness-raising campaigns, online petitions or virtual protests. Hacktivism, on the other hand, would be characterised by the use of hacking tools - such as distributed denial of service (DDoS) attacks, data breaches or website alteration - for similar purposes, albeit by more disruptive or even illicit means.

However, this interpretation, while widespread, is problematically reductionist and does not stand up to closer scrutiny from the historical and critical theory of digital movements. Firstly, the assumption of a linear and progressive evolution - from "moderate" cyberactivism to "radical" hacktivism - ignores the distinct historical trajectories of the two concepts. Hacktivism, far from being a late derivation of cyberactivism, emerges simultaneously and even earlier in certain contexts, rooted in the hacker culture of the 1980s and 1990s, and articulated around principles such as freedom of information, open access to knowledge and civil disobedience in cyberspace (Jordan & Taylor, 2004; Coleman, 2014).

In fact, the term "hacktivism" arises from the etymological combination of "hacker" and "activism", describing the use of computer skills to promote political or social causes; and its roots go back to the mid-1990s, when groups like the "*Cult of the Dead Cow*" (a reference to the Texas slaughterhouse where the group holds its meetings) advocated universal access to online information as a fundamental human right and the fight against oppressive governments .[2]

"Cult of the Dead Cow, considered one of the founders of modern hacktivism, not only disseminated manifestos critical of state and corporate control of the Internet, but

[2] The website of "The Cult of the Dead Cow" can still be consulted at: https://cultdeadcow.com/about.html

also developed tools with a clear disruptive vocation. Among them is *Back Orifice* (1998), a software designed to expose vulnerabilities in the Windows operating system and denounce deficiencies in users' privacy[3] . A year later, in 1999, several of its members promoted the *Hacktivismo* project, a branch explicitly oriented towards the fight against digital censorship that gave rise to the development of tools such as *Six/Four* or *Peekabooty*, designed to circumvent the filters imposed by authoritarian regimes and facilitate free access to information.

In the *Cult of the Dead Cow*'s ideology, access to online information was not only a fundamental right, but also a field of political contestation that demanded innovative forms of technical and symbolic intervention. However, these actions, while non-violent in physical terms, implied a direct confrontation with restrictive legislation on network use and intellectual property; in other words, they revealed the ambiguous character of hacktivism.

On the other hand, conceptualising hacktivism as a simple tactical intensification of cyberactivism makes us lose sight of the ideological and epistemological divergences between the two. While cyberactivism tends to be framed within the logic of citizen participation, institutional advocacy and the strategic use of social media, hacktivism often operates on the basis of direct antagonism, resistance to power structures and the questioning of existing legal frameworks.

While it may be useful to think of hacktivism as a subcategory of cyberactivism from certain descriptive approaches, it is epistemologically insufficient and empirically questionable when addressing the genealogy, normative framework and ethical-political implications of both forms of digital activism. In this article we will focus solely on the evolution of hacktivism, understood as a phenomenon in its own right, leaving aside the formulation of a critical review of this classification.

In the early stages of hacktivism, the main objective was to carry out attacks against government and corporate entities as a form of protest against censorship and social injustices. These messages became more intense as the anti-globalisation movement of the mid-1990s emerged on the social scene (Auty, 2004).

A key milestone in the consolidation of hacktivism as a tool of political confrontation was the Kosovo war in the 1990s (often described as the first war fought online), where the contenders not only shared information and testimonies about the war online, but also spread propaganda and disinformation. *Hackers* even emerged and actively intervened in the conflict by defacing government websites and executing denial-of-service attacks against the opposing side's online infrastructures (Denning, 2001).

Academically and socially, hacktivist movements were perceived as the natural expression of a pre-existing political activism that had found in a new tool (the Internet) the possibility of employing a type of activist with a technical profile to spread its messages in a more mediatic way (Jordan, 2002).

[3] Although initially conceived as a security auditing tool, its creation generated some controversy and was perceived as a threat by the technology industry.

However, the manifest disregard for established norms, the names chosen by the groups (*The Legion of Doom, Bad Ass Mother Fuckers, Toxic Shock*, etc.) and the context of social insecurity opened up by the 9/11 attacks, meant that a phenomenon that was initially perceived positively began to arouse some mistrust. (Torres Soriano, 2018).

The figure of the *hacker* began to be identified with that of the criminal, and by extension, in a geopolitical context marked by the fight against Terror, with that of the cyberterrorist. And hacktivist actions began to be identified basically as a new form of illegitimate political participation, using cyber-attacks to carry out sabotage and cyber-espionage (Vegh, 2005).

At the academic level, the identification of hacktivism with the illegal or criminalisable, frequent in certain discourses, reduces hacktivism to a "radical form of cyberactivism", and thus impoverishes the analysis and explanatory capacity of the social sciences in the face of the complexity of contemporary digital political practices.

The beginnings of this decade reflect a hacktivism marked by the desire of its members to transgress social conventions for the fun of it. In fact, the roots of the best-known hacktivist group (Anonymous) can be traced back to the Japanese forum *2chan*, where the virtual community was dedicated to sharing all kinds of aberrant content related to anime, porn and practical jokes (Bartlett, 2015).

However, around 2003, the first internal tensions arose in a virtual community that had found in the *4chan* forum an ideal place to have fun regardless of the consequences. Precisely in this forum, some users (known as *moralfags*) proposed to focus their activities on more transcendental causes such as the fight against Internet censorship, in order to clean up the image of hacktivism and represent the defence of freedom of expression, transparency and other civil rights.

Under the slogan "*We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.*" and the Guy Fawkes mask, a decentralised collective of activists emerged that combined the exfiltration of information and DDoS attacks to vindicate the fight against corruption, censorship and abuses of power.

From the powers-that-be, Anonymous was quickly interpreted as a premonition of the risk posed by a new generation of motivated virtual actors, with a leaderless structure and an operation based on voluntarism and spontaneity (Olson, 2012). However, it was not until the collective began to support the actions of WikiLeaks that the group was perceived as a top-level cyber threat.

In a short time, Anonymous grew from a small group of politically minded *hackers* to a global movement with thousands of followers around the world. However, their appeal did not lie in a structured ideology or a defined programme of action. Beyond their anti-establishment stance, which led them to denounce the manipulation and control exercised by governments and corporations, their philosophy lacked a clear orientation on how politics, society or the economy should be organised. This made Anonymous a difficult phenomenon to pigeonhole, as its identity was based more on action and protest than on a concrete agenda for change (Torres Soriano, 2018).

Under the Guy Fawkes mask gathered individuals who certainly believed they supported positive social change, but also others: those whose inspiration was the nihilistic destruction of the world as we know it and those who sought to hide under the banner of Anonymous for political or economic gain.

From the main legacy of Anonymous - turning hacktivism into a popular practice that transcended the *hacker* sphere - comes a new era of hacktivists operating in a landscape of fragmentation and complexity, where multiple actors with diverse motivations coexist.

Today, while groups such as Anonymous continue to operate in a decentralised way, their impact has diminished compared to the boom they reached in the early 2010s. At the same time, new generations of hacktivists have emerged, who, although they have a lower level of technical expertise, compensate with the use of automation tools and a mastery of media impact and social mobilisation.

Today, hacktivism is used both by independent collectives denouncing injustice and by state-sponsored groups instrumentalising these tactics for geopolitical purposes. The conflict between Russia and Ukraine has highlighted the existence of a cyber war, with pro-Ukrainian and pro-Russian hacktivists carrying out coordinated attacks for the benefit of their respective sides.

The boundary between legitimate digital activism, cybercrime and covert intelligence operations is increasingly blurred. However, we might consider that there are currently three types of hacktivists: cyberterrorists, civic *hackers* and patriotic *hackers* (Dahan, 2013; Denning, 2001; Johnson and Robinson, 2014; Sauter, 2013).

Cyberterrorism would include all hostile actions in cyberspace aimed at perpetrating acts of violence against people or property, with the aim of intimidating or coercing governments or societies to achieve specific political, religious or ideological ends. Their actions mainly involve spreading viruses and *malware*, vandalising *websites* and carrying out denial-of-service (DDoS) or *botnet* attacks (Denning, 2001; Jordan and Taylor, 2004; Goode, 2015).

In the category of civic *hackers* we would find all those organised groups that carry out actions against computer systems with the aim of contributing some good to the community, generally bordering on legality (Hunsinger and Schrock, 2016; Schrock, 2016).

Finally, patriotic *hackers* are those individuals or groups whose efforts are aligned with nationalist ideology and are considered a 'cyber militia' in pursuit of specific interests (Dahan, 2013; Green, 2016). Although from the outside these *hackers* may not appear to be directly sponsored by any state, we can now infer that they are instrumentalised as part of a larger web of state forces.

Patriotic *hacking* originated in China in the 1990s in response to anti-Chinese riots in Indonesia, and has since been used as a tactic by China, Russia, Syria and other states as a means to damage their enemies in the cyber domain. However, none of the operations prior to the Ukrainian war had achieved the scale, impact and governmental ties as robust

and prolonged, nor so blatantly transgressed international norms, as contemporary hacktivism (Healey & Grinberg, 2022).

3. THE NEXUS BETWEEN HACKTIVISM AND APT

Throughout history, states have resorted to proxy actors to carry out their conflict strategies without directly engaging their armed forces. Auxiliary units, mercenary groups, insurgencies, terrorist organisations or private military companies (PMCs) are just some of the forms that third actors have taken to act as substitutes for the strategic action of states.

It is therefore not surprising today that, in the light of an increasingly digitalised society, state action has found in hacktivist groups a new actor to personify the externalisation of authorship, and in cyberspace, the ideal environment to project geopolitical influence.

The concept of *surrogate warfare* has been the subject of extensive debate in the academic and security community, not least because of the difficulty in differentiating it from *proxy* warfare, given the closely intertwined nature of the two concepts.

In both terms, the objectives of the principal actor (the state) and the proxy agent coincide. However, while in *proxy warfare* there are two or more hierarchically related actors (the principal actor works for, with and through the proxy to achieve a common goal), in *surrogate warfare* these actors are aligned only if the principal actor is able to mobilise the adequate support required by the proxy (Fox 2019). In other words, the concepts of *surrogate warfare* and *proxy warfare* differ according to the relationship between the actors and their motivations.

Since hacktivist groups have little independence to resist the control of the state that sponsors (or at least influences or tolerates) them, in our case study we will speak in terms of *proxy* actors.

More specifically, to refer to them we will use Rondeaux and Sterman's (2019) definition of "*proxy* actors", who define them as "*subjects outside the security structure of the states involved in a conflict who act under direct or indirect sponsorship of a conventional actor (a state)*"; and Maurer's (2018) definition of *cyber proxies* as "*intermediaries who carry out offensive actions in cyberspace for the benefit of a principal actor*".

Historically, *cyberproxies* have been personified through various entities linked to the world of cybercrime and cyberespionage. However, the term encompasses a large number of organised entities that, directly or indirectly, pose a risk factor for companies and states. In fact, the list of actors is very long: criminal groups, private *sector offensive actors* (PSOA), terrorist groups, insurgents, insurgents, hacktivists, state actors or APTs are just some of them.

The reasons behind their use are varied: (1) the use of *proxy* actors by governments reduces the risk of escalation in conflicts, since the difficulty of attributing responsibility for a cyber-attack is complex; (2) there is a possibility of plausible deniability that deflects responsibility for an attack to an actor outside government control; (3) it helps states to

prolong the tense situation in conflicts by wearing down their adversary on a social, political and economic level; (4) it allows states to act outside domestic regulations and the criticism of opposing governmental sectors - or even public opinion itself in democracies; (5) it gives states speed and flexibility in responding to their adversaries' offensive actions, as it does not require technical evidence or public legitimation; (6) it offers states an additional tool of deterrence; (7) it allows states to circumvent the application of international law; (8) it facilitates the use of expert personnel without the need to offer legal recruitment; (9) it makes it possible to participate in international conflicts that would otherwise be economically and politically unmanageable (Torres Soriano, 2017; Expósito Guisado, 2024; Marín Gutiérrez, 2023).

However, achieving these benefits is not without its problems. In fact, the main attraction of using a *proxy* (which is none other than obtaining plausible deniability of an aggression) is also its main weakness, as anonymity and clandestinity dilute the coercive and dissuasive capacity of the sponsoring state - after all, we cannot ignore Clausewitz's theories that suggest that for one state to modify its conduct based on the will of another, the latter must know the origin of the coercive act suffered.

Another drawback of the use of *cyber proxies* lies in how the state selects and controls them when they are used. The existence of divergent interests between the two parties can lead to disloyalty on the part of the *proxy*, causing economic or political damage to the actor using them - a fact that is aggravated if we take into account that these *proxies* generally operate in areas where the state neither can nor wants to intervene.

The benefit of *proxies* lies in their ability to act covertly, although it is this very lack of transparency that limits the state sponsor in verifying their background and reliability. The academic literature highlights that control over *proxies* is further complicated if the state does not have effective mechanisms to sanction disloyalty, or if there are decentralised structures that prevent proper enforcement of hierarchical orders (Popovic 2015).

In this paper we will only focus on two actors that represent the two different poles (open activism and silent espionage) of the same phenomenon, but which are not so different in terms of the ends they pursue and the instrumentalisation of them by states.

Broadly speaking, hacktivism and APTs differ in motivation, methods and degree of state support. Thus, while hacktivism is driven by a social-political context (protest, activism, moral causes), APTs focus on strategic espionage and gaining an economic-military advantage.

Operationally, APTs act through stealth and persistence, employing custom *malware*, backdoors and lateral movement; unlike hacktivist actions that usually seek public attention and generally focus on short-term DDosS attacks.

However, it is not uncommon to observe how APTs temporarily act as hacktivists (when they publicly disclose the data they exfiltrate to provoke a political impact) and how hacktivists are instrumentalised by states to achieve their strategic ends.

At the organisational level, hacktivists and APTs also differ: hacktivists generally act decentralised, spontaneously, even anonymously, and without a unified command.

APTs, on the other hand, are usually structured teams, often integrated into a larger organisation (an army, intelligence agency or criminal group), with a defined hierarchy and considerably more powerful funding (CyberZaintza, 2021).

Indeed, the difference in resources and technical training suggests a closer link between APTs and states than hacktivist groups. However, the lines between the two concepts have recently been blurred by the realisation that some pro-Russian hacktivist groups have been receiving covert state support, or act in line with the state agenda, blurring the hitherto clear distinction between "activist *hackers*" and "state operatives" (Muncaster, 2024).

In fact, it cannot be ruled out that certain hacktivist groups are actually formed or backed by APTs or directly by state actors. One example is the "XakNet Team", "Infoccentr" and "CyberArmyofRussia_Reborn", pro-Russian hacktivist groups that, according to Mandiant, are cyberthreat actors sponsored by the Russian Main Intelligence Directorate (GRU) through the APT44 (Mandiant, 2022).

Over the last decade there have been multiple documented cases in which states have used both their own APT groups and hacktivist collectives (or their identities) to carry out cyber-espionage, conflict sabotage and political manipulation.

A paradigmatic example illustrating the interdependence of both concepts can be found in the 2016 US elections, when "*DCLeaks*" and "*Guccifer 2.0*", two identities linked to Russia's Main Intelligence Directorate (*Glavnoe Razvedyvatel'noe Upravlenie*, GRU), stole Democratic Party emails and disseminated them posing as "patriotic American hacktivists" (DOJ, 2018).

In the wake of the war in Ukraine, it is not uncommon to find interdependence between Russian hacktivists and APTs, groups such as *Killnet*, *NoName057(16)*, *Anonymous Sudan* that have attacked government websites and Western companies in support of the Kremlin's narrative show that, while these groups call themselves "spontaneous activists", they suspiciously act in coordination with Russian state action (Van Der Walt, 2025).

However, Russia is not the only state actor that employs APTs and hacktivists to deploy its power. Other states such as China, North Korea or Iran have also been accused for years of conducting their offensive activities in cyberspace in this way.

Specifically, China has been accused for years of sponsoring vast cyber espionage campaigns through military units and paid *hackers*, such as those of the APT1 group, considered by Mandiant in 2013 to be Unit 61398 of the Chinese People's Liberation Army.

Chinese APT operations tend to focus on strategic targets (aerospace, energy, telecommunications, defence, etc.) and are considered part of Chinese state intelligence, but unlike Russia, the use of hacktivism is not as prominent in Chinese strategies.

The government has tolerated and even inspired Chinese "patriotic *hackers*" in some conflicts, one example being the "*Honker Hacker Network*", a *hacker* community

outside government control - according to Chinese sources - that has attacked China's adversarial actors during territorial disputes or diplomatic incidents.

Iran, on the other hand, has shown a tendency to instrumentalise supposedly activist *hacker* groups to carry out retaliatory operations against its adversaries, while developing its own APTs. A significant example of this was the DDoS attacks against US banks in 2012-2013, in retaliation for Western sanctions: an entity claiming to be religious hacktivists and calling itself the '*Cyber Fighters of Izz ad-Din al-Qassam*' claimed credit for the offensive, citing outrage over an anti-Islamic video (CFR, 2012).

US intelligence agencies subsequently concluded that this was an operation orchestrated by Iran (probably its Revolutionary Guard) in response to measures taken against its nuclear programme. In fact, in 2016 the US Department of Justice indicted seven Iranians linked to the Islamic Revolutionary Guard Corps (IRGC) for these attacks.

Another example is the 2012 "*Shamoonj*" attack by the "*Cutting Sword of Justice*", an alleged hacktivist group that wiped data from 30,000 computers at the Saudi oil company Aramco, but which analysts later attributed to an Iranian state operation in response to the *Stuxnet* offensive and regional tensions.

North Korea, despite its isolation, has also managed to build one of the most active cyberthreats, mainly to raise funds and destabilise its geopolitical adversaries. Its most notable APT group, *Lazarus Group* (linked to APT38) has stolen hundreds of millions through attacks on banks.

Another case that illustrates the instrumentalisation of activist campaigns by states can also be found in one of their actions, the *hacking* of Sony Pictures in 2014, when a group called "*Guardians of Peace*" exfiltrated confidential data and destroyed Sony systems in apparent retaliation for the satirical film about the North Korean leader "*The Interview*". (FBI, 2014).

North Korea is the paradigm of direct instrumentalisation, its *hackers* are agents of the state who sometimes assume the names of fictitious groups to disseminate their messages or justify their attacks, but unlike other states, the North Koreans do away with the distinction between APT and state apparatus altogether, keeping the cover only in the public narrative to the outside world.

For their part, Western powers obviously also employ offensive cyber capabilities to attack other states. Perhaps the most relevant case is the 'Olympic Games' operation attributed to the NSA agencies and the (unofficially recognised) 8200 unit, in which the US and Israel developed the *Stuxnet* malware to sabotage Iran's nuclear centrifuges around 2010 (The Guardian, 2017).

However, in the West, although there are APT entities supported by states to act offensively in espionage campaigns, the instrumentalisation of hacktivist groups to hide their actions is practically non-existent. In fact, we can only find one case where a Western hacktivist group links its activity to the cyber offensive capacity of a state: the "*IT Army of Ukraine*".

This case is particularly controversial, as public state support by the Ukrainian government openly violates recently agreed norms on the conduct of states in cyberspace, as well as the foreign policy positions of NATO members (Healey and Grinberg, 2022).

If we use Healey and Grinberg's (2022) "Spectrum of Responsibility" table, where they correlate the activity of groups according to the degree of state responsibility for their *cyber proxy*, we can see how the Ukrainian government's support for the *IT Army of Ukraine* started at least as "state-coordinated (level 6)", (when Ukrainian Minister of Digital Transformation Mikhail Fedorov openly called on hacktivist volunteers from all over the world to support Ukraine on the digital front) and even "encouraged by the state (level 4)".

Table 1: *Spectrum of State responsibility.*

State position	*State-proxy* relationship
1. Banned by the State.	The national government will help stop a third party attack.
2. State ban but inadequate.	The national government cooperates, but it is unable to stop the attack by third parties.
3. Ignored by the state.	The national government is aware of the attacks by third parties, but is unwilling to take no official action.
4. State-sponsored.	Third parties control and direct the attack, but the national government promotes them as a political issue.
5. Shaped by the State.	Third parties control and lead the attack, and the The state provides some support.
6. Coordinated by the State.	The national government coordinates the attack by third parties, e.g. by suggesting details operational.
7. State-mandated.	The national government orders third parties to carry out the attack on their behalf.
8. Managed, but not recognised by the state.	Elements outside the control of the forces cybernetic attacks by the national government lead to orderly attack.
9. State-implemented.	The national government carries out the attack using cybernetic forces under their direct control.
10. State-integrated.	National government attacks using embedded proxies and cyber forces governmental.

(Healey, 2022).

It is especially in geopolitical conflicts that we see the most accelerated convergence between hacktivism and state operations. In the case of the Ukrainian war,

three years after the start of the conflict and despite the fact that the number of hacktivist actors has decreased considerably (from more than 130 groups in 2024 to only about 80 groups in 2025), we can still observe how both sides maintain a crossover of destructive cyberattacks, coordinated with their military campaign and supported in their actions by "patriotic hackers" (Cyberknow, 2025).

On the Ukrainian side, the *IT Army of Ukraine* remains Ukraine's most important hacktivist force, still mobilising volunteers inside and outside the country to attack Russian infrastructure, conduct counter-propaganda and support intelligence missions. In the period 2023-2024, it is credited, for example, with temporarily bringing down internet services in Russian-occupied areas and continuously deploying DDoS campaigns against high-profile Russian entities (Optiv, 2023).

On the pro-Russian side, the most prominent group at present is *NoName057(16)*, a group linked to the GRU, which acts in coordination with the Kremlin's agenda by selecting targets in tune with Russian strategic interests and considers itself a sort of permanent "cyber-spontaneous arm" of the Russian military.

Table 2: *Chronological cases of state instrumentalisation of hacktivism.*

Year	***State***	***Group hacktivist***	***Feature***	***Level of state linkage (Healey & Grinberg).***
1998-1999	Kosovo	Patriotic hackers	First conflict with notable hacktivist intervention.	Ignored / Spontaneous
1999	China	Red Honker	Patriotic hackers active in territorial conflicts. Industrial espionage campaigns and cyber-attacks on critical infrastructure.	Encouraged / Shaped
2012-2013	Iran	Cyber Fighters of Izz ad-Din al-Qassam	DDoS attacks on US banks in retaliation for sanctions. Operation Shamoon against Aramco with mass deletion.	Coordinated / Orderly
2014	North Korea	Lazarus Group	Cyber-attacks for state funding. Attack on Sony Pictures (2014) as symbolic retaliation.	Implemented / Integrated
2022-present	Russia	Killnet/ Cyber Army of Russian Reborn/ NoName057(16)	Hacktivist groups coordinated with the Russian strategy in the Ukrainian war. DDoS attacks.	Coordinated / Encouraged
2022-present	Ukraine	IT Army of Ukraine	Government's public call for hacktivism against Russia. DDoS, sabotage and pro-Ukrainian propaganda.	Coordinated / Encouraged

4. THE FUTURE OF HACKTIVIST GROUPS.

The survival of hacktivist groups indicates that war-integrated hacktivism is here to stay, at least for as long as the underlying conflict lasts and states in conflict find this layer of decentralised action useful. Moreover, the current hacktivist landscape leads us to observe that hacktivism is moving beyond DDoS and into more sophisticated APT attacks, such as attacks on critical infrastructure SCADA and industrial control systems (ICS) . [4]

The fact that groups belonging to the pro-Russian hacktivist ecosystem, such as *Z-Pentest Alliance* or *Sector 16*, have been actively intruding into power plants, drinking water facilities and industries in general, reflects not only a maturation and stateisation of the hacktivist phenomenon, but also the existence of increasingly physical risks of their actions (Antoniuk, 2024).

The reduction in the number of hacktivist groups in the pro-Russian environment suggests that the initial effervescence has given way to a natural selection process in which those groups with better support, organisation and protection survive. A phenomenon that translates into more effective and coordinated operations, but also more predictable as they are aligned with the Russian state agenda.

At the same time, the persistence of daily attacks indicates that low-intensity cyber warfare has become routine. Constant DDoS maintains psychological and propaganda pressure on target populations (daily reminders of the presence of conflict), while the adoption of *ransomware* and attacks on industries raises the potential for real damage to critical infrastructure, blurring the line between hacktivism and cyberterrorism - a fact that may ultimately lead to more forceful responses by victim states and the potential for escalation of conflict.

Another development of relevance is the remarkable development of emerging alliances between hacktivist causes that transcend the theatre of operations beyond Ukraine and involve third countries. One example is the recent alliance between pro-Russian and pro-Palestinian hacktivists, which unites seemingly distinct geopolitical causes under a common narrative of attacking the West.

The global tensions of 2024 (including the Gaza war) created a strange united front of hacktivists. Russian groups (especially *NoName057(16)*) began coordinating operations with Middle Eastern-linked collectives (such as *Mr. Hamza* or *Anonymous Guys*), and synchronised their attacks under the banner of the "*Holy League*" union against countries they perceived as shared adversaries, such as France.

This type of alliance is well known in Spain, and particularly by the Guardia Civil, since in July 2024, the institution was the direct target of a joint cyber-attack campaign, "*#FuckGuardiaCivil*", which responded to an initiative promoted by the group *NoName057(16),* to "take revenge on the Spanish authorities" who had arrested three people in Manacor (Mallorca), Huelva and Seville on suspicion of participating in

[4] Centralised system to monitor, control and collect data from processes and devices in real time.

cyberattacks against public entities and strategic companies in Spain and other NATO countries.

In fact, in April 2025, a new alliance was already registered, including the *Keymous+, Mr Hamza, Alixsec and NoName057(16)* groups, to attack Poland, Germany, France, Italy and Spain under the slogan "*Operation Hack For Humanity V2!*

In the case of Spain alone, on the first day of the "Operation Hack For Humanity V2!" campaign, more than 30 attacks on companies and government websites were registered, with *Mr Hamza*, *NoName057(16)*, *TwoNet* and *Keymous+* being the most active groups in the attack.

The frequency with which this convergence has been occurring in recent months shows that the phenomenon is becoming increasingly international and interconnected. The alliances between hacktivist groups have become mutually supportive, transcending the borders of the Russian-Ukrainian conflict with a single goal: to expand their actions towards the common Western enemy.

The fact that NATO countries such as France, Italy and Spain itself could become targets of Russian patriotic *hackers* could lead to an escalation of the conflict, especially if one of their attacks were to severely damage critical infrastructure, low-intensity cyber warfare could draw a stronger response than usual.

5. CONCLUSIONS

The analysis of hacktivism and its relationship with states shows that this phenomenon has evolved from digital protest to state instrumentalisation with geopolitical and strategic implications. The boundary between activism, cybercrime and state operations is increasingly blurred, especially in conflicts such as the war in Ukraine, where we have observed a growing instrumentalisation of hacktivist groups by government forces in the defence of their national interests.

Indeed, the conflict between Russia and Ukraine has marked a turning point in the use of cyberspace as a battleground, where both state and non-state actors have actively engaged in denial of service (DDoS) attacks, cyber espionage and sabotage of critical infrastructure.

This study, developed through the study of the most prominent cases on the international scene, has allowed us to establish a distinction between civic *hackers* and patriotic *hackers*. While the former embrace nihilistic or socially conflictive causes, the latter are used by states as a covert tool in international conflicts, which entails an externalisation of governmental cyber capabilities and offers a series of strategic advantages: plausible deniability of responsibility, prolongation of situations of tension or the reduction of political and economic costs.

In short, we could say that states have learned to exploit hacktivism as an additional weapon, either by pretending to be hacktivists in order to disinform or exfiltrate data or by encouraging their sympathisers to launch mass cyberattacks against their enemy.

However, this instrumentalisation poses serious challenges at the strategic level. The progressive sophistication of attacks that have moved from digital vandalism to more advanced operations against critical infrastructures only seriously increases the possibilities of retaliation by the affected states and increases the potential risk of escalation in asymmetric conflicts.

Moreover, the convergence between APTs and hacktivists calls into question existing international norms, as attacks perpetrated by *proxy* actors blur state responsibility and make it difficult to implement deterrence or direct retaliation. Especially as hacktivist collectives seem to be evolving towards a new landscape of alliances capable of bringing together hacktivist groups with diverse geopolitical agendas to attack Western countries.

State cyber security must adapt to a new reality in which hacktivist groups play a key role in the projection of state power. Western democracies, traditionally more reluctant to use such tactics, face the dilemma of how to respond effectively without compromising their values.

The current trend not only shows a clear evolution of hacktivism towards an increasing linkage with the state interests of the government that supports them, but also reinforces the idea that cyberspace will continue to become more important in future conflicts. Cases such as Russia, where groups like *Killnet* or *NoName057(16)* have claimed cyber operations coinciding with the Kremlin's geopolitical interests -especially during the war in Ukraine-, or Iran, with groups like *Tapandegan*, whose oppositionist rhetoric does not prevent suspicions of indirect coordination with state agendas, exemplify this drift, and demonstrate a progressive blurring between non-state and state actors in the digital sphere, where hacktivism ceases to be exclusively a form of citizen dissidence and becomes, in certain contexts, an informal tool for the projection of state power.

6. BIBLIOGRAPHICAL REFERENCES

Antoniuk, D. (2024). *Cybervolk: Hacktivists from India and Russia collaborate on ransomware attacks.* The Record. https://therecord.media/cybervolk-india-hacktivists-russia-ransomware

Antoniuk, D. (2024). *Cybervolk: Hacktivists from India and Russia collaborate on ransomware attacks.* The Record. https://therecord.media/cybervolk-india-hacktivists-russia-ransomware

Auty, C. (2004). Political hacktivism: Tool of the underdog or scourge of cyberspace? *Aslib Proceedings, 56*(4), 212-221.

Bartlett, J. (2015). *The dark net: Inside the digital underworld.* Melville House.

CFR (2012). *Denial of service attacks against U.S. banks in 2012-2013.* Council on Foreign Relations (CFR). https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous.* Verso Books.

Cyberknow (2025). *Russia-Ukraine war: Hacktivist update.* https://cyberknow.substack.com/p/russia-ukraine-war-hacktivist-update

CyberZaintza (2021). *APT Group.* https://www.ciberseguridad.eus/ciberglosario/grupo-apt

Dahan, M. (2013). Hacking for the homeland: Patriotic hackers versus hacktivists. *International Conference on Information Warfare and Security*, 51-VII. Academic Conferences International Limited. https://search.proquest.com/docview/1549245919

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239-288). RAND Corporation.

DOJ (2018). *Grand jury indicts 12 Russian intelligence officers for hacking offenses related to the 2016 election.* U.S. Department of Justice. https://www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

Expósito Guisado, J. (2023). *Cyberproxies: APTs as a future risk factor.* Spanish Institute for Strategic Studies (IEEE). *IEEE Bulletin*, (32), 815-831.

FBI (2014). *Update on Sony Investigation.* Federal Bureau of Investigation (FBI), Washington, D.C. https://www.fbi.gov/news/press-releases/update-on-sony-investigation

Fox, A. C. (2019). *Conflict and the need for a theory of proxy warfare. Journal of Strategic Security, 12*(1), 44-71. JSTOR. www.jstor.org/stable/26623077

Goode, L. (2015). Anonymous and the political ethos of hacktivism. *Popular Communication, 13*(1), 74-86. https://doi.org/10.1080/15405702.2014.978000

Green, K. (2016). People's war in cyberspace: Using China's civilian economy in the information domain. *Military Cyber Affairs, 2*(1). https://doi.org/10.5038/2378-0789.2.1.1022

Healey, J., & Grinberg, A. (2022). *Patriotic hacking: No exception*. Lawfare. https://www.lawfaremedia.org/article/patriotic-hacking-no-exception

Hern, A. (2017). NSA contractor leaked US hacking tools by mistake, Kaspersky says. *The Guardian.* https://www.theguardian.com/technology/2017/oct/26/kaspersky-russia-nsa-contractor-leaked-us-hacking-tools-by-mistake-pirating-microsoft-office

Hunsinger, J., & Schrock, A. (2016). The democratization of hacking and making. *New Media & Society, 18*(4), 535-538. https://doi.org/10.1177/1461444816629466

Johnson, P., & Robinson, P. (2014). Civic hackathons: Innovation, procurement, or civic engagement? *Review of Policy Research, 31*(4), 349-357. https://doi.org/10.1111/ropr.12074

Jordan, T. (2002). *Activism! Direct action, hacktivism and the future of society*. Reaktion Books.

Jordan, T., & Taylor, P. A. (2004). *Hacktivism and cyberwars: Rebels with a cause?* Psychology Press.

Mandiant (2022). *GRU's rise: Telegram minions.* https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions

Marín, F. (2023). *Hacktivism in the service of the state: cyberproxies in Ukraine.* Opinion Paper. Spanish Institute for Strategic Studies (IEEE).

Maurer, T. (2018). *Cyber Mercenaries: The state, hackers, and power*. Cambridge University Press.

Muncaster, P. (2024). *Hacktivism: Evolving threats to organisations*. WeLiveSecurity. https://www.welivesecurity.com/es/cibercrimen/el-hacktivismo-evolucionando-amenazas-organizaciones

Olson, P. (2012). *5 things every organization can learn from Anonymous*. Forbes. http://www.forbes.com/sites/parmyolson/2012/06/05/5-things-every-organization-can-learn-from-anonymous/

OPTIV (2023). *Russia/Ukraine Update - December 2023*. https://www.optiv.com/insights/discover/blog/russiaukraine-update-december-2023

Popovic, M. (2015). Fragile proxies: Explaining rebel defection against their state sponsors. *Terrorism and Political Violence*. https://doi.org/10.1080/09546553.2015.1092437

Rondeaux, C., & Sterman, D. (2019). *Twenty-first century proxy warfare: Confronting strategic innovation in a multipolar world since the 2011 NATO intervention*. New America. https://d1y8sb8igg2f8e.cloudfront.net/documents/Twenty-First_Century_Proxy_Warfare_Final.pdf

Sauter, M. (2013). "LOIC will tear us apart": The impact of tool design and media portrayals in the success of activist DDOS attacks. *American Behavioral Scientist, 57*(7), 983-1007. https://doi.org/10.1177/000276

Schrock, A. R. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. *New Media & Society, 18*(4), 581-599. https://doi.org/10.1177/1461444816629469

Torres Soriano, M. (2017). Proxy wars in cyberspace. *Revista del Instituto Español de Estudios Estratégicos, (9)*, 15-36.

(2018). Hacktivism as a communication strategy from Anonymous to the cybercaliphate. *Cuadernos de Estrategia, (197)*, 197-224.

Van Der Walt (2025). *Reflecting on three years of cyber warfare in Ukraine. ComputerWeekly.* https://www.computerweekly.com/opinion/Reflecting-on-three-years-of-cyber-warfare-in-Ukraine

Vegh, S. (2005). *The media's portrayal of hacking, hackers, and hacktivism before and after September 11. First Monday.* http://uncommonculture.org/ojs/index.php/fm/article/view/1206/1126

ORCID: 0009-0003-4977-3899

Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Research Article

INTERNATIONAL PROTECTION AND SOVEREIGNTY: THE COMPLICATED BALANCE BETWEEN INDIVIDUAL RIGHTS AND NATIONAL SECURITY

English translation with AI assistance (DeepL)

Alejandro Gómez García
Captain of the Guardia Civil
Master in Operational Security Management
Law Degree
alejandrogomezg@guardiacivil.es
ORCID: https://orcid.org/0000-0003-0162-4213

Received 31/03/2025
Accepted 28/04/2025
Published 27/ 06/2025

Recommended citation: Gómez, A. (2025). International protection and sovereignty: the complicated balance between individual rights and national security. *Revista Logos Guardia Civil*, 3(2), p.p. 123-146.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

ORCID: https://orcid.org/0000-0003-0162-4213

INTERNATIONAL PROTECTION AND SOVEREIGNTY: THE COMPLICATED BALANCE BETWEEN INDIVIDUAL RIGHTS AND NATIONAL SECURITY

Abstract: The aim of this article is to analyse the current legal status of some of the most relevant concepts in the field of the protection of national borders, as well as their sociopolitical context and legal scope, with the ultimate aim of supporting and promoting the development of a doctrinal debate that is as hot in its positions as it is complex in its context: ensuring an adequate balance between the guarantee of the Fundamental Rights of individuals passing through European borders and the exercise of the sovereign powers inherent to States. Thus, first of all, a detailed examination will be made of the most important notions in the field of border security, establishing the field of study from a scientific point of view. Immediately afterwards, from a legal perspective, we will study the implications of the most important pronouncements made by the judicial bodies (fundamentally international) that have dealt with the matter, as well as the position of international doctrine and practice. And finally, in the light of the analyses presented, a series of conclusions will be offered that are coherent with the findings made.

Resumen: En el presente artículo se pretende analizar el estatus jurídico que ostentan, en la actualidad, algunos de los conceptos más relevantes dentro del ámbito de la protección de las fronteras nacionales, así como su contexto sociopolítico y su alcance jurídico, con el fin último de fundamentar e impulsar el desarrollo de un debate doctrinal tan candente en sus posturas como complejo en su contexto: Asegurar un adecuado balance entre la garantía de los Derechos Fundamentales de los individuos que transiten por las fronteras europeas y el ejercicio de las potestades soberanas consustanciales a los Estados. Así, en primer lugar, se realizará un examen pormenorizado de las nociones más importantes en el ámbito de la seguridad fronteriza, fijando el campo de estudio desde un punto de vista científico. Inmediatamente a continuación se estudiarán, desde una perspectiva jurídica, las implicaciones que han tenido los pronunciamientos más importantes efectuados por los órganos judiciales (fundamentalmente internacionales) que han entendido de la materia, así como la posición de la doctrina y la práctica internacional. Y finalmente, a la luz de los análisis expuestos, se ofrecerá una serie de conclusiones coherentes con los hallazgos efectuados.

Keywords: International Law, Asylum, Sovereignty, Borders, Immigration.

Palabras clave: Derecho Internacional, Asilo, Soberanía, Fronteras, Inmigración.

ORCID: https://orcid.org/0000-0003-0162-4213

ABBREVIATIONS

AN: Audiencia Nacional

PNA: Palestinian National Authority

CFREU: Charter of Fundamental Rights of the European Union

ECHR: European Convention on Human Rights

IMO: *International Maritime Organisation - International Maritime Organisation*

SAR: *Search and Rescue* - Search and *Rescue*

SOLAS: *Security Of Life At Sea - Safety Of Life At Sea*

ECtHR: European Court of Human Rights

ICJ: International Court of Justice

PCA: Permanent Court of Arbitration

PCIJ: Permanent Court of International Justice

EU: European Union

1. INTRODUCTION

Following the Judgment of the European Court of Human Rights (hereinafter ECHR), Third Section, of 3 October 2017, by which the Spanish State was condemned, in the context of the practice of "rejection at the border", for violation of Article 13 of the European Convention on Human Rights (hereinafter ECHR) and Article 4 of its Protocol No. 4, providing for the payment of compensation to the plaintiffs N. D. (Malian national) and N.T. (Ivorian national) in the amount of 5,000 euros each; there were many voices calling for a complete change of course in the migratory policy developed by the Kingdom of Spain and, by extension, in European migratory policy. In fact, the news made headlines in the press[1] , as well as strong pronouncements by non-governmental organisations[2] and even public law entities[3] , in a country not used to following the judicial chronicle in such detail, and even less so at the international level.

And the situation was not to be taken lightly. The growing concern about the migratory context in the European Union (hereinafter EU) had given rise, over the years, to the emergence of certain debates that, until then, had remained outside the political dynamics, which accepted as something almost anecdotal the sustained increase in the number of third-country nationals residing in the Union, whose number had risen by more than 10% in the three years prior to the aforementioned pronouncement[4] . Of course, the rise of this debate had also been fuelled by the so-called 'Refugee Crisis' of 2015, in which hundreds of thousands of displaced persons from the Middle East (mostly Syrians) had entered European territory as a result of instability and war in the region. And it would definitely not help to ease the tension in European society if some of those involved in various terrorist acts that took place during those years (for example, the Ansbach and Berlin attacks in 2016 or, of course, the Paris attacks of 2015) were subsequently identified as refugees or illegal immigrants, coming from Syria via the eastern Mediterranean route.

But, as if this were not enough, the future held a new major surprise in store that would once again turn the script of European migration policy on its head. In an unprecedented event, the same ECHR that had overturned the Spanish doctrine on border rejections would reverse its decision at first instance and, in a Grand Chamber ruling of 13 February 2020, proceeded to declare, by a majority of 16 to 1, the full legality of border rejections. Then came the pandemic. And with it came the reactivation of the Atlantic migratory route to the Canary Islands, as well as a new boom in migratory movements to the EU in general, which would rise from 125,226 illegal entries detected in 2020 (Frontex, 2021, p. 14) to 380,227 in 2023 (Frontex, 2024, p. 1). Today, immigration occupies a predominant place among the main concerns of the continent's citizens. Thus, the latest "Eurobarometer", published in November 2024, highlights immigration as the second

---

[1] RTVE (3 October 2017), *The European Court of Human Rights condemns Spain for two "hot returns" in Melilla*, https://www.rtve.es/noticias/20171003/tribunal-europeo-derechos-humanos-condena-a-espana-por-dos-devoluciones-caliente-melilla/1625420.shtml.

[2] Spanish Commission for Refugee Aid (3 October 2017), *European Court of Human Rights condemns Spain for two 'hot returns'*, https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/.

[3] Consejo General de la Abogacía Española (3 October 2017), *La Abogacía reitera la ilegalidad de las devoluciones en caliente, tras la condena del TEDH*, https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/.

[4] Eurostat data, https://ec.europa.eu/eurostat/databrowser/view/migr_pop1ctz/default/table?lang=en.

priority in terms of areas where the EU should take action in the opinion of Europeans, a position supported by 29% of respondents (European Commission, 2024, p. 14), behind only Security and Defence.

However, although the European Commission does not hesitate to respond to these concerns by repeatedly pointing to the "progress" being made in "border management" (European Commission, 2022, p. 5), the fact is that when the factor of safeguarding fundamental rights is introduced into the equation, the situation becomes more complicated. The fact is that policies aimed at reinforcing border control, developed on the basis of the objectives of strengthening the system on which national security rests and guaranteeing the sovereignty of States, entail measures aimed at hindering illegal immigration that, by their very nature, affect the rights of the population concerned. And, in accordance with the basic rules governing the rule of law, in the event that this impact is not suitable, coherent and proportional with respect to the lawful ends pursued, it could represent an illegal intrusion into the most essential core of fundamental rights, especially when they condition key areas such as the right to asylum. This research article aims to analyse this delicate balance, revealing the points of friction between the two conflicting realities through a detailed examination of national and international jurisprudence; as well as clarifying, as far as possible, how far the legality of the actions of civil guards can go in their capacity as border guards.

2. THEORETICAL-METHODOLOGICAL ANALYSIS: STATES, BORDERS AND INTERNATIONAL PROTECTION

2.1. CONCEPTUAL MAP OF THE BORDER ENVIRONMENT

2.1.1. The border concept

The term "border" has almost as many meanings as there are branches of science that have contemplated the study of any concept derived from the intuitive notion of "boundary". From mathematics to political science, from international relations to law. Sanz Donaire (2023, p. 254) states that the term in question comes from the classical Latin term *frons*, the meaning of which would refer to "front" or "façade", and would already offer an idea of the antagonistic or distinctive context in which it would develop from its formulation, strongly linked to the military sphere, to protection against the foreign, the exterior. Indeed, borders have been linked to conflict and confrontation since the Treaty of Mesilim, considered the "oldest treaty on record" (Doebbler, 2018, pp. 374-375), which was nothing more than an agreement regulating the recognition of the boundaries between several Mesopotamian kingdoms around 2500 BC. Curzon (1907) also expressed himself in this sense at the dawn of the scientific study of International Relations, when he stated that border tensions have been the most important factor in conflicts between states (p. 4).

In any case, it is on such etymological antecedents that the current conceptions of frontier are based, among which the Dictionary of Legal Spanish stands out for its discursive power, which states the following:

"Border (Public International Law): *Line marking the outer limit of the territory of a State, understood as the land, sea and air space over which it exercises sovereignty,*

which makes it possible to speak of land, sea and air borders depending on the physical nature of the delimited space.

2.1.2. Borders and sovereignty

According to Lacan's thesis (1966), the understanding of concepts is based on the understanding of the relations that they develop with respect to those previous notions that make up their meaning, by means of a concatenation of references in what the French psychoanalyst knew as "chains of signifiers" (pp. 501-502). In this sense, and taking into account the definition set out in the previous epigraph, it seems evident that we cannot reach a satisfactory understanding of the reality under study without first studying the other technical concept that is at stake in it: that of sovereignty.

A great deal has been written about this concept. Ever since John Bodin's first approach in the sixteenth century, in which national, territorial and theological components were intrinsically linked, the notion of sovereignty has been linked to the existence of a link that goes beyond the mere physical and social extension in which power is exercised, and which in some way transcends the strictly territorial. Perhaps this is why there are not many written sources of international law that offer a crystalline and universal definition of sovereignty. One of the few texts that can give us some clue in this respect is the 1933 Montevideo Convention on the Rights and Duties of States. This treaty offers what, in practice, has ended up becoming a definition of sovereignty, by establishing, in article 1, the basic requirements for a state entity to be considered a subject of international law:

1. Permanent population.
2. Territory determined.
3. Government.
4. Ability to enter into relations with other states.

It is noteworthy that, despite the fact that formally this treaty is only applicable to the very small number of states that signed it (it was agreed at the Seventh International Conference of American States, the direct predecessor of the Organisation of American States), it "has received general adherence from the doctrinal point of view" (Infante Caffi, 2016, p. 66), with its postulates gradually extending -either by direct reference or by reference to an international custom supported by them- to a generality of international actors, including the European Union itself. 66), gradually extending its postulates - either by direct reference or by reference to an international custom based on them - to a generality of international actors, including the European Union itself[5] .

Likewise, international case law has gradually defined the concept of sovereignty, being that, in the absence of an objective title (for example, a boundary treaty signed and observed by all the States concerned), a State is considered to be sovereign over a territory

[5] See, for example, the European Council Conclusions on the Middle East Peace Process of 20 July 2015; or the European Parliament resolution on the role of the EU in the Middle East Peace Process of 10 September 2015; which promote a path towards the recognition of Palestine as a political entity ('two-state solution') on the basis of a permanent population (repeatedly referred to as the 'Palestinian population'), a permanent territory (noting its commitment to the '1967 borders'), an effective government (embodied in the 'Palestinian Authority', hereafter PNA, which is expressly cited) and an ability to enter into relations with other states (citing and recognising the agreements reached with the aforementioned PNA).

when it shows its intention to be so by means suitable for this purpose in international law (e.g., a unilateral declaration) and, at the same time, when the State is capable of exercising this authority in a practical manner, through the effective development of jurisdiction over the territory (Judgment of the Permanent Court of International Justice of April 19, 1955), a unilateral declaration) and, at the same time, when that State is capable of exercising this authority in a practical manner, through the effective development of jurisdiction over the territory (Judgment of the Permanent Court of International Justice of 5 April 1933, pp. 45-27 in fine, 46-28 in limine; Judgment of the International Court of Justice of 17 December 2002, para. 134, pp. 182-61; Award of the Permanent Court of Arbitration of 9 October 1998, para. 239, p. 268; among others).

It will be on the basis of this sovereignty that the legitimate right of states to protect their borders, usually protected under the traditional rules of customary international law and the reference to Article 51 of the United Nations Charter, will be founded; and in the European case it will transcend to the national level, in view of the international obligation that the Schengen agreement entails for its signatories.

2.2. MIGRATION AND ASYLUM

On the other hand, when dealing with concepts related to the rights held by individuals within the border area, it is not unusual for certain misunderstandings to arise (for example, with regard to the notions of "immigrant" and "refugee"), which makes it advisable to study briefly but rigorously such a legal environment, especially with regard to the content and scope of international protection.

2.2.1. The right to asylum and subsidiary protection

The term "asylum" comes from the Greek *asylon*, a word whose translation is close to that of "inviolable place". In its initial conception, it was the condition that was granted to the *hieron*, a kind of special space located within the *témenos*, areas consecrated to the gods (Harris Díez, 2011, p. 70), which were outside the jurisdiction of the state, "and could thus become a refuge for persecuted individuals, escaped slaves or politicians" (Zaidman and Schmitt-Pantel, 2002, p. 45). It was on this background that the Christian dogma of "asylum in the sacred", a status of immunity traditionally conferred on places of worship in order to protect the needy and redeem repentant criminals, was formed (Golmayo, 1866, pp. 88-89), from which in turn the modern concept of the "right of asylum" would later derive.

This modern concept of the right to asylum will be established fundamentally through the proclamation of two texts: the 1951 Geneva Convention relating to the Status of Refugees (hereinafter the Geneva Convention), which establishes the concept of refuge; and its 1967 Protocol, which generalises such protection, initially created for a very limited list of beneficiaries. By combining these two texts, a single definition can be reached which recognises as a refugee or beneficiary of asylum any person who:

"...owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country; or, being unreasonably situated outside the country of

his former habitual residence, is unable or, owing to such fear, is unwilling to return to it".

On the other hand, although this is the general definition, the fact is that the different models of protection of existing fundamental rights have developed a whole battery of rules that expand and clarify the content of this right. In the European Union, this work is carried out through Directive 2011/95/EU, which establishes core aspects within the process of obtaining refugee status, such as the criteria for assessing the circumstances that may be considered as persecution, while (and this is extremely relevant) introducing into Community law the so-called "subsidiary protection", a guarantee that safeguards the legal situation of those third-country nationals and stateless persons who, "without meeting the requirements for obtaining asylum, [...] there are serious grounds for believing that they are in a situation of persecution", and who "do not meet the conditions for obtaining asylum, [...] there are serious grounds for believing that they are in a situation of persecution".there are substantial grounds for believing that if they were to return to their country of origin [...] they would face a real risk" (art. 4). This subsidiary protection - which, together with the right of asylum, forms what is generically referred to in EU terminology as "international protection" - is designed to extend the indemnity of refugee status to persons at risk of being sentenced to death, subjected to torture or even suffering the consequences of a military conflict.

In any case, all the aforementioned regulations explicitly establish the inapplicability of such protection to those who may be considered perpetrators of serious international crimes (war criminals, genocides, etc.), fugitives of serious common crimes or persons who represent a danger to the security of the host country.

2.2.2. Rights applicable to beneficiaries of international protection

All international protection grants a series of minimum rights to its beneficiaries, although certain accidental aspects of these (time limits, extension, etc.) may vary slightly depending on whether the status granted is that of asylum (more protected) or subsidiary protection (less protected). Furthermore, an important part of these rights will also be exercisable not only by those who have been officially recognised as beneficiaries of any type of protection, but European regulations also recognise their applicability to mere applicants, as long as their case has not been resolved[6] . In any case, there are two basic rights that are intrinsically linked to any form of international protection -including applicants- and whose nature will be decisive in the conflict between individual rights and national security: effective judicial protection and non-refoulement.

2.2.2.1. The right to effective judicial protection

The right to effective judicial protection, understood as the guarantee that citizens have "access to the jurisdiction, the processing of the proceedings, the [reasonable] resolution of the case and the enforcement of the sentence" (Carrasco Durán, 2020, p. 20), within the framework of a fair and impartial judicial system, is not a specific guarantee of the right to asylum, but its scope is universal, and as such it is included in the Spanish Constitution (art. 24) and the Spanish Constitution (art. 24). 20) in the framework of a fair and

[6] For example, and in line with the provisions of Directive 2013/33/EU, the right to access health care (Art. 19), public support (Art. 18) or the labour market (Art. 15).

impartial judicial system, is not a specific guarantee of the right to asylum, but rather its scope is universal, and as such it is included in the Spanish Constitution (art. 24) and in the EU Charter of Fundamental Rights (art. 47), under the permanent reference to the rights to a fair trial (art. 6) and to an effective remedy (art. 13).

However, its impact in the area of the right to asylum has been notable, to the point that Directive 2013/32/EU guarantees (art. 46) access to appeal in asylum procedures, explicitly stating that it must be heard by a "judicial" body. Thus, one of the most recurrent allegations when challenging the actions of the State in the border area has been an alleged lack or precariousness of access to judicial remedies. In this sense, and within the European sphere, the ultimate jurisdictional guarantee of effective judicial protection has been channelled - prior exhaustion of national instances - through recourse to the ECtHR for violation of Article 13 of the ECHR[7] . However, the case law of this court is clear: in order to find a violation of Article 13, there must first be a plausible claim of a violation of any other of the rights guaranteed by the Convention. Although it is not necessary for such a violation to have actually occurred, it has been required that there be such an *arguable complaint* under the Convention - ECHR (Grand Chamber) judgment of 23 February 2012, *Hirsi Jamaa v. Italy*, §197, which, from a first plausible approximation, then makes it possible to compose a reliable account of the facts, given that the Convention is intended to guarantee practical and effective rights, not theoretical or illusory ones - ECHR (Grand Chamber) Judgment of 13 February 2020, Case of *N. T. and N. D. v. Spain*, §171-. It is therefore rare to find isolated violations of Article 13 where no other violation is found, although doctrinally the possibility exists, and indeed has occurred - ECHR (Grand Chamber) Judgment of 8 July 2003, *Hatton and Others v.* United *Kingdom.* Within the field of the right to asylum, this relationship has almost invariably been conveyed through the connection of the infringement with violations of Article 3 of the ECHR[8] and Article 4 of Protocol 4 of the ECHR . [9]

2.2.2.2.2. Right of non-refoulement

For its part, the right to non-refoulement (enshrined in Article 33 of the Geneva Convention and usually referred to as *non-refoulement* in international doctrine) is a basic principle of international protection that implies the guarantee that the beneficiary of protection will not be returned to his or her State of origin or to any other where he or she runs the risk of being persecuted, as long as he or she maintains his or her status. This right extends directly to applicants during the examination of their case and, at the EU level, even to those whose international protection has not been officially granted or has been withdrawn (Art. 14(6) of Directive 2011/95/EU), insofar as 'it is the de facto circumstances of a person, [and] not the official validation of those circumstances, that give rise to Convention refugee status' (Hathaway, 1995, 303-304). And, at the same time, its observance is independent of whether or not the applicant is in a legal situation in the country, a fact which - despite not being explicitly mentioned in the articles of the Convention - has been imposed by means of customary international law and, in the European case, has been established by Article 19 of the CDFUE and Article 9 of Directive 2013/32/EU,

[7] "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.
[8] "No one shall be subjected to torture or to inhuman or degrading treatment or punishment".
[9] "Collective expulsions of foreigners are prohibited".

being endorsed through a repeated and peaceful jurisprudence in this regard in the framework of the European system for the protection of human rights[10] . This means that the right to non-refoulement has been configured as part of the most essential core of refugee rights, in the logic that its systematic violation would mean, in practice, the emptying of the content of international protection.

It is noteworthy that this principle admits an exception: article 33.2 of the Geneva Convention guarantees its inapplicability in those cases in which there are "serious reasons" to consider that the beneficiary or applicant for international protection may be considered "a danger to the security of the country where he is" (art. 33.2). This provision, which reinforces the prerogatives of states in the framework of their legitimate right to protect their borders, has been endorsed, with certain nuances[11] , by international jurisprudence. A good example of this is the judgment of the ECHR (Grand Chamber) of 29 April 1997, *L.H.R. v. France, in the case of L.H.R. v. France. v. France*, in which the court endorsed the deportation of a Colombian national convicted of drug trafficking to his country of origin, on the grounds that his presence posed a "serious threat to public order", despite the applicant's warnings - shared by the now defunct European Commission for Human Rights, and even tepidly by the court itself - that the completion of his deportation could pose a danger to his life.

Finally, one last noteworthy issue is that the development of the principle of non-refoulement has given rise, over time, to the emergence of a complementary principle that has been generally taken up by the most important international legal instruments on the subject: the prohibition of collective expulsions of foreigners. This precept, which some authors such as Kamto (2007) consider (not without controversy) to be a "general principle of international law" (p. 129), has been normativised in the ECHR (Article 4 of Protocol 4) and in the CFREU (Article 19.1). Its content refers to the approach that any expulsion of foreigners must be based on non-arbitrary circumstances, and thus requires an individual assessment of the context of each foreigner.

---

[10] Judgments of the ECtHR of 7 July 1989, *Soering v. the United Kingdom* and, in particular, of 15 November 1996, *Chahal v. the United Kingdom*.

[11] For example, the implementation of this precept at the European level should not mean that, by omission, it leads to the violation of Article 3 of the ECHR, which proscribes torture and inhuman or degrading treatment or punishment; A factor which, on the other hand, is applicable to the entire international community, having been considered as an argument of a *jus cogens* nature (Judgment of the International Criminal Tribunal for the former Yugoslavia of 22 February 2001, *Prosecutor v. Dragoljub Kunarac Radomir Kovac And Zoran Vukovic*, §466; or Judgment of the International Court of Justice of 20 July 2012, Questions relating to the obligation to prosecute or extradite, *Belgium v. Senegal*, §99).

3. LEGAL ANALYSIS: CONFLICTING POSITIONS AND COURT RESPONSE

3.1. *HIRSI JAMAA V. ITALY*: THE GENESIS OF A DOCTRINE

On the basis of the aforementioned legislation, successive judicial pronouncements have gradually chiselled out the final regulatory framework which, at least for the time being, governs the complicated balance between legitimate state powers and the safeguarding of fundamental rights. To this end, one judgment stands out above all others which, due to the time frame in which it was handed down and its subsequent political implications, has been an unavoidable reference when it comes to establishing the minimum criteria for action at the border: the Judgment (Grand Chamber) of the ECtHR of 23 February 2012, *Hirsi Jamaa et al. v. Italy*.

Hirsi Jamaa is the name of a Somali national who was part of a group of approximately two hundred illegal immigrants who were disembarked in the port of Tripoli between 6 and 7 May 2009. This disembarkation took place directly from the three Italian State vessels (*Guardia di Finanza* and Coast Guard) which had proceeded, a few hours earlier, to intercept and rescue the group while they were sailing in precarious boats, some 35 nautical miles south of the island of Lampedusa, in the Maltese search and rescue area (hereinafter SAR). As a result of these events, Italy was sued before the ECHR, with a total of twenty-five parties joining the case.

However, what was relevant - for its novelty - in *Hirsi Jamaa* was not so much the application of Article 3 of the ECHR in the context of a return of immigrants - a practice already consolidated in judgments such as *Chahal v. the United Kingdom* - but rather that, for the first time, the court had the opportunity to rule on the rejection of immigrants intercepted in the maritime environment at the same time as assessing the extraterritorial application of the ECHR (Alarcón Velasco, 2015, p. 4). And it did so by delivering a resounding blow to the Italian thesis, as it declared the violation of articles 3 and 13 of the ECHR, as well as article 4 of its protocol number 4, in all cases unanimously.

The core reasoning behind the court's position was as follows:

1. On a general level, the ECHR is applicable insofar as, according to Articles 92 and 94 of the United Nations Convention on the Law of the Sea, the ships on which the events took place are subject to the jurisdiction of their flag State, being a case of "extraterritorial exercise of jurisdiction [...] liable to engage the responsibility of the State".
2. With regard to Article 3, the determining factor was the impossibility of considering Libya as a "*place of safety*" for disembarkation, as the court considered that not only safety from a maritime point of view should be taken into account[12] , but also issues relating to the protection of their fundamental rights (breach of the principle of non-refoulement).

[12] The absence of risk in the concepts related to safety at sea that can be found in the international conventions on the subject (especially in the SAR and SOLAS conventions) mostly refers, by reference, to aspects related to navigational or operational safety (*safety*, safety as protection against shipwreck, against drowning, against the risks inherent in the ship's cargo, etc.). Notwithstanding the above, and in relation to the concept of "*place of* safety" existing in the SAR Convention of 1979, the International Maritime Organisation (hereinafter IMO) itself has ended up integrating nuances that complement this vision, resulting in

3. With regard to Article 4 of Protocol 4, the determining factor was the failure to individualise the expulsion of the immigrants, insofar as they were not identified and it was not assessed whether any of them might have relevant personal circumstances (violation of the prohibition of collective expulsions).
4. With regard to Article 13, the determining factor was the immigrants' inability to have access to an effective remedy against the expulsion decision (infringement of the right to effective judicial protection), a factor that could be assessed in view of the violation of Article 3.

3.2. CASE *N.D. AND N.T. V. SPAIN*: THE LIMITS TO PROTECTION

As discussed in the previous sections, the universality of the right to seek international protection does not imply that such a right can be claimed or exercised in an unlimited manner. The Judgment of the ECtHR (Grand Chamber) of 13 February 2020, in the framework of the case of *N. D. and N. T. v. Spain*, will be but one of the best examples of how nations can, on their own, establish efficient border control schemes that, in turn, are respectful of international humanitarian law, combating the abuse of rights from a guarantee perspective.

Emulating the analysis carried out in the previous section regarding *Hirsi Jamaa*, the present case involves two foreign nationals, N. D. and N. T., who, as part of a group of some 600 people, attempted to storm the border fence in the city of Melilla in the early hours of 13 August 2014. Their attempt was thwarted thanks to the action of the Guardia Civil and the Moroccan security forces, the two plaintiffs were escorted to the other side of the border, an act that will motivate the lawsuit. Subsequently, both actors would participate in two new assaults on the fence, managing to gain illegal access to Spanish territory. It is relevant that one of them would later apply for international protection, although this was denied at all procedural instances.

At this point, the interest of the ruling is twofold. On the one hand, because it was the definitive endorsement of the practice of "*rejection at the border*" (sometimes pejoratively referred to as "*hot return*"): the execution of an immediate return to Morocco of any immigrant caught trying to illegally overcome the border containment elements. And, on the other hand, because it represents a counterpoint to *Hirsi Jamaa*, since both mark the limits of legality from a different perspective: positive in *N. D. and N. T.* (what can be done), negative in *Hirsi Jamaa* (what cannot be done), thus indicating the two boundaries between which border legislation must run. All of this in the context of the existence, in this case, of a lower court ruling that contradicted Spain's arguments, which gave rise to a more detailed process of substantiation by the Grand Chamber in response to the claims of the plaintiffs, who challenged the actions of the border guards for violation of Article 3 of the ECHR and Article 4 of Protocol 4 of the ECHR, as well as Article 13 of the ECHR in relation to the two previous ones.

Thus, the core reasoning underpinning the court's position was as follows:

---

texts such as Annex 34 of IMO Resolution MSC.167(78), *Guidelines on the treatment of persons rescued at sea*, in which reference is made to regulations such as the Geneva Convention of 1951.

1. With regard to Article 3, already at the same stage of admission (decision of 7 July 2015), the Court flatly rejects the admissibility of the plaintiffs' arguments regarding the possibility that the principle of non-refoulement (Article 3 ECHR) had been breached by the refusal to return the immigrants to Morocco. Although the legal reasoning is not particularly detailed, it does clearly highlight the absence of evidence to consider Morocco an unsafe place for such purposes, and does not even - as it did in the case of Hirsi Jamaa - consider it necessary to consider the issue in greater depth.
2. With regard to Article 4 of Protocol 4, the Court's position is that a collective expulsion cannot be considered to exist in the context of an action in force triggered by the applicant himself, and which causes "a clearly disruptive situation which is difficult to control and endangers public safety" (§201). This is particularly relevant if we take into account that, in the judgment of the lower court, the Chamber had directly established - without even raising a justification that would affect the merits of the case - a total parallelism of this case with Hirsi Jamaa, despite the fact that they are totally different contexts. Thus, the court provides that such an "individualised examination" to overcome the conceptual obstacle of collective expulsion must be carried out taking into account "the particular circumstances of the expulsion and the 'general context at the time of the facts'" (§197), which in turn allows assessment procedures to be simplified or omitted, especially if this context depends largely "on the applicant's own conduct" (§200) and if the State provides "available legal procedures to enter [the country]" (§208) and "guarantees the right to seek protection [...] in a real and effective manner" (§208) and "the right to seek protection [...] is guaranteed [...]" (§209).in a real and effective manner" (§208).
3. With regard to Article 13, the Court clarifies that no violation of the right to effective judicial protection can be found, also attributing the lack of judicial remedy to "the applicants' own conduct in attempting to enter Melilla without authorisation" (§242).

Finally, an interesting observation on the grounds of the judgment is that, while the Court rejects Spain's thesis regarding the limitation of jurisdiction on the basis of operational criteria -similar to those upheld by Italy in *Hirsi Jamaa*-, stating that the effective exercise of authority that Spain, through the Guardia Civil, exercises from the perimeter of the outer fence inwards (§§107-108), is undeniable, it establishes that the Spanish Government cannot be held responsible for circumstances occurring outside its sovereign territory, through the Guardia Civil from the perimeter of the outer fence inwards (§§107-108), establishes that the Spanish Government cannot be held responsible for circumstances occurring outside its sovereign territory, and in particular those carried out by agents of a third State (§218).

3.3. COMPARATIVE ANALYSIS: THE COMPATIBILITY OF A DISPARATE JURISPRUDENTIAL DOCTRINE

As we have seen, both *Hirsi Jamaa et al. v. Italy* and *N.D. and N.T. v. Spain* represent two cases in which, for a priori analogous conduct (the surrender to non-European authorities of foreigners attempting to illegally enter Community territory), the ECtHR has offered different rulings. And this is fundamentally due to the existence in the *N.D. and*

N.T. case of a common thread that was duly and opportunely claimed by Spain in the framework of the proceedings followed during the aforementioned litigation, and which articulates, from beginning to end, the judgement: the doctrine of "culpable conduct".

The corollary of this reasoning is that the State cannot be held responsible for the fact that immigrants evade legal procedures to enter the country, especially if they "deliberately take advantage of their large numbers and use force" (*N.D. and N.T. v. Spain*, §201). Thus, for this doctrine to be applicable, the reprehensible conduct attributable to the migrants must generate a serious situation, arising from wilful conduct - i.e. conscious of its illegality and possible consequences - that represents an objective danger to public safety, including that of the migrants themselves.

Indeed, the Court's interpretation transcends all the alleged breaches alleged by the applicants, even those which (a priori) are furthest removed from their individual sphere of action. Thus, with regard to the prohibition of collective expulsions of foreigners (Article 4 of Protocol 4 of the ECHR), the ECtHR will situate the differential aspect in the immigrants' possibilities of access to legal procedures for entry into European territory. Thus, in *N. D. and N. T.*, it is repeatedly stated that Spanish law offered various possibilities for the applicants to process their entry into Spain, as well as to apply for asylum[13] (§212), but that these tools were refused (culpable conduct) by the applicants (§231). The same reasoning applies in respect of the right to effective judicial protection (Article 13 ECHR), as the arguments used by the Court of Guarantees are the same (§242).

Having set out these premises, the question inevitably arises: could *the* doctrine of culpable conduct be used, *mutatis mutandis*, for expulsions taking place in the maritime sphere? And, if so, what would need to be changed in the framework of state action in order to do so? The answer to these questions is not trivial. Following *N.D. and N.T.*, the ECtHR has used this doctrine - which, moreover, was not entirely new at the time of its formulation[14] - on a few occasions[15] , although none of them have served to endorse a maritime refusal. However, what is certain is that there is no passage in *N.D. and N.T.* in which the court states that its doctrine is not valid for expulsions of immigrants intercepted at sea. Quite the contrary: the judgment stresses the need for an assessment of the "circumstances of the individual case" (§201). As a result of this, and under the principle *permissum videtur id omne quod non prohibitur*[16] , it seems logical to deduce that the admissibility of such a principle should depend only on the fulfilment of its intrinsic presuppositions; that is, on the existence of real legal tools that allow access to the State of destination and to initiate an asylum procedure before its authorities; as well as on the

[13] The possibility offered by Spanish legislation of accessing certain asylum-related procedures in embassies and consulates (Article 38 of Law 12/2009, of 30 October, regulating the right to asylum and subsidiary protection) is particularly noteworthy, both because of the Court's repeated emphasis on this possibility and because it is not a common practice in other European states (Italy, for example, does not include it in its Legislative Decree of 19 November 2007, on the recognition of international protection).

[14] The ECtHR had already used a precursor approach to this in 1996 in the case of *John Murray v. United Kingdom* - Judgment (Grand Chamber) of 8 February 1996 - when it refused protection to a man convicted of terrorism who alleged that his silence had been used against him in the context of his judicial proceedings. The court ruled that it was he who had chosen to remain silent despite being aware of the consequences that such conduct could entail, and that it was therefore he who had exposed himself to the inference that his silence was prejudicial to him (§56).

[15] Judgment of the ECtHR (Third Section) of 24 March 2020, *Asady and others v. Slovakia*.

[16] "Everything that is not prohibited is considered permitted".

finding of reprehensible conduct on the part of immigrants who, while disregarding the existence of such legal tools, defy the border control mechanisms by means of coercive action. Moreover, both prerequisites must be duly invoked by the state in the judicial process, which Italy failed to do in *Hirsi Jamaa*. None of these prerequisites seems necessarily invincible in a typical maritime scenario in which hundreds of men of unknown origin and background put themselves, their fellow travellers and European border and coast guards in manifest danger by proposing a massive, planned and coordinated departure of boats bound for an isolated territory, which has limited reception capacities, with the consequent risk of collapse - such as Lampedusa. All of this is subject to the need for the coastal state to have an adequately sized diplomatic deployment with powers granted in the field of asylum, which allows it to justify the sufficiency of mechanisms for access to asylum. In this respect, mention should also be made of the community that the EU represents in terms of migration and asylum, which would even make it possible to suggest - although perhaps for this it would be necessary to make further progress in the ever-slowing European integration process - that the existence of diplomatic delegations from other EU countries is an asset that must necessarily be valued for the purposes of adequately weighing up the possibilities of access offered by the litigant state, as it represents an inherent reinforcement of the state's own resources .[17]

And, in line with the above, it is also pertinent to bring up certain inferences regarding the problem of the factual limitations of the state in its international action. Despite the fact that certain authors such as Sánchez Tomás (2018, p. 110) or Martínez Escamilla (2021, pp. 6-7) claim territoriality as the dominant perspective in terms of determining international responsibility, the truth is that both international doctrine and practice (already referred to in point 2.1.2 of this text) point to the need for a practical exercise of territoriality in the determination of international responsibility.2 of this text) point to the need for a practical exercise of authority in that territory in order to be considered sovereign, which is why the court, in its Grand Chamber judgment, amends its ruling at first instance by eliminating or greatly softening the mentions relating to the preponderance of the layout of the border as opposed to the actual route of the fence (included in §53 of the judgment at first instance). Thus, as we have already mentioned, the rejection of the exemption from the general principle of attribution does not hinge on the territoriality of the point where the acts take place, but on the fact that the action is carried out by agents of the signatory state, regardless of where the action takes place. This will be relevant in cases (for example, the events of 24 June 2022 in Melilla) in which Spain has been held responsible for acts carried out by foreign officials in areas which, although formally within the "historical" Spanish border, in practice are located beyond the fence, and therefore no effective control is exercised over them by Spain.

Finally, we must highlight the different treatment that the court gives to the study of possible violations of Article 3 ECHR (prevention of torture and inhuman or degrading treatment) in *Hirsi Jamaa* and in *N.D. and N.T.* Despite the scant justification offered by

[17] After all, it seems obvious to think that, given the pre-existence of a common area of freedom, security and justice, in the framework of which internal borders have been abolished and which has articulated mechanisms for implementing a common immigration and asylum policy, a network made up of each and every one of its embassies and consulates provides candidates for immigration with a much greater, more diversified access platform with a greater number of procedural guarantees than that offered by a separate state. Especially if we take into account the homogeneity implied by European legislation with respect to the recognition, qualification, assessment and resolution of asylum, stay and legal residence procedures, which are common to all its member states.

the decision to reject *N.D. and N.T.* in this regard, it seems clear that the justification for this difference lies, at least for the most part, in the country of expulsion. Part of the doctrine (Del Valle Gálvez, 2018, pp. 25-49; Freedman, 2024, 204-220) has come to put forward theses that come close to a generalised questioning of what has come to be called "border externalisation policies", a concept with which it is necessary to be very cautious. Firstly, because this pejorative term has been used to define what are, in most cases, nothing more than international police cooperation policies in the area of border control, through which capacity building is promoted to strengthen law enforcement in developing countries. Thus, even the very term chosen seems rather unfortunate, since it is difficult to "outsource" border control and law enforcement tasks, which are nothing more than "obligations derived from both conventional and customary law", and therefore the object of "*ius cogens*" (Soler García, 2017, p. 41). And, on the other hand, because irrationally accepting positions tangentially contrary to these policies would jeopardise not only the application of legitimate state measures - the expression of its sovereignty in matters of national security or migration policy - but also the interests of the international community and the protection of human rights: after all, the capacity building of states of origin and transit in vital matters such as the search and rescue at sea of their own compatriots is also an essential part of this cooperation. It follows that such cooperation *per se* cannot contradict the ECHR.

And this is where the truly differential factor in *Hirsi* Jamaa comes in: Libya. In this sense, Libya's situation is certainly idiosyncratic. It is a state that has not signed the Geneva Convention, which has been repeatedly defined by different authors as a "chaos", in which "migrants expelled from Europe were often left to an uncertain fate" (Cole, 2012, p. 6). And this perfectly explains the fears expressed by the court in *Hirsi Jamaa* (§136), on the basis of various reports incorporated into the case (UNHCR, European Commission, Council of Europe, Human Rights Watch, etc., see §33-42). This situation is not comparable to that existing in practically all the states with which Spain has active and reasonably functional repatriation agreements, mainly Morocco and Algeria, states that are part of the European Neighbourhood Policy - which requires, according to Article 8 TEU, sharing the EU's democratic principles - and which have benefited greatly from it, becoming privileged economic and political partners. After all, there is a wealth of judicial pronouncements[18] that explicitly endorse their status as "safe third countries" (see SAN 1441/2018 of 15 March 2018 for the case of Morocco or SAN 3838/2016 of 17 October 2016 for the case of Algeria). And this is a point of great interest not only for the purposes of the return of irregular migrants to their countries of origin, but also in relation to the possibility (endorsed by Article 3(3) of Regulation 604/2013 on the determination of the Member State responsible for the examination of an application for international protection) of referring asylum seekers to centres located in safe third countries during the review of their application. However, this possibility could be the subject - given its

[18] Practically all of these pronouncements come from national spheres, given that the ECtHR avoids categorical pronouncements on the security of states and prioritises a case-by-case analysis, as do the Spanish high courts. On the other hand, several European countries have drawn up lists of safe third countries, including Morocco on some of them, as is the case, for example, in the Netherlands (Immigration and Naturalisation Service, 2018). This practice is gaining ground among European states and is in line with the provisions of the Migration and Asylum Pact, which has introduced this concept in the new Asylum Procedures Regulation (Regulation (EU) 2024/1348), which will start to apply as of 12 June 2026 (Section V, arts. 57 et seq.).

complexity and foreseeable controversy - of a whole separate article, with its corresponding doctrinal debate.

4. CONCLUSIONS

To conclude, we will make a brief synthesis of the doctrine reviewed in the previous chapters, offering some guidelines that describe the findings of greatest interest in the matter under analysis.

Firstly, the most general and obvious conclusion that can be drawn from the above is that numerous social phenomena converge in the border environment, which generate a high level of litigation on the protection of fundamental rights. These processes, all derived from the permanent tension between migration control policies and individual guarantees, require a balance that is often settled in the courts, putting national and international legal frameworks to the test; as well as a series of concepts handled by the doctrine - border, sovereignty, territory, asylum, etc. - which, despite being habitually used in a trivial manner, possess a content of great legal, political, social and even historical power. It is therefore essential that the security forces that provide their services at borders have sufficient knowledge of the legislation that protects them, in order to carry out their duties efficiently, but also with respect for the rights of those who pass through such environments.

On the other hand, it is noteworthy that the majority of these judicial proceedings are substantiated in relation to the violation of very specific guarantees, which are regularly repeated in the pronouncements of the judicial bodies in charge of their prosecution. These are fundamentally the transgression of the principles of non-refoulement and the right to effective judicial protection, doctrines whose safeguard, in the European framework, is enshrined in Articles 3 and 13 of the ECHR; as well as the prohibition of collective expulsions of foreigners, protected in Article 4 of Protocol 4 of the said Convention. These judicial proceedings, however, are lengthy and very complex, and their decisions are often in direct conflict with previous rulings by other courts or even by the same bodies that issue them. For these reasons, it is also essential that the bodies responsible for the representation and defence of sovereign states have a thorough knowledge of international law, and know how to make such doctrines compatible with their domestic law - even proposing the necessary legislative amendments - in order to ensure, as guarantors of the legal system, that the rulings affecting their spheres of representation are in line with international law and practice.

Finally, and in line with the above, the mutability that characterises the interpretation of the international legal order cannot be overlooked. This is not a weakness of the system in itself: the rules, especially in anarchic environments such as this one, are in a permanent process of transformation, and therefore legal operators have no choice but to adapt their positions to existing realities, something that has been done since antiquity, when there were legal figures that were unthinkable in the contemporary world. In this sense, such a volatile scenario as that which governs current world geopolitics requires - with respect for the consensuses inherent to the maintenance of international peace and security, among which is the consideration of the dignity of the individual as an inalienable source of human rights- a certain margin in the interpretation of the norms that govern the obligations of states, a position that is not new in doctrine (Koskenniemi, 2004). In

this way, adequate compliance with these is guaranteed, respecting the will of their promoters while favouring coexistence, thus deepening the development of a prosperous international environment for all its inhabitants.

BIBLIOGRAPHICAL REFERENCES

Alarcón Velasco, N. (2015), El abogado ante las normas de asilo: vigilancia de su aplicación, Consejo General de la Abogacía Española. Available online: https://www.abogacia.es/actualidad/noticias/el-abogado-ante-las-normas-de-asilo-vigilancia-de-su-aplicacion/. [Accessed on: 31/03/2025].

Carrasco Durán, M. (2020). La definición constitucional del derecho a la tutela judicial efectiva, in Revista de derecho político, núm. 107, 13-40.

Cole, P. (2012), Borderline Chaos? Stabilizing Libya's Periphery, Middle East, October 2012, Washington: Carnegie Endowment for International Peace.

Spanish Commission for Refugee Aid (3 October 2017), European Court of Human Rights condemns Spain for two 'hot returns'. Available online: https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/. [Accessed on 31/03/2025].

European Commission (2022), State of Schengen Report 2022, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2022) 301 final. Available online: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri= CELEX:52022DC0301. [Accessed on: 31/03/2025].

European Commission (2024), Standard Eurobarometer. Europeans' opinions about the European Union's priorities, No. 102, Brussels: Publications Office of the EU. Available online: https://europa.eu/eurobarometer/surveys/detail/3215. [Accessed on 31/03/2025].

Council of the European Union (2015), Council Conclusions on the Middle East Peace Process. Available online: https://www.consilium.europa.eu/en/press/press-releases/2015/07/20/fac-mepp-conclusions/pdf/. [Accessed on 31/03/2025].

Consejo General de la Abogacía Española (3 October 2017), La Abogacía reitera la ilegalidad de las devoluciones en caliente, tras la condena del TEDH. Available online: https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/. [Accessed on 31/03/2025].

Curzon, G. (1907), Frontiers, Oxford: Clarendon Press.

Del Valle Gálvez, A. (2019), La fragilidad de los derechos humanos en las fronteras exteriores europeas, y la externalización/ extraterritorialidad de loscontroles migratorios in Anuario de los cursos de derechos humanos de Donostia-San Sebastián, Vol. XVIII, Valencia: Tirant lo Blanch.

Doebbler, C. (2018), Dictionary of Public International Law, London: Row-man & Littlefield.

Eurostat (2025), Population on 1 January by age group, sex and citizenship. Available online: https://ec.europa.eu/eurostat/databrowser/view/migr_pop1ctz/default/ table?lang=en. [Accessed on 31/03/2025].

Freedman, J. (2024), The violent externalisation of asylum in Research Handbook on Asylum and Refugee Policy, pp. 204-220, Cheltenham: Edward Elgar Publishing.

Frontex (2021), Risk Analysis for 2021, Warsaw. Available online: https://www.frontex.europa.eu/publications/risk-analysis-for-2021-MmzGl0. [Accessed on 31/03/2025].

Frontex (2024), Annual Brief 2023, Warsaw. Available online: https://prd.frontex.europa.eu/document/annual-brief-2023/. [Accessed on 31/03/2025].

Golmayo, P. B. (1866), Instituciones de Derecho Canónico, Madrid: Imprenta de A. Peñuelas.

Harris Díez, R. (2011), El paisaje de los dioses: los santuarios griegos de la época clásica y su entorno natural, in AISTHESIS: Revista Chilena de Investigaciones Estéticas, núm. 49, Santiago de Chile: Instituto de Estética de la Pontificia Universidad Católica de Chile.

Hathaway, J. C. (2005), The rights of refugees under International Law, Cambridge: Cambridge University Press.

Infante Caffi, M.T. (2016), Las fronteras desde la perspectiva del Derecho Internacional, in Revista de Estudios Internacionales, núm. 185, pp. 59-86, Santiago: Instituto de Estudios Internacionales de la Universidad de Chile. Available online: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692016000300004. [Accessed on: 31/03/2025].

Kamto, M. (2007), Third report on the expulsion of aliens, Geneva: United Nations International Law Commission.

Koskenniemi, M. (2004), The Gentle Civilizer of Nations: The Rise and Fall of International Law 1870-1960, Cambridge: Cambridge University Press.

Lacan, J. (1966), Écrits, Paris: Éditions du Seuil.

Martínez Escamilla, M. (2021), Las "devoluciones en caliente" en el asunto N. D. y N.T. contra España (Sentencia de la Gran Sala TEDH de 13 de febrero de 2020) in Revista Española de Derecho Europeo, Núm. 77.

Office of the High Commissioner for Human Rights (2018), Recommended Principles and Guidelines on Human Rights at International Borders, Geneva: UNHCR. Available online: https://acnudh.org/principios-y-directrices-recomendados-sobre-los-derechos-humanos-en-las-fronteras-internacionales/. [Accessed 31/03/2025].

European Parliament (2015), European Parliament Resolution on the role of the EU in the Middle East peace process. Available online: https://www.europarl.europa.eu/doceo/document/TA-8-2015-0318_EN.html. [Accessed on: 31/03/2025].

Real Academia Española (2014), Diccionario de la lengua española (23rd Edition).

Real Academia Española, Diccionario panhispánico del español jurídico (DPEJ). Available online: https://dpej.rae.es/. [Accessed on 31/03/2025].

RTVE (3 October 2017), The European Court of Human Rights condemns Spain for two "hot returns" in Melilla. Available online: https://www.rtve.es/noticias/20171003/tribunal-europeo-derechos-humanos-condena-a-espana-por-dos-devoluciones-caliente-melilla/1625420.shtml. [Accessed on: 31/03/2025].

Sánchez Tomás, J. M. (2018), Las "devoluciones en caliente" en el Tribunal Europeo de Derechos Humanos (STEDH, As. N.D. Y N.T. vs España, de 03.10.2017), in Revista Española de Derecho Europeo, núm 65, pp. 102-135.

Sanz Donaire, J. J. (2023). Del concepto de frontera, in Boletín de la Real Sociedad Geográfica, Número extraordinario 2023, pp. 253-262. https://doi.org/10.22201/ceiich.24485691e.2014.12.49710.

Immigration and Naturalisation Service (2018), Beoordeling veilige derde landen - Marokko, Informatiebericht SUA IB 2018/105. Disponible en línea: https://puc.overheid.nl/ind/doc/PUC_9890080000_1/1?solrID=PUC_9890080000_1_1&solrQ=morocco. [Accessed 31/03/2025].

Soler García, C. (2017), The European Border and Coast Guard: An advance on Frontex? Una valoración provisional, in Revista Electrónica de Estudios Internacionales, núm. 34. Available online: https://www.reei.org/ index.php/revista/num34/articulos/guardia-europea-fronteras-costas-avance-respecto-frontex-una-valoracion-provisional. [Accessed on: 31/03/2025].

Zaidman, L. B., Schmitt-Pantel, P. (2002), La religión griega en la polis de la época clásica (Díez Platas Trad.), Colmenar Viejo: Akal.

LEGISLATION AND JURISPRUDENCE

Charter of the United Nations (1945), United Nations Conference on International Organisation, signed in San Francisco on 26 June 1945.

Convention on the Rights and Duties of States (1933), Seventh International American Conference of Montevideo, League of Nations Treaty Series, volume 165, page 19.

Convention Relating to the Status of Refugees (1951), United Nations Conference of Plenipotentiaries on the Status of Refugees and Stateless Persons, signed at Geneva on 28 July 1951, United Nations Treaty Series, Volume 189, page 137.

Convention for the Protection of Human Rights and Fundamental Freedoms (1950), done at Rome on 4 November 1950.

Protocol Relating to the Status of Refugees (1967), signed at New York on 31 January 1967, UN Treaty Series No. 8791, Vol. 606, p. 267.

Decreto legislativo del 19 novembre 2007, n. 251, Attuazione della direttiva 2004/83/CE recante norme minime sull'attribuzione, a cittadini di Paesi terzi o apolidi, della qualifica del rifugiato o di persona altrimenti bisognosa di protezione internazionale, nonchè norme minime sul contenuto della protezione riconosciuta.

Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection.

Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection.

Directive 2013/33/EU of the European Parliament and of the Council of 26 June 2013 laying down standards for the reception of applicants for international protection.

Law 12/2009, of 30 October, regulating the right to asylum and subsidiary protection.

Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person.

Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 establishing a common procedure on international protection in the Union and repealing Directive 2013/32/EU.

European Court of Human Rights (1997), case of H.L.R. v. France, Judgment (Grand Chamber) of 29 April 1997.

European Court of Human Rights (2012), Hirsi Jamaa and others v. Italy Judgment (Grand Chamber) of 23 February 2012.

European Court of Human Rights (2015), case of N. D. and N. T. v. Spain, Decision (Third Section) of 7 July 2015.

European Court of Human Rights (2017), case of N. D. and N. T. v. Spain, Judgment (Third Section) of 3 October 2017.

European Court of Human Rights (2020), Case N.D. and N.T. v. Spain, Judgment (Grand Chamber) of 13 February 2020.

Permanent Court of International Justice (1933), Legal status of Eastern Greenland, Judgment of 5 April, Series A./B., Fascicle No. 53, Leiden: A. W. Sijthoff's Publishing Company.

International Court of Justice (2002), Affaire relative à la souveraineté sur Pulau Ligitan et Pulau Sipadan, Judgment of 17 December, Sales No. 858.

International Court of Justice (2012), Questions relating to the Obligation to Prosecute or Extradite (Belgium v. Senegal), Judgment of 20 July 2012,

Permanent Court of Arbitration at The Hague (1998), Territorial Sovereignty and Scope of the Dispute (Eritrea and Yemen), Award of 9 October, in Reports of International Arbitral Awards, Volume XXII pp. 209-332.

International Criminal Tribunal for the former Yugoslavia (2001), Prosecutor v. Dragoljub Kunarac Radomir Kovac and Zoran Vukovic, Judgement of 22 February 2001.

Audiencia Nacional (2018), Judgment 1441/2018, 15 March 2018.

Revista Científica del Centro Universitario de la Guardia Civil

Revista Logos Guardia Civil

Research Article

NIXON'S WAR ON DRUGS AND THE RISE OF VIRTUAL BORDER ENFORCEMENT IN THE UNITED STATES

J. Luigi M. Kunz Saponaro
Doctoral researcher at Carlos III University of Madrid
Masters in Geopolitics and Strategic Studies
Master's degree Security Defence and Geostrategy
jkunz@hum.uc3m.es

Received 31/03/2025
Accepted 21/05/2025
Published 27/06/2025

Recommended citation: Kunz Saponaro, J. L. M. (2025). Nixon's War on Drugs and the Rise of Virtual Border Enforcement in the United States. *Logos Guardia Civil Magazine*, 3(2), p.p. 147-170.

Legal deposit: M-3619-2023
Online NIPO: 126-23-019-8
Online ISSN: 2952-394X

NIXON'S WAR ON DRUGS AND THE RISE OF VIRTUAL BORDER ENFORCEMENT IN THE UNITED STATES

Abstract: This paper investigates the evolution of the United States–Mexico border from a historically symbolic boundary into one of the most fortified and technologically advanced frontiers in the world. Initial symbolic physical demarcations placed along the border, served to formalise the division between the two nations. However, recent decades have witnessed a significant transformation in border enforcement practices, characterised by the integration of digital surveillance mechanisms that strengthen traditional physical barriers. This study addresses this phenomenon by exploring the nexus between Nixon's War on Drugs and the digitalisation of the US–Mexico border during the Nixon Administration (1969–1974). By conceptualising the drug crisis as an existential threat, President Nixon's rhetoric framed these substances as the "enemy number one" starting his War on Drugs. This shaped a securitisation process that enabled the allocation of extraordinary resources to counter this new perceived menace. By employing the securitisation theory developed by the Copenhagen School, this paper analyses the role played by Nixon in framing the security threat to elucidate how this discourse justified the creation of virtual border control practices in the United States. The findings suggest that the securitisation of the drug crisis provided the necessary political and ideological foundation for adopting innovative digital surveillance technologies, a process that has since transformed border enforcement practices. This inquiry contributes to the academic debate on border digitalisation and offers a methodological framework for comparative studies on the virtual evolution of national boundaries.

Resumen: Este trabajo investiga la evolución de la frontera entre Estados Unidos y México, que pasó de ser históricamente un límite simbólico para convertirse en una de las fronteras más fortificadas y tecnológicamente avanzadas del mundo. En las últimas décadas se ha observado una transformación significativa en las prácticas de control fronterizo, caracterizada por la integración de mecanismos de vigilancia digital que refuerzan las barreras físicas tradicionales. El estudio que se presenta aborda este fenómeno explorando el nexo entre la Guerra contra las Drogas de Nixon y la digitalización de la frontera entre Estados Unidos y México durante la Administración Nixon (1969–1974). Al conceptualizar la crisis de las drogas como una amenaza existencial, la retórica del presidente Nixon definió las definió como el "enemigo número uno", iniciando así su Guerra contra las Drogas. Comenzó así un proceso de securitización que permitió asignar recursos extraordinarios para contrarrestar esta nueva amenaza percibida. Mediante el uso de la teoría de la securitización desarrollada por la Escuela de Copenhague, se analiza el papel desempeñado por Nixon al enmarcar la amenaza de seguridad, con el fin de dilucidar cómo su discurso justificó la creación de prácticas de

control fronterizo virtual en Estados Unidos. Los hallazgos sugieren que la securitización de la crisis de las drogas proporcionó la base necesaria para adoptar tecnologías innovadoras de vigilancia digital. Esta investigación contribuye al debate académico sobre la digitalización de fronteras y ofrece un marco metodológico para estudios comparativos sobre la evolución virtual de las fronteras nacionales.

Keywords: US–Mexico Border, Digital Surveillance, Securitisation Theory, War on Drugs, Nixon Administration

Palabras clave: Frontera EE. UU.–México, Vigilancia Digital, Teoría de la Securitización, Guerra contra las Drogas, Administración Nixon

1. INTRODUCTION

The border separating the United States (US) from Mexico is amongst the largest boundaries in the world. An altogether of mountains, deserts, and rivers characterise the 3,141 kilometres' orography separating the two countries. The first physical demarcations of the border were introduced with the end of the Mexican American War of 1847 resulting in the Treaty of Guadalupe (see Trist *et al.*, 2022). The political changes introduced by this Treaty were translated onto the territory by 52 stone mounds positioned from coast to coast along the entire margin (US Customs and Border Protection, 2019). Much changed since the symbolic separation demarcating the United State (US) southern limit. Today it has become one of the most fortified and technologically advanced borders that exist.

The virtual aspect of this border is of particular interest to the monitoring practices that countries worldwide engage in to secure their edges. In fact, the potential that contemporary surveillance systems have in terms of national edges' control has been subject to numerous studies until recent times (see Adams, 2001; Amoore, Marmura, & Salter, 2008; Heyman, 2008). Yet little is known on when and why specifically the US decided to intertwine the physical and virtual aspects of its boundaries to enhance the control over it. A puzzling hiatus especially considering the leading position the States have in terms of digitalised arsenal employed along the US-Mexican border combined with a rather meagre consideration of where it all started.

Research shows that there is a link between the Vietnam War and the US' implementation of virtual enforcement mechanisms along the US-Mexico border (see Barkan, 1972; Grandin, 2019; Rosenau, 2001). However, not enough attention has been granted to the link that unites these two separate events in US history. To be more precise, the nexus in question is Nixon's War on Drugs. It was by describing drugs as the enemy number one of the States and declaring a full out war on drugs in 1971 that the President managed to open a window for the digitalisation of the southern border. By addressing the following research question, this paper aims at filling this gap in the academic literature: How did the War on Drugs under the Nixon Administration contribute to the transition from a physical border control along the southern border to virtual enforcement mechanisms?

A valuable tool to find an answer to this question is offered by the securitisation theory. This theory was forwarded by the Copenhagen School and offers a theoretical framework that can be used to identify patterns in the securitisation process of an issue that awards extraordinary resources to counter it. In this research, these patterns elucidated by one of the School's main components Wæver (1995) are applied to Nixon's remarks on the War on Drugs and the subsequent investment in digital assets for the US' southern border.

This study sustains that the discourse that Nixon framed on drugs as a national threat enabled the US to advance in the virtualisation of the US-Mexican border. The timeframe subject of this paper's analysis coincides with the Nixon Administration's term, that is

from 1969 to 1974. Establishing at what time exactly and how the US managed to start its virtual border fortification is valuable to the academic debate. This is the case as the findings of this research can be used to compare the technological development on border studies in other countries during their initial phases of border virtualisation too.

In order to unfold the research with diligence, this paper is divided into the following sections. The first section gives space to the literature review on the most relevant theoretical approaches that have been adopted to conduct studies on virtual borders. The second section introduces the securitisation theory as the theoretical framework adopted by this study used to carry out its analysis. The third section summarises the operationalisation and methodology used to formalise this research. The fourth section is composed of the analysis of this study. In this section, the principles of the securitisation theory are applied to two emblematic speeches by Nixon. Thereafter, the resulting findings are commented based on the backing of secondary sources. The last section proposes a conclusion summarising the findings and considerations achieved throughout the present study.

2. LITERATURE REVIEW ON BORDERS AND VIRTUAL SURVEILLANCE

There are a number of theories that are used to appreciate the diverse foundations of borders and its transformative patterns. With a specific regard to the virtualisation processes of borders, the scope of theories that apply reduce consistently. So as to identify what has been written on the relation of borders and its digitalisation according to political needs, four main theories manage to capture the attention. This section is dedicated to discussing these distinct academic contributions. Each of them adds a different vision to the study's research topic and can be used to understand its origin.

A more philosophical perspective on surveillance studies was pushed forward by Michel Foucault. While reviewing the theory of the French philosopher, Lemke (2015) stated that "Foucault's work on governmentality not only offers important insights for an analysis of the state, it also provides analytical tools to investigate the relationship between liberal and technologies of security" (p. 5). More precisely, the Foucauldian governmentality theory describes how states employ power through disciplinary techniques and surveillance rather than direct force (Lemke, 2015). This theory discusses the extraterritorial dimension of border control managed by state actors that can go beyond the physical demarcation of its own country.

This idea proves to be luring for understanding border digitalisation since it can be applied to state practices that counter national security threats by reinterpreting physical demarcations. The idea behind this theory is to try blocking specific risks before they reach the border. To be more precise, national laws can be used to forward governmental changes that would see the computerisation of security issues threatening national safety. In doing so, states can move towards an increasingly virtual surveillance system used to monitor and eliminate hazards before they manage to enter its territory (see Armstrong, 1992; Paden, 1984). This stream of actions highlights how conventional borders can change once virtual configurations are embedded in border control practices.

Foucauldian governmentality's theory, nevertheless, falls short when applied to the research of drug related border securitisation. Although the theory mentions the technological prominence in the making of borders, it is mainly directed to a study of surveillance and control instead of focusing on border securitisation *per se*. This theory is unable to explain why policymakers act when confronted with unpredicted events – such as was the case of the 1960s drug crisis in the US. Along these lines, Kerr (1999) came to the conclusion that the theory cannot "account for the changing limits of government, apart from noting the mere fact that government often fails due to unplanned outcomes" (p. 196). Hence, even though this Foucauldian governmentality has proven to be pioneering in the virtualisation of borders, it does not allow to give a comprehensive response to the research question orienting the present study.

Another relevant theory used to analyse smart borders is technological determinism. This theory bases its fundamentals on identifying technological advancements as social and political drives. Particularly, it underlines the importance that technology has in shaping policy changes. As Smith (1994) put it: "technology's power [is] a crucial agent of change [that] has a prominent place in the culture of modernity" (p. ix). The push that makes novelties happen is not driven by the people, according to this theory, but rather by technology itself. This, in turn, causes changes that are first presented onto the political agenda and then implemented by policymakers.

Border transformations are thus understood as being the result of technological advances instead of socio-political impulses. In this sense, the rise of electronic surveillance along with biometric tracking and remote sensing made virtual enforcement viable in the first place. Hence, linking this perspective to the research question of this paper, drug enforcement strategies evolved resulting from technological possibilities instead of policy decisions. Accordingly, US politicians were pushed rather than pushing for technological change to implement virtual border enforcement to counter drug influx into the country.

Although technological determinism manages to give relevant insights to the change in border-regimes, it has been pinpointed for oversimplifying this process. It is largely debated that the social and political members are capable of swaying technology too instead of being at its mercy. That is, a deeper understanding of technology has allowed to control it (Dafoe, 2015, p. 1049; Lynch, 2008). The digital aspect of borders, correspondingly, is not the result of technological drive but rather controlled by politicians. Hence, the adaptation of the southern border of the US during Nixon's term can be seen as taking on a clear technological turn. However, this turn was controlled by men-led actions thereby making it hard to rely on technological determinism for the research this paper proposes.

The digital composition of borders can also be understood by Nail's border theory. This theory offers a vision of the border that sees an ever growing mobile and dispersed quality in conventional physical borders. In Nail's (2016) opinion, "the border is not reducible to the classical definition of the limits of a sovereign state" (p. 2). Borders, the author noticed, are inevitably evolving towards informational, or digital identity affecting

a country's societal comprehension. This means that borders have adopted a virtual form since modern problems affect the cross-border movement of people and goods deemed for up-to-date responses. In the case of drug trafficking in the US, for instance, new methods adopted by Cartels demanded innovative actions taken on by US' border control to counter this trend. In the 1960s and 1970s, these actions boiled down to the transformation of borders into networked control spaces.

Border theory, therefore, eludes the conventional understanding of boundaries as such. Instead of exclusively focusing on the territorial and physical aspect of it, as Sharma (2023, pp. 163-164) elucidated, it is necessary to expand this conception to intangible assets composing states' boundaries. The implications that this theory forwards adds a new dimension to the power of governments. That is, borders have not to be seen as a simple line, but instead as a large area surrounding the physical demarcation (Nails, 2016). In fact, states can reach far beyond their physical boundaries by means of virtual enforcement mechanisms with the goal of securitising its borders. Practical models of this being the US Border Patrol databases and intelligence sharing networks that has largely been used to securitise its southern border. In the 1970s, these Border Patrol systems led expansions that paved the way for today's digital border enforcement structures.

Border theory forwards the idea that states can monitor movement beyond its own boundaries. Territorial delimitations, according to this conception, become less relevant for governments when taking actions related to border monitoring (Sharma, 2023. P. 164). Although keeping on representing an important aspect of border policymaking, governments tend to act beyond the territorial delimitation with the idea to intercept potential threats. Said differently, prevention becomes as relevant as physical deterrence. The pitfalls of this mentality are extraterritorial political interventions that have a high chance to harm international relations. This theory proves to be useful to understand the general change of US' southern border conceptualisation. However, it can be used to study societal separation while lacking a clear link to border security issues.

In order to understand borders from a security related point of view, the securitisation theory of the Copenhagen school has to be taken into account. Otukoya (2024, p. 1750) noticed that the creation of a security problem can be key for creating extraordinary resources used to protect a nation from an imaginary hazard. This theory is useful to understand how digital features are used to reinforce the physical aspect of the boundary. Here the focus is set on, amongst other things, movement sensors, video surveillance, and any other technological feature that is used to monitor the territorial border with greater effect. Therefore, it presents itself as being the suitable theoretical framework necessary to identify such patterns along the US southern border.

When looking at the beginning of the War on Drugs, manoeuvres such as Operation Intercept undertaken in 1969, were justified as a necessary deed to fight US' public enemy number one of that time. In this operation, new forms of electronic border surveillance started to be needed for the first time in US border regime history. These needs epitomise the founding pillars of the complex technological dimension that characterise the country's contemporary border. Given the close relation that this securitisation theory has

with the goals of this research, a deeper look at its composition has to be taken into account. In the upcoming section, the securitisation theory is summarised. This enables to find key indicators to comprehend how US' border securitisation changed during the Nixon Administration taking on a virtual aspect.

3. SECURITISATION THEORY AS THEORETICAL FRAMEWORK

Securitisation theory is a useful framework that can be used to understand border security in the US during Nixon's presidency. The overall function of this theory is to explain how issues come to lead a country's decision-making process on matters such as border control. Applied to the study this paper engages with, this theory appears to be of valuable help to understand the virtual enforcement mechanisms that the US have added to their southern physical border. It is by applying securitisation theory to this topic that the present study aims at elucidating the role that President Nixon played in contributing to a virtual border implementation. This section is dedicated to point out the main tenets of the securitisation theory to formally being able to apply them to the paper's analysis.

The Copenhagen school based its theory on five main pillars. The pillars in question are (1) securitisation as a speech act, (2) elite framing of threats, (3) audience acceptance requirement, (4) referent object identification, and (5) reversibility and de-securitisation. All these factors combined can be used in this paper's analysis to discover how the US' War on Drugs contributed to the transition from physical border control to virtual enforcement mechanisms. Before delving into the analysis, however, each indicator is summarised and contextualized so as to clarify in what way it is then used applied to the revision's case study.

Declaring an issue as a security threat constitutes a performative act undertaken by a government. With this conception of security, Ole Wæver – the mastermind of securitisation theory – uncovers a performative act that governments take on when indicating to the audience the presence of a security-related issue (Wæver, 1995, p. 52). It is by directing attention to a problem that an elite can engage in a performance that opens a window for exceptional policy measures meant to halt a given hitch. It is irrelevant whether this issue represents an ordinary problem or real threat to national security. What matters is the state representatives are granted with a considerable freedom of action by its audience thereby legitimising their actions. This is what is called the speech act.

Speech acts are based on the vertical creation of trust between state officials and citizens. A successful speech act depends on the extent to which a promise or a declaration is accepted by the public. State representatives make leverage on the feeling of trust which people delegate them with to create a new political reality whose existence depends on the conceived security issue. It is by employing speech acts that legitimation for taking actions to face security threats are disclosed. This legitimisation, in turn, allows the unblocking of state resources to be mobilised creating actions that go beyond normal procedures and allow the formation of extraordinary measures (Wæver, 1995, p. 53).

This practice, however, is not exempt from risk. Wæver (1995) emphasised that this is the case since it made it difficult to distinguish between the act and the real degree of threat a country face (p. 6). In other words, the state can become a victim of its own narrative giving too much importance to a matter that in reality does not pose a real hazard to the nation's security. In doing so, there can be a counter effect of compromising the country's security by focussing too much on an inexistent problem and neglecting its real priorities.

The second indicator retrieved in the securitisation theory is the elite's practice of framing threats. Securitisation theory underlines the influence that key actors have on shaping policy actions. This process is initiated by these selected few who have significant influence within higher political ranks. Once these individuals manage to create a threat narrative, they assume the power to define what can be defined as being existential dangers to the country's security. The result is a cohesive state action meant to tackle the problem that stemmed from the creation of that same narrative.

The authority that the elite holds, nevertheless, is a double-edged sword. On the one hand, it allows the creation of a swift state reaction (Wæver, 1995, p. 54). This is particularly positive as often states are bounded by convoluted bureaucracy that considerably prolong the implementation time of official measures. On the other hand, this dominance enables elites to bypass conventional democratic processes (Wæver, 1995, p. 54). This means that, by speeding up the normally slow policymaking process, only a selected few concentrate decision-making power in their hands. The implication of this concentration of power allows the elite not only to decide how to deal with security threats, but also to decide what has to be considered a menace and what not. Thus, the framing of security issues can easily be linked to strategic interests that elites have (Wæver, 1995, p. 54). In other words, elites can decide whether to act to guarantee public security or personal interests.

This brings us to the third indicator: the audience acceptance requirement. Securitisation moves, according to the Copenhagen school, depends on the acceptance by relevant audiences. The main audiences of interest to the elite are the public, legislative bodies, or international partners. All of them – independently or not – must trust the constructed threat narrative to be true for creating the *momentum* needed to take practical actions. These, in turn, Wæver (1995, p. 53) sustained allow finding a solution to the proposed threat. Without the acceptance of the audience, even the most compellingly enunciated security claims can falter. Hence, the non-acceptance of a security issue backfires and creates a process of desecuritisation. The effort of the elite would thus vanish at the expenses of their strategic interests (Wæver, 1995, pp. 53-54). This is why the audience acceptance requirement indicator proposes itself as an essential factor. It is needed to analyse in what way public approval or defiance to unusual procedures can authorise or dent the shift from traditional and democratic practices.

The fourth indicator composing the securitisation theory can be identified with the referent object identification. The process of securitisation needs a clear specification of what is at stake. The stake, in this case, is referred to as the referent object. According to

Wæver (1995, p. 52), the referent object is generally identified with the state's integrity, sovereignty, or the security of its citizens. The process of defining the referent object is fundamental for the mobilisation of resources. In fact, a clear delineation of the object drawn by securitising actors unblocks the material means needed to defend that particular entity against alleged existential coercions (Wæver, 1995, pp. 52-53). This clear definition is fundamental for condoning the usage of exceptional actions as it determines what must be defended by all means.

Reversibility and desecuritisation embody the last indicator of the securitisation theory. According to the Copenhagen school, securitisation is subject to constant change. Once the audience ascertains that a security threat is not being existential anymore, they can reverse the securitisation measures taken so far and re-transform the issue into a normal political debate (Wæver, 1995, p. 55). This retraction allows for putting a check on the elite who framed the issue. This reversibility highlights how temporary emergency responses can be put apart after having experienced a momentaneous build-up. Hence, Wæver (1995, pp. 54-55) suggested that the act of securitisation comes with intrinsic risks that are inherent to the securitisation process. Said differently, securitisation measures can surge and fade easily making it difficult to predict the future actions a government can take in the area of security.

Overall, the principles that make up the securitisation theory forwarded by the Copenhagen school are valuable analytical tools. This is specifically the case with the research topic of this paper. Understanding how the War on Drugs might have been transformed into a security issue used to create space for exceptional measures can be facilitated by applying the analytical tools put at disposition by this theory. As a matter of fact, the principles listed in this section help evaluate the transformation of conventional criminal practices – such as drug smuggling and consumption – and health problems to unusual actions taken by the states to face these issues. Significant policy shifts were created by elites who engaged in speeches that gave birth to unheard of policies resulting in the adoption of virtual enforcement mechanisms to fight drug trafficking along the southern US border. The following section expounds the operationalisation and methodology that this paper adopts to conduct its analysis.

4. OPERATIONALISATION AND METHODOLOGY

Toshkov (2016, p. 100) described operationalisation as being the translation of abstract concepts into concrete notions that can be observed, classified, and empirically measured. The principles composing securitisation theory can be used with the same purpose. This paper operationalised four of the five key concepts to understand the role that the War on Drugs had in contributing to the US' transition to virtual borders. The four indicators composing the theory that are used in this paper to analyse the study's case study are: (1) securitisation as a speech act, (2) elite framing of threats, (3) audience acceptance requirement, and (4) referent object identification. The last principle pointed out in securitisation theory – reversibility and de-securitisation – is of no use to this research. That is, this last principle is useful to study the deconstruction of a security measure – a

part which this study does not intend to cover. Nevertheless, this does not compromise the soundness of this work as the patterns leading to the securitisation remain unchanged.

The four indicators are able to give a deeper understanding of the virtual dimension the southern border of the US took during Nixon's term. Consequently, a critical qualitative reflection on the research topic is pushed forward to understand the present-day US importance of enhancing digitalisation along its territorial border separating it from Mexico. The five indicators, therefore, are of fundamental importance to identify why the drug crisis managed to epitomise a key factor in virtual border enforcement mechanisms.

The methodology of this paper has to be clarified too. This research consists of a single case study. More precisely, it analyses the southern border of the United States during the Presidency of Nixon. Single case studies allow to give precise information on a specific case to create knowledge that then can be applied to similar cases too. That is, with this research, the model of investigation can then be used in similar cases to identify analogous patterns of evolution in virtual border control. The decision to opt for this case study is based on the fact that the US is amongst the very first countries that decided to opt for the partial digitalisation of its border. Therefore, the justification of the case selection resides within the interest to add new information to the academic research gap that is present on this topic.

A number of primary and secondary sources are used throughout the analysis of the subject-matter. The goal of a large range of information stemming from diverse sources helps consolidate and guarantee the quality of the findings of this research. As in primary sources, political statements, news articles, and public speeches are considered. In these sources, important features regarding the securitisation theory can be recognised. Whereas the secondary sources used in this study stem from academic studies that have been conducted on the topic of border security, virtual security, and the War on Drugs. This is a useful practice that enables to place the study's findings in a broader academic debate.

Discourse analysis represents the backbone of this study. The information retrieved from two speeches Nixon did with regards to the War on Drugs are scrutinised. Based on a qualitative method, the interpretation of given sources helps to identify the indicators presented in the theoretical framework. Political speeches forwarded by the US president are, thus, key to complete this study. Moreover, by applying this research method, it is possible to test the theory employed in this study. In fact, by applying the indicators proposed by the securitisation theory to speeches, it is possible to understand if there truly are patterns in political discourses that can lead to the securitisation of constructed risks.

The timeframe of this research is based on the Nixon Administration's term. More specifically, the time considered ranges from 1969 until 1974. This reduced time frame helps give space to a number of key actions undertaken by the US President at the time with regards to virtual control mechanisms along the US-Mexico border.

5. ANALYSIS

5.1. NIXON'S CREATION OF A SECURITY ISSUE

The surveillance of the border separating Mexico from the US from 1969 to 1974 predominantly shifted its focus to illegal drug trafficking. The Sinaloa region in Mexico's north-west stripped away the cultivation of opium from Chinese immigrants in the 1910s. Ever since, the Sinaloa Cartel became rich by exporting this substance mainly to the US. With the hippie generation and the trafficking of Marijuana, however, illegal importation of substances to the US became problematic for society (Grillo, 2013, p. 255). The drug problem became the pivotal topic around which President Nixon based most of its political activity. Beyond this, Timmons (2017, p. 15) called attention to the fact that Richard Nixon became the first president who made a promise to close the US-Mexican border to illegal drugs. As a matter of fact, while the war in Vietnam went on, "the Nixon Administration is quietly Americanizing the war's technology, and the war on the home front escalates" (Barkan 1972, p. 1).

In order to delve into the role Nixon played in starting this trend, the first part of the analysis is dedicated to the discourse analysis of two speeches held by the President in question. The communications in the query are *Remarks About an Intensified Program for Drug Abuse Prevention and Control* and *Special Message to the Congress on Drug Abuse Prevention and Control*. Both speeches were held on June 17, 1971. Both speeches took place on the same day and followed each other. In fact, the former epitomises the press conference held to explain what he mentioned during his address to the Congress.

Both speeches are key to understanding in what way an elite framing of a threat was proposed to the political and public audience. It is by taking a closer look at them that it is possible to understand how Nixon managed to unblock extraordinary resources to counter the new and constructed existential threat of drugs in the US. Both speeches are presented together in a document facilitated by the US Department of Defense (2017). After identifying the most relevant points in both of them, the paper proceeds to clarify the relevance that these unique measures have had on the virtualisation process of the southern US border from 1969 to 1974.

5.1.1. The creation of a National War of Drugs

When considering Nixon's speeches from the securitisation theory's point of view, it is necessary to look for a performative act. This act needs to bring to the audience's attention the existence of a security-related issue that is jeopardising their well-being. President Nixon did so by boldly declaring a full-out War on Drugs. At the press conference held, once having addressed the Congress with a special message, he opened his communication by stating that "America's Public enemy number one in the United States is drug abuse" (US Department of Defense, 2017, p. 1). A bombastic opening as such proved to be captivating for public spectators. It helped create a sensation of fear among the US population who was 15 years in the catastrophic Vietnam War. It is of no surprise

that any reference to national security threats, wars, and enemies in those years easily spiked feelings of paranoia and the desire to act.

In order to propose the new threat, Nixon had to point out what the threat actually consisted in. He did so by stating that:

> There are several broad categories of drugs: those of the cannabis family – such as marihuana and hashish; those which are used as sedatives, such as the barbiturates and certain tranquilizers; those which elevate mood and suppress appetite, such as the amphetamines; and drugs such as LSD and mescaline, which are commonly called hallucinogens. Finally, there are the narcotic analgesics, including opium and its derivatives – morphine and codeine. Heroin is made from morphine." (US Department of Defense, 2017, p. 10).

This is what the securitisation theory identifies with the referent object identification. By pointing out and insisting on who or what represents a threat, the audience can identify the problem and spur actions against it.

Furthermore, representing himself as a cautious President helped the performative act to become more convincing. Hence why he stated that "I very much hesitate always to bring some new responsibility into the white House, […] but I consider this a problem so urgent […] that it had to be brought" (US Department of Defense, 2017, p. 2). In doing so, Nixon attempted to portray himself as the protector and guarantor of the US whose actions were guided by the needs of US citizens and not by personal interests.

A number of exceptional measures were created so as to face this national security threat. Nixon affirmed that "it is necessary to wage a new, all-out offensive" (US Department of Defense, 2017, p. 1) evoking the necessity of a common effort to halt a peril that managed to enter US soil. These words clarified the extent to which the US was committed to actively fight off drug-related security threats. The enforcement of war-like measures, such as deploying and creating military and federal departments to control and fight drug routes heading to the US, epitomised the basis of this new plan of action.

At this point, it is necessary to highlight the acceptance of the audience of Nixon's speech act. It is, as a matter of fact, possible to say that the audience did accept his discourse adopted with the War of Drugs. Signalling this acceptance are a number of actions proposed by the Administration and then executed with overall support by the majority of the country. The most emblematic operation that started the War on Drugs was Operation Intercept launched throughout September and October 1969. This operation resulted in an almost complete closure of the border between Mexico and the US.

Operation Intercept presented a debacle due to the impossibility to control the entire border by means of physical disposition. Although two thousand Customs agents were deployed, no effective results were managed to be reached (see Reid, 2022). Nonetheless, public and political support yielded for further actions that opened the door for new types

of procedures. This was the case for the Comprehensive Drug Abuse Prevention and Control Act (CDAPC Act) of 1970 adopted to strengthen US control, amongst other things, along the southern border.

Operation Intercept and the CDAPC Act represent the milestones upon which his 1971 speeches were based on. In fact, these actions sparked a number of further government procedures to intensify the War on Drugs. An indicator of how President Nixon wanted to increase these procedures meant to halt this security threat is visible in the following passage: "We must now candidly recognize that the deliberate procedures embodied in present efforts to control drug abuse are not sufficient in themselves. The problem has assumed the dimensions of a national emergency" (US Department of Defense, 2017, p. 3). It was in this way that he succeeded in gaining bipartisan support for tackling this new and apparently devastating security threat.

To be more precise, the most important legislative actions taken since the two speeches analysed in this section were: the founding by Executive Order of the Special Action Office for Drug Abuse Prevention in 1971, broadening the Narcotic Addict Rehabilitation Act of 1966 in 1971, organising the International Security Assistance Act of 1971 along with the International Development and Humanitarian Assistance Act of 1971, crafting the Office of Drug Abuse Law Enforcement in 1972, and establishing the Drug Enforcement Administration (DEA) in 1973.

It is important to underline that these sorts of actions were only possible to attain with an extended political support. This was a trait which the President was aware of since he repeatedly focused on the bipartisan support of his actions throughout his press conference. It consists of an important aspect when considering securitisation theory since it underscores the power that the general acceptance gives to the elite framing the security threat. A power that allows the elite to take extraordinary actions in little time – something that clashes with the lengthy bureaucratic procedures that in these situations are overruled.

Beyond political support, Nixon managed to gain the societal acceptance of the threat he managed to frame. He did so by stressing how any member of the US society was being affected by the drug-threat. By stating that "In 1960, less than 200 narcotic deaths were recorded in New York City. In 1970, the figure had risen to over 1,000" (US Department of Defense, 2017, p. 2) Nixon accomplished to establish a vertical relationship between the author of the speech act and his audience. The point which the US President made here is that the average population of the US was falling to drugs. This is a compelling point that people were able to identify with since it was taking place close to them. The effort to convince his audience exemplifies another fundamental aspect mentioned in the securitisation theory. That is, it unveils how elite members try to create an issue and achieve its acknowledgment among a wide public.

A similar situation is depicted in the same speech where Nixon tried to call for a communal response by making leverage on individual sentiments. The sentence in question is: "In order to defeat this enemy, which is causing such great concern, and correctly so, to so many American families, money will be provided" (US Department of

Defense, 2017, p. 1). What the US President tried to do here was to make sure to gain the definite favour of his audience. It is by statements like this that legitimation is achieved and thus must be considered as an inherent part of the securitisation framing of threat process.

The process of legitimation was necessary to take actions on the borders of the US and even beyond. As he put it: "No serious attack on our national drug problem can ignore the international implications of such an effort, nor can the domestic effort succeed without attacking the problem on an international plane" and then "I am initiating a worldwide escalation in our existing programs for the control of narcotics traffic" (US Department of Defense, 2017, p. 11). These actions were mainly directed towards those who introduced drugs onto US soil. As the President put it: "to halt the drug traffic by striking at the illegal producers of drugs […] and trafficking in these drugs beyond our borders" (p. 4). In other words, Nixon framed foreign drug traffickers as a threat enlarging the scope of who was the root of the cause that produced the threat jeopardising US' security. These were key aspects that would thereon shape the country's foreign relations especially with states below its southern border.

The speeches used for this discourse analysis proved to be useful to identify patterns proposed by the securitisation theory. By addressing the Congress and the US population with subsequent speeches, President Nixon managed to reinvigorate the transformation of the drug issue into a persisting security issue. The indicators of the securitisation theory thus helped tracing the evolution from a relatively conventional criminal and public health problem to one that vindicated substantial policy shifts. With the goal of enlarging the securitisation process taken on by the US to introduce virtual enforcement mechanisms to its southern territorial border from 1969 to 1974, the next section examines a number of secondary sources that have been written on this topic.

5.1.2. The Virtualization of the Border during Nixon's term

The first concrete measure to fight off drug smuggling from Mexico to the US was taken by President Richard Nixon in 1969 with Operation Intercept. According to Grillo (2013), this operation consisted in searching "every vehicle or pedestrian coming across the southern border while the army set up mobile radar units between posts" (p. 256). This plan resulted in a fiasco since it soon became evident that conducting such a thorough terrestrial control was utopic. On-ground personnel alone were simply not capable of sealing off the entire border with Mexico. As Ghaffaray (2019) noticed, the border separating the US from Mexico was too broad and its orography too unwarranted to be enclosed in its entirety. For this reason, the $30 million USD Operation Intercept only lasted 17 days.

Regardless, Mendoza (2023) highlighted that Nixon aimed at fortifying the border by means of a virtual fence, not a material one, to achieve better results in diminishing drug flows. That is, after noticing that physical border closure alone was quixotic, Nixon invested in the control structure of the already existing border to improve the securitisation of it technologically speaking. Adding to this, Koslowski (2019) explained

that at that time the US government deployed motion, infrared, seismic and magnetic sensors that were able to detect motion as well as heat from a 50 to 250-foot range. The justification Nixon used to legitimise the investment in digital mechanisms went along the motto of protecting the border shared with Mexico was the War on Drugs.

The need of Nixon coincided with interests of military high-tech firms of the US. The looming end of the Vietnam War forced these firms to diversify and start investing in US's domestic Army support systems. In order to do so, they had to convince the US Government to keep on investing in different types of military spending, namely a defence that had to be carried out domestically instead of solely internationally. Hence, commencing from the late 1960s, a number of research and development firms contracted by the US to support the military intervention in Vietnam managed signing federal contracts.

Sylvania Electronics, for instance, succeeded in doing so. More precisely, it sold in 1970 to the US government its ground sensors used to remotely detect on-ground movements. This was a ground-breaking event since it symbolised the first application of virtual technologies used to monitor the US southern border. Grandin (2019) specified that these sensors were industrialised as part of Defense Secretary Robert McNamara's plan to construct a material and virtual fence unravelling north from south Vietnam and were used to detect troop and truck movements on the Ho Chi Minh Trail. The main function of these sensors was to perceive seismic activities caused by people or trucks passing close by the sensors and move the ground (Rosenau, 2001, pp. 11-12). This technology was handy to detect movements across and in proximity to the US border as well; reason for which it was implemented during Nixon's term.

A further technological feature first used during the Vietnam War and then for the US-Mexico border were drones. These drones, Novak (2015) suggested, were known as RPVs (Remote Piloting Vehicles) – whereas today they are known as Unmanned Aerial Vehicle (UAV) – and were used to scan the area from above. While describing the Mexican border of 1972, Novak explained that:

The US Air Force's *QU-22b* remote controlled pilotless aircraft – made surplus in Vietnam by the introduction of more sophisticated drones – have been returned to the US where they [flew] over the border to monitor the sensors and relay data to central control points (Novak, 2015)

With the arrival of drones, a surveillance center receiving the information collected by the unmanned aerial vehicle was put together. Barkan (1972, p. 1) rationalised that these UAVs were flying over remote stretches of the border to relay signals from hundreds of ground sensors that then were sent to the so-called Infiltration Surveillance Center where huge computers diagnose the data.

5.2 RESULTS AND APPLIED EFFECTS OF NIXON'S SECURITISATION

The Vietnam War represents a milestone for the virtual securitisation of the US-Mexico border under the Presidency of Nixon. In fact, there was a clear shift from applying war technologies onto the US home-borders translating into a virtualisation of the boundary. These novelties were handy for the Nixon Administration to fuel the desire of engaging in the War on Drugs. Accordingly, all of this was accompanied by an increasingly determined political participation of sealing the border – a term normally used in military missions though linked for the first time to the US border at that time (Lee, 2005), amongst the central goals was to hold drug traffickers entering through US's southern border.

Even though the surveillance systems introduced by Nixon's Administration were not always functioning – as Barkan (1972, p. 2) relentlessly remarked, it "is not able to distinguish friend from foe" – it is undeniably an important step in US border control. This innovation proved to be a cornerstone for almost each President that followed with regards to the management of the southern US border. Understanding that such an important new trend was built upon a performative act – as described by the securitisation theory – is explicative of how important the creation of security threats amongst an audience's perception is in terms of instigating security measures.

As it had been discussed decades after the War on Drugs, there was not really such a thing as a drug threat – or at least not to the extent President Nixon first remarked. John Ehrlichman, the then Assistant to the President for Domestic Affairs under President Nixon, admitted that the Administration was lying with regards to the drug threat to make political and military moves possible (see Lopez, 2016). If anything, there was a real drug issue amongst US armies abroad and far away from US territory (see Vulliamy, 2011).

There are related consequences of adopting a security-driven approach to the US-Mexico border as initiated under Nixon. It is necessary to consider literature on the use of allegories as means of polarisation. These, in fact, elucidate the relation that exists between securitisation, speech acts, and the creation of societal struggles within the broader process of justifying border surveillance and emergency powers. This is the case of Kruglanski (2007) who concentrated on the idea of metaphors to illustrate in what way language is able to frame threats determining the process of policy response. Nixon's speech act focusing on "enemy number one" aligns with Kruglanski's war metaphor. To be more precise, Nixon's war metaphors mirror those in terrorism discourse as proposed by Kruglanski (2007). This signals that the securitisation of the US border has been used even in more recent times. In both cases, a totalistic response was made possible thanks to the legitimisation of emergency measures such as border surveillance.

The disadvantages of using such an approach in the securitisation process of the US can be found in the polarising and radicalising effects they have in the long run. For example, Moyano *et al.* (2016) criticised the Bush-era securitisation process (the War on Terror) caused by the 9/11 terror act. In their opinion, the US society would have benefited more from a less polarising narrative avoiding societal disjunctions affecting

the present-day societal division. The same can be said about Nixon's approach with regards to the War on Drugs. In fact, following this idea, framing the issue as a war instead of a human challenge eclipsed the associated public health and community development issues afflicting the US. It would have been advisable, therefore, to adapt the conception of his speech acts. It would have been more profitable in the long run to opt for a more holistic response. These should have been based on a multidisciplinary approach so as to avoid backlashes created by securitisation processes that consider only one issue.

6. DISCUSSION

This paper engaged in finding an answer to the following research questions: How did the War on Drugs under the Nixon Administration contribute to the transition from a physical border control along the southern border to virtual enforcement mechanisms? So as to find an answer to this query, this research made use of the main principles composing the securitisation theory. These principles were used as indicators to conduct a discourse analysis of two speeches held by Nixon officially declaring his War on Drugs. What resulted from this analysis is that President Nixon actively engaged in the framing of a security threat proposed to his public and political audience as being detrimental to the national security of the entire country. Thanks to the audience's acceptance of the given narrative, extraordinary measures to halt drug influx entering the States were adopted. Amongst these measures it was possible to identify the introduction of virtual enforcement mechanisms.

Previous research has pointed out the importance that the virtual border has had in defining the southern US border. Heyman (2008) highlighted how walls and fences are reinforced by the virtual aspect defining the coercive side of US immigration policy. An idea that was forwarded by Amoore *et al.* (2008, pp. 99-100) listing the array of technologies used to help the US Border Patrol to sort out by means of algorithms what can be considered a threat and what not. Their study thus focused on the change of the human role in border management along with the US capacity of controlling beyond the physical border thanks to the virtual aspect of its boundary. Another sort of research conducted on the virtualisation of the US border was linked to military development. As Adams (2001) suggested, military advances in the use of technology to conduct warfare was used to reinvigorate the smart border separating the US from Mexico to guarantee an optimal supervision.

Considering this existing research, a gap in the literature became manifest. That is, although border securitisation, virtualisation, and militarisation along the US southern border has been studied, the outset of this transformation was not considered adequately. What this paper attempted to do was precisely filling in this gap. After conducting this research, it became evident that Nixon's presidency proved to be ground-breaking for the US' history of border management. In fact, it was the first time that the States implemented technological features – such as on-ground sensors and the first versions of UAVs – to monitor the US-Mexico border. By filling this gap present in the academic debate on the origins of the States' smart border, it is possible to further impulse the research on and comparison of borders from a perspective of security studies. Moreover, by testing the securitisation theory to successfully accomplish a discourse analysis undertaken by political elites to frame security needs, the findings of this research can be applied to other cases too. For instance, it would be possible to apply this research to similar cases such as the Spanish border shared with Morocco. Securitisation theory used as in the present study could shed light onto how and when virtual border mechanisms were introduced to the Spanish border regime.

It is, however, necessary to mention the limitations of this paper too. Even though the choice of undertaking a single-case study was necessary to offer a precise account of Nixon's role in fostering the virtualisation of the US-Mexican border, a comparative study could have offered an overarching understanding of borders in general. Similarly, making use of a mix-method for conducting this study could enhance the validity of the findings too. Integrating a quantitative perspective to the qualitative approach favoured in this research could give important insights in terms of locating what parts of the borders were fortified the most with regards to the virtualisation process.

The limitations of this paper represent, nevertheless, an opportunity to stimulate further research on this topic. Comparing the findings of this study with other cases that have seen important developments of border virtualisation as part of a more general fortification process. The Spanish Autonomous Cities Ceuta and Melilla, for instance, could benefit from this sort of analysis. Understanding their border fortification process starting from its accession to the Schengen Area would give significant insights into how border management has changed due to virtual border practices. Establishing whether the outset of this digitalisation was complemented by the example furnished by the US earlier on could help conceive the borders of Ceuta and Melilla in a more complete fashion. In addition, pairing the securitisation theory to these specific cases could unveil the dual importance of national narrative justifying this change in the border regime along with the narrative implemented by the European Union. In doing so, it would be possible to analyse the idea of Fortress Europe from a virtual securitisation point of view.

Overall, Nixon's attempts to counter drugs being smuggled through the southern US border laid the foundation for decades of the US-Mexico border policy. The importance of this change in the border regime is visible in the present *modus operandi* of the Border Patrol. Maintaining the control of the southern border would virtually be impossible without the US military technologies used in Vietnam and introduced to the national border under Nixon. In tracing the origins of virtual border enforcement to Nixon's War on Drugs, this study reveals how the politics of security can quietly transform the very architecture of a nation's boundaries.

BIBLIOGRAPHIC REFERENCES

Adams, J. (2001). Virtual Defense. *Foreign Affairs, 80*(3), 98–112.

Amoore, L., Marmura, S., & Salter, M. B. (2008). Smart borders and mobilities: Spaces, zones, enclosures. *Surveillance & Society, 5*(2).

Armstrong, W. G. (1992). Punishment, Surveillance, and Discipline in Paradise Lost. *Studies in English Literature, 1500-1900*, *32*(1), 91–109. https://doi.org/10.2307/450942

Barkan, R. (1972, February 18). They are watching you, through walls, in the dark of night while you walk around, and it comes from vietnam. *Free Press.*

Dafoe, A. (2015). On Technological Determinism: A Typology, Scope Conditions, and a Mechanism. *Science, Technology, & Human Values*, *40*(6), 1047–1076. http://www.jstor.org/stable/43671266

Ghaffary, S. (2019, May 16). The “smarter” Wall: How drones, sensors, and ai are patrolling the border. Vox.

Grandin, G. (2019, February 9). How the U.S. weaponized the Border Wall. The Intercept.

Grillo, I. (2013). Mexican Cartels: A Century of Defying U.S. Drug Policy. The Brown Journal of World Affairs, 20(1), 253–265. http://www.jstor.org/stable/24590897

Heyman, J. McC. (2008). Constructing a Virtual Wall: Race and Citizenship in U.S.-Mexico Border Policing. *Journal of the Southwest*, *50*(3), 305–333.

Kerr, D. (1999). Beheading the King and Enthroning the Market: A Critique of Foucauldian Governmentality. *Science & Society*, *63*(2), 173–202.

Koslowski, R. K. (2019, May 29). *Immigration reforms and border security technologies*. Items. https://items.ssrc.org/border-battles/immigration-reforms -and-border-security-technologies/

Kruglanski, A. W., Crenshaw, M., Post, J. M., & Victoroff, J. (2007). What Should This Fight Be Called? Metaphors of Counterterrorism and Their Implications. *Psychological Science in the Public Interest*, *8*(3), 97–133. http://www.jstor.org/stable/40062365

Lee, J. (2005, August 31). James H. Scheuer, 13-term New York congressman, is dead at 85. The New York Times.

Lemke, T. (2015). *Foucault, governmentality, and critique*. Routledge.

Lopez, G. (2016, March 22). *Nixon official: Real reason for the drug war was to criminalize black people and hippies.* Vox. https://www.vox.com/2016/3/22/11278760/war-on- drugs-racism-nixon

Lynch, M. (2008). *Ideas and Perspectives.* In *The Handbook of Socience and Technology Studies* edited by Hackett, E. J., Amsterdamska, O., and Wajcman, J., 9-11. Cambridge, MA: MIT Press

Mendoza, M. E. (2023, October 30). *The history of the U.S.-Mexico Border Wall*. Time. https://time.com/6324599/bidens-trump-history-border-wall/

Moyano, M., Bermúdez, M. I. ., & Ramírez, A. (2016). ¿Psicología positiva para afrontar la radicalización y el terrorismo? Un análisis del discurso de Obama en el Cairo. *Escritos De Psicología - Psychological Writings*, *9*(3), 53–58. https://doi.org/10.24310/espsiescpsi.v9i3.13219

Nail, T. (2016). *Theory of the Border*. Oxford University Press.

Novak, M. (2015, September 24). How the Vietnam War brought high-tech border surveillance to America. Gizmodo.

Otukoya, T. A. (2024). The securitization theory. *International Journal of Science and Research Archive*, *11*(1), 1747–1755. https://doi.org/10.30574/ijsra.2024.11.1.0225

Paden, R. (1984). Surveillance and Torture: Foucault and Orwell on the Methods of Discipline. *Social Theory and Practice*, *10*(3), 261–271.

Reid, Justin M. "'An Exercise in International Extortion': Operation 'Intercept' and Nixon's 1969 War on Drugs." Master's thesis, Chapman University, 2022. https://doi.org/10.36837/chapman.000412

Sharma, V. (2023). A review of Thomas Nail's 'Theory of the border.'. New Zealand Journal of Asian Studies.

Smith, M. R., & Marx, L. (Eds.). (1994). *Does technology drive history?: The dilemma of technological determinism*. Mit Press.

Timmons, P. (2017). Trump's Wall at Nixon's Border: How Richard Nixon's Operation Intercept laid the foundation for decades of U.S.-Mexico border policy, including Donald Trump's wall. *NACLA Report on the Americas*, *49*(1), 15–24. https://doi.org/10.1080/10714839.2017.1298238

Toshkov, D. (2016). Research Design in Political Science. Basingstoke: Palgrave Macmillan.

Trist, N., Cuevas, L., Couto, B., & Atristain, M. (2022). The Treaty of Guadalupe Hidalgo. In G. M. Joseph & T. J. Henderson (Eds.), *The Mexico Reader: History,*

Culture, Politics (pp. 599–603). Duke University Press. https://doi.org/10.2307/j.ctv2rr3g8m.96

US Customs and Border Protection. (2019). *Did you know... Century-old obelisks Mark U.S.-Mexico Boundary Line?*. U.S. Customs and Border Protection. https://www.cbp.gov/about/history/did-you-know/obelisk

US Deparment of Defense (2017). *41 Nixon Remarks Intensified Program for Drug Abuse*. US Government.

Vulliamy, E. (2011, July 23). *Nixon's "War on Drugs" began 40 years ago, and the battle is still raging*. The Guardian. https://www.theguardian.com/society/2011/jul/24/war-on- drugs-40-years

Wæver, O. (1995). Securitization and Desecuritization. In R. D. Lipschutz (Ed.), *On Security* (pp. 46-87). Columbia University Press.

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Research Article

SEXUAL VIOLENCE BY STRANGERS IN MADRID AND BARCELONA: A SITUATIONAL ANALYSIS

English translation with AI assistance (DeepL)

Francisco Pérez Fernández
PhD in Philosophy and Educational Sciences, Associate Professor (Criminal Psychology, Personality Psychology and History of Psychology), Departments of Psychology and Criminology and Security, HM Hospitals Faculty of Health Sciences, Camilo José Cela University.
fperez@ucjc.edu
ORCID ID: 0000-0002-3039-2397
Google Scholar: https://scholar.google.es/citations?hl=es&user=O_7qrwgAAAAJ

Heriberto Janosch
PhD in Legal and Economic Sciences,
Professor of History of Psychology and of Biological Bases of Behaviour, Faculty of Health, UNIE University
heriberto.janosch@universidadunie.com
ORCID ID: 0000-0002-0188-2434
Google Scholar: https://scholar.google.com/citations?user=uA4iKy0AAAAJ

Enrique López López
Magistrate of the Audiencia Nacional of Spain.
Professor of Constitutional Law and Criminal Procedural Law, Faculty of Legal Sciences and International Relations, UNIE University
enrique.lopezl@universidadunie.com

Francisco López-Muñoz
PhD in Medicine and Surgery and PhD in Spanish Language and Literature, Professor of Pharmacology and Vice-Rector for Research and Science, Faculty HM Hospitals of Health Sciences, Camilo José Cela University.
flopez@ucjc.edu
ORCID ID: 0000-0002-5188-6038
Google Scholar: https://scholar.google.es/citations?user=IbuwtWgAAAAJ&hl=es

Received 28/03/2025
Accepted 23/05/2025
Published 27/06 /2025

Recommended citation: Pérez, F, Janosch, H, López, E and López, F (2025). Sexual violence by strangers in Madrid and Barcelona: a situational analysis. *Revista Logos Guardia Civil*, 3(2), p.p. 171-196.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

SEXUAL VIOLENCE BY STRANGERS IN MADRID AND BARCELONA: A SITUATIONAL ANALYSIS

Abstract: Sexual assaults, as crimes of particular victimisation and media significance, are of great public alarm, concern and interest. As a result, they are often at the epicentre of the general debate on criminal policy. As a result, sexual assaults and their protagonists - offender and victim - are not always adequately analysed , treated and understood outside of criminological, police and legal environments. In the same way, criminological research itself, as well as the legislative, legal and penitentiary developments linked to the subject - necessarily controversial - often tend to blur into theoretical generalities that are difficult to confront and even to fit with particular facts and cases which, when studied in detail, seem impossible to fit into the general explanatory frameworks available. The present study, which is based on the approach provided by the Theory of Situational Action (TAS), proposed by Wikström and his collaborators, and makes use of the qualitative and quantitative analysis of judicial sentences issued in the provinces of Madrid and Barcelona, aims to show how the criminal ecosystems in which crimes are committed substantially modify their course, as well as the actions of the aggressor and his victim. A fact that can be extremely useful as a tool for police investigation and behavioural analysis, as well as for the understanding of criminogenetic events and specific criminal dynamics.

Resumen: Las agresiones sexuales, en tanto que delitos de especial significación victimal y mediática, suscitan gran alarma, preocupación e interés públicos. En consecuencia, suelen formar parte del epicentro del debate general en torno a las políticas criminales. Ello motiva que las agresiones sexuales y sus protagonistas -agresor y víctima- no siempre sean adecuadamente analizados, tratados y entendidos fuera de los entornos criminológicos, policiales y jurídicos. Del mismo modo, la propia investigación criminológica, así como el devenir legislativo, jurídico y penitenciario vinculados al tema -necesariamente controvertido-, tienden a menudo a difuminarse en generalidades teóricas que cuesta confrontar e incluso encajar con hechos y casos particulares que, al estudiarse en detalle, parece imposible de encajar en los marcos explicativos generales de que se dispone. El presente estudio, que se realiza partiendo del enfoque aportado por la Teoría de la Acción Situacional (TAS), propuesta por Wikström y sus colaborares, y se vale del análisis cualitativo y cuantitativo de sentencias judiciales emitidas en las provincias de Madrid y Barcelona, pretende mostrar cómo los ecosistemas criminales en que se cometen los delitos, modifican sustancialmente su curso, así como las acciones del agresor y su víctima. Un hecho que puede ser extremadamente útil como herramienta para la investigación policial y el análisis de conducta, así como para la comprensión de eventos criminogenéticos y dinámicas criminales específicas.

Keywords: Sexual Aggression, Situational Action Theory, Multidimensional Scaling, Behaviour Analysis.

Palabras clave: Agresión Sexual, Teoría de la Acción Situacional, Escalamiento Multidimensional, Análisis de Conducta.

1. INTRODUCTION

Sexual assaults are a source of suffering for the victims . This is aggravated in those cases which, for particular reasons, become particularly "famous" and arouse the interest of public opinion. The fact is that sexual assaults, often highly publicised, provoke great alarm and social debate, which usually triggers investigations and particularly mediatic trials that have a strong impact on the victims through secondary victimisation and *ex post attendentes*[1] (Gutiérrez de Piñeres, Coronel and Pérez, 2009; Domínguez Vela, 2016). To provide some data for reflection, it should be recalled that, according to the Statistical Yearbook of the Spanish Ministry of the Interior, in 2022, 19,013 crimes against sexual freedom were "known" by the State Security Forces and Corps (FCSE) - they speak of complaints and investigations - of which 11,426 were sexual abuse/assaults and, of these, 4,270 became sexual abuse/assaults with penetration[2] . A high percentage of these assaults/abuses took place in commercial premises, dwellings and other attached spaces such as garages or storage rooms, one of the most frequent modalities of this type of crime being that in which the sexual aggressor, usually a man acting alone, attacks a woman in the entrance hall of a residential building, or in the garage, for which he is commonly known as a "portalero" (Janosch González, Pérez-Fernández and Soto Castro, 2020).

Be that as it may, the "grey figure" in the statistics reflects the ominous police, victimisation and judicial evidence that underlies this problem: the clarification of sexual assaults committed by individuals unknown to the victims is more complex than in those cases in which there is some kind of link between victim and offender that facilitates FCSE investigators to positively identify the aggressor and, if necessary, to obtain evidence that can be used as evidence in court (Corovic, Christianson and Bergman, 2012; Janosch, Pérez-Fernández and Herrero, 2025). It should be borne in mind that the cognitive-behavioural dynamics of these individuals tend to operate through a process of escalation, which implies that, in relation to their potential dangerousness, it is very possible that there is a bias of seriality - or at least repetitiveness - that leads them to commit more than one sexual assault in the course of their criminal career if they are not identified and arrested (Pueyo and Redondo Illescas, 2007). Especially because, rather than a direct link to more or less serious diagnosable disorders, in this class of offenders it seems to be driven by the influence of a complex amalgam of socio-cultural elements, life stressors and personality structures (Arqué-Valle et al., 2024).

---

[1] Both types of victimisation are often confused. Secondary victimisation relates to the personal and psychological costs to the victim of being more or less constantly exposed to situations that make him or her relive (or recall) the harm suffered over and over again (Kühne, 1986). *Ex-post* victimisation - also called "fourth level" victimisation - is triggered when the person experiences hopelessness and helplessness after not receiving the expected help from those institutions and professionals they trusted (e.g. police, health, administration, justice) and from whom they do not receive the expected moral and material support (Triviño, Winberg and Moral, 2021).

[2] In total, a total of 14,555 crimes against sexual freedom were solved, counting all types of crimes against sexual freedom, which gives a total of 4,518 "grey figure" - crime investigated but not solved - of 4,518 complaints. In terms of abuse/assault with penetration, the number of unsolved cases in 2022 was 860 (Ministry of the Interior, 2023).

On the other hand, and to expand on the last idea, it is well known that the context - material and human environment - in which the offender acts modifies his behaviour, so that strategies and resources that may be perfectly useful in a certain place do not necessarily have the same value of applicability in a different criminal-delinquent ecosystem. Wikström, faced with this contingency, developed the so-called Situational Action Theory of Crime Causation (or CAS), whose foundational proposals appeared between 2004 and 2006 (Serrano Maíllo, 2017). There, an attempt has been made to integrate, within the framework of an adequate theory of action, the main achievements of theoretical formulations and research in criminology, as well as theoretical and empirical knowledge from the social and behavioural sciences in general. This is because the correlates of criminality are fairly well known, but there is little agreement about the causes of crime, which are offered as a confusing mixture of elements to which each researcher attaches greater or lesser importance according to his or her interests. This explains the inflation of theories - and internal contradictions - that affect criminological studies (Pérez-Fernández, Janosch and Popiuc, 2023).

In short, TAS states that criminal acts can be explained as processes - systemic and interactive, but not deterministic, mechanisms - that mobilise "actions" that ultimately transgress formal or informal rules of conduct (Wikström, et al., 2012). It would thus be a subset of behaviours included in the more general set of *acts that violate moral rules of conduct*. Although these constructs of moral conduct are not specified in any law and therefore not all of them are crimes per se, they could respond to the same mechanisms that mobilise crimes in a legal sense (Janosch González, 2013). In other words, the TAS defines crime as an act that breaks some rule of conduct established by law -inserted in the penal code of each state-, and that can be analysed in terms of *moral action*. Moral action, in turn, would be understood as conduct that is guided by rules that establish what, under certain specific circumstances - or situations - would be right or wrong to do (Wikström and Treiber, 2016).

Defining crime in these terms, as an act that violates a rule of moral conduct that is embodied in the form of laws, has the advantage that it can be applied to any kind of crime, anywhere, and at any time. Thus, what is defined is an act of violation of a rule of moral conduct that is specified in the form of some particular law "there given". It can thus be argued that TAS is, fundamentally, a general theory of moral action (Wikström, et al., 2012), as it would explain all types of moral rule-breaking in any time or place, with the emphasis on the mechanism inducing the moral rule-breaking, rather than on the content of the disobeyed moral rule as variable and subject to constant modification according to the variations of the particular positive law in a specific space-time (Pauwels, 2018a; Pauwels, 2018b). The causal mechanism of perception and action would be present in petty theft as well as in sexual assaults or homicides. Consequence: criminal policies, in the medium and long term, would be more successful if they were aimed at education in conformity with the prevailing moral rule, rather than at punishment or mere control (Pérez-Fernández, Janosch and Popiuc, 2023; Janosch, Pérez-Fernández, Popiuc and López-Muñoz, 2024).

Ultimately, it is the interaction between the crime propensity of a particular person and the criminogenic characteristics of the setting that will trigger the process that will - or will not - lead to the criminal act itself. The propensity to offend will depend on the person's moral standards and ability to exercise self-control - bearing in mind that this ability may be diminished by alcohol or drug use, or by intense stress with emotional imbalance. These criminogenic characteristics of the scenario, in turn, will depend on the so-called "moral environment" - the one perceived by the individual rather than the real one - and on the existence or not of deterrent factors, which encourage or discourage the violation of rules (Wikström, et al., 2012). The corollary of all this, as far as this study is concerned, is clear: the sexual aggressor will not always act in the same way and with total independence of the place where he is, because the general situation in which he is inserted - which has to be analysed and understood - will necessarily modify his perception of rules, his moral considerations, his attention to laws and restrictions and, finally, his criminal action (Pérez-Fernández, Popiuc and López-Muñoz, 2024).

Considered in this way, it will be understood that for the CAS, beyond any debatable ideas, a person's nationality, political ideology, sexual identification or religion are not in themselves causes of crime in any form, or at least should not be assessed as more important than other personal circumstances, such as age or level of education, because in reality they are merely attributes of the person which, moreover, are changeable. Just as it would not make sense to say that someone is more likely to commit crime because he or she is taller, neither does it make sense to emphasise other personal attributes which, moreover, would fall within the controversial area of individual rights and freedoms. Thus, variables such as nationality or religion should be evaluated with the same rigour as other contributory causes of different forms of crime recognised in the literature, such as poverty, level of education, living in criminogenic environments, lack of opportunities, polyconsumption, truancy, inappropriate companionship and so on (Pérez-Fernández, Janosch and Popiuc, 2023). In other words, just as it would make no sense to say that a person commits crimes - or does not commit crimes - because of the colour of their hair or their weight in kilograms, it is also inconsistent to argue that they could be driven to commit crimes simply because they were born in a certain country, or because they share a certain ideological sentiment, identify with a specific gender or practice a certain religion (Janosch, Pérez-Fernández and Herrero Roldán, 2024).

1.1. A NECESSARY LEGAL NOTE

This introduction concludes by recalling something that is well known, and that is that in Spain there have been relatively recent changes in the Penal Code (PC) with respect to sexual crimes, which have come to modify the different existing perspectives with respect to the police and judicial approach to the problem. To begin with, and linking with the TAS model described above, they entail an alteration of statistical counts - which will also alter future media discourses - whose effects will only be perceptible in the medium term and, consequently, open up new perspectives on the general perception of criminality, as well as on reactive policies of action with respect to it whose effects are yet to come. It is therefore worthwhile, in order to anticipate what is to come and in order

to properly contextualise the results presented here, to provide a brief critical overview of these changes.

The LO 10/2022, of 6 September, popularly known as the *Law of the only yes is yes*, has meant a notable change with respect to the consideration of crimes against sexual freedom. This regulation has introduced significant changes in the PC, especially in the unification of the crimes of sexual abuse and aggression, the redefinition of consent and the modification of the associated penalties. But, apart from these legislative novelties, it has also generated an intense debate as a consequence of the sentence reductions that have taken place: 1205 sentence reductions that include 121 releases from prison (CGPJ, 2023). The enactment of this law was contextualised in the need to reinforce the protection of sexual freedom and to guarantee a comprehensive response to all forms of sexual violence.

Prior to the entry into force of LO 10/2022, the Spanish Criminal Code distinguished between sexual abuse and sexual assault. Abuse referred to acts without violence or intimidation, while assault involved the use of violence or intimidation. With the new law, this distinction disappears. Thus, any sexual act without consent is considered sexual assault, regardless of whether violence or intimidation was involved. This unification seeks to recognise that any non-consensual sexual action is an assault on a person's sexual freedom.

The law establishes that consent is only understood to exist when it has been freely expressed through acts that, given the circumstances of the case, clearly express the will of the person. This definition places consent at the centre of sexual relations, eliminating interpretations that could justify non-consensual conduct. This implies that any non-consensual sexual act is an assault, regardless of whether or not there is violence or intimidation, because the absence of consent alone implies implied violence. Although consent was not explicitly defined, this did not mean that the jurisprudence did not understand that such consent was substantial, as an element in this negative case of the type, that the agent acted: 1) without the consent of the person sexually assaulted; 2) through the existence of consent vitiated by concurrent circumstances derived from the position of the perpetrator of the act, significantly derived from kinship or an equivalent situation, or from the dominance that his position as a consequence of an employment relationship, teaching, superiority, ascendancy, even as a consequence of a range of age with respect to the victim, could restrict the victim's sexual self-determination; and 3) that the agent took advantage of a position of privilege derived from the victim's vulnerability or state of unconsciousness[3] . These last sequences of attacks on sexual freedom were previously classified as sexual abuse, while the cases in which the perpetrator acted against the victim's consent opened the category of sexual aggression, being committed by means of violence or intimidation, which was the characteristic required for such aggression. However, the concurrence of the absence of consent that permeates the title that embraces these crimes was always necessary, as they are crimes against sexual

3 See, for example: STS 3865/2024; SAP A 872/2018.

freedom, which is naturally based on the existence of consent in the provision of consent to carry out actions with sexual content.

The formula used today by the legislator is therefore an open formula, and one that was already taken into consideration in case law, in similar terms, to understand consent as concurring. The aforementioned formula is based on acts, so that "consent will only be understood to exist when it has been freely manifested through acts which, in view of the circumstances of the case, clearly express the will of the person" (LO 10/2022). By *acts*, all kinds of manifestations or signs of the person who is going to consent are to be understood, whether verbal, gestural or situational, but they must be considered as explicit. Thus, consent is constructed as positive and conclusive, and must be freely given (implicitly, not vitiated: it must depend exclusively on the will of the person, as in any crime whose generic object of protection is freedom in any of its expressions).

The reform motivated by the approval of LO 10/2022 has also adjusted the penalties associated with sexual offences. For example, sexual assault without penetration was previously punishable by 1 to 5 years in prison, while the new law establishes a range of 1 to 4 years. In the case of penetrative assaults, the minimum sentence is reduced from 6 to 4 years, while the maximum sentence remains at 12 years. These modifications have been the subject of controversy, especially because of the effect of their retroactive application for the benefit of convicted offenders. The retroactive application of the law, a basic principle of criminal law when a rule favours the offender, has led to the review of numerous final sentences. This unforeseen effect has generated an intense debate on the need to adjust the law to avoid undesired consequences, something that was finally done by LO 4/2023, of 27 April.

There is no doubt that Organic Law 10/2022 was guided by a laudable objective in the protection of sexual freedom by unifying offences and focusing on consent. However, the reduction of penalties in certain cases has highlighted the complexity of reforming the PC, so it is essential that future changes consider in detail the practical implications of legislative amendments to ensure effective protection of victims and adequate punishment of perpetrators. The controversy described above has arisen from the fact that both the maximum and minimum criminal limits have been touched upon without providing for the possibility of introducing a transitional provision. The PC in a democracy is an extremely important instrument and should remain outside ideologies and sectarianism.

2. HYPOTHESIS

It is true that the legislation to be applied is the same in Madrid and in Barcelona, and that the conditions for its application are identical, which means that the initial legal approach - and its vicissitudes - will be basically the same. However, if attention is paid to the TAS model described above, it becomes clear that, accepting that the context in which the potential offender develops his activities will modify his behaviour, it is implied that the strategies and resources that may be perfectly useful in the province of Madrid do not necessarily have the same value of applicability in another different criminal-delinquent

ecosystem, such as that of the province of Barcelona, in which, moreover, it operates under the control of police forces and penitentiary models that are also differentiated.

Consequently, the interest of this article is based on the formulation and study of a basic hypothesis: the sexual aggressions perpetrated in the province of Madrid must be, in some way and insofar as they are mediated by different models of situational action, significantly different from the sexual aggressions committed in the province of Barcelona.

3. METHODOLOGY

It is true that criminological research does not find sufficient or appropriate data in the different public databases in Spain to test its approaches. The problem, already widely criticised by other researchers, lies in the fact that this information is collected for public-administrative purposes that respond to the competences of the competent body, and therefore rarely takes into account the needs of researchers and tends to meet other criteria that are not coherent with the pretensions of science (Linde and Aebi, 2021). Particularly exceptional, however, is the information provided by the Judicial Documentation Centre (CENDOJ) of the General Council of the Judiciary (CGPJ), which offers unfiltered data, allowing researchers to process it to suit their specific needs. However, given other shortcomings inherent to the very nature of this database, the documentation it provides must be properly categorised and filtered, based on very specific starting criteria (Janosch, Pérez-Fernández, Nut and Marset, 2023). Furthermore, and no less important, the information provided by CENDOJ is anonymous, public and free of rights.

Taking the above into account, 76 cases of sexual assault committed by a perpetrator initially unknown to the victim in the provinces of Madrid and Barcelona were analysed for this study, based on the analysis of court rulings published in the CENDOJ database. The sample size corresponds to a representation of the total number of known and judged sexual assaults committed by unknown perpetrators in the provinces indicated. The inclusion criteria delineated were the following:

1. The sexual offender was a male unknown to the victim until at least 24 hours before the crime, and always acted alone.
2. The victim, always female, was 16 years of age or older at the time of the offence.
3. The cases are legally defined, in the sentence itself, as "sexual assaults" (actual or at least attempted penetration with a penis, through the vagina, mouth and/or anus; or actual penetration with fingers or other objects, through the vagina and/or anus).

Based on these inclusion criteria, 38 crimes were found, by chance, in the province of Madrid and 38 in the province of Barcelona. Subsequent analyses were carried out using the statistical package R version 4.4.2 (2024), *Pile of Leaves*, Copyright (C) 2024 The R Foundation for Statistical Computing. Libraries used: *vegan*, *ggplot2*, *ggrepel*, *cluster*, *factoextra*, *readxl*, *mclust* and *clue*.

3.1. CATEGORISATION OF JUDGMENTS

In order to properly compile the data from the judgements for subsequent statistical analysis, the criteria and nomenclatures described below have been followed:

- Judicial record of the accused. These are coded in variables called *Ag_Sex* (judicial record for sexual offence), *Ag_Theft* (judicial record for robbery), *Ag_Viol* (judicial record for non-sexual violence), and *Ag_Unesp* (judicial record for unspecified offence). These variables were coded in the database as follows: 0 if the offender has no psychiatric history or problems, 1 if he/she does, and 2 if none of these is stated in the sentence.
- Specific situational variables. A group of seven variables respond to situational circumstances related to the rape itself - they could be considered as "scenographic". The victim may or may not have resisted the commission of the crime (*Ver_Resist*); she may or may not have screamed for help (*Ver_Shout*); third persons, such as possible witnesses or police forces alerted by the event, may or may not have been present during the commission of the sexual assault (*Ver_Third*); or the rape may or may not have been interrupted for some reason (*Ver_Inte*). As far as the sexual aggressor is concerned, it is assumed that he could have acted under the influence of alcohol (*Ver_Alc*), or drugs (*Ver_Drug*), or he could even have had his volitional and intellectual capacities diminished (*Ver_Vic*). In all detected cases the variables were coded as 0 (absence of the behaviour), 1 (presence of the behaviour), or 2 (behaviour not stated in the sentence).
- Sexual behaviour of the offender. The following variables take on three possible values, with 0 indicating no conduct, 1 indicating presence of conduct, and 2 indicating conduct not recorded in the court file. The variables *Ver_Vag*, *Ver_Anal*, and *Ver_Fel* indicate that the victim suffered penetration with the penis in the vagina, anus, or mouth, respectively. The variables *Ver_Vag_Attempt and Ver_Anal_Attempt* indicate that the sexual assailant unsuccessfully attempted to penetrate the victim with his penis in the vagina or anus, respectively. The variable *Ver_Finger* indicates that the assailant penetrated the victim with his fingers in the vagina or anus.
- Non-sexual behaviours of the aggressor. These variables have also taken the values 0 (absence), 1 (presence), and 2 (no record). If the offender approached the victim by means of a deceptive manoeuvre, the variable *Ver_Con* was coded with 1. If the offender attacked the victim by surprise, then the variable *Ver_Surp* was coded with 1. If he used some kind of weapon (usually a knife) the variable *Ver_Weap* was coded with 1. If the victim was robbed of some kind of valuables (money, mobile phone, credit card, etc.), the variable *Ver_Val* was coded with 1. If the theft was of personal objects (underwear, photos, diary, etc.) that could be used for some fetishistic purpose, the variable *Ver_Pers* was coded with 1.
- Other variables. They arose in relation to other alternative issues raised by the judgments and which are of interest for the detailed analysis of the cases. Thus:

a. Did the sex offender display forensic knowledge in his behaviours (condom use, gloves, cleaning behaviours and so on)? If yes, the variable *Ver_Fore* was coded with 1.
b. Did the sex offender act between 22:00 and 6:00 local time? If so, the variable *Ver_Darkness* was coded as 1.
c. Did the offender act between noon on a Friday and noon on the following Monday? If the answer to this question was yes, the variable *Ver_Wend* (*weekend*) was coded as 1.

4. RESULTS

Table 1 shows the percentage presence of the variables described above in the sentences for sexual assault referring to the provinces of Madrid and Barcelona. As can be seen in Table 2, two variables have a significant difference between Madrid and Barcelona, and one variable is not significant, but is at the limit of significance -$p \leq 0.05$-. It can also be seen that sex offenders act more under the influence of drugs and use more weapons in the province of Barcelona than in Madrid. However, more vaginal penetrations are committed in the cases detected in Madrid than in those sentenced in Barcelona.

Table 1. Percentages of "presence" of the different behaviours referred to the crimes analysed.

Variables	Meaning	Madrid	Barcelona
Ag_Sex	Offender's criminal record for sexual offences.	5,3%	13,2%
Ag_Theft	Assailant's criminal record for robbery.	13,2%	13,2%
Ag_Viol	Offender's judicial record of non-sexual violence.	10,5%	10,5%
Ag_Unesp	Judicial record for unspecified offence.	15,8%	15,8%
Ver_Resist	The victim resisted.	52,6%	60,5%
Ver_Shout	The victim screamed.	23,7%	28,9%
Ver_Third	Alerted third parties appeared.	31,6%	18,4%
Ver_Inte	The sexual assault was interrupted by unexpected circumstances.	28,9%	34,2%
Ver_Alc	The assailant was under the influence of alcohol.	5,3%	21,1%
Ver_Drug	The assailant was under the influence of drugs.	5,3%	28,9%
Ver_Vic	The perpetrator had diminished volitional and intellectual capacities.	7,9%	18,4%
Ver_Vag	The victim suffered vaginal penetration.	76,3%	50,0%
See_Anal	The victim suffered anal penetration.	7,9%	15,8%
Ver_Fel	The victim suffered oral penetration (fellatio).	34,2%	47,4%
Ver_Vag_Attempt	There was an unsuccessful attempt at vaginal penetration.	7,9%	13,2%
View_Anal_Attempt	There was an unsuccessful attempt at anal penetration.	10,5%	10,5%
Ver_Finger	The assailant penetrated the victim with his fingers in the vagina or anus.	13,2%	13,2%
See_Con	The assailant approached the victim by means of deception.	55,3%	36,8%
See_Surp	The assailant approached the victim by surprise.	44,7%	63,2%

Ver_Weap	The assailant used some kind of weapon.	23,7%	47,4%
Ver_Vehi	The assailant drove to the scene of the attack in a vehicle.	10,5%	5,3%
Ver_Val	The assailant stole financial assets from the victim.	36,8%	36,8%
See_Pers	The assailant took an object that could be used as a fetish.	7,9%	5,3%
Ver_Fore	The assailant demonstrated forensic expertise.	5,3%	15,8%
Ver_Darkness	The assault was committed between 22:00 hours and 6:00 hours.	42,1%	39,5%
Ver_Wend	The robbery was committed on the weekend (between noon on Friday and noon on Monday).	71,1%	60,5%

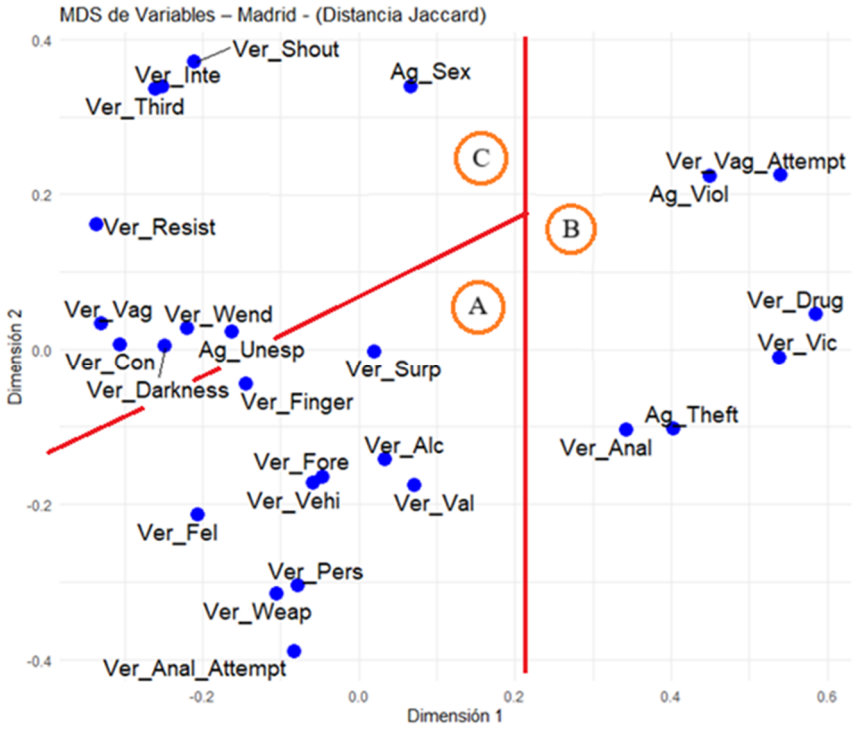
Table 2. Variables that have shown significant differences between sexual assaults committed by strangers in Madrid and Barcelona.

Variable	p-value	Test used
Ver_Drug	0,012	Fisher's Exact
Ver_Vag	0,032	Chi-Square
Ver_Weap	0,055	Chi-Square

The result of the multidimensional scaling procedure (MDS) for the Madrid cases can be seen in Figure 1. The 3 clusters found (A, B and C, in the figure), formed by the groupings of the data and which determine as many typologies, were found by means of *K-Means clustering* analysis. The typologies detected in the province of Madrid, analysed independently, would be as follows:

- Type A, impulsive, is a person with a history of other sexual assaults who usually acts in the dark, during the weekend, and approaches the victim using some kind of subterfuge. However, the victim often resists and screams, alerting third parties, so that the rape, despite the existence of anal or vaginal penetration, is interrupted. Nevertheless, the victim may be robbed of valuables.
- Type B, of a versatile nature, shows a sexual offender who operates under the influence of drugs and therefore has diminished intellectual and/or volitional capacities. In this case, in which the offender may have a history of robbery and other violent crimes, there is usually an unsuccessful attempt at vaginal penetration, as well as anal penetration. Possibly, one could think of a person with impaired reasoning, initially motivated by the robbery, who tries to take advantage of the occasion.
- Type C suggests the presence of a planning and more specialised sexual aggressor, with some forensic awareness, who travels in a vehicle and who uses some kind of weapon during the assault to intimidate and subdue the will of his victims. In this case there is usually alcohol consumption by the aggressor, who will force the victim to perform fellatio, may attempt vaginal insertion with his fingers and will try to perform anal penetration. This third type of aggressor usually takes objects from the victim to use as fetishes or trophies.

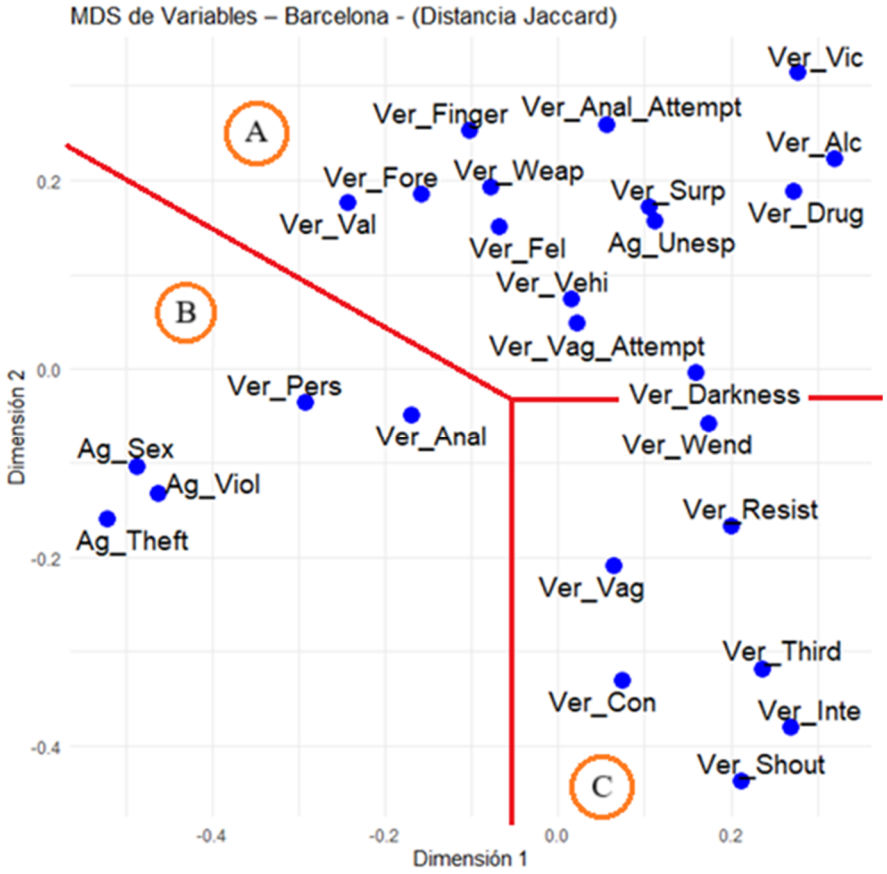
Figure 1. Multidimensional scaling of sexual assaults committed in Madrid.



As in the previous case, the 3 clusters (A, B and C in the figure), formed by the groupings of the data, were found by means of *K-Means clustering* analysis. The typologies detected in the province of Barcelona are as follows:

- Type A, occasional bias, would be a person with some forensic awareness, who travels in a vehicle, uses drugs and has a history of other offences not specified in the sentence. This person, often using weapons to subdue the victim and under the influence of drugs and alcohol, approaches his victims by surprise and may try to force them to perform fellatio on him. He will try, after inserting his fingers into the victim's genitals, and indistinctly, to proceed to anal and/or vaginal penetration, but is usually unsuccessful.
- Type B, very versatile, poly-criminal and therefore poorly defined, is an offender with a history of other sexual offences, robbery and non-sexual violence, who will take from the victim objects of no apparent value that can be used as fetishes.
- Type C, casual and recreational bias, operates at night and usually on weekends. He approaches the victim by deception and/or various subterfuges in order to proceed to vaginal penetration, but in the absence of weapons or prior planning to facilitate his activities, the victim will resist, scream and alert third parties who may interrupt the assault.

Figure 2. Multidimensional scaling of sexual assaults committed in Barcelona.

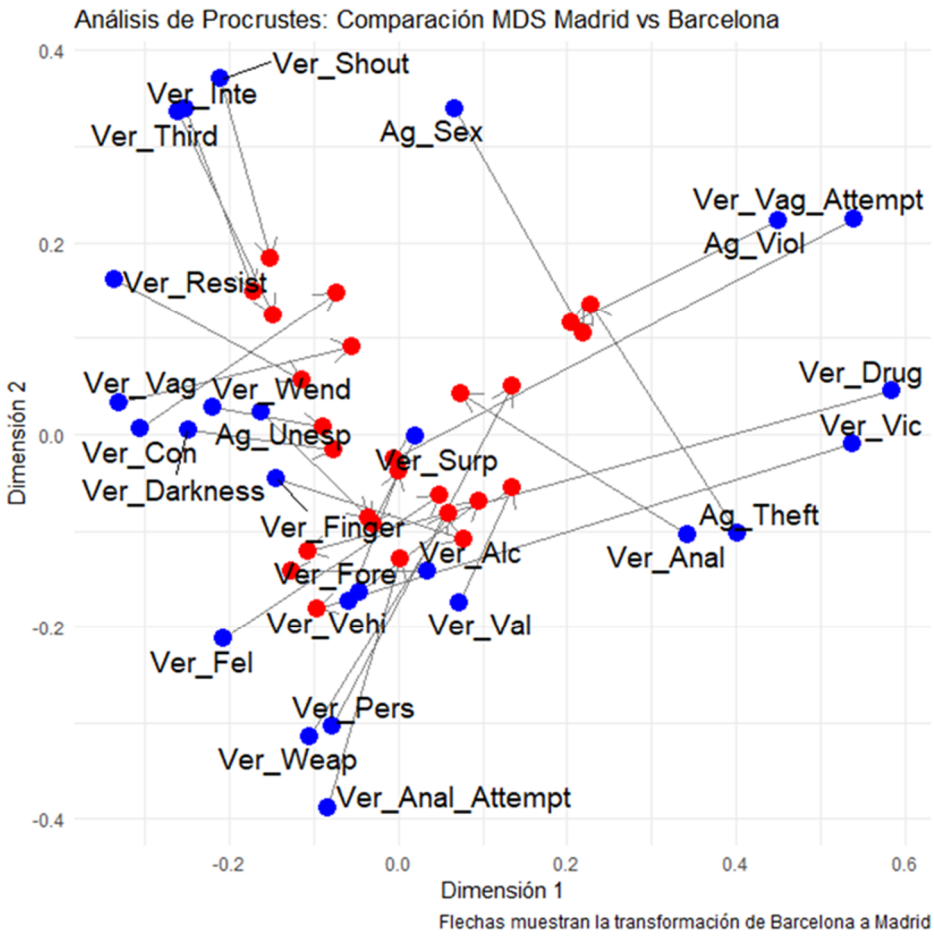


In order to make a comparison between the aggressions and typologies present in both contexts, the Procrustes test was applied to the multidimensional scalings (MDS) that show the clusters/typologies of Madrid and Barcelona, in such a way as to achieve the best fit between the two. After this process, the Jaccard Index (0.393) and the ARI Index (0.332) have been calculated. This has resulted in an overlap and differentiation of the typologies described for each of the crime settings. Figure 3 appears as the result of the Procrustes test to compare the MDS result applied to the Madrid data with the MDS result applied to the Barcelona data[4] . It is significant at this point that the Procrustes analysis is useful for assessing the similarity between two spatial configurations -or clouds- of data. The results obtained by this procedure, therefore, show how the spatial configurations of the Madrid and Barcelona data align after an optimal transformation

[4] Procrustes analysis is a Euclidean transformation process within the series of statistical methods that apply group theory to the analysis of homogeneous data sets in order to compare them with each other and make inferences from these comparisons. It is one of the procedures included in the so-called "multivariate statistical analysis". Its name comes from the myth of Procrustes, one of the sons of Poseidon, who also happened to be a terrible serial killer. He had a house where he offered lodging to weary travellers who ventured into the area. There he invited them to lie down on an iron bed which, while they slept, he tied hand and foot to its four corners. If the propitiatory victim was so tall that his body was longer than the bed, Procusto proceeded to saw off the protruding parts of his body. If it was shorter than the bed, then he would hammer the victim to stretch it to the proper dimensions (Hurley and Cattell, 1962; Gower, 1975).

(rotation, scaling and translation) aimed at minimising as much as possible the differences between them.

Figure 3. Comparison between the DMEs of the provinces of Madrid and Barcelona.



4.1. TYPOLOGIES A

In the case of Madrid, as indicated above, this cluster groups variables related to crimes where there is a theft of objects or a less violent aggression in physical terms. In Barcelona, however, within this cluster there is a predominance of offenders with a history of violent crime and robbery, without variables that directly indicate consummated sexual violence.

The main differences between the two environments have to do with criminal records, as in the case of Barcelona there is a high presence of offenders with a history of sexual offences, robbery and violence. In Madrid, however, the cluster is more related to the theft of material goods, trophies or fetishes. Significant variations can also be found with regard to sexual aggression itself. While in the cases of the province of Barcelona there is a greater relationship with anal penetration, in Madrid, unsuccessful attempts at anal penetration and aggression with fingers or fellatio are observed.

As a general rule, it could be indicated that in cluster A, for Madrid, there are more cases of deception, subterfuge or excuse to approach the victim and robbery, while in Barcelona the offender's criminal record becomes a key factor to be taken into account when assessing his potential dangerousness.

4.2. TYPOLOGIES B

With regard to Madrid, the variables included in this cluster indicate a profile of aggressors with a judicial record for violent and/or sexual crimes, as well as circumstances in which the aggressor is under the influence of various substances. The victim, on the other hand, suffers consummated or attempted sexual aggression. With respect to Barcelona, the variables provide a profile of aggressors without a specific criminal record, but with characteristics that reflect a clear planning of the attack and a consumption of substances.

The main differences in terms of criminal records are that, for Madrid, there is a clearer presence of records for robbery and violence, while in Barcelona there is a rather more ambiguous category of unspecified records. Regarding the aggressor's mode of operation, in the Barcelona cases there is more evidence of planning, as evidenced by the very systematic presence of the use of deception, vehicles and weapons. In Madrid, however, direct violence seems to play a much more relevant role.

With respect to the use of substances and sexual aggression itself, in both cases the presence of drugs or alcohol is observed, but in Madrid sexual violence is more evident in terms of consummated aggression. In Barcelona, within type B, there is a greater tendency towards unsuccessful attempts at aggression, but with more diverse methods such as penetration with fingers.

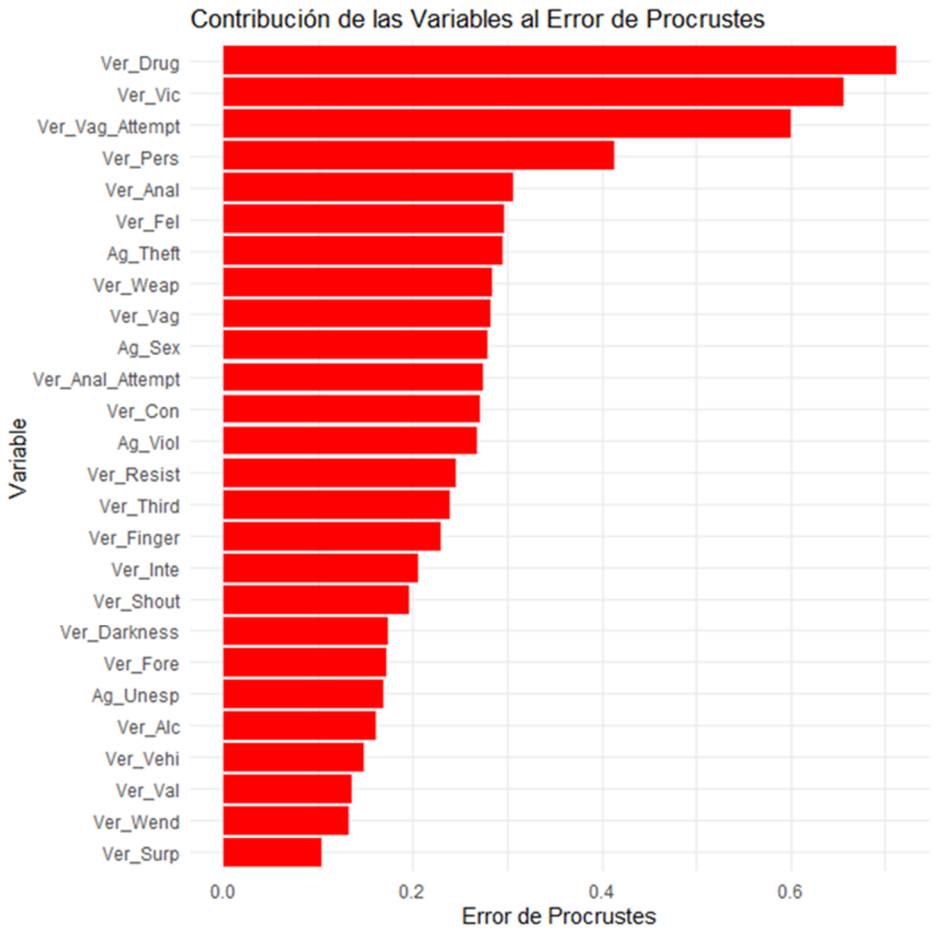
4.3. TYPOLOGIES C

In the context of Madrid, the variables in this cluster reflect aggressors who do not necessarily have a serious judicial record, but who operate impulsively, without much planning and in environments where the victim tries to resist and there is usually third party intervention. In the case of Barcelona, interrupted attacks are also found, but with less emphasis on the use of deception to approach the victim and with less intervention by third parties who can thwart the attack.

The main differences, as far as criminal records are concerned, have to do in Madrid with the fact that this group includes aggressors with a history of sexual offences, while in Barcelona there is no mention of such a criminal record. As mentioned above, in both cases there is resistance from the victim and a possible interruption of the attack, but in Madrid there are more variables associated with the presence of third parties. Similarly, in the assaults in the province of Madrid, night-time occurrence is a stronger factor, while in Barcelona the variable of night-time does not appear in this cluster.

Figure 4, on the other hand, is illustrative in that it represents the contribution of each variable to the Procrustes error - that is, to the mismatch of the two data sets. This indicates which aspects of aggression differ most between the data configurations found between the Madrid and Barcelona clusters after transformation.

Figure 4. Differences of each of the variables in the spatial position of the MDS obtained with the Madrid data and the Barcelona data.



When looking at the general interpretation of the results described above, several elements have to be taken into account:

1. Number of objects and dimensions: 26 variables were compared in a 2-dimensional space.
2. Fit measure (Procrustes sum of squares): 2.6286, indicates the level of difference between the configurations before and after the transformation.
3. Procrustes root mean square error (RMSE): 0.31796, represents the average magnitude of the error in the alignment of the points (Table 3).

Distribution of the mean squared errors found in the Procrustes analysis.

Minimal error	0,1041
First quartile (Q1)	0,1719
Medium	0,2568
Third quartile (Q3)	0,2919
Maximum error	0,7121

Taking all of the above into account, what the data in Table 3 suggest, then, is that most of the variables have a relatively low error of fit, but there are some with higher errors. In any case, to achieve the best possible fit of the graphs presented in figures 1 and 2, a rotation of 180º had to be made, with practically zero translation, and a scaling of approximately 0.5. This did not imply a significant alteration of the results and responded to the fact that the graph for the province of Barcelona had a linear size of approximately half that obtained with the data from the province of Madrid, which prevented adequate comparisons from being made . The fact is that the Madrid and Barcelona configurations are similar in structure, but differ in scale and orientation. This in itself indicates that there are differences between the data for the two provinces which cannot be ignored and that, therefore, we are dealing with different realities in relation to the subject studied. Thus, although the correspondence between the data sets is acceptable, some items have higher errors that indicate differences in the way certain types of aggression - and offender behaviours - are structured in both provinces.

Having made this clarification, a closer look at Figure 3 shows that the blue dots represent the original configuration of Madrid before the transformation, while the red dots represent the transformed configuration of Barcelona in order to align with Madrid's. The arrows show the magnitude and direction of the adjustment needed to align Barcelona with Madrid. The arrows show the magnitude and direction of the adjustment needed to align Barcelona with Madrid. As seen in the numerical results, the Barcelona structure was rotated almost 180°, as well as scaled from the Procrustes procedure, in order to align it with Madrid. This is evident from the fact that some blue and red points are in opposite positions in certain areas. Dots with longer lines relating the same variable indicate that there were significant differences in the representation of that variable between the two cities. For example, *Ver_Drug*, *Ver_Vic* and *Ver_Vag_Attempt* show large shifts, suggesting that Madrid's spatial representation in the MDS is different from that of Barcelona.

On the other hand, in the areas with higher concordance, i.e. where the variables where the red and blue dots are close, similar structures are suggested in both provinces. For example: *Ver_Finger*, *Ver_Fore* and *Ver_Alc* show less displacement, indicating that their patterns are similar in both cities. The general structure of the types of aggressions and behaviours attached to them is similar in both cities, but with interesting differences in orientation and scale. As we have already seen, some variables show greater discrepancy, as in the cases of *Ver_Drug*, *Ver_Vic* and *Ver_Vag_Attempt*, indicating that these factors are perceived or structured differently in each province. Other variables have similar structures, suggesting common patterns of aggression and response in both cities that criminology should explain in order to deepen its field of research and not simply assume.

Such differences in the structures of the corresponding Madrid and Barcelona SDMs must necessarily be related to the typologies found by the *K-Means* procedure. Refer now to Figure 4, as it will help to clarify numerically what is going on. The variables with the highest Procrustes error - i.e. those that differ the most between the two cities - are:

- *Ver_Drug* (0.71): The offender was under the influence of drugs.
- *Ver_Vic* (0.66): The offender's volitional and intellectual capacities were impaired.
- *Ver_Vag_Attempt* (0.60): There was an unsuccessful attempt at vaginal penetration.
- *Ver_Pers* (0,41): The perpetrator stole an object that could be used as a fetish.
- *Ver_Anal* (0,30): Victim suffered anal penetration.
- *Ver_Fel* (0,29): The victim suffered oral penetration (fellatio).
- *Ag_Theft* (0,29): Offender's judicial record for robbery.
- *Ver_Weap* (0.28): The aggressor used some kind of weapon. There are differences in the assaults in which the aggressor uses a weapon, being more frequent in Barcelona.
- *Ver_Vag* (0,28): The victim suffered vaginal penetration.

5. DISCUSSION

It seems clear that the comparative study between sexual assaults committed by strangers in the provinces of Madrid and Barcelona has revealed significant differences in the way in which these crimes are perpetrated in each of the contexts and that, therefore, the initial hypothesis is fulfilled. Based on the analysis of 76 cases extracted from court sentences and examined using robust statistical tests - Fisher's exact test, chi-square, multidimensional scaling and Procrustes analysis - distinctive patterns have been identified in the sexual assaults committed in both territories.

In terms of the relevance of the statistics used, the use of Fisher's exact test and chi-square to compare the presence of certain characteristics in the crimes committed in Madrid and Barcelona allowed us to establish significant - or almost significant - differences in key aspects such as drug use by the aggressor *(Ver_Drug*, $p = 0.012$), the use of weapons (*Ver_Weap*, $p = 0.055$, at the limit of significance), and vaginal penetration (*Ver_Vag*, $p = 0.032$). These tests were appropriate for assessing associations between categorical variables in a representative but relatively small dataset.

The MDS and *K-means* analysis allowed us to identify typologies of offenders and patterns of assault in each province, showing structural differences in the way these crimes are committed. The Procrustes analysis showed - always within the reference sample, which should lead to reasonable caution - that, although there is a similar structure to sexual assaults in both areas, the scale and orientation of the factors differ significantly, indicating specific patterns in each area.

Regarding the differences between Madrid and Barcelona, the statistical and spatial analysis of the data has revealed that, although sexual crimes committed by strangers show structural similarities in Madrid and Barcelona, there are important differences in the methods and circumstances of the assaults that call for the importance of a detailed study of both criminal ecosystems, as mentioned in the introduction, and as predicted by the TAS:

- Higher drug use by offenders in Barcelona: 28.9% of offenders were under the influence of drugs at the time of the offence, compared to only 5.3% in Madrid. This could indicate a stronger association between substance use and aggression in Barcelona or a different criminological context in which offenders in Barcelona have a greater history of drug use at the time of the attack.
- Greater use of weapons in the province of Barcelona: 47.4% of the aggressors used some type of weapon to subdue the victim, while in Madrid this percentage was 23.7%. This suggests a higher degree of instrumental violence in assaults committed in Barcelona, which could be related to context-specific environmental or criminological factors.
- Differences in the way of perpetrating the sexual aggression: in Madrid, vaginal penetration was more frequent (76.3%) compared to Barcelona (50%). But, on the other hand, assaults with oral penetration (fellatio) were more frequent in Barcelona (47.4%) than in Madrid (34.2%). Similarly, anal penetration was also more common in Barcelona (15.8%) than in Madrid (7.9%).
- Differences in the aggressor's approach strategy: in Madrid, aggressors used more strategies of deception, distraction or subterfuge to approach the victim (55.3%) than in Barcelona (36.8%). In contrast, a greater number of surprise and unplanned attacks were observed in Barcelona (63.2% compared to 44.7% in Madrid). This suggests that aggressors in Barcelona province opt more frequently for direct and violent attacks, while those in Madrid rely more on the use of manipulation and deception to reduce the resistance of the potential victim.
- Differences in victim response and crime interruption: victims in Barcelona tended to resist in greater proportion (60.5%) compared to Madrid (52.6%). Perhaps because of this, the interruption of the aggression due to unexpected circumstances was more frequent in Barcelona (34.2%) than in Madrid (28.9%), which suggests that in Barcelona the aggressions tended to take place in contexts less controlled by the aggressor, a fact that makes sense given the idea of a greater use of violence, and, therefore, of a component of greater impulsivity and less practical control of the scene in the unknown sexual aggressor in the province of Barcelona.
- Criminal records of the offender: offenders in Barcelona had a higher number of records for previous sexual offences (13.2%) compared to Madrid (5.3%). There were, however, no significant differences in the records for robbery or non-sexual violence.

6. CONCLUSIONS

From the findings described in this study, it is possible to describe a profile of sexual assaults by strangers found in the sentences issued in each of the provinces analysed.

In Madrid, there was a greater use of deception to approach the victim, a greater frequency of vaginal penetration, a lower use of weapons and drugs at the time of the aggression, and a group of aggressors with less previous convictions for sexual offences. In Barcelona, on the other hand, there was a higher frequency of surprise attacks, a higher use of weapons and drugs, and a higher number of perpetrators with a criminal record for sexual offences. A higher frequency of assaults with oral and anal penetration was also detected, as well as a greater tendency of the victim to resist, although with a higher proportion of assaults interrupted by external factors.

The results of this study confirm that sexual assaults perpetrated by strangers present significant differences in both territories, suggesting the need for prevention and response strategies adapted to the specific criminological characteristics of each city. This, in the context of the TAS, would only be possible by paying attention to a detailed analysis of the delinquent-criminal context in which the aggressors act in each case, which would require concrete, specific, detailed and detailed studies that, quite simply, call into question the validity of the TAS, call into question the validity of the great theories and methodologies - which explain the general with certain guarantees, but tend to fail in their approach to the particular - and impose the need for a surgical study of each criminal ecosystem in order to specify precise and efficient policies - of detection, investigation and prevention. Thus, for example, this work suggests that in the province of Barcelona, given the greater use of weapons and drugs in attacks, it would be advisable to implement the relevant control measures on these aspects, as well as to proceed to a more profuse, detailed and accurate study of the criminal history of potential aggressors. In Madrid, however, the marked tendency detected in the use of deception in the approach to the potential victim by the sexual aggressor could indicate the need for awareness campaigns to help women to identify the use of possible strategies of manipulation, control and isolation in strangers.

From a criminological perspective, and always taking into account ecosystemic variables, the findings highlight the importance of further research into the relationship between the criminal background -their previous criminal career, in general- of the aggressors and their behaviour during the aggression, as well as the detectable differences in the specific response of the victims and the factors that may lead to the interruption of an attack, which may suggest interesting advances and developments in the framework of criminal policies at the regional and even provincial level.

On the other hand, it should be noted the relevance of this study for the development of criminological techniques auxiliary to police investigation, and more specifically to the growth of inductive criminological profiling -behavioural analysis-, as the data found are useful for the detailed qualification of current criminal typologies which often, because they are excessively broad, tend to be of little use in terms of their

practical application. We see, for example, that in the province of Madrid the aggressors have more differentiated clusters depending on the seriousness of the crime committed, while in the province of Barcelona the aggressor shows a behavioural organisation more linked to his specific criminal history. In both cases, indistinctly, the consumption of substances and the planning of the attack play a relevant role, but there are clear differences in terms of the execution and interruption of the crime that should be known and properly nuanced, as they would be of great help in terms of the design of specific criminal profiles, as well as in police investigation processes.

Ultimately, this study, which only addresses two provinces here, but could be expanded nationally with adequate funding and infrastructure, contributes to a better understanding of stranger sexual violence, while showing that a situational-ecological study of crime not only provides useful data to improve crime prevention, intervention and prosecution, but also its criminological understanding beyond generalities.

7. BIBLIOGRAPHICAL REFERENCES

Arqué-Valle, P., Pastor-Cárcel, A., Roca-Mercadé, C. and Soria M.A. (2024). Cultural influence on the sexual motivation of serial killers. *Logos Science & Technology Journal, 16*(1), 145-159, doi: https://doi.org/10.22335/rlct.v16i1.1908

CGPJ (2023). Courts have granted 1,205 sentence reductions in application of Organic Law 10/2022 [available at: **https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/En-Portada/Los-tribunales-han-acordado-1-205-reducciones-de-pena-en-aplicacion-de-la-Ley-Organica-10-2022** , collected March 2024].

Corovic, J., Christianson, S.A. and Bergman, R. (2012). From crime scene actions in stranger rape to prediction of rapist type: single victim or serial rapist? Behavioral Science and the Law, 30, 764-781.

Domínguez Vela, M. (2016). Gender violence and secondary victimization. Digital Journal of Psychosomatic Medicine and Psychotherapy, Vol. 6(1). [available at: **https://www.psicociencias.org/pdf_noticias/Violencia_de_geneo_y_victimizacion_secundaria.pdf** , retrieved May 2024].

Gower, J.C. (1975). Generalized Procrustes analysis. Psychometrika, 40, 33-51.

Gutiérrez de Piñeres Botero, C., Coronel, E. and Pérez, C.A. (2009). Theoretical review of the concept of secondary victimisation. Liberabit [online], 15(1), 49-58 [available at: **https://pepsic.bvsalud.org/scielo.php?script=sci_abstract&pid=S1729-48272009000100006** , retrieved March 2024].

Hurley, J. R., and Cattell, R. B. (1962). The Procrustes Program: Producing direct rotation to test a hypothesized factor structure. Behavioral Science, 7(2), 258-262**. https://doi.org/10.1002/bs.3830070216**

Janosch González, H. (2013). Philosophical foundations of criminology in Hirschi and Wikström: Popper or Bunge? In Serrano Maíllo, A., and Birkbeck, C., (Eds.) The Generality of Self-Control Theory. A first extension of the general theory of crime to Spanish-speaking countries. Madrid: Editorial Dykinson.

Janosch, H., Pérez-Fernández, F., Nut, D. and Marset, M. (2023). Sexual assailants unknown to the victim in Spain. A multidimensional scaling analysis (MDE) based on an analysis of sentences. Revista de Derecho Penal y Criminología, 3ª Época, 30, 395-411.

Janosch, H., Pérez-Fernández, F. and Herrero, S. (2025). Sexual assailants unknown to the victim in the Community of Madrid: an exploratory analysis of sentences handed down by the Provincial Court. H. Janosch and F. Pérez-Fernández

(coords.), Panorámica de los delitos sexuales en España. Madrid: Dykinson, 43-85.

Janosch, H., Pérez-Fernández, F. and Popiuc, M. (2023). Low self-control in non-heterosexual men as a predictor of sexual assault behaviors against women. Behavior & Law Journal, 9(1), 65-79, **https://doi.org/10.47442/blj.2023.100**

Janosch, H., Pérez-Fernández, F., Popiuc, M. and López-Muñoz F. (2024). Relationship between low personal morality and impersonal sex with sexual aggression behaviors towards women in a sample of Spanish heterosexual men. Journal of Asia Pacific Studies, 7(2), 109-139.

Janosch González, H., Pérez-Fernández, F. and Soto Castro, J.E. (2020). A profiling model for unknown sex offenders who assault at building entrances. Revista de Derecho Penal y Criminología, 3ª época, 24, 243-258.

Kühne, H.H. (1986). Kriminologie: Victimologie der Notzucht. Juristische Schulung, 5, 388-394.

Linde, A. and Aebi, M.F. (2021). Does theft really mean theft? and other dubious equivalences between legal and criminological definitions of offences. Consequences for the study of crime. Revista Española de Investigación Criminológica, 19, Extra-2 [www.criminologia.net], **https://doi.org/10.46381/reic.v19i2.529 .**

Spanish Ministry of the Interior (2023). Statistical Yearbook of the Ministry of the Interior 2022. Publications Catalogue of the General State Administration**: https://cpage.mpr.gob.es**

Pauwels, L., 2018a. Analysing the perception-choice process in Situational Action Theory. A randomized scenario study. European Journal of Criminology, 19(1), 130-147.

Pauwels, L. (2018b). The conditional effects of self-control in situational action theory. A preliminary test in a randomized scenario study. Deviant Behavior.

Pérez-Fernández, F., Janosch, H. and Popiuc, M. (2023). Low self-control in non-heterosexual men as a predictor of sexual assault behaviors against women. Behavior & Law Journal, 9(1), 65-79**. https://doi.org/10.47442/blj.2023.100**

Pueyo, A.A. and Redondo Illescas, S. (2007). Predicting violence. Between dangerousness and the assessment of the risk of violence. Papeles del Psicólogo, 28(3), 157-173.

Serrano Maíllo, A. (2017). Crime, individual morality and controls. Valencia: Tirant Lo Blanch.

Triviño, C., Winberg, M. and Moral, M. (2021). Credibility of Testimony in Child Sexual Assault and Abuse: Evolution of Non-Believable Testimony in the Last Decade. Behavior & Law Journal, 7(1), 43-57**. https://doi.org/10.47442/blj.v7.i1.83**

Wikström, P.-O., Oberwittler, D., Treiber, K. & Hardie, B. (2012). Breaking Rules: The Social and Situational Dynamics of Young People's Urban Crime. Oxford: Oxford University Press.

Wikström, P.-O., & Treiber, K. (2016). Social Disadvantage and Crime: A Criminological Puzzle. American Behavioral Scientist 60(10), 1232-1259.

Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Research Article

DRUGS AND DRIVING: "ZERO TOLERANCE" SYNLAB SALIVARY REPORT METHODOLOGY AND NATIONAL ACCREDITATION BODY APPROVAL CRITERIA

English translation with AI assistance (DeepL)

Juan Carlos Rodríguez Bello
Corporal 1 of the Guardia Civil
Guardia Civil Traffic Grouping
University Expert in Road Crime by the UNED (UNED)
Judicial Expert in Documentary Scrutiny by the UNED (UNED)
jcrbello@guardiacivil.es

Received 18/02/2025
Accepted 14/05/2025
Published 27/06/2025

Recommended citation: Rodríguez, J. C. (2025). Drugs and driving: "zero tolerance" methodology of the salivary report of the Synlab laboratory and homologation criteria of the National Accreditation Entity. *Revista Logos Guardia Civil*, 3(2), p.p. 197-220.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

DRUGS AND DRIVING: "ZERO TOLERANCE" SYNLAB SALIVARY REPORT METHODOLOGY AND NATIONAL ACCREDITATION BODY APPROVAL CRITERIA

Abstract: Legislation on the control of alcohol and drug consumption has a great impact on society, not always without controversy, depending on how this information is conveyed to public opinion. A clear example is the criteria used to establish the legal limit of alcohol consumption compatible with driving. Although society accepts the zero tolerance criterion for drug consumption, it is essential to standardise the methods used to detect and quantify the presence of drugs that influence driving and, consequently, affect road safety. In this context, establishing and determining the quantity of the minimum concentrations, in the event of a positive drug test, is essential and especially important in the case of repeat offenders or road offenders. However, this qualitative and quantitative determination must be properly audited. This article reviews the history that has led to the determination of the detectable quantities of drugs, but, above all, the traceability criteria that are typical of accredited systems in the field of Road Safety.

Resumen: La legislación sobre el control del consumo de alcohol y drogas tiene una gran repercusión en la sociedad, no siempre exenta de polémica, dependiendo de cómo se traslade esta información a la opinión pública. Un claro ejemplo, lo tenemos con los criterios que se utilizan para establecer el límite legal de consumo de alcohol compatible con la conducción. Si bien es aceptado por la sociedad el criterio de tolerancia cero en cuanto al consumo de drogas, es fundamental la estandarización de los métodos por los que se detecta y cuantifica la presencia de drogas que influye en la conducción y, consecuentemente, afecta a la Seguridad Vial. En este contexto, establecer y determinar la cantidad de las concentraciones mínimas, en caso de detectarse un positivo en drogas, es imprescindible y especialmente importante en conductores reincidentes o en los delincuentes viales. Sin embargo, esta determinación cualitativa y cuantitativa debe estar debidamente auditada. En este artículo, se hace una revisión del histórico que ha llevado a la determinación de las cantidades detectables de drogas, pero, sobre todo, a los criterios de trazabilidad que son propios de sistemas acreditados en el ámbito de la Seguridad Vial.

Palabras clave: Seguridad Vial, tolerancia cero, conducción, drogas, detección, concentración mínima, estandarización, acreditación.

Keywords: Road safety, zero tolerance, driving, drugs, detection, minimum concentration, standardisation, accreditation.

ABBREVIATIONS

Art.: Article.

PC: Penal Code.

DED: Electronic Detection Device (portable drug).

DGT: Dirección General de Tráfico.

ENAC: Entidad Nacional de Acreditación (National Accreditation Entity)

FSCSV: Prosecutor for Road Safety Coordination Chamber

FGE: Fiscalía General del Estado.

ISO: International Stantarization Organization (internationally recognised standard).

LOQ: Limit Of Quantification.

LSV: Road Safety Law.

Ng: Nanogram (1ng = 1.0E-9 g).

SV: Road Safety.

WHO: World Health Organisation.

ONSV: National Road Safety Observatory.

UN: United Nations.

SV: Road Safety.

TC: Constitutional Court.

UNE: A Spanish Standard.

EU: European Union.

1. INTRODUCTION.

In the "Global Plan - Decade of Action for Road Safety[1] 2021-2030" of the World Health Organization (WHO-UN) it has been determined that one of the main behaviours contributing to fatalities and casualties in road crashes is drink-driving. Therefore, the WHO urges governments to: design the operation of a safe road transport system through the creation of Road Safety (RS) laws, to enforce these laws and to promote road safety education. In addition, the UN body not only urges official bodies, but also private companies to address and mitigate actions that negatively affect road safety and to spread the message that high consumption of alcohol and other substances, such as drugs, contributes to "dangerous driving". The WHO also sets two targets for 2030: to halve the number of deaths and casualties from road crashes caused by alcohol-impaired drivers and to achieve a reduction in crashes caused by the use of psychoactive substances.

In relation to the above, in Spain, the National Road Safety Observatory (ONSV)[2] as a body under the Ministry of the Interior and managed through the Directorate General of Traffic (DGT), has published the so-called "Systematic review on drugs and driving (2021)". This document refers to the "Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial" (LSV)[3] , and specifically to Art. 14, which prohibits driving with the presence[4] of drugs in the body (excluding those substances used under medical prescription and for therapeutic purposes). However, in this section of the LSV the legislator warns that "(...) provided that (the driver) is able to use the vehicle in accordance with the obligation of diligence, caution and non-distraction[5] established in Art.10".

Moreover, in Spain, driving a motor vehicle "under the influence of toxic drugs, narcotics or psychotropic substances" may constitute an offence against the SV as defined in Article 379.2 of Organic Law 10/2015 of the Criminal Code (CP). For this reason, on 17 July 2019, the General State Prosecutor's Office (FGE), through the Prosecutor's Office for the Coordination of Road Safety (FSCSV), issued an Instruction for the preparation of attestations for offences of driving under the influence of toxic drugs, narcotics and psychotropic substances of Art. 379.2 of the Criminal Code. In this Instruction, the importance of the report of external signs to determine the influence of these substances is emphasised, since the Spanish legislator did not have an objective rate to determine the impairment of the subject's psychophysical faculties for safe driving, and therefore, the typical element of influence. In his own words, "the theses applied to alcohol are not transferable per se to toxic drugs, narcotics and psychotropic substances, where the scientific premises differ from alcohol for various reasons", and this is due to the fact that it has not been possible to establish the influence on the subject's

[1] See: https://www.who.int/es/publications/m/item/global-plan-for-the-decade-of-action-for-road-safety-2021-2030.

[2]See: https://www.interior.gob.es/opencms/es/el-ministerio/funciones-y-estructura/subsecretaria-del-interior/direccion-general-de-trafico/

[3] Royal Legislative Decree 6/2015, of 30 October, approving the revised text of the Law on Traffic, Circulation of Motor Vehicles and Road Safety of the Interior. BOE no. 261, of 31 October 2015 Reference: BOE-A-2015-11722.

[4] Positive for drugs: a fine will be imposed for infringement of art. 14.1. 5ª of the LSV for the presence of drugs (1000 Euros / 6 points)".

[5] The driver must use the vehicle with the necessary diligence, caution and care to avoid any damage to himself or others, taking care not to endanger himself, the other occupants of the vehicle and other road users, especially those whose characteristics make them more vulnerable".

psychophysical aptitudes that enable him to drive safely, based on a level of drug concentration detected in a saliva test.

Thus, in our country and according to data provided by the DGT[6] , "almost a third of those killed in road accidents exceeded the alcohol limit", but we can also affirm from the evidence of the observation made during more than two decades of professional practice "on the road" by the author of this research work, that the leisure and nightlife lifestyle is one of the factors that increase the probability of consuming alcohol and drugs (cannabis, cocaine and ecstasy) on the part of some drivers (Calafat, A. et al, 2000). And this consumption has become increasingly consolidated in recent years, becoming one of the most important risk factors for road accidents in Spain.

We can also state, thanks to the author's professional experience, that another risk factor is riding as a passenger in a motor vehicle whose driver has consumed alcohol or drugs, which causes every year a constant trickle of what we can call "innocent victims" (passengers, motorcyclists, pedestrians and cyclists) who die in road accidents as a result of a driver driving under the influence of alcohol or drugs, albeit after joint participation of both (driver and passenger) in night-time activities associated with leisure.

This is why, despite the DGT's SV policies, its awareness campaigns on alcohol and drug consumption prior to driving, and the surveillance and control campaigns carried out by traffic enforcement officers, there is still no real "community SV awareness" or "social road awareness" that would make us understand the dangers of this type of behaviour, but above all to prevent it and in any case, as drivers or users, to reject and report it.

Finally, we are obliged to mention those drivers who are repeat offenders or multiple offenders (classified as such according to the time elapsed between the commission of one offence and another and the number of offences committed) and who, being habitual consumers of alcohol or drugs (or both substances at the same time) could be called "addicted drivers", and who can be considered as potentially dangerous for the SV and should therefore be subject to special monitoring and treatment as patients by the health authorities[7] , in coordination with the surveillance and control work of the DGT .

2. THE STRATEGY OF THE DIRECTORATE-GENERAL FOR TRAFFIC: "ZERO TOLERANCE".

In June 2012 the DGT adopted the "zero tolerance" measure as its main line of strategy on driving and drug use, applying this "zero tolerance" to all drivers who use drugs and who get behind the wheel of a vehicle. The reasons given by the DGT[8] were that: "Spain is among the countries with the highest consumption of drugs, especially cocaine and cannabis, which results in an increased risk of road accidents and fatal or serious injuries".

---

[6]See: https://revista.dgt.es/es/noticias/nacional/2022/04ABRIL/0404_Campana-alcohol-Cifal.shtml.

[7]The national regulation RD 818/2009 General Regulation for Drivers and the European regulation CD 439/1991, CD 126/2006 and CD 36/2012, state that these patients (addicts) cannot be granted or renew their driving licences as they do not have adequate aptitudes for safe driving.

[8]Document "Drugs and Driving - Zero Tolerance" (DGT).
https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2012/Presentacion-Tolerancia-cero-con-los-conductores-que-consuman-drogas-al-volante.pdf

Thus, according to the 2017 study by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA[9]), in the age group 15-34 years, Spain is the most affected by drug addiction in the European Union:

The sixth EU country with the highest rate of cocaine use (with a prevalence of 2.8%), after the UK (4.7%), the Netherlands (4.5%), Denmark (3.9%), France (3.2%) and Ireland (2.9%).

The fourth EU country with the highest rate of cannabis use (18.3%), behind France (21.8%), Italy (20.9%) and the Czech Republic (19.3%).

Therefore, the actions to be taken by the DGT, in line with its "zero tolerance" strategy, included the following:

Raise the awareness of society as a whole about the problem, inform drivers of the risk of drug use (without forgetting the risk posed by alcohol consumption), know the minimum consumption of alcohol and drugs that cause major driving impairment, extend drug and alcohol + drug controls on all types of roads, days and times; collaborate with other administrations in legislative, educational and training matters related to drugs and driving, and promote applied research in the field of drugs and road safety.

Likewise, and as an objective for the year 2030, the DGT's strategic area of surveillance and control has extended "zero tolerance" to the risk behaviours that have the greatest impact on road accidents, with the following priorities: acting on speeding, alcohol and drug consumption, use of mobile phones while driving and not using safety equipment (seat belts, helmets, child restraint systems, etc.).

2.1. RATIONALE AND PROCEDURE FOR SALIVARY DRUG TESTING.

Until relatively recently, and due to the lack of portable Electronic Detection Devices (DED) with the appropriate technology, it was not common for "on the road" tests to be carried out to detect whether the driver had consumed drugs. The reason for this is that only by carrying out a blood test could one be sure of the results, but, in addition, carrying out these blood tests and their subsequent transfer to the laboratory for analysis was relatively complex and legally difficult.

Subsequently, the importance of the issue and the DGT's commitment to detecting recent drug use and the presence of drugs in the driver's system became very relevant for both the SV and the professional driver's working environment. Gradually, drug testing was implemented with portable DED devices[10] that allow the detection and analysis of recent drug use in the driver's saliva. Through the rapid collection of oral fluid samples (as a non-invasive procedure), an "indicative positive[11] " for recent use of five drugs

[9]See: https://www.euda.europa.eu/publications_en

[10] See: https://www.toxicology.abbott/es/es/screening-devices/sotoxa-mobile-test-system.html

[11] It is called an "indicative" sample and detects the possible **presence** of illegal substances. See: https://revista.dgt.es/es/sabia-que/normas/2018/0703como-se-hace-un-control-de-drogas.shtml

(amphetamines, methamphetamines, opiates, cannabis and cocaine) can be obtained. However, a second saliva sample, called an "evidential test", is required to be collected in order to name and quantify the type of drug detected in this second sample, and thus confirm the "indicative positive" obtained; this second saliva analysis will be carried out in a reference laboratory. The transfer to the laboratory of this 'evidential test' is carried out in a sealed 'saliva collection tube' identified with a bar code, which is placed in a cooler, after being recorded in a document governed by a strict chain-of-custody protocol.

The obligatory nature of this complementary laboratory test (evidential test) after the initial control (circumstantial test) and the ratification in the reference laboratory of the type of drug detected and its quantity, will give presumption of legal veracity to the offence for the presence of drugs in the driver's organism, as well as the corresponding opening of an administrative sanctioning file by the DGT.

3. THE DOCTRINE OF THE STATE ATTORNEY GENERAL'S OFFICE FOLLOWING THE "POSITIVE" SALIVARY DRUG TEST.

According to the doctrine of the Attorney General's Office (FGE)[12] , and once a "positive result[13] " has been obtained in the salivary index test carried out in a portable DED that is capable of analysing oral fluid, the subsequent analysis of the saliva in an "approved laboratory" is mandatory, depending on the necessary control activities by the competent administration, also guaranteeing the "chain of custody[14] " of the saliva collected for analysis to ensure the legality of the procedure for obtaining saliva samples and subsequently converting them into prosecution evidence. The FGE also specifies that the agents in charge of traffic surveillance must receive specific training for their performance, as this type of test is more complex than alcohol detection tests.

Once in the laboratory, salivary samples are processed by analytical equipment consisting of a gas chromatograph[15] (capable of vaporising substances of different volatilities) and a mass spectrometer[16] (capable of generating ions from neutral molecules in the gas phase, separating them according to their mass and detecting them by recording the information appropriately), determining what type of drug and how much is in the salivary sample. These kits are capable of detecting up to forty types of drugs and quantities as small as one nanogram[17] (ng). These laboratory results are then reviewed one by one by specialised medical staff, who sign and validate the final report to be sent to the DGT.

---

[12] Circular 10/2011 of 17 November (BOE FIS-C-2001-000010).

[13] The term "positive" does not indicate a certain rate in nanograms, but any result that indicates the mere presence of drugs in the body, i.e. it is not a quantitative test, but a qualifying test with a positive or negative result.

[14] Chain of custody is understood as the process by which it is accredited that the seized object is the same as the one that has finally been analysed. A possible breach of the chain of custody could lead to a violation of the right to due process.

[15]See:https://www.mncn.csic.es/docs/repositorio/es_ES/investigacion/cromatografia/espectrometria_de_masas.pdf

[16]University of La Rioja. Laboratory and Workshops Service**.** Gas Chromatography**:** Qualitative analysis by gas chromatography mass detection Without previous sample preparation operations. 75 € / hour. Mass spectrometry: Qualitative analysis by electrospray mass spectrometry/high resolution Without previous sample preparation operations. 120 € / hour.

[17] Billionth part of a gram: 1 ng = 1e-9 gr.

However, as we have already indicated, unlike alcohol tests, a "zero tolerance" SV policy has been adopted in the case of toxic drugs, since the LSV[18] expressly and tacitly prohibits the presence of narcotic substances in the driver's body. A road policy that is not exempt from criticism, as several authors reproach the discrepancy between the positive results detected in the DED and the positive laboratory results (Ramírez, J, 2024).

These authors state that the "cutoff" (analytical cut-off points determined in ng/ml)[19] , of the brands of portable DED, the laboratory-confirmed detection limits and the quantity of the psychoactive substance detected cannot be contrasted.

4. PRESENCE OF DRUGS IN THE BODY: THE ADMINISTRATIVE SANCTION AND THE DOCTRINE OF THE CONSTITUTIONAL COURT.

The LSV imposes an administrative penalty of 6 points and a fine of 1,000 euros on anyone who drives with the presence of drugs in their system. At this point we will mention the Plenary 174/2017 of the Constitutional Court[20] (TC), due to the question of unconstitutionality raised in relation to several articles of RD 339/1990 [21] , and specifically on the relevance of raising a question of unconstitutionality in relation to Art. 12 of Law 6/2015, by classifying as an administrative offence driving a vehicle "with the presence of drugs in your body", without it being necessary to prove that the presence of these drugs has influenced your ability to drive. The High Court "does not consider that the challenged precepts are unconstitutional for prohibiting drug use, through a rule that aims to protect the SV". It also clarifies that the challenged precepts "are not intended to prohibit drug use in general". Therefore, what it prohibits is: drivers driving "with the presence of drugs in the organism (...)". Thus, it is "typified as an administrative offence, so that the prohibited conduct constituting an administrative offence is not consuming drugs, but driving if this type of substance has been consumed". But what is even more interesting is that the High Court equates the consumption of toxic drugs with the consumption of drugs under medical prescription and for therapeutic purposes, since: "The risk that driving with the presence of this type of substance in the body may entail for traffic safety will be the same both in the case that the drugs consumed are under medical indication and in cases in which the consumption of these is not for therapeutic purposes".

As a result, the TC does not consider that the challenged precepts violate constitutional articles and that this invalidates the approach and the concept of what should be understood by "drugs"; moreover, it guarantees that this concept is defined as a substance that has sufficient entity to alter the psycho-physical capacities of the person who consumes it, and that "The aim of the rule, in classifying driving with the presence of drugs in the body as an administrative offence, is to prevent people from driving if they have taken substances that can alter the psycho-physical conditions for driving, given the risk that driving under such conditions can entail for traffic safety (...)".)".

[18] RD 6/2015 of 30 October, amended Law 18/20221 of 20 December BOE no. 304. A cutoff point is the concentration of a substance at which a diagnostic test is considered positive.
[19] A *cutoff* point is the concentration of a substance at which a diagnostic test is considered positive.
[20] BOE no. 15 of 17 January 2018. Sec. TC.
[21] BOE no. 63 of 14 March 1990, approving the articles of the Law on Traffic, Circulation of Motor Vehicles and Road Safety.

5. CUT-OFF POINTS AND MINIMUM PSYCHOACTIVE QUANTITIES.

Once again, the DGT warns, in the document "Systematic review on drugs in driving" (2021), that there are no international or national agreements on the cut-off points (quantified in ng/ml)[22] to be established in the procedures for controlling substance consumption in drivers and that Spain was one of the first countries to regulate testing by saliva sample. To this end, the DGT claims to have taken into account the values recommended at international level in the field of occupational safety, where a number of prestigious bodies, the Substance Abuse and Mental Health Services Administration (SAMHSA)[23] in the United States, the European Workplace Drug Testing Society (EWDTS)[24] , or the National Safety Council's Alcohol, Drugs and Impairment Division (NSC-ADID)[25] in Europe and the United Kingdom), have issued updated reports on the recommendations of the cut-off points to be established, in accordance with the requirements of the ISO[26] /IEC[27] standards in Europe.

Thus, based on the above, the Ministry of the Interior established positivity values for evidential analysis in the laboratory published in the document "Systematic review on drugs in driving" (2021). So much so that the DGT claims to adjust these values to the most recent and applicable international recommendations, and also to the evidence generated by the Spanish experience in this field.

TABLE 1.

Comparison of the analytical cut-off points for the oral fluid evidence test for the consumption of psychoactive substances in drivers of the Directorate General of Traffic and other international organisations.

ANALITO	**Cutoff saliva (ng/ml)**			
	EWDTS	SAMSHA	NSC-ADID	**DGT**
Amphetamine	15	15	15	**15**
Cocaine	8	8	8	**8**
Ketamine	10			**10**
MDA	15	15	15	**15**
MDEA	15	15		**15**
MDMA	15	15	15	**15**
Methadone	20		10	**10**
Methamphetamine	15	15	15	**15**
Morphine	15	15	5	**5**
THC	2	2	2	**2**

Source: Own elaboration according to DGT (2021).
"Systematic review on drugs and driving".

[22] Nanogram (ng): A unit of mass corresponding to one billionth of a gram.
[23] See: https://www.samhsa.gov
[24] See: http://www.ewdts.org
[25] See: https://www.nsc.org/workplace/get-involved/divisions/alcohol-drugs-impairment-division
[26] Royal Spanish Academy: International Organisation for Standardisation, the international standardisation system for the regulation of products and services.
[27] International Electrotechnical Commission, the world's leading standards commission that develops and publishes international standards for electronic technologies.

Note: EWDTS: European Workplace Drug Testing Society (UK).
SAMHSA: Substance Abuse and Mental Health Service Administration (USA).
NSSC-ADID: National Safety Council - Alcohol, Drugs and Impairment Division (USA).

Comparative analysis of the detection limits (cutoff) of the analytes in table 1:

5.1.1 International Consensus: Analytes such as amphetamine, methamphetamine, MDMA, MDA, cocaine and THC show homogeneous values (15 ng/ml for stimulants; 8 ng/ml for cocaine and 2 ng/ml for THC, demonstrating that the standards are widely accepted for their detection.

5.1.2. Variability in specific analytes: Methadone and morphine show lower limits in NSC-ADID and DGT, indicating more sensitive criteria, possibly for forensic and road safety reasons.

5.1.3. Trend of the DGT standard: Spanish DGT regulations include all relevant analytes, but also adopt stricter limits in some cases, indicating a prioritisation of early detection for administrative and also criminal preventive purposes.

TABLE 2.

Comparison of cut-off points (positive): DED Sotoxa[28] , SynLab laboratory and those established by the DGT.

ANALITO	ABBOT SOTOXA[29] TOX400SEU	SYNLAB Laboratory SYNLAB[30]	DGT DGT[31]
6-AM (morphine) (OPI)[32]	40 ng/ml	>2.6 ng/ml	2 ng/ml
Amphetamine (AMP)	**50 ng/ml**	>18.8 ng/ml	15 ng/ml
Benzoylecgonine (BE)	30 ng/ml	>9.9 ng/ml	8 ng/ml
Cocaine metabolite (COC)	**30 ng/ml**	>10 ng/ml	8 ng/ml
Codeine (OPI)	**40 ng/ml**	>12.2 ng/ml	5 ng/ml
Ketamine		>12.6 ng/ml	10 ng/ml
MDA	50 ng/ml	>18.3 ng/ml	15 ng/ml
MDEA	50 ng/ml	>18.2 ng/ml	15 ng/ml
Methamphetamine (MDMA)	**50 ng/ml**	>18.7 ng/ml	15 ng/ml
Methadone (OPI)	**40 ng/ml**	>12.2 ng/ml	10 ng/ml
Morphine (OPI)	**40 ng/ml**	>6.2 ng/ml	5 ng/ml
Cannabis (THC)	**25 ng/ml**	>2.5 ng/ml	2 ng/ml

[28] See: ANNEX I. Explains the "composition and operating principles of the Abbot-SoToxa analyser".
[29] See: https://www.toxicology.abbott/es/es/screening-devices/sotoxa-mobile-test-system.html
[30] Extracted from the report of the confirmatory assay for drugs in saliva by LC-MS/MS of the SYNLAB laboratory.
[31] DGT (2021); "Systematic review on drug driving" (2021).
[32] OPI: Opioids.

Source: Own elaboration (2023); based on reports from the commercial SYNLAB, drug monitoring and toxicology company SYNLAB.

Key observations from table 2:

5.2.1 SOTOXA (DED). Shows the highest values and reflects more permissive positive cut-off points, not an actual concentration.

5.2.2. SYNLAB. Reports actual values above a detectable minimum and reports quantitative results above a threshold, but not normative.

5.1.3. DGT. Provides the lowest values, and are legal cut-off thresholds of toxicological confirmation, establishing the legal limits of the administrative offence and the corresponding sanction.

6. THE CLINICAL ANALYSIS COMPANY SYNLAB.

"Any test, anywhere, anytime" - that is the motto of the German company Synlab Group (SYNLAB) .[33]

SYNLAB was founded in 1998 by Dr. Bartl Wimmer in Augsburg together with a group of partners as an association of independent laboratory physicians. Since then it has grown mainly through acquisitions, offering tests for the presence of the coronavirus during the pandemic. SYNLAB has not gone unnoticed by large institutional investors worldwide, who over the years have taken equity stakes in the company. Currently, the main shareholder is the well-known British venture capital fund Cinven (also with an office in Madrid), which holds around 43% of the shares, according to the German company's estimates. This is followed by the Danes of Novo Holdings (17%); the Canadians of the Ontario Teachers' Pension Fund (OTPP) with 8%; the same percentage as the founder of SYNLAB and his close associates; and the State of Qatar through its sovereign wealth fund (5%).

In Spain, its relationship with the Ministry of the Interior (according to the Public Sector contracting platform of the Ministry of Finance), has been forged through the DGT, which has tendered the "service of determination and quantification of drugs and alcohol in oral fluid and blood samples" on the basis of a contract[34] awarded for a value of 4,999,980.00 Euros to SYNLAB DIAGNÓSTICOS GLOBALES S.A.U (A59845875). In addition to the DGT, this clinical laboratory has been contracted by other administrations: the Regional Government of Andalusia for clinical analyses for the Jaén Centre for the Prevention of Occupational Risks in Jaén, the Madrid Metro and the Generalitat de Catalunya[35] among others.

[33] See: https://valenciaplaza.com/asi-es-synlab-empresa-alemana-compra-sistemas-genomicos

[34] See:https://contrataciondelestado.es/wps/portal/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfIjU1JTC3Iy87KtUlJLEnNyUuNzMpMzSxKTgQr0w_Wj9KMyU1zLcvQj_byycwN9yy2dXPLygvNDIoyrVA3Myx1tbfULcnMdAUNYE4U!/ and BOE 97 of 23 April 2019.

[35] See: https://contractaciopublica.cat/ca/detall-publicacio/200026255

7. LIMITS OF QUANTIFICATION AND UNCERTAINTY RANGES IN SYNLAB LABORATORY RESULTS.

There is additional information on the saliva samples submitted by the SYNLAB laboratory for the substances listed above in the table; it is used as a "positivity criterion" that the concentration of the substances is greater than or equal to the values of the limit of quantification (LOQ)[36] , plus the "uncertainty value" of the test, otherwise the result is negative. Furthermore, SYNLAB refers to the fact that their laboratory has "the expanded uncertainty for K=2 for the whole working range".

To clarify the concept of "uncertainty", we must say that it is the "doubt" that may exist about the result of any measurement, i.e. it tells us about the reliability of that measurement.

Therefore, all measurements that are made have some "uncertainty" and must be quantified in order to decide whether the measurement made is sufficiently reliable for the purpose that has been required. Furthermore, it should be noted that, "error" is not the same as "uncertainty", namely:

Error: The difference between the measurement value of a device and the standard or reference value[37] that is taken as accurate. When making a comparison between values, error and uncertainty are generated according to metrology. Thus, together error and uncertainty can be used to know if an instrument is within the maximum tolerated error.

Uncertainty[38] : After making several measurements during a calibration process, small differences between them are discovered. But which measurement is the correct one, the mean and its standard deviation are found, finding out what is the normal difference between the measurements, making the final measurement sufficiently reliable.

Accuracy: Measures the degree of agreement between the result obtained and the true value (or the one taken as such).

Accuracy: Shows the agreement between two or more measurements that have been taken in the same way**.**

Expanded uncertainty[39] : Before publishing the combined uncertainty component, it is necessary to multiply the result by the selected sigma value to obtain the required confidence level. After multiplication, the result is the expanded uncertainty, i.e. the uncertainty with a given confidence level included.

---

[36] The term refers to the lowest concentration that can be reliably achieved, provided it is within the precision limits specified in routine laboratory operation.

[37] Standard, with the highest accuracy available at a given location or in a given organisation, and from which measurements are derived.

[38] NSGT (2012) Uncertainty of a measurement result, expressed as an experimental standard deviation. Ver: https://www.insst.es/documents/94886/326879/930w.pdf/f657c677-ebab-4f99-8474-667d73e22882

[39]INSGT (2012): A quantity that defines a range around the outcome of a measurement, and in which a significant fraction of the distribution of values that could reasonably be attributed to the measurand is expected to be found.

Evaluation of the uncertainty K=2: The calibration is performed by an authorised laboratory (external calibration) and the expanded uncertainty data are given in %, where K=2 corresponds approximately to a confidence level of 95 %.

Therefore, we can state that the salivary drug analytical results of the SYNLAB laboratory have a level of confidence or expected accuracy that is around the 95 % range/boundary.

8. THE SYNLAB LABORATORY AND ITS ACCREDITATION BY THE NATIONAL ACCREDITATION BODY THROUGH AUDITS.

The National Accreditation Body (ENAC G-78373214 - C/Serrano 240, 4ª A-B, 28016 Madrid) is the only body designated by the Government to operate in Spain as the National Accreditation Body[40] , regulating the functioning of accreditation in Europe, which is based on five fundamental principles: "Non-profit, independence, non-competition, international evaluation and mutual recognition[41] ". Furthermore, ENAC may sign collaboration agreements with the General State Administration and with the Administrations of the Autonomous Communities as may be appropriate for the better performance of its activities and functions[42] .

ENAC "accreditation" should be a guarantee of the correct execution of a certain type of activities, through a certificate issued by this entity.

By way of example, ENAC has carried out the following activities:

In 2013, it has accredited the Instituto de Salud Carlos III[43] de Investigación en enfermedades raras according to the UNE-En ISO 15189 standard for the performance of analyses.

Year 2016, "external audit of accreditation of testing and technical ocular inspection activities" of the Guardia Civil crime laboratories .[44]

Year 2018, has performed "audit services" at the University of A Coruña .[45]

Year 2022, has accredited[46] to the Scientific Police of the National Police Force for the "performance of technical-police inspections at crime scenes", in accordance with the ISO 17020 standard.

---

[40] RD 1715/2010 BOE 7 de núm. 7 of 8 January 2011, "(...) in accordance with the provisions of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No.: 339/93.

[41] See: *https://www.innotec-laboratorios.es/que-es-la-acreditacion-enac/*

[42] BOE no. 7, 8 January 2011.

[43]See:https://www.isciii.es/QueHacemos/Servicios/DiagnosticoGenetico/Documents/ACREDITACION_SDG_IIER_sin_anexo_tecnico.pdf

[44]See:https://www.isciii.es/QueHacemos/Servicios/DiagnosticoGenetico/Documents/ACREDITACION_SDG_IIER_sin_anexo_tecnico.pdf

[45]See: https://www.udc.es/export/sites/udc/contratacionadministrativa/contratos-menores/publicar-Disp-adic-54.xls_2063069239.xls

[46] See: https://www.enac.es/actualidad/policia-cientifica-inspeccion-ocular

Year 2023, has carried out "accreditation activities aimed at the evaluation of laboratories" of the Complutense University of Madrid .[47]

On the other hand, in relation to the activities of a private laboratory (such as SYNLAB), they can be: testing, calibration, inspection, certification or verification entities among others, however, any activity that aims to assess whether a product, service, system, installation, etc. must conform to certain requirements and may be subject to accreditation.

These requirements may be established by law and therefore have regulatory status or be legislated in standards, specifications or other voluntary documents. ENAC accreditation not only gives any laboratory or company being assessed a way of knowing whether its activity is being carried out correctly, but also guarantees the maximum efficiency of its services to the clients of those laboratories.

To assess the correct operation of the laboratory, annual follow-up audits are scheduled and every four years a reassessment audit is scheduled. Follow-up audits review whether there have been changes in procedures, new equipment purchased, etc.

In short, what ENAC can assess and certify is the correct compliance with the standard[48] UNE-EN ISO/IEC 17025 in that year. For information, in the reassessment audits, all the points of the standard during the previous four years are reviewed more exhaustively. If the laboratory fails to meet the requirements in any of these audits, the accreditation may be suspended.

For information, reassessment audits review more comprehensively all points of the standard during the previous four years. If the laboratory fails to meet the requirements in any of these audits, the accreditation may be suspended.

[47] See:[47] https://www.ucm.es/file/208-2023-enac-1-

[48] BOE 19 of 22 January 2018 - Ministry of Economy, Industry and Competitiveness publishing the "General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025:2017)".

9. TABLE 3. SCOPE OF ACCREDITATION[49] ENAC Nº 1169/LE2347, ISSUED TO LABORATORIOS SYNLAB DIAGNÓSTICOS GLOBALES SA. ON TESTING (REVISED 23/12/2022).

NATIONAL ACCREDITATION BODY (ENAC)

PRODUCT/ MATERIAL TO BE TESTED *PRODUCTS/MATERIALS TESTED*	**ESSAY** *TYPE OF TEST*	**STANDARD / TEST PROCEDURE** *STANDARD SPECIFICATIONS/ TEST PROCEDURE*
Saliva (direct or saliva in buffer) Whole blood *Saliva (direct or saliva in buffer) Blood*	Quantitative determination of substances of abuse by ultra-fast high performance liquid chromatography with tandem mass spectrometry detection.	Internal procedure LCMS-004 Rev.15 LCMS-0010 Rev.9

SUBSTANCE	LOQ[50] ng/ml Saliva	LOQ ng/ml Blood
Morphine	**1**	**1**
Codeine	1	2
Heroin	**2**	**2**
Amphetamine	**1**	**2**
Methamphetamine	**1**	**2**
MDA	2	2
MDMA	2	2
MDEA	2	2
Cocaine	**1**	**2**
Methadone	**2**	**2**
Ketamine	2	2
LSD	2	2
Clonazepam	2	2
Alprazolam	2	2
Diazepam	1	2
Lorazepam	2	2
Oxazepam	2	2
Nordiazepam	1	2
Tramadol	1	2
Phencyclidine	2	2
Dextropropoxyphene	1	2
Zolpidem	1	2

ENAC CALIBRACIÓN ISO 17025 Nº62 / LC10.039

Source: SYNLAB (Own elaboration)

[49]See:https://synlab.es/fileadmin/user_upload/Calidad_docs/Anexo_Tecnico_ISO_17025_version_7.pdf
[50] LOQ: Limit of Quantification or lowest level.

KEY OBSERVATIONS FROM TABLE 3:

9.1. INCREASED SENSITIVITY IN SALIVA.

For fifteen of the twenty-two substances in the table, the LOQ in saliva is lower than in blood, highlighting the effectiveness of this matrix for early detection of the substance.

9.2. EQUAL SENSITIVITY IN MATRICES FOR CERTAIN COMPOUNDS.

Seven substances (e.g. LSD, ketamine, benzodiazepines) have the same LOQ in both matrices (2 ng/ml), indicating that the matrix does not significantly affect the analytical sensitivity for these compounds.

9.3. POSSIBLE CLINICAL AND FORENSIC IMPLICATIONS.

Saliva has established itself as a non-invasive and highly sensitive alternative for toxicological analysis, such that the lower LOQ in saliva favours its use in settings such as: drug checkpoints, detoxification programmes or occupational monitoring, where access to a blood test may be limited and not very operational.

9.4. SALIVARY ANALYSIS VS. BLOOD ANALYSIS.

Saliva has positioned itself as a high-value matrix in analytical toxicology, not only because of its lower invasiveness, but also because of its ability to offer higher levels of sensitivity for rapid detection of recent consumption.

Early detection is particularly relevant in prevention and real-time control situations, both at drug checkpoints and in road accidents involving a driver under the possible influence of these substances.

The use of saliva, in combination with laboratory analysis, represents an efficient analytical tool with a higher sensitivity than blood. This is in terms of limit of quantification for a broad spectrum of substances of abuse.

The recommendation to incorporate salivary analysis as a reference matrix in early detection protocols and modern toxicological diagnosis has proved to be correct.

10. CONCLUSIONS.

First. The UN urges governments and institutions (public and private), through the enforcement of SV laws, to achieve a reduction in drug-related road fatalities.

Secondly. In Spain, the DGT (Ministry of the Interior) has established a policy of "zero tolerance" at the wheel, classifying driving with the presence of drugs in the body as risky behaviour. This behaviour is always punished, either as an administrative offence or as a criminal offence.

Thirdly. Despite the lack of international agreements on "cut-off points", the DGT has established the "cutoff" of the minimum psychoactive quantities. These quantities are in line with those of public and private organisations in both the EU and the USA. With

this, the DGT has determined the quantitative positivity of any drug recently consumed by a driver, which will then be analysed in the reference laboratory.

Fourth. The doctrine of the FGE supports the procedure for collecting salivary samples after the positive circumstantial test, through: the specific training of the agents in the collection of the sample, the guarantee of the chain of custody and a subsequent salivary analysis in a reference laboratory.

Fifth. The TC upholds Art. 14 of the LSV, clarifying that the Law does not prohibit the consumption of drugs; what it prohibits is driving with the presence of drugs in the body.

Sixth. The TC equates and places on the same level the risk that a driver who has consumed drugs, even those taken under medical prescription, can generate for the SV.

Seventh. The "cut-off points" of the portable DED (SoToxa Abbott) used to carry out the first "index test", double or triple the "cut-off points" of reference carried out by the SYNLAB laboratory.

Eighth. The "cut-off points" of the SYNLAB clinical laboratory are higher than those determined by the ISO standard, which the DGT applies to establish minimum psychoactive quantities in laboratory analysis equipment.

Ninth. The approval of the clinical salivary analysis of the SYNLAB laboratory is endorsed by the National Accreditation Entity (ENAC), which certifies compliance with the UNE standard of the equipment and the procedure used by the SYNLAB laboratory in obtaining salivary diagnoses, both in the type of drug detected and in its quantity.

Tenth. The evaluation of the equipment and the procedure for obtaining the analysis of saliva samples from the SYNLAB laboratory by ENAC, accredits the 95% level of confidence or precision of the final results obtained and reflected in its final report.

11. REFERENCES.

Abbot. (2020). SoToxa portable toxicology test analyser. https://www.tecmedica.es/cmsAdmin/uploads/o_1f24002cp1ieo17701uni19v4vaja.pdf.

Abbot. (2020). SoToxa Portable Oral Fluid Analyser (User Manual). https://testdealcoholydrogas.cl/wp-content/uploads/2022/08/Manual-APOC0798-v2.a-SoToxa-Mobile-Analyser-User-Guide-FWO-LA.pdf

Spanish Association for Standardisation (2017). General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025:2017). https://www.une.org/

Bequir, S. (2020). Saliva drug test, how long does it last? https://institutocastelao.com/test-de-droga-en-saliva/

Calafat, A et al. (2002). Nightlife recreational life of Spanish young people as a risk factor compared to other more traditional ones. https://www.redalyc.org/pdf/2891/289122037002.pdf

Certum Diagnostics (2019). Drug testing (urine). https://industriasquimicasybiologicas.com/wp-content/uploads/2020/09/Brochure-cassete-individualPrueba-de-Drogas-Certum_Kabla.pdf

Dirección General de Tráfico (2021). Systematic review on drugs and driving. https://www.dgt.es/conoce-la-dgt/que-hacemos/conocimiento-e-investigacion/revision-sistematica-sobre-drogas-y-conduccion

Dirección General de Tráfico (2022). Road Safety Strategy 2030. https://seguridadvial2030.dgt.es/inicio/

Entidad Nacional de Acreditación (n.d.). Institutional ENAC brochure. https://www.enac.es/actualidad/material-multimedia

National Accreditation Body (2022). Report 2022. https://www.enac.es/memoria-2022

Attorney General's Office (2021). Circular 10/2011 FGE, of 17 November, on criteria for the specialised action unit of the Public Prosecutor's Office in matters of road safety. https://www.boe.es/buscar/doc.php?id=FIS-C-2011-00010

National Institute of Toxicology (2021). Table of minimum psychoactive doses of the main toxic substances trafficked. https://pnsd.sanidad.gob.es/ciudadanos/legislacion/delitos/pdf/20210730_INTF_dosis_minimas_psicoactivas_trafico_de_drogas.pdf

Spanish Observatory on Drugs and Addictions (2023). Report 2023 - Alcohol, Tobacco and Illicit Drugs in Spain.

https://pnsd.sanidad.gob.es/profesionales/sistemasInformacion/informesEstadisticas/pdf/2023OEDA-INFORME.pdf

National Road Safety Observatory. (2021). Systematic review on drugs and driving. https://www.dgt.es/conoce-la-dgt/que-hacemos/conocimiento-e-investigacion/revision-sistematica-sobre-drogas-y-conduccion

World Health Organization. (2021). Global Plan - Decade of Action for Road Safety 2021-2030. https://www.who.int/es/publications/m/item/global-plan-for-the-decade-of-action-for-road-safety-2021-2030

Ortega Matus, M. (2022). Monoclonal antibodies and their use to identify morphine in biological fluids. https://riiad.org/index.php/riiad/article/view/riiad-2023-1-09/389

Parra, M. & Vega, V. (2021). Analysis of drugs of abuse in the clinical laboratory. https://www.seqc.es/download/tema/38/7601/85888673/142010/cms/tema-9-analisis-de-drogas-de-abuso-en-el-laboratorio-clinico.pdf/

Ramírez, J. (2024). Los controles de drogas a conductores en España. https://observatoriocannabis.com/wp-content/uploads/2024/10/controlesdedrogas.pdf

Ruiz Viera, L. (2018). Therapeutic monoclonal antibodies. https://riull.ull.es/xmlui/bitstream/handle/915/12352/Anticuerpos+monoclonal+therapeutic.pdf;jsessionid=3462A6DCEAB9DA8E32233B47C6D926E0?sequence=1

GSC-Laboratories (2023). How to evaluate measurement uncertainty without being a mathematical expert. https://sgc-lab.com/guia-para-estimar-la-incertidumbre-de-la-medicion-hecha-para-personas-normales/

ANNEX I

COMPOSITION AND PRINCIPLES OF THE ABBOT-SOTOXA ANALYSER

1.1. COMPOSITION .[51]

The Abbot SoToxa analyser consists of a portable analyser system (DED), a test cartridge or kit and an oral fluid collection device.

1.1.1. The analyser:

It is a portable digital saliva testing device, which uses algorithms to determine the intensity of contrast lines (which will appear on the test cartridge strip after the whole process) and can also display on a screen and print the qualitative and nominative results of the detected drugs.

1.1.2. The test cartridge:

Composed of an immunoassay strip [5253] a single-use, disposable, fast paper chromatographic strip containing dry reagents and a buffer solution. This kit is inserted into the analyser which heats it to the optimal temperature for the test.

1.1.3. The collection device:

It is a disposable device that collects oral fluid (saliva). It should be rubbed on the gums, tongue and inside of the cheeks until the presence indicator turns blue.

1.2. TESTING PROCESS:

The oral fluid collected in the collection device is combined with the buffer solution, then mixed and incubated before contacting the immunoassay strips installed in the test cartridge with a *'moisture-controlled membrane'*.

The mixture of the solution and the saliva obtained flows down the capillary of the cartridge strip and carries away the labelled anti-drug antibodies deposited on it. In the absence of drug in the sample, the antibody binds to the drug-protein mixture forming a line. In the presence of drug, the formation of this line is weaker.

The DED then reads the intensity of the lines on the immunoassay strip from the cartridge and compares this intensity to a predetermined threshold or cut-off point of drug

---

[51] Abbott (2020); "SoToxa Portable Oral Fluid Analyser" (User Manual).
[52] A rapid chromatographic immunoassay is used for the quantitative detection of multiple drugs and drug metabolites in saliva, providing only a preliminary analytical test result.
[53] Chromatography is a technique performed in laboratories to separate components in simple or complex mixtures. There are many different types of chromatography, ranging from paper chromatography and thin layer chromatography to gas chromatography.
See:https://www.onelab.com.ar/cromatografia-que-es-y-para-que-sirve-informacion-completa

concentration, giving a qualitative (not quantitative) result. The results are then displayed on the DED screen and can be printed out.

1.3. POSITIVE RESULTS.

The Abbot SoToxa DED manual specifies that positive results obtained must be confirmed by a second method such as gas chromatography mass spectrometry (GC-MS). In addition, the DED and its results are not intended for home use, clinical, therapeutic or diagnostic settings.

1.4. COMPOSITION OF THE IMMUNOASSAY STRIP OF THE CARTRIDGE.

The chromaticity immunoassay content consists of a strip that is impregnated with a series of dried reagents containing monoclonal antibodies[54] (mAbs). These antibodies (AC) are laboratory-created proteins and are used to identify drug of abuse metabolites in biological fluids.

mAbs have a high sensitivity and bind, for example, to morphine and its metabolites, so they can be used to generate a marked result by "screening" the test strip or cartridge membrane, selectively detecting elevated levels of specific drugs in saliva.

[54] Monoclonal antibodies have a multitude of applications today, both in biomedical research and in the diagnosis and treatment of numerous pathologies. This quality of monoclonal antibodies is due to their high specificity and high affinity for the therapeutic target.

Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Research Article

PROTECTING CRITICAL UNDERSEA INFRASTRUCTURE AND STRENGTHENING BALTIC SEA SECURITY: NATO'S OPERATION BALTIC SENTRY

English translation with AI assistance (DeepL)

Mónica Román González
PhD Candidate in the Political Science and Administration and International Relations Programme at the Complutense University of Madrid.
Master in International Politics: sectorial and area studies at the Complutense University of Madrid.
monicaromangz@gmail.com
ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Received 31/03/2025
Accepted 28/05/2025
Published 27/06/2025

Recommended citation: Román, M. (2025). The protection of critical underwater infrastructures and the strengthening of Baltic Sea security: NATO's Baltic Sentry operation. *Revista Logos Guardia Civil*, 3(2), p.p. 221-256.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

PROTECTING CRITICAL UNDERSEA INFRASTRUCTURE AND STRENGTHENING BALTIC SEA SECURITY: NATO'S OPERATION BALTIC SENTRY

Abstract: Damage to undersea cables in the Baltic Sea has raised alarms about the potential for hybrid warfare and the vulnerability of Western critical undersea infrastructures to sabotage, with repeated incidents in this area being one of the main examples of the geopolitical tensions that exist today. The main objective of this article is to analyse NATO's Operation *Baltic Sentry* in the context of the Atlantic Alliance's growing need to ensure the protection of this type of critical infrastructure in the strategic Baltic Sea and thus reinforce security over the latter. Using mixed research methods, this article first explains the importance of protecting critical undersea infrastructure in the geostrategically important Baltic Sea and then outlines NATO's general framework for protecting such infrastructure. The study then sets out the main characteristics of Operation *Baltic Sentry* launched by NATO in January 2025, concluding that it meets the needs required to be a good strategy capable of enabling the Alliance to make progress in achieving two of its main priority objectives: the protection of increasingly important infrastructures such as critical undersea infrastructures and the consequent reinforcement of security in the Baltic Sea in order to guarantee its resilience.

Resumen: Los daños sobre los cables submarinos en el Mar Báltico han encendido las alarmas sobre una potencial guerra híbrida y la vulnerabilidad de las infraestructuras críticas submarinas occidentales ante posibles sabotajes, siendo así los reiterados incidentes sobre la zona señalada uno de los principales ejemplos de las tensiones geopolíticas existentes en la actualidad. El presente artículo tiene como principal objetivo analizar la Operación *Baltic Sentry* de la OTAN en un contexto en el que impera la creciente necesidad de la Alianza Atlántica de asegurar la protección de este tipo de infraestructuras críticas en el estratégico Mar Báltico y de reforzar así la seguridad sobre este último. Para ello, a través del empleo de métodos mixtos de investigación, el presente artículo primero explica la importancia de la protección de infraestructuras críticas submarinas en una zona de gran relevancia geoestratégica como es el mencionado Mar Báltico para después exponer el marco general de acción de la OTAN respecto a la protección de estas infraestructuras. Tras ello, el estudio expone las principales características de la Operación *Baltic Sentry* lanzada por la OTAN en enero de 2025 concluyendo que esta se ajusta a las necesidades requeridas para ser una buena estrategia capaz de permitir a la Alianza avanzar en la consecución de dos de sus principales objetivos prioritarios: la protección de unas infraestructuras cuya importancia es cada vez mayor como son las infraestructuras críticas submarinas y el consiguiente refuerzo de la seguridad en el Mar Báltico en pro de garantizar su resiliencia.

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Keywords: North Atlantic Treaty Organisation (NATO), Baltic Sea, critical undersea infrastructure, security, Baltic Sentry.

Palabras clave: Organización del Tratado del Atlántico Norte (OTAN), Mar Báltico, infraestructuras críticas submarinas, seguridad, Baltic Sentry.

ABBREVIATIONS

CCD COE: Cooperative *Cyber Defence Centre of Excellence*

CCOE: Civil-Military *Cooperation Centre of Excellence*

CMRE: NATO *Centre for Maritime Research and Experimentation*

CONVEMAR: United Nations Convention on the Law of the Sea

RRC: Resilience *Reference Curriculum*

CTF: *Commander Task Force* Commander

LNG: Liquefied Natural Gas

GUGI: *Glavnoye upravlenie glubokovodnikh issledovanii* or Main Directorate for Deep-sea Research

MARCOM: *Allied Maritime Command* or NATO Naval Command *UK*

NATO: *North Atlantic Treaty Organisation*

NSC: *NATO Shipping* Centre

NATO: North Atlantic Treaty Organisation

SOFCOM: Allied *Special Operations Forces Command*

EU: European Union

USSR: Union of Soviet Socialist Republics

USV: Unmanned *Surface Vehicle*

EEZ: Exclusive Economic Zone

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

1. INTRODUCTION

In recent times, the importance of critical undersea infrastructures has increased dramatically as they facilitate the provision of basic services such as energy, financial transactions, communications or the Internet. This makes the vulnerability of these infrastructures a major concern for international actors, especially given that control of the seabed continues to emerge as a determining element in the power relations of this century (Conte de los Ríos, 2025, p. 34). While the recent proliferation of undersea technology and the consequent acquisition of the capacity to conduct sophisticated operations have favoured their protection capabilities, such innovations also offer a range of possibilities to those actors who wish to exploit their weaknesses (Cassetta, 2024, p. 2).

In this sense, any attack against the North Atlantic Organisation's (NATO) submarine infrastructure would have serious consequences for the security of its member states, making it a target for its rivals. Bearing in mind that an attack on these cables requires the availability of precise means, Russia and to a lesser extent China are the countries that could be identified as the most direct threat, according to the Insikt Group (2023, p. 11-15) in its latest report on the risks to submarine cables.

Thus, the so-called "seabed *warfare*", more commonly known as *Seabed Warfare*, is now an immediate threat to the Atlantic Alliance. Episodes such as the repeated incidents involving submarine cables in the geostrategic Baltic Sea highlight the magnitude of the risks posed by a threat that requires coordinated efforts and investments to complement the strategies designed by each state. This is where NATO's new operation to protect critical undersea infrastructure in the Baltic Sea - Operation *Baltic Sentry* - comes into play.

There is a wide range of literature on this issue. On the one hand, the main reasons that explain the importance of protecting critical underwater infrastructures are widely covered in research by experts in the field such as Noelia Arjona Hernández (2023), Rafael García Pérez (2024) and Augusto Conte de los Ríos (2025). On the other hand, regarding NATO's role in protecting these infrastructures, the report by Njall Trausti Fridbertsson (2023) or the article by Sean Monaghan, Otto Svendsen, Michael Darrah, and Ed Arnold for the *Center for Strategic & International Studies* (2023) are noteworthy. In light of this, the overall objective of this study is to analyse the recently announced Operation *Baltic Sentry* within NATO's framework for strengthening Baltic Sea security through the protection of critical undersea infrastructure.

Accordingly, the overall research question guiding this study is: How does NATO's Operation *Baltic Sentry* respond to the protection of critical undersea infrastructure in the Baltic Sea? The general hypothesis of the research is that Operation *Baltic Sentry* enhances the protection of critical undersea infrastructure in the Baltic Sea and the Alliance's presence in the Baltic Sea, thus adjusting to the new threat environment.

To this end, two specific objectives have been defined. First, to explain the importance of protecting critical undersea infrastructures in an area of great geostrategic relevance such as the Baltic Sea, especially in the current international context marked by the Russian threat following its invasion of Ukraine and the increase in damage suffered by this type of infrastructure since then. Second, to set out NATO's general framework for action with respect to the protection of critical undersea infrastructures.

Thus, having used mixed research methods, the study concludes with conclusions regarding NATO's new project as it attempts to address two increasingly important security issues: the protection of critical undersea infrastructures and the consequent strengthening of Baltic Sea security.

2. FRAMEWORK OF THE STUDY

2.1. THE GEOSTRATEGIC IMPORTANCE OF THE BALTIC SEA

Located in northern Europe (see Figure 1), the Baltic Sea has historically been an area of geopolitical competition, which has now re-emerged as a crucial point of threat to European security following the invasion of Ukraine. Beyond its commercial and marine resource benefits, this enclave is a key hub for infrastructures that contribute significantly to the energy supply of several European states, themselves NATO members (Fridbertsson, 2023, p. 2).

The Alliance itself defines it as "a vital hub for trade and energy transport connecting numerous allied nations" by being a conduit for both energy supplies and a support for undersea cables that transfer data, two crucial elements for the Allied economy and security (NATO Allied Maritime Command, 2025a).

Figure 1

Political map of the Baltic Sea.

Source: McNamara (2016).

With Finland and Sweden joining NATO in 2023 and 2024, the Baltic Sea has become known as 'NATO's Lake'. However, this label is not adequate enough considering that the Allies in the region still face numerous threats and, as defined by John Deni (2023), a dynamic regional security landscape that forces them to join forces through the different cooperation frameworks at their disposal. This situation stems mainly from Russia's presence in the region, which poses increasing challenges to Allied security,

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

especially in the current context that makes the protection of NATO's so-called eastern flank a priority security issue.

Historically, Russia has been a major player in the Baltic region. On the one hand, it has the port city of St. Petersburg, an important economic and cultural centre of the country through which most of its maritime trade has passed since the time of Peter the Great. On the other, Russia also controls the Kaliningrad enclave between Poland and Lithuania, where it has military bases with the Baltic Fleet (Savitz and Winston, 2024, p. 5).

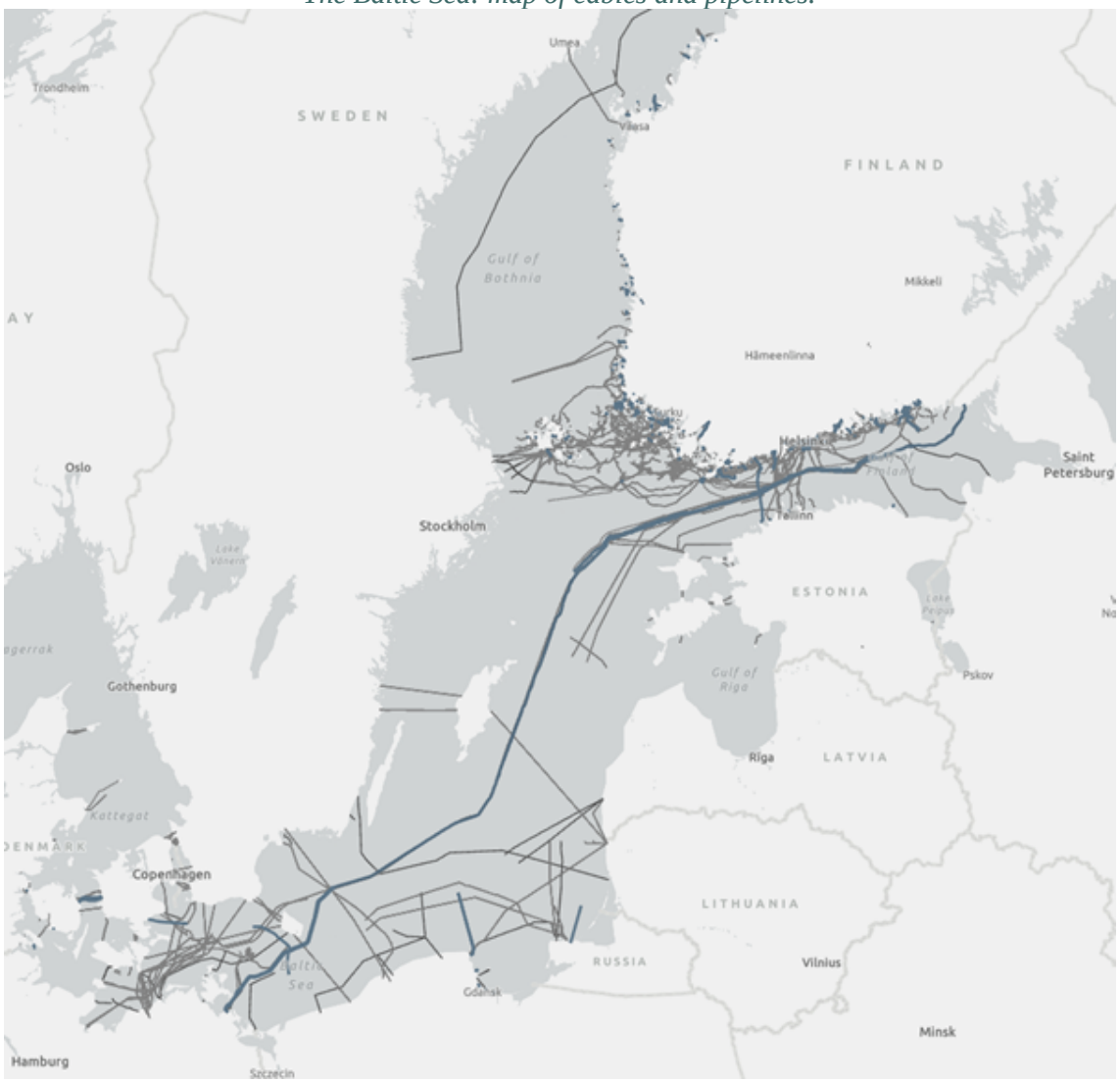
In addition, the so-called 'Russian Ghost Fleet', a Kremlin-created tanker fleet that sails under the flags of other nations in order to evade sanctions imposed after its illegal aggression against Ukraine, is currently operating in the Baltic Sea (Childs, 2025, p 5). Like other Russian vessels, this one is equipped with technology capable of monitoring the seabed and is therefore also suspected of participating in Russia's hybrid campaign against the West through intelligence gathering and the subsequent preparation of sabotage of critical undersea infrastructure (Jones, 2025, p 8). Added to this is the fact that Moscow has repeatedly demonstrated its expansionist ambitions over a region that could be its next target, especially at the height of its hostility towards NATO.

Consequently, Russia is the main challenge to the Alliance in the region. In the region, Moscow finds hybrid tactics to be the main tool for pressuring allies to mitigate conventional military weaknesses and minimise the risks of provoking a direct confrontation between the parties (Cassetta, 2024, p. 2). As is well known, sabotage is executed in a way that makes it difficult to identify those responsible, causing the countries concerned to be cautious in assigning responsibility for fear of escalation. Thus, they are useful to Russia in undermining NATO by preventing the activation of Article 5 collective defence (Jones, 2025, p. 3).

At the same time, it is worth noting that Russia's submarine capabilities are its main strength in competing in the region. As Sidharth Kaushal (2023) explains, Moscow has the Main Directorate for Deepwater Research (*Glavnoye upravlenie glubokovodnikh issledovanii*, GUGI), a secret agency under the Russian Ministry of Defence that operates submarines and vessels capable of engaging in sabotage.

Considering that Russia's critical infrastructure attack capabilities are a fundamental component of its strategy (Fink and Kofman, 2020, p. 16), they could be used to intercept critical communications in the Baltic region (Metrick and Hicks, 2018, p. 7). This region is home to a complex network of undersea infrastructure that is key to communication and energy supply between European nations (see Figure 2).

Figure 2
The Baltic Sea: map of cables and pipelines.



Source: Baltic Marine Environment Protection Commission (2024).

The protection of these critical maritime infrastructures in this key geostrategic region relies heavily on NATO (Fridbertsson, 2023, p. 11), which opens a window of opportunity for Moscow in its desire to weaken the West.

2.2. PROTECTION OF CRITICAL INFRASTRUCTURE UNDERWATER

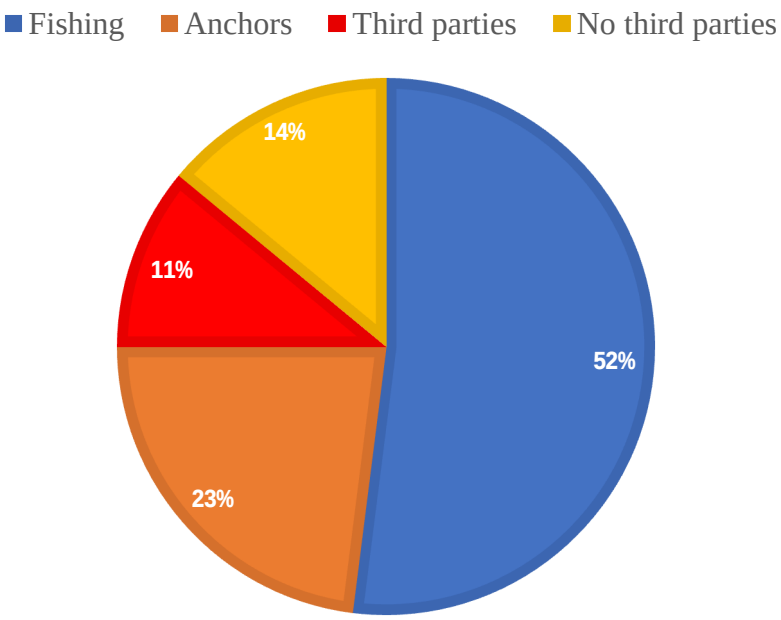
Communications, financial transactions, energy and a wide range of essential daily activities depend on critical undersea infrastructures. According to data provided by the *Submarine Telecoms Forum* (2025, p. 8-9) in its latest report, 99% of international data traffic transits through submarine cables, making them "the backbone of global communications".

Its importance is such that any damage to it can have serious consequences for the stability of society, which makes its security of key geostrategic importance, making it a priceless asset whose protection must be a priority in security agendas (Quijarro Santibáñez, 2023, p. 15-22) (Fridbertsson, 2023, p. 2) (García Pérez, 2024, p. 265-298).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

The increasing dependence on undersea critical infrastructure and the current convergence of traditional and emerging threats make their protection one of the greatest security challenges (Conte de los Ríos, 2025, p. 26), especially given their vulnerability to natural and man-made threats (Guilfoyle, Paige and McLaughlin, 2022, p. 657-696). The *International Cable Protection Committee* (2024, p. 5) argues that human interaction is the most common cause of damage to cables, generally caused by fishing and anchors (see Figure 3).

Figure 3
Chart of the main causes of cable breaks/breaks according to the International Cable Protection Committee.



Source: International Cable Protection Committee (2024, p. 5).

Already in 2016, in the face of increasing Russian submarine activity to an extent not known since the Cold War, James Foggo and Alarik Fritz (2016) proposed their idea of the existence of "The Fourth Battle of the Atlantic" in which undersea infrastructures, in particular energy supply platforms and telecommunications cables, would be threatened. A battle that, according to James Foggo (2023), began in earnest after the apparent attack on the Nord Stream pipeline in 2022.

The fact is that the importance of these infrastructures has made them not only a priority target for protection, but also a possible target for attacks by actors interested in destabilising others. Incidents such as the one mentioned above have raised awareness of the vulnerabilities of these infrastructures in the context of international tensions, which has led to a turning point in the understanding that the adoption of measures to guarantee their protection is fundamental (Fridbertsson, 2023, p. 11) (Monaghan et al., 2023, p. 2).

On the other hand, the constant technological evolution entails important repercussions in terms of the submarine capabilities that the different actors must acquire (Clark, 2015, p. 18), something that has significantly contributed to the consolidation of the submarine domain as the so-called "sixth domain". This new operational domain,

which is increasingly disputed, concentrates economic, strategic and military interests due to the wealth of resources it harbours and which make it a theatre of conflict known as *Seabed Warfare* (Conte de los Ríos, 2025, pp. 29-30). Although its conceptualisation is still being developed by actors such as NATO, Conte de los Ríos (2025, p. 29) defines it as the set of operations carried out in, to, from, on and under the seabed for strategic or military purposes, using the sabotage of the Nord Stream gas pipeline as a representative case.

The maritime domain is particularly vulnerable to hybrid threats. In addition to the fact that the latter are difficult to distinguish from accidental damage, aggressors may use the cover of vessels of various kinds that are difficult to track, such as fishing vessels or private vessels (Monaghan et al., 2023, p. 6). In this regard, it should be recalled that, as sabotage is not considered a violation of the prohibition of the use of force under the UN Charter, international law restricts the military response to damage to cables, especially when non-military vessels are involved (Conte de los Ríos, 2023, p. 33).

Christian Bueger and Tobias Liebetrau (2021) argue that the governance of underwater critical infrastructures is more complex due to two factors: (1) the need for international cooperation by various state actors -who act on the basis of their strategic benefits- and (2) the fact that part of these infrastructures are owned by the private sector -whose role is relevant considering that their interests may be misaligned with the interests of states-. This complexity makes it difficult to apply effective legal provisions in case of damage to critical underwater infrastructures (Conte de los Ríos, 2023, p. 32).

The legal regime applicable to submarine infrastructure is based on international instruments, among which the Convention for the Protection of Submarine Telegraph Cables of 1884 and the United Nations Convention on the Law of the Sea (UNCLOS) of 1982 stand out. The latter establishes that all states have the right to install submarine cables and pipelines on the continental shelf, in accordance with the national legislation of the coastal state concerned (Arjona Hernández, 2023, p. 48). Likewise, UNCLOS delimits different maritime spaces - territorial waters, Exclusive Economic Zones (EEZs) and the high seas - attributing full sovereignty in the former, limited rights in EEZs and a less well-defined regulatory framework in international waters, where the military activity of other states cannot be legally restricted (McNamara, 2024).

It should be noted that among the emerging challenges to international maritime law are Unmanned Underwater Vehicles (UUVs) and Unmanned Maritime Systems (MUS), whose legal status remains undefined. The absence of a specific regulatory framework for their international operation complicates their integration into current regimes, particularly with regard to UNCLOS (Conte de los Ríos, 2023, p. 32). In this context, the growing importance of critical underwater infrastructures makes it indispensable to advance towards an effective international legal framework that guarantees their protection (García Pérez, 2023, p. 50).

Given the importance of these infrastructures and their complex legislation, Michael McNamara (2024) explains that, as geopolitical tensions between the West and its competitors increase, these infrastructures are a target as hybrid interference is a useful tool in its aim to challenge the interests of Euro-Atlantic democracies. These currently face their main threat in Russia's hybrid actions (Monaghan et al., 2023, p. 2), particularly in the Baltic Sea where it has strengthened its presence by investing in submarine capabilities, considered its main asset (Gresh, 2023, pp. 3-4).

Taking into account the complex context and the situation of the Baltic Sea, experts such as Conte de los Ríos (2025), Njall Trausti Fridbertsson (2023) and Monaghan et al (2023) agree on a series of key elements for defining an effective protection strategy.

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Recognising that it is essential to strengthen detection, deterrence-prevention, adaptation and response capabilities, the elements to be highlighted are: (1) increased presence or surveillance, (2) collaboration between actors, (3) coordination with the private sector, (4) advanced technology, (5) regulatory frameworks, (6) response measures and (7) renewing maritime strategies.

2.3. THE SITUATION OF CRITICAL UNDERWATER INFRASTRUCTURE IN THE BALTIC SEA SINCE THE START OF THE RUSSIAN FULL-SCALE INVASION OF UKRAINE IN 2022

On 26 September 2022, the Danish Maritime Authority reported several methane leaks caused by a series of underwater explosions off the Danish island of Bornholm that severely damaged the Nord Stream pipeline (see Figure 4), cutting off the supply of Russian gas to the European market via the Nord Stream pipeline (Energistyrelsen, 2022).

Figure 4

Map of the Nord Stream 1 and Nord Stream 2 pipelines next to the methane leaks detected in September 2022.

Source: The European Space Agency (2022).

Regardless of the unknown perpetrator of the apparent sabotage, experts agree that this was a turning point for the Allies to consider efforts to improve their ability to defend against hybrid tactics in the submarine domain (Monaghan, 2022) (Fridbertsson, 2023) (Conte de los Ríos, 2025).

A similar case was recorded in October 2023 with the Balticconnector pipeline incident. This infrastructure, together with the Inkoo liquefied natural gas (LNG) terminal, safeguards the security of supply and energy independence of the countries in the area (see Figure 5).

Figure 5

Map of the gas transmission network in Finland and the Baltic States.

Source: Gasgrid (n.d.)

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

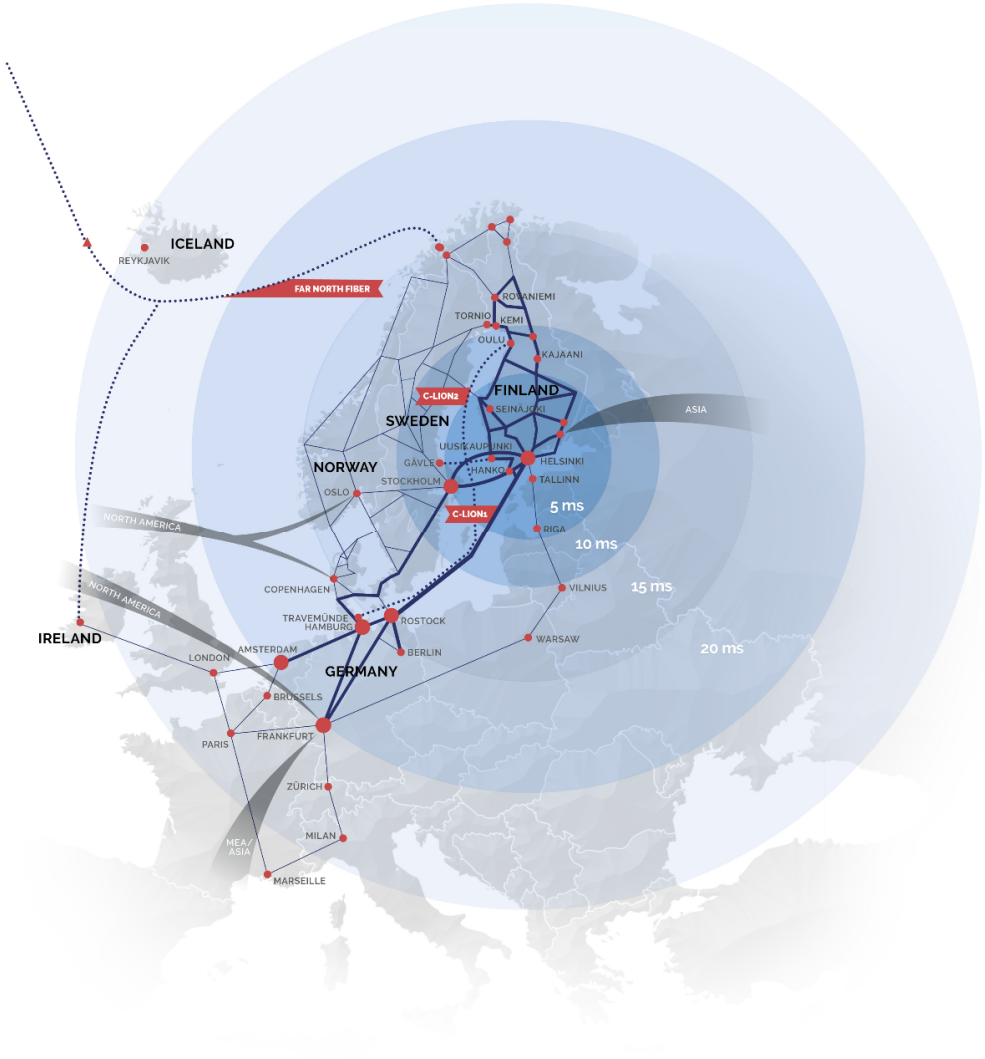
According to data provided by the Finnish National Bureau of Investigation, the damage to the pipeline was probably caused by the Chinese shipping company's Newnew Polar Bear, which continued its journey to Russian waters escorted by a Eurasian state icebreaker (Police of Finland, 2023a). In addition, the Sevmorput, a Russian nuclear-powered cargo ship, was also detected in the area during the incident (Police of Finland, 2023b).

Russia's alleged involvement in this attack could be aimed at destabilising the energy supply of these countries, which were heavily dependent on Russian gas until it was banned as a response to the invasion of Ukraine (Lietuvos Respublikos Energetikos Ministerija, 2022) (Latvijas Vēstnesis, 2022) (Republic of Estonia Ministry of Foreign Affairs, 2022) (Ministry of Economic Affairs and Employment of Finland, 2024). Already in 2014, in the Baltic States' attempts to expedite their disconnection from Russian supply through the synchronisation of their electricity grids with the support of the European Union (EU), Lithuania reported cases of interference by Russian military vessels in the installation of NordBalt, an undersea power cable connecting the country to Sweden (McNamara, 2024).

In November 2024, the submarine cable C-Lion1 , owned by the Finnish company Cinia, was apparently deliberately damaged. As this cable is essential for direct communication between Finland and Germany (see Figure 6), the damage resulted in the disruption of telecommunications between the two states. Such was the seriousness of the matter that the foreign ministers of these countries stated in a joint declaration that suspicions of an intentional attack were high, noting that "European security is not only threatened by Russia's war of aggression against Ukraine, but also by the hybrid warfare of malicious actors" and urging the strengthening of the defence of this type of infrastructure in the region (Ministry for Foreign Affairs of Finland, 2024).

Figure 6

Map of connectivity between the Nordic States and Central Europe via the C-Lion1 and C-Lion2 submarine cables.



Source: Cinia (n.d.)

Simultaneously, the BCS East-West Interlink telecommunications cable connecting Lithuania and Sweden was damaged as a result of "more than just an accident", as Andrius Šemeškevičius, Chief Technology Officer of the Telia Lietuva company, told Lithuanian national broadcaster LRT TV (2024).

The investigations undertaken by the countries concerned by both incidents focused on the Chinese vessel Yi Peng 3, which had previously departed from the Russian port of Ust-Luga. Unable to board the vessel, Danish naval forces kept a close eye on its situation once it entered the Kattegat Strait, as confirmed on their social media (Forsvaret, 2024). Based on Šemeškevičius' statements to LRT TV (2024), the likelihood of sabotage is quite high as the cables from both incidents intersect (see Figure 7).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

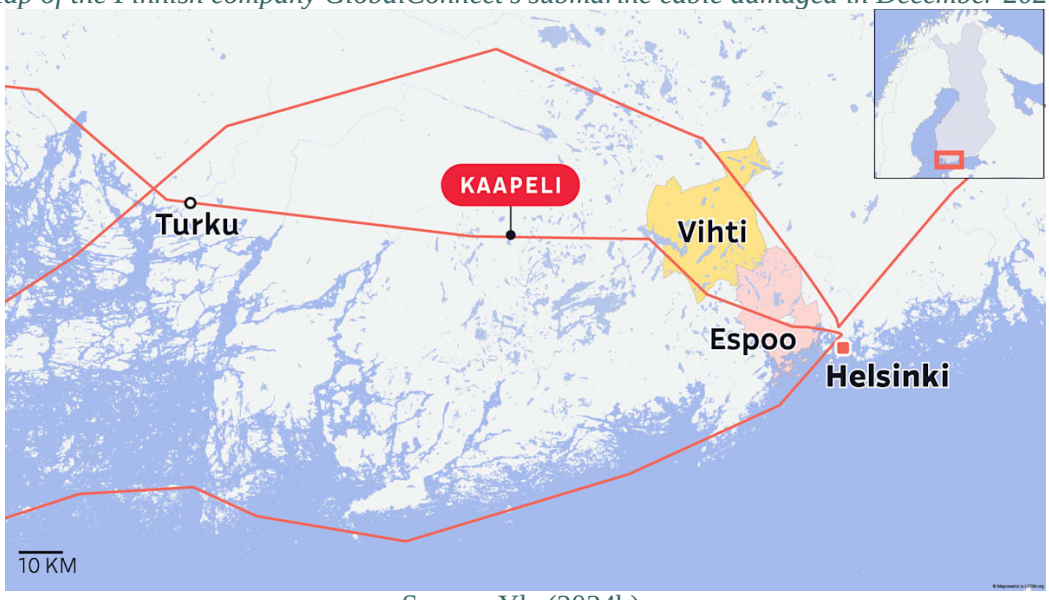
Figure 7
Map of damaged submarine cables in the Baltic Sea in November 2024 and the location of the vessel Yi Peng 3.

Source: Reuters (2024).

A month later, on 3 December 2024, the Finnish company GlobalConnect reported that its telecommunications cables connecting the country to Sweden had been damaged at two separate points between the Vithi and Espoo areas (see Figure 8), as confirmed by the company's communications manager, Niklas Ekström, to the Finnish public broadcaster Yle (2024a). However, the Finnish police said in a statement that there were no indications of sabotage, but rather an accident due to damage caused during excavations (Police of Finland, 2025a).

Figure 8

Map of the Finnish company GlobalConnect's submarine cable damaged in December 2024.

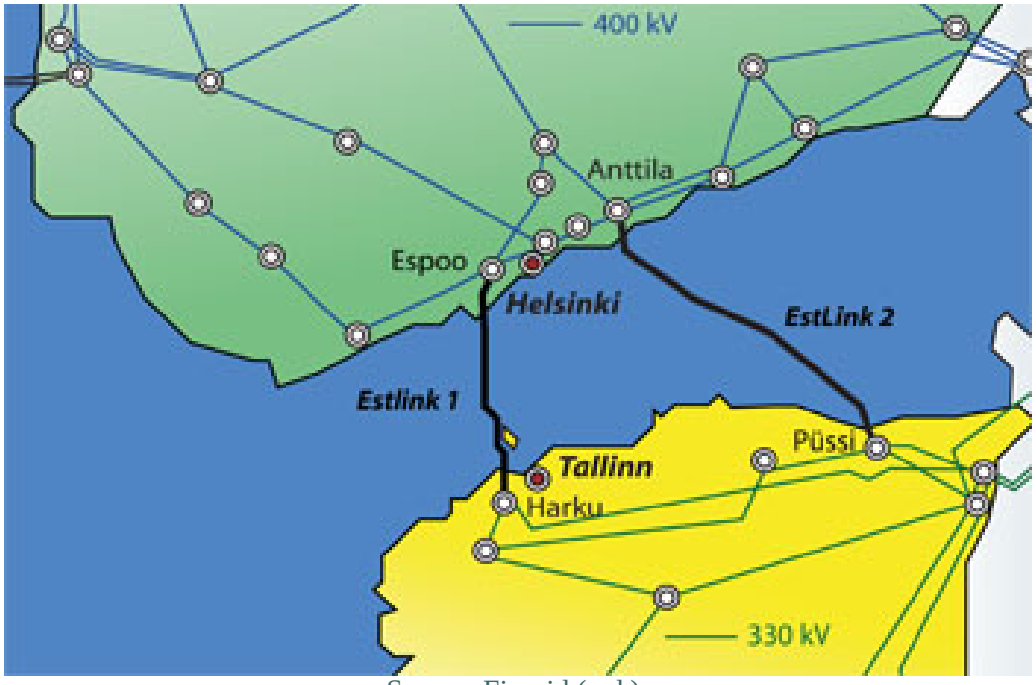


Source: Yle (2024b).

On 25 December 2024, the Finnish operator Fingrid reported that the Estlink 2 submarine cable of the electricity grid connecting Finland and Estonia was damaged (see Figure 9). Finland launched a sabotage investigation and seized the Russian "Ghost Fleet" tanker Eagle S, as it was in the area transporting Russian oil and apparently caused the damage by dragging its anchor (Police of Finland, 2025b). This event prompted NATO to announce in late December its intention to reinforce its military presence in the Baltic Sea to prevent future incidents and address possible new threats to this infrastructure (NATO, 2024a).

Figure 9

Map of connectivity between Finland and Estonia via the Estlink 1 and Estlink 2 submarine cables.



Source: Fingrid (n.d.).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

On 26 January 2025, damage was discovered to a communications cable between Sweden and Latvia (see Figure 10) as reported by the company responsible, Latvia State Radio and Television Center (2025). Although the Nordic country launched a preliminary investigation for sabotage and seized the Bulgarian cargo ship Vezhen, the Swedish prosecutor's office eventually determined that the cable break between the two countries was not the result of a deliberate attack but an accident (Swedish Prosecution Authority, 2025). Similarly, at the request of the Latvian authorities, Norway seized the Russian-crewed Silver Dania, which was sailing between St. Petersburg and Murmansk (Politiet, 2025).

Figure 10

Map of the submarine cable in the Baltic Sea connecting Latvia and Sweden damaged in January 2025.

Source: Reuters (2025).

In February 2025 another submarine cable connecting Finland and Germany was damaged in the Swedish EEZ, specifically near the Swedish island of Gotland. While Finland has already launched an investigation into the damage to the cable belonging to one of its companies (Police of Finland, 2025c), there is talk from Sweden of possible sabotage. Patrik Johansson, head of the Water and Sanitation Department in the affected region of Gotland, confirmed after the first inspection of the site that the main cause was human influence (Region Gotland, 2025).

Simultaneously, the Finnish company Cinia (2025) again reported disturbances in the operation of the C-Lion1 submarine cable. Although the investigation is still ongoing, the German media Kieler Nachrichten (2025) reported that the German authorities investigated the freighter Arne, a ship suspected of being part of the "Russian Ghost

Fleet", which was sailing in the area under the flag of Antigua and Barbuda and was heading from St. Petersburg to Seville without one of its anchors, raising suspicions of apparent Kremlin-orchestrated sabotage.

These incidents demonstrate that critical undersea infrastructure in the area is vulnerable to attack. Already in 2017, NATO Submarine Force Commander Andrew Lennon confirmed the existence of "Russian submarine activity in the vicinity of undersea cables" at previously unknown levels, highlighting Russia's strategic interest in NATO's undersea infrastructure (Birnbaum, 2017). As Monaghan et al. (2023, p. 1) note, these potential attacks are 'aimed at disrupting transatlantic cohesion and economic activity, undermining Western support for Ukraine, and shaping possible future military operations'. The situation since the outbreak of the war has therefore made security in this area a priority for NATO.

3. NATO AND THE PROTECTION OF CRITICAL UNDERSEA INFRASTRUCTURES

At a general level, the protection of critical undersea infrastructure for NATO is framed in several articles of its founding treaty. Specifically, article 2 on economic collaboration, article 3 on resilience and article 5 on collective defence from the North Atlantic Treaty (1949). With regard to the latter, NATO's New Strategic Concept (2022) mentions hybrid threats to critical infrastructure, reaffirming their inclusion in the framework of the aforementioned article and highlighting the commitment to international cooperation for their protection.

The growing concern for the protection of these infrastructures has made their security a particularly important objective for NATO. Given their importance for the functioning of society, threats such as the control acquired by Chinese companies over some of these infrastructures and the growing Russian activity near them made the Atlantic Alliance consider the state of its critical infrastructure in 2020 (García Pérez, 2023, p. 3).

Regarding the latter, then NATO Secretary General Jens Stoltenberg (2020) highlighted the importance of critical undersea infrastructure in the Alliance's efforts to strengthen its resilience:

> I think it's important to address this, because it is important to understand that most of these cables are privately owned and it's publicly known where they are. And that makes them potentially vulnerable. So we need to monitor the potential vulnerabilities. That's partly the reason why we have produced this report. We have tools to protect them and to monitor threats. And we have also established a new Atlantic Command in Norfolk, a new NATO command in Norfolk. And one of the tasks of this new North Atlantic Command is also to look into how to protect, how to monitor threats against undersea infrastructure. For instance, the internet is dependent on these cables and that just highlights the importance of the undersea cables. One of the main issues at the meeting today was resilience, and that's about civilian infrastructure, health services, telecommunications. But, of course, as part of our effort to strengthen the resilience, undersea cables, undersea infrastructure is an important part of that.

However, the main measures to protect these infrastructures were adopted after the start of the full-scale war in Ukraine in 2022. Until then, this issue was part of the work of limited institutions mostly linked to the maritime domain or to countering hybrid threats, two of which are particularly noteworthy.

On the one hand, the *Strengthened Resilience Commitment*, created in 2021 by a decision of NATO Heads of State and Government, which recognises the Alliance's commitment to intensify efforts to ensure the resilience of its critical infrastructures (NATO, 2021). On the other hand, the *NATO Resilience Committee,* a body responsible for the political-strategic direction, guidance, planning and overall coordination of resilience activities in the Atlantic Alliance (NATO, 2022) (see Table 1).

Table 1

NATO institutions in which critical infrastructure protection was framed ahead of Ukraine's full-scale war in 2022.

	Leading institutions
2006	*NATO Shipping Centre (NSC)*
2007	*Civil-Military Cooperation Centre of Excellence (CCOE)*
2008	*Cooperative Cyber Defence Centre of Excellence (CCD COE)*
2012	*NATO Allied Maritime Command (MARCOM)*
	Multinational Maritime Security Centre of Excellence (MARSEC COE)
2014	*Strategic Communications Centre of Excellence*
2018	*Counter Hybrid Support Teams*
2021	*Strengthened Resilience Commitment*
2022	*NATO Resilience Committee*

Source: Own elaboration based on information provided by NATO on its websites.

In response to the apparent sabotage of Nord Stream in late 2022, NATO established the *Critical Undersea Infrastructure Coordination Cell* (NATO, 2023a) in February 2023. A month before the adoption of this measure, on 11 January 2023, the creation of a NATO-EU working group on critical infrastructure resilience was announced in the framework of the existing NATO-EU Structured Dialogue on Resilience, within which it is embedded (European Commission & NATO, 2023, p. 2).

In their report published in June 2023, both sides point to the existence of a variety of threats to be faced, ranging from possible terrorist attacks to natural disasters. However, they directly point out that since the Russian aggression in Ukraine, these infrastructures have become a vulnerable asset whose protection must be a priority (European Commission & NATO, 2023, p. 4).

Another example of the effects of the Nord Stream incident as a turning point for strengthening Western efforts on the resilience of its critical undersea infrastructure is the creation of the *NATO Maritime Centre for the Security of Critical Undersea Infrastructure* (NMCSCUI) at the Vilnius Summit in 2023:

> The threat to critical undersea infrastructure is real and it is developing. We are committed to identifying and mitigating strategic vulnerabilities and

> dependencies with respect to our critical infrastructure, and to prepare for, deter and defend against the coercive use of energy and other hybrid tactics by state and non-state actors. Any deliberate attack against Allies' critical infrastructure will be met with a united and determined response; this applies also to critical undersea infrastructure. The protection of critical undersea infrastructure on Allies' territory remains a national responsibility, as well as a collective commitment. NATO stands ready to support Allies if and when requested. We have agreed to establish NATO's Maritime Centre for the Security of Critical Undersea Infrastructure within NATO's Maritime Command (MARCOM). We also agreed to set up a network that brings together NATO, Allies, private sector, and other relevant actors to improve information sharing and exchange best practice (NATO, 2023b).

In line with Stoltenberg (2020) and the joint report of the European Commission and NATO (2023, p. 3), the Vilnius Summit Communiqué reaffirms the Alliance's growing concern about threats to critical undersea infrastructure. In this extract, NATO recognises the need to proactively identify vulnerabilities, underlines that such threats can emanate from both state and non-state actors and stresses the importance of effective coordination with relevant actors, especially from the private sector. It also explicitly contemplates the possibility that hybrid attacks against these infrastructures could be considered as acts justifying the activation of Article 5 of the North Atlantic Treaty's collective defence.

The NMCSCUI was therefore inaugurated in May 2024. NATO defines it as a network and knowledge centre specialising in critical undersea infrastructure, whose main function is to support strategic decision-making processes, facilitate the operational deployment of forces and coordinate joint actions to ensure their protection. This is done through the integration of efforts between member states, strategic partners and the private sector (NATO Media Centre, 2024).

However, this is not the only measure resulting from the Vilnius Summit implemented by NATO to ensure that threats in the maritime domain are better addressed. In October 2023, the *Digital Ocean Vision*, an initiative aimed at improving maritime domain understanding by further harmonising national and allied maritime surveillance capabilities using a diverse range of assets, was adopted (NATO, 2023c).

Moreover, in view of the growing challenges to these infrastructures, on 23 May 2024 NATO held the first meeting of the Critical Undersea Infrastructure Network by decision of the defence ministers with the aim of improving coordination and information exchange. The meeting discussed measures such as strengthening naval patrols, promoting technological innovation and the use of advanced detection and response capabilities, consolidating the Alliance's central role in this area (NATO, 2024b).

In November 2024, Exercise *Bold Machina 24* was conducted in La Spezia, Italy, coordinated by the *Allied Special Operations Forces Command* (SOFCOM) and the *Centre for Maritime Research and Experimentation* (CMRE) with the aim of testing underwater sensors for critical infrastructure protection (NATO Centre for Maritime Research and Experimentation, 2024, p. 2). Such exercises reflect the aforementioned interest in integrating emerging technologies, such as unmanned systems, to enhance security in the undersea domain (Conte de los Ríos, 2025, p. 26).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

In this regard, it is also noteworthy that NATO has developed new tools that enable allies to detect suspicious activity in order to protect against sabotage. These include the use of artificial intelligence as exemplified by *Mainsail*, a software tool developed by CEMR that detects vessels behaving suspiciously with the intention of gathering information about and damaging undersea infrastructure (NATO Multimedia, 2025).

With regard to the specific protection of the Baltic Sea's undersea infrastructure, NATO has promoted the technological innovation necessary for effective detection of any suspicious activity to complement the work of its patrols in the region. These measures have been progressively intensified as a direct consequence of the apparent sabotage of Nord Stream, as the Alliance itself acknowledges (NATO, 2023d).

In February 2025, NATO conducted a demonstration of unmanned surface vehicles (USVs) in the Baltic Sea in order to advance their operational integration in maritime surveillance tasks. This initiative is part of the Alliance's efforts to incorporate emerging and disruptive technologies - such as autonomous systems and artificial intelligence - aimed at optimising situational awareness and strengthening the protection of critical undersea infrastructure, in particular along sea lines of communication (NATO Allied Maritime Command, 2025b). Furthermore, in the framework of the Resilience Committee, NATO presented its first *Resilience Reference Curriculum* in 2025 with the aim of strengthening allied capabilities against threats, including those targeting critical infrastructure (NATO, 2025a).

At the same time, cooperation with the European Union has gained importance through initiatives such as the *EU Hybrid Toolbox*, the *Hybrid Fusion Cell* and the *Hybrid Rapid Response Teams*, designed to promote synergies and strengthen anti-hybrid coordination with NATO (European External Action Service, 2022, p. 34). This convergence of initiatives between the above-mentioned entities demonstrates the importance of developing robust defensive capabilities, and their coordinated implementation together with the effective integration of new technologies and operational capabilities is essential to ensure the successful protection of European submarine infrastructures, especially in view of the rapidly evolving threats affecting this area (Conte de los Ríos, 2025, p. 33).

Finally, it should be noted that NATO considers strengthening cooperation with the private sector as a key dimension of improving its ability to respond to threats to critical undersea infrastructures. This cooperation is justified, on the one hand, by the fact that a significant proportion of such infrastructure is privately owned or operated, and on the other hand, by the potential of the private sector to provide essential technological solutions in an increasingly complex operating environment (Fridbertsson, 2023, p. 11).

4. OPERATION BALTIC SENTRY

On 14 January 2025, NATO held a Baltic Sea Allies Summit to address the growing threats to the region's critical undersea infrastructure. As a result, the Atlantic Alliance Secretary General and participants issued the *Joint Statement of the Baltic Sea NATO Allies Summit* (2025) announcing the launch of a military initiative aimed at strengthening the protection of this infrastructure: Operation *Baltic Sentry.*

Citing deep concern over the increase in actions that threaten the operation of critical undersea infrastructure, the Alliance signalled its readiness to "deter, detect and counter any attempted sabotage" and to respond to any attack "with a firm and decisive response" (Tasavallan Presidentti, 2025). This comes at a time when NATO recognises the need to modernise its capabilities to strengthen its deterrence and defence in order to address and counter evolving security threats (Tasavallan Presidentti, 2025).

MARCOM, under the direction of the *Joint Forces Command* Brunssum (JFCBS), is recognised as playing a key role in coordinating operations within what it defines as a "multi-domain surveillance activity aimed at increasing maritime situational awareness in the Baltic Sea to deter and defend against attacks on critical undersea infrastructure" (NATO Allied Maritime Command, 2025a). To that end, Operation *Baltic Sentry* includes the deployment of additional sea, air and land assets by allies to enhance surveillance and deterrence.

By conducting regular patrols and joint exercises, NATO seeks to maintain a constant presence in the Baltic Sea that is continuously monitored by warships, submarines, aircraft and the support of advanced maritime surveillance technology. For example, ships from *Standing NATO Maritime Group 1* (SNMG1) and *Standing NATO Mine Countermeasures Group 1* (SNMCMG1) will participate in *Baltic Sentry* alongside other allied maritime patrol vessels, while NATO will continue to invest in cutting-edge military technology to detect and minimise threats such as artificial intelligence, advanced sensors and specialised sonar systems (MARCOM, 2025).

This is in addition to the inclusion of two key actors within the Alliance. On the one hand, the recently inaugurated *Commander Task Force* (CTF) in the Baltic Sea itself, based in the port city of Rostock. In addition to coordinating allied ships in the Baltic, the CTF works to build a unified regional vision for critical infrastructure in the Baltic Sea in order to support NATO's strategic protection efforts (Tasavallan Presidentti, 2025). On the other, the aforementioned NMCSCUI will focus its efforts on protecting and securing vital submarine assets (Tasavallan Presidentti, 2025).

To achieve these goals, NATO considers it essential not only to work within the Alliance itself, but also to collaborate and cooperate with other actors ranging from the EU to the private sector. While in the former case cooperation will focus on strengthening existing mechanisms, in the case of the private sector NATO stresses the importance of cooperating with infrastructure operators and cutting-edge technology companies in developing the different response measures needed to increase resilience (Tasavallan Presidentti, 2025).

The Atlantic Alliance also envisages the adoption of new measures in accordance with international law, aimed at both prevention and response to threats or irresponsible acts against critical undersea infrastructures in the region (Tasavallan Presidentti, 2025). In the framework of the launch of Operation *Baltic Sentry*, the current NATO Secretary General Mark Rutte underlined the need for strict enforcement of the existing legal framework, warning that any potential threat against these infrastructures could lead to coercive measures such as boarding, seizure or detention of vessels. In this context, he pointed to Finland's response to incidents as an outstanding example of action (NATO, 2025b).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

The implementation of these measures is justified by the constant mention of the existence of threats. With regard to the latter, one threat in particular is mentioned, the so-called "Russian Ghost Fleet". This is defined as a significant threat to maritime and environmental security both in the Baltic Sea region and globally, as it compromises the integrity of underwater infrastructure, increases the risks associated with chemical munitions dumped on the seabed and represents a major source of funding for Russia's illegal war of aggression against Ukraine (Tasavallan Presidentti, 2025).

Similarly, it is recognised that the threat to critical undersea infrastructures is not limited to the Baltic Sea. It therefore points out that Operation *Baltic Sentry* also represents a turning point in favour of greater cooperation to strengthen the resilience of these critical infrastructures and, therefore, to strengthen NATO's security. Hence, the launch of the operation itself goes hand in hand with the announcement of the renewal of the alliance's maritime strategy (Tasavallan Presidentti, 2025).

5. CONCLUSIONS AND PROPOSALS

Critical undersea infrastructures are vital for the economy and the global communications system. Their growing importance and the constant technological advances in this area have made them a priority target for defence, but also for possible attacks. In this way, *Seabed Warfare* is no longer a distant concept, but an immediate threat to the Allies. The close link between the security of these infrastructures and global stability, particularly in economic and communications terms, means that protecting them and managing their vulnerabilities is now a defence priority for all international actors.

Given the current context of rivalry with a Russia that publicly announces its desire to destabilise NATO, this makes the implementation of critical infrastructure protection strategies an extremely urgent objective for the defence of the Atlantic Alliance, especially in the Baltic region. As mentioned in the paper, the Baltic Sea is not only an enclave of geopolitical competition between NATO and Russia, but also a key area for the security of critical undersea infrastructures that guarantee the stability of the Allies. Joining forces in this region to strengthen its security must therefore be a priority for NATO, especially since the 2022 war in Ukraine and the accession of Sweden and Finland to the Alliance.

This allows us to draw the main conclusion linked to specific objective number one of this study. While the protection of these infrastructures should already be an objective for NATO given their importance for the resilience of society and their extreme vulnerability to a wide range of threats, the current geopolitical situation makes these infrastructures a clear target for possible attacks. This is demonstrated by the increase in incidents involving submarine cables in the Baltic Sea since the start of the conflict in 2022, with eight incidents to date in which critical infrastructures in the region have been damaged, practically all of them occurring within the EEZ of Finland and Sweden, countries that coincidentally applied to join NATO that same year despite fierce opposition from the Kremlin (see Table 2).

Table 2

Incidents in the critical underwater infrastructure in the Baltic Sea since 2022.

	Infrastructure	**Location of the incident**	**Countries affected**	**Causes**
Nord Stream	Subsea pipeline	Swedish and Danish EEZs	European Union	High indications of sabotage
Balticconnector	Subsea pipeline	Finnish EEZ	Finland and Estonia	High indications of sabotage
C-Lion 1	Telecommunications cable	Swedish EEZ	Finland and Germany	High indications of sabotage
BCS East-West Interlink	Telecommunications Cable	Swedish EEZ	Lithuania and Sweden	High indications of sabotage
GlobalConnect	Telecommunication cables	Finnish EEZ	Finland and Sweden	Accident
Estlink 2	Electricity grid	Swedish EEZ	Finland and Estonia	High indications of sabotage
Latvia State Radio and Television Center	Telecommunications cable	Swedish EEZ	Sweden and Latvia	Accident
Gotland	Maritime cable owned by a Finnish company	Swedish EEZ	Finland and Germany	High indications of sabotage

Source: Own elaboration

With regard to the second specific objective of this study on NATO's overall framework for action in protecting critical undersea infrastructure, several conclusions can be drawn. Despite the Russian military's attrition in its performance in the Ukrainian war and the severe setbacks suffered in the naval domain, Russian hybrid tactics remain the most pressing threat to European infrastructure in the Baltic Sea. NATO is positioning itself as a central actor in preventing attacks against such infrastructure, stepping up its efforts with progressive measures from 2022 onwards following the invasion of Ukraine and subsequent incidents.

While this issue was part of the work of mostly maritime-related institutions, since the apparent sabotage of Nord Stream - in the midst of tensions with Moscow - NATO has adopted almost a dozen measures. These include the creation of the *Critical Undersea Infrastructure Coordination Cell* or the *NATO Maritime Centre for the Security of Critical Undersea Infrastructure*, the *Digital Ocean Vision* initiative, military exercises such as *Bold Machina 24*, the technological innovation necessary to take advantage of artificial intelligence such as *Mainsail*, and the adoption of complementary initiatives with third actors such as the EU.

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Operation *Baltic Sentry* is NATO's main response to the challenge of protecting critical undersea infrastructure in the Baltic Sea and strengthening security in the region. In keeping with the main objective of the study focused on analysing this operation, it can be observed that the measures implemented within its framework are geared towards strengthening detection, deterrence-prevention, adaptation and response capabilities, thus being in line with the main criteria proposed by the specialised literature for adopting an effective strategy (see Table 3).

Table 3

Implementation of the necessary elements for an effective strategy for the protection of critical undersea infrastructure in the framework of NATO's Operation Baltic Sentry.

	NATO Operation Baltic Sentry
Increased presence or surveillance	✓
Collaboration with international actors	✓
Coordination with the private sector	✓
Use of advanced technology	✓
Development of regulatory frameworks	✓
Renewal of the maritime strategy	✓
Implementation of response measures	✓

Source: Own elaboration based on Conte de los Ríos (2025), Monaghan et al. (2023), Fridbertsson (2023) and information provided by NATO.

In short, Operation *Baltic Sentry* demonstrates that critical undersea infrastructures are currently identified by NATO as a strategic vulnerability whose protection is essential to ensure the resilience and security not only of the Alliance, but also for the day-to-day life of society. A lesson that finds a turning point in the different episodes that have occurred in the framework of the war in Ukraine since 2022, with the apparent attack on Nord Stream at the end of the same year being noteworthy, as shown both by the chronological framework of the measures adopted by NATO in this sector and by the Alliance itself when justifying the latter.

Thus, answering the overall research question, the general hypothesis of the study is that Operation *Baltic Sentry* enhances the protection of critical undersea infrastructure in the Baltic Sea and the Alliance's presence in the Baltic Sea, thus adjusting to the new threat context.

BIBLIOGRAPHICAL REFERENCES

Arjona Hernández, N. (2023). The protection of submarine telecommunications cables: Digital sovereignties and submarine cable network security. *International Journal Of Policy Thinking*, *18*(18), pp. 41-67. https://doi.org/10.46661/revintpensampolit.8753

Baltic Marine Environment Protection Commission (2024). *HELCOM Map and Data Service*. https://maps.helcom.fi/website/mapservice/

Baltic Marine Environment Protection Commission (2024). *HELCOM Map and Data Service*. https://maps.helcom.fi/website/mapservice/

Birnbaum, M. (22 December 2017). Russian submarines are prowling around vital undersea cables. It's making NATO nervous. *The Washington Post.* https://www.*washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html?hpid=hp_hp-top-table-main_russiasubs712pm%3Ahomepage%2Fstory*

Bueger, C., Liebetrau, T., and Franken, J. (2022). *Security Threats to Undersea Communications Cables and Infrastructure - Consequences for the EU*. European Parliament In-Depth Analysis, https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

Bueger, C., and Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, *42*(3), pp. 391-413. https://doi.org/10.1080/13523260.2021.1907129

Cassetta, M. (2024). How to Respond to the Emerging Threats to Critical Underwater Infrastructure at the Time of Russia's War Against Ukraine. *Istituto Affari Internazionali (IAI), IAI Commentaries 24-31 June 2024*, pp. 1-5. https://www.iai.it/en/pubblicazioni/c05/how-respond-emerging-threats-critical-underwater-infrastructure

Childs, N. (2025). Russia's 'Shadow Fleet' and Sanctions Evasion: What Is To Be Done? *The International Institute for Strategic Studies (IISS), January 2025*, pp. 1-15. https://www.iiss.org/globalassets/media-library---content--

migration/files/research-papers/2025/01/russias_shadow-fleet_and-sanctions-evasion/iiss_russias_shadow-fleet_and-sanctions-evasion_31012025.pdf

Cinia (20 February 2025). *Disturbance in Cinia's C-Lion Submarine Cable.* https://www.cinia.fi/en/news/disturbance-in-cinia-c-lion-submarine-cable

Cinia (n.d.). *International connectivity by Cinia.* https://www.cinia.fi/hubfs/Cinia%20Theme%202024/Muut%20kuvat/Cinian-kansainvaliset-verkkoyhteydet-kartta.jpg

Clark, B. (2015). *The Emerging Era in Undersea Warfare*. Center for Strategic and Bidgetary Assessments (CSBA), https://csbaonline.org/research/publications/undersea-warfare

Conte de los Ríos, A. (2025). Security threats: seabed and critical infrastructure. *Global Affairs Journal*, (7), pp. 26-35. https://www.unav.edu/documents/16800098/147587031/amenazas-seguridad.pdf

Deni, J. R. (18 December 2023). *Is the Baltic Sea a NATO Lake?* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/12/is-the-baltic-sea-a-nato-lake?lang=en

Energistyrelsen (26 September 2022). *Leak at North Stream 2 in the Baltic Sea.* https://ens.dk/en/press/leak-north-stream-2-baltic-sea

European Commission & NATO . (2023). *EU-NATO TASK OF FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE. FINAL ASSESMENT REPORT.* https://www.nato.int/cps/en/natohq/news_216631.htm

European External Action Service (2022). *A STRATEGIC COMPASS FOR SECURITY AND DEFENCE: For a European Union that protects its citizens, values and interests and contributes to international peace and security.* https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

Fingrid (n.d.). *EstLink 2 - second high-voltage direct current link between Finland and Estonia.* https://www.fingrid.fi/en/grid/construction/arkisto/estlink-2/

Fink, A. and Kofman, M. (2020). Russian Strategy for Escalation Management: Key Debates and Players in Military Thought. *CNA Information Memorandum, April 2020*, pp. 1-48. https://www.cna.org/cna_files/pdf/DIM-2020-U-026101-Final.pdf

Foggo, J. (17 January 2023). The Fourth Battle of the Atlantic Is Underway. *Center for European Policy Analysis (CEPA)*, https://cepa.org/article/the-fourth-battle-of-the-atlantic-is-underway/

Foggo, J. and Fritz, A. (2016). The Fourth Battle of the Atlantic. *U.S. Naval Institute, 142*(6), https://www.usni.org/magazines/proceedings/2016/june/fourth-battle-atlantic

Forsvaret. [@forsvaretdk] (20 November 2024). *Regarding the Chinese ship Yi Peng 3: The Danish Defence can confirm that we are present in the area near the Chinese ship Yi Peng 3. The Danish Defence currently has no further comments.* [Post in X]. X. https://x.com/forsvaretdk/status/1859195509866381402

Fridbertsson, N. T. (2023). *Protecting Critical Maritime Infrastructure - The Role of Technology*. General Report. 032 STC 23 E. NATO Parliamentary Assembly: Science and Technology Committee (STC). https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc

García Pérez, R. (2023). Spain in the global network of submarine cables. *Instituto Español de Estudios Estratégicos, IEEE Framework Document 10/2023*, pp. 1-51. https://www.defensa.gob.es/ceseden/-/espa%C3%B1a-en-la-red-global-de-cables-submarinos

García Pérez, R. (2024). "La seguridad de los cables submarinos", in Fernándo Ibáñez Gómez (Coord.), *Seguridad marítima. Una incertidumbre permanente*, Bosch Editor, Barcelona, pp. 265-298.

Gasgrid (n.d.). *Map of Finnish and Baltic gas transmissions.* https://gasgrid.fi/wp-content/uploads/Gasgrid_maakaasu_lisaversiot_eu_EN-scaled.jpg

Gasum (2023). *Gasum has terminated its pipeline natural gas supply contract with Gazprom Export. https://www.gasum.com/en/news-and-customer-stories/news-and-press-releases/2023/gasum-has-terminated-its-pipeline-natural-gas-supply-contract-with-gazprom-*

export/#:~:text=The%20parties%20were%20not%20able,details%20of%20the%20contract%20termination.

Gresh, G. F. (2023). *Europe's new maritime security reality: Chinese ports, Russian bases, and the rise of subsea warfare.* Foreign Policy at Brookings, Policy Brief, February 2023. https://www.brookings.edu/articles/europes-new-maritime-security-reality-chinese-ports-russian-bases-and-the-rise-of-subsea-warfare/

Guilfoyle, D., Paige, T. P., and McLaughlin, R. (2022). THE FINAL FRONTIER OF CYBERSPACE: THE SEABED BEYOND NATIONAL JURISDICTION AND THE PROTECTION OF SUBMARINE CABLES. *International and Comparative Law Quarterly*, *71*(3), pp. 657-696. https://doi.org/10.1017/S0020589322000227

Insikt Group (2023). *The Escalating Global Risk Environment for Submarine Cables.* Recorded Future Threat Analysis, https://www.recordedfuture.com/research/escalating-global-risk-environment-submarine-cables

International Cable Protection Committee (2024). *Report of the International Cable Protection Committee Docs: HSSC16-07.10A: ICPC activities affecting HSSC.* International Hydrographic Organization, Tokyo, Japan, 27-31 May 2024. https://iho.int/uploads/user/Services%20and%20Standards/HSSC/HSSC16/HSSC16_2024_07.10A_EN_ICPC%20activities%20affecting%20HSSC.pdf

Jones, S. G. (2025). Russia's Shadow War Against the West. *Center for Strategic and International Studies (CSIS), CSIS Briefs March 2025*, pp. 1-20. https://www.csis.org/analysis/russias-shadow-war-against-west

Kaushal, S. (25 May 2023). *Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure*. Royal United Services Institute (RUSI), May 2023. https://www.rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure

Kieler Nachrichten (2025). *Verdacht der Sabotage: Ermittler suchen Anker vom russischen Frachter "Arne"* [Suspicion of *sabotage*: Investigators *search for* the anchor of the Russian freighter "Arne"]. https://www.kn-online.de/schleswig-holstein/verdacht-der-sabotage-gegen-russischen-frachter-arne-in-kiel-ermittlungsstand-ORSQRUDZZRGJHC7KSCB4SKJCDM.html

Latvia State Radio and Television Center (2025). *LVRTC Submarine Optical Fiber Cable Damaged.* https://www.lvrtc.lv/en/news/jaunumi/lvrtc-submarine-optical-fiber-cable-damaged/

Latvijas Vēstnesis (28 July 2022). *Grozījumi Enerģētikas likumā* [Energy Law Amendments]. https://www.vestnesis.lv/op/2022/144.5

Lietuvos Respublikos Energetikos Ministerija (20 May 2022). *No more Russian oil, gas and electricity imports in Lithuania from Sunday.* https://enmin.lrv.lt/en/news/no-more-russian-oil-gas-and-electricity-imports-in-lithuania-from-sunday/

LRT TV (18 November 2024). *Undersea cable between Lithuania and Sweden damaged - Telia.* https://www.*lrt.lt/en/news-in-english/19/2416006/undersea-cable-between-lithuania-and-sweden-damaged-telia?srsltid=AfmBOoowPquC_SbY0w-dUT2dfxJTzPrj-OPvif6IxXoDTJQuKnQx11fF*

McNamara, E. M. (17 March 2016). *Securing the Nordic-Baltic region*. NATO Review. https://www.nato.int/docu/review/articles/2016/03/17/securing-the-nordic-baltic-region/index.html

McNamara, E. M. (28 August 2024). Strengthening resilience: NATO's role in enhancing the security of critical undersea infrastructures. *NATO Review: Opinion, Analysis and debate on Security Issues*, https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/index.html

Ministry for Foreign Affairs of Finland (18 November 2024*). Joint statement by the Foreign Ministers of Finland and Germany on the severed undersea cable in the Baltic Sea.* https://um.fi/statements/-/asset_publisher/6zHpMjnolHgl/content/joint-statement-by-the-foreign-ministers-of-finland-and-germany-on-the-severed-undersea-cable-in-the-baltic-sea/35732

Ministry of Economic Affairs and Employment of Finland (7 May 2024). *Hallituksen esitys laiksi laiksi maakaasun ja nesteytetyn maakaasun maahantuonnin väliaikaisesta kieltämisestä Venäjän federaatiosta ja Valko-Venäjältä* [The government's proposal for a law on the temporary ban on the import of natural gas and liquefied natural gas from the Russian Federation and Belarus]. https://tem.fi/en/project?tunnus=TEM036:00/2024

Monaghan, S. (6 October 2022). Five Steps NATO Should Take after the Nord Stream Pipeline Attack. *Center for Strategic and International Studies (CSIS),* https://www.csis.org/analysis/five-steps-nato-should-take-after-nord-stream-pipeline-attack

NATO Allied Maritime Command (2025a, 14 January 2025). *NATO's Baltic Sentry steps up patrols in the Baltic Sea to safeguard Critical Undersea Infrastructure*. https://mc.nato.int/media-centre/news/2025/nato-baltic-sentry-steps-up-patrols-in-the-baltic-sea-to-safeguard-critical-undersea-infrastructure

NATO Allied Maritime Command (2025b, 20 February 2025). *NATO Conducts Unmanned Surface Vehicle Demonstration in Baltic Sea.* https://mc.nato.int/media-centre/news/2025/page228602539

NATO Centre for Maritime Research and Experimentation (2024). *NATO STO CMRE NEWSLETTER.* January-June 2024. https://www.cmre.nato.int/wp-content/uploads/2024/09/v2%20NATO%20STO%20CMRE%20Newsletter_1_20240712_114854_0000_EDITED_4PAGES%20(002).pdf

NATO Media Centre (2024, 28 May 2024). *NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure.* https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui

NATO Multimedia (06 February 2025). *Protecting undersea cables with artificial intelligence.* https://www.natomultimedia.tv/app/asset/718197

NATO (2021, 14 June 2021). *Strengthened Resilience Commitment.* https://www.nato.int/cps/en/natohq/official_texts_185340.htm

NATO (2022, 07 October 2022). *Resilience Committee*. https://www.nato.int/cps/in/natohq/topics_50093.htm

NATO (2023a, 15 February 2023). *NATO stands up undersea infrastructure coordination* cell. https://www.nato.int/cps/en/natohq/news_211919.htm

NATO (2023b, 11 July 2023). *Vilnius Summit Communiqué. Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023.* https://www.nato.int/cps/en/natohq/official_texts_217320.htm

NATO (2023c, 12 October 2023). *NATO Defence Ministers launch initiative to enhance maritime surveillance capabilities.* https://www.nato.int/cps/ra/natohq/news_219441.htm

NATO (2023d, 19 October 2023). *NATO steps up Baltic Sea patrols after subsea infrastructure damage.* https://www.nato.int/cps/en/natohq/news_219500.htm

NATO (2024a, 30 December 2024). *NATO to enhance military presence in the Baltic Sea.* https://www.nato.int/cps/en/natohq/news_231800.htm

NATO (2024b, 23 May 2024). *NATO holds first meeting of Critical Undersea Infrastructure Network.* https://www.nato.int/cps/en/natohq/news_225582.htm

NATO (2025a, 21 February 2025). *NATO launches the Resilience Reference Curriculum.* https://www.nato.int/cps/en/natohq/news_233458.htm

NATO (2025b, 14 January 2025). *NATO launches 'Baltic Sentry' to increase critical infrastructure security.* https://www.nato.int/cps/en/natohq/news_232122.htm

Police of Finland (2025b, 2 March 2025). *Eagle S tanker to move to international waters under Border Guard's control.* https://poliisi.fi/en/-/eagle-s-tanker-to-move-to-international-waters-under-border-guard-s-control

Police of Finland (2023a, 24 October 2023). *National Bureau of Investigation has technically clarified the cause of gas pipeline damage.* https://poliisi.fi/en/-/national-bureau-of-investigation-has-clarified-technically-the-cause-of-gas-pipeline-damage

Police of Finland (2023b, 17 October 2023). *National Bureau of Investigation examines background of vessels sailing in the gas pipeline damage area.* https://poliisi.fi/en/-/national-bureau-of-investigation-examines-background-of-vessels-sailing-in-the-gas-pipeline-damage-area

Police of Finland. (2025a, 3 December 2025). *Police do not suspect any criminal offence in either of the cable damage incidents in Southern Finland.* https://poliisi.fi/en/-/police-do-not-suspect-any-criminal-offence-in-either-of-the-cable-damage-incidents-in-southern-finland

Police of Finland (2025c, 21 February 2025). *National Bureau of Investigation to conduct a preliminary inquiry into suspected cable damage in Baltic Sea.*

https://poliisi.fi/en/-/national-bureau-of-investigation-to-conduct-a-preliminary-inquiry-into-suspected-cable-damage-in-baltic-sea

Politiet (31 January 2025). *Ship can leave Tromsø.* https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2025/01/31/troms2/

Quijarro Santibáñez, L. (2023). Seabed Warfare: Submarine Warfare in the 21st Century. *Revista de Marina, 141*(997), pp. *15-22*. https://revistamarina.*cl/revista/997*

Region Gotland (3 March 2025). *Misstänkt sabotage* [Suspected sabotage]. https://gotland.se/bygga-bo-och-miljo/vatten-och-avlopp/dricksvatten/misstankt-sabotage

Republic of Estonia Ministry of Foreign Affairs . (2022). *Estonia imposes a ban on natural gas imports and purchases from Russia.* https://www.vm.ee/en/news/estonia-imposes-ban-natural-gas-imports-and-purchases-russia

Reuters (2024). *Damaged fibre-optic cables in the Baltic Sea.* https://www.reuters.com/graphics/BALTICSEA-CABLES/zdpxqaaxwvx/chart.png

Reuters (2025). *Damaged fibre-optic cable in the Baltic Sea*. https://www.reuters.com/graphics/BALTIC-SECURITY/xmvjbdamavr/chart.png

Stoltenberg, J. (22 October 2020). *Online press conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defence Ministers.* https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en

Submarine Telecoms Forum (2025). *Global Outlook.* SubTel Forum Magazine #140. https://subtelforum.com/subtel-forum-magazine-140-global-outlook/

Swedish Prosecution Authority (2025). *Prosecutor revokes decision on seized ship.* https://www.aklagare.se/en/media/press-releases/2025/february/prosecutor-revokes-decision-on-seized-ship/?_t_id=ajCngOfkVK4qcLdxSmm4EA%3d%3d&_t_uuid=ajbjBKKES7uVHPgMJkVsvA&_t_q=baltic&_t_tags=language%3aen%2csiteid%3a764c28f6-3ce5-48e7-a8ec-b8f5f22e4245%2candquerymatch&_t_hit.id=Aklagare_Web_Business_PressRel

eases_Models_PressReleasePage/_847c0fdb-df1d-4d16-9b4a-0db494be3af4_en&_t_hit.pos=2

Tasavallan Presidentti (14 January 2025). *Joint Statement of the Baltic Sea NATO Allies Summit.* https://www.presidentti.fi/joint-statement-of-the-baltic-sea-nato-allies-summit/

The European Space Agency (06 October 2022). *Nordstream pipeline map with shipping traffic.* https://www.esa.int/ESA_Multimedia/Images/2022/10/Nordstream_pipeline_map_with_shipping_traffic

Yle (2024a, 31 December 2024). *Police: No crime suspected in Finland-Sweden cable break.* https://yle.fi/a/74-20128835

Yle. (2024b). *The cable was damaged in two separate places between Espoo and Vihti. Image: Laura Merikalla / Yle, Mapcreator, OpenStreetMap, GlobalConnect.* https://images.cdn.yle.fi/image/upload/c_crop,h_1080,w_1919,x_0,y_0/ar_1.7777777777777777,c_fill,g_faces,h_675,w_1200/dpr_2.0/q_auto:eco/f_auto/fl_lossy/v1733216443/39-1389673674ec7f18a492

REGULATION

United Nations Convention on the Law of the Sea, New York, 30 April 1982. https://www.un.org/depts/los/convention_agreements/texts/unclos/convemar_es.pdf

Convention for the Protection of Submarine Telegraph Cables, Paris, 14 March 1884. https://iscpc.org/information/Convention_on_Protection%20_of_Cables_1884.pdf

NATO's New Strategic Concept, Madrid, 29 June 2022. https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_otan.pdf

North Atlantic Treaty, Washington, 4 April 1949. https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Research Article

INTELLECTUAL CAPITAL IN THE INSTITUTION OF THE CIVIL GUARD AND ITS CONTRIBUTION TO THE SOCIAL ECONOMY

English translation with AI assistance (DeepL)

Virginia Belén Subiris Moriel
PhD student at the Universidad Rey Juan Carlos.
Social and Legal Sciences Programme. Business Branch
Master International Human Resources Management
(International Human Resources Management)
virbelsu@gmail.com
ORCID: Https://orcid.org/0009-0000-2569-3710

Received 31/03/2025
Accepted 10/06/2025
Published 27/06/2025

Recommended citation: Subiris, V. (2025). Intellectual capital in the institution of the Guardia Civil and its contribution to the social economy. *Revista Logos Guardia Civil*, 3(2), p.p. 257-292.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

ORCID: Https://orcid.org/0009-0000-2569-3710

INTELLECTUAL CAPITAL IN THE CIVIL GUARD AND ITS CONTRIBUTION TO THE SOCIAL ECONOMY

Abstract: Security is a key issue for cooperation between the countries that make up the European Union in the current socio-economic environment. This implies that public sector policies should not only strengthen defence capabilities, but also implement measures that contribute to economic and social security. Connecting these terms: security, cooperation, public and social economy, leads us to think of an institution that has aligned them in its strategy for more than 181 years of existence, the Civil Guard Institution. However, no research, articles or projects have been found that address this issue in the academic sphere. This study analyses how the intellectual capital (IC) of the institution contributes to generating socio-economic value through its solidarity and humanitarian actions. The methodology used is based on a content analysis of the information disclosed on its IC in its social responsibility and sustainability reports between 2014-2023. The Intellectus model adapted to the public context was used to identify and quantify intangible assets. The results show that the Institution's IC, through knowledge management, organisational culture, external relations, benevolent character and social commitment, provides tangible and intangible value that goes beyond its public safety functions. This research demonstrates the relevance of IC in public institutions and its potential in strengthening a social economy integrated in the 2030 Agenda.

Resumen: La seguridad es un tema clave para la cooperación entre los países que conforman la Unión Europea en el entorno socioeconómico actual. Esto implica que las políticas del sector público no sólo fortalezcan las capacidades en defensa, sino que también implementen medidas que contribuyan a la seguridad económica y social. Conectando estos términos: seguridad, cooperación, público y economía social, nos lleva a pensar en una institución que los ha alineado en su estrategia, durante más de 181 años de existencia, la Institución de la Guardia Civil. Sin embargo, no se han encontrado investigación, artículos o proyectos que aborden esta cuestión en el ámbito académico. El presente estudio analiza cómo el capital intelectual (CI) de la institución, contribuye a generar valor económico-social a través de sus acciones solidarias y humanitarias. La metodología utilizada se basa en un análisis de contenido de la información divulgada de su CI en sus memorias de responsabilidad social y de sostenibilidad entre 2014-2023. Se ha empleado el modelo Intellectus adaptado al contexto público, para identificar y cuantificar los activos intangibles. Los resultados evidencian que el CI de la Institución, a través de la gestión del conocimiento, la cultura organizativa, las relaciones externas, el carácter benemérito y el compromiso social aporta valor tangible e intangible que va más allá de sus funciones de seguridad pública. Esta investigación demuestra la relevancia del CI en instituciones públicas y su potencial en el fortalecimiento de una economía social integrada en la Agenda 2030.

Keywords: social economy, intellectual capital, civil guard, sustainability, social value.

Palabras clave: economía social, capital intelectual, guardia civil, sostenibilidad, valor social.

ORCID: Https://orcid.org/0009-0000-2569-3710

ABBREVIATIONS

ASGC: Association of Civil Guards in Solidarity.

CEPES: Spanish Social Economy Business Confederation.

EC: Structural Capital.

CH: Human Capital.

IQ: Intellectual Capital.

CIC: Centre for Research on the Knowledge Society.

CIS: Centre for Sociological Research.

RC: Relational Capital.

EUROPOL: European Police.

IADE: Institute of Business Administration.

KBW: Knowledge- Based View.

MITES: Ministry of Labour and Social Economy.

MRSCGC: Corporate Social Responsibility Report of the Guardia Civil.

MS: Sustainability Report.

RBV: Resources- Based View.

CSR: Corporate Social Responsibility.

SDGs: Sustainable Development Goals.

OECC: Spanish Climate Change Office

OECD: Organisation for Economic Co-operation and Development.

NGO: Non-governmental organisation.

UN: United Nations.

NATO: North Atlantic Organisation.

EU: European Union.

VRIN: Value, Rarity, Inimitability and Non-Substitutability.

1. INTRODUCTION

The social economy is an economic model focused on the collective interest that puts people at the centre of its activity, prioritising cooperation, sustainability and solidarity rather than individual profit (Retolaza & Alzola, 2021). The continuous development of economies and societies requires prioritising those measures that improve productivity in all industrial sectors. It is particularly interesting to analyse how a public institution such as the Guardia Civil, which places people at the centre of its business model, integrates the principles of the social economy into its mission of ensuring public safety.

Currently, the social economy has been promoted by the European Economic and Social Committee, focusing on the interdependence between the economy and society. The concept in Spain has been widely disseminated by the Spanish Business Confederation of the Social Economy (CEPES). Moreover, the law 5/2011, of 29 March, in its Preamble, groups together the principles of differentiation in social economy entities, one of them being: the focus on people and social purpose, as the main one. In this context, the participating organisations host social projects carried out individually, as institutions with another legal form (Sánchez et al., 2018). Aligned to the Comprehensive Plan for a Culture of National Security, as it is developed in accordance with the Sustainable Development Goals (SDGs) set by the 2030 Agenda. In order to evolve, it requires the active collaboration of all sectors that make up the social ecosystem, from private to public organisations, including civil society organisations, not forgetting the academic sector (García-Flores & Palma, 2020).

Following on from the previous point, it could be said that the Civil Guard institution belonging to the public sector presents an integrated approach in the social economy through the dimensions or capitals that make up its intellectual capital (IC). Since its creation, the Civil Guard Institution has based its actions on security, prevention and protection of citizens' rights and freedoms, but also on their care and assistance when they are in a situation of vulnerability (human capital). In this sense, it encourages participation and coordination internally and externally with different entities, which is known as benevolent character (structural capital). This intangible, combined with other tangibles such as the structure and diversification of the institution, not only serves to strengthen alliances that foster already established social networks, but is also used as a facilitator of connections between distant communities and individuals (Burt, 2004) (relational capital). Not forgetting that the cohesion and trust generated in these relationships facilitate the transmission of knowledge, which is a valued intangible in the economy (Arteaga et al., 2020).

Research on IC has shown the value relevance attached to it. Garanina et al., (2021), in a structured review in different countries carried out in the period (2010-2020), observed the convergence of researchers to conceptualise the concept of IC as a generator of business value. In this paper, we will avoid entering into the rhetoric on the value of intangibles vs. tangibles as today, the controversy of the 1970s post-industrial era has been left behind. There, the value of a company's intangibles was beginning to be the subject of debate in financial reporting. Equally forgotten are the controversies raised about them after the bursting of the dotcom bubble, the global financial crisis of 2008, when companies started to assess the "risks" and a period of relative economic stagnation (Hazan et al., 2021).

The academy indicates that the IC paradigm is considered established as a system for the achievement of business value among academics at the end of 2010 and, therefore, has reached theoretical consolidation in our days. Consequently, the aim of this study is to analyse to what extent the solidarity and humanitarian actions of the Civil Guard Institution generate social value for stakeholders, impacting on the social economy through the management of the elements that make up its IC, as they are key to social growth and development (Haskel & Weslake, 2018; Stratone, 2023). Our decision is based on filling a gap found in applying an IC approach to a public institution as an active agent in the social economy and traditionally studied through an operational and legal prism. By making these principles visible in the Civil Guard Institution, we aim to open up other lines of research that have not been as explored in the social economy and in national and international law enforcement bodies in their study of IC.

This article is structured as follows: in the first section, we briefly review and define the concept of Intellectual Capital (IC). Then, in the second section, we analyse the synergies between the Social Economy and the institution that is the object of our research and we infer our research hypotheses. These hypotheses are set out in the third section, which deals with the methodology used. In line with the latter, the fourth section sets out the results obtained from the research, ending with the fifth section on the conclusions drawn, contributions and limitations.

2. THEORETICAL FRAMEWORK

2.1. INTELLECTUAL CAPITAL (CI)

Companies at the micro or macro level in any sector must consider both their tangible and intangible assets useful for value creation, which is often referred to as intellectual capital (Cañibano, et al., 2002; Bueno et al., 2008; Fernández et al., 2022). This acquires prominence when the importance of intangibles in the business economy is established, positioning investment in intangible assets as opposed to tangible assets. Studies show that intangible assets are key to economic and business growth (Haskel & Weslake, 2018; Stratone, 2023), especially given their acceleration after the COVID-19 pandemic (Hazan, 2021). However, this was not always the case, if we review previous studies on intangibles we find in the early 1990s the genesis of the IC concept.

After the post-industrial era in the 1970s, companies started to ask themselves about intangibles. A few decades later, the globalised and networked economies of the 1990s demonstrated the importance of the intangible asset of having both an internal and external flow of information, accumulated knowledge and proprietary procedures. These were intangibles that were not reflected in the financial statements, but contributed to the achievement of the company's objectives. Thus, we can say that IC arose as a result of wanting to know the product resulting from subtracting the real value of a company and its market value.

Edvinsson and Malone (1999), try to explain it with the metaphor that IQ would be the roots of a tree, something that is not seen, but necessary for growth. For these authors, it is made up of infrastructure, relationships with partners and customers, and employee skills. Other authors, such as Johnson (1999), emphasise in this group of intangibles, human intelligence and innovation as profit generators. A review of the literature on IQ leads us to extract the influential theories as pillars of its development:

1. *Resource-Based View (RBV)*. Barney (1991), postulates that a company's resources to be competitive must be valuable, rare, inimitable and non-substitutable, popularising in academia and in practice, the so-called RBV criteria. Where business strategy focuses on the practices and processes involved in the daily activity developed in the organisation and its results (Potter, 1996). This theory will begin to conceptualise not only tangible resources, but also intangible resources such as knowledge (Grant, 1996).
2. *Knowledge-Based View (KBW)* theories. In the new knowledge society, this will be the resource par excellence. Its major exponential is the knowledge spiral, widely popularised by its creators Nonaka and Takeuchi (1995). Their vision of the firm is as an active knowledge-creating and knowledge-disseminating entity. To this end, tacit knowledge, that which is inarticulate, intuitive, arises from the individual with experience "in" and "with" the work he or she performs "*know how*" (Nonaka & Takeuchi, 2021). It is transmitted and at the same time transformed in the organisation when it is applied (Grant, 1996) into explicit knowledge. It can be codified, written down, objective and easily transferred (Nonaka & Konno, 1998), the "*know about*", being created at the organisational and individual level. This theory imbues it with a dynamism and external projection, which the previous theory lacked (Bontis, 2002).
3. Dynamic capabilities theory. As stated by its precursors (Teece et al., 1997), it focuses on the combinatorial ability of firms to ensure that their knowledge, skills and experience remain embedded in their products and processes and are difficult to imitate. Although more modern than those discussed above, it has expanded into the following fields: entrepreneurship (Alvarez & Barney, 2001); business performance (Wang et al., 2011; Stratone, 2023); return on investment (Chen et al., 2009; Tan et al., 2007); networked environments (Zheng et al., 2011) and environment (Chen, 2008; Haarhaus & Liening, 2020).

These theories result in defining IC as the set of intangible and tangible resources and the ability of firms to manage them, making them competitive and sustainable.

2.1.1. Definition and dimensions of the IQ

The literature review has not found a universally accepted definition of IC. Despite this, authors agree in showing how its identification and use creates benefits for the organisation (Hazan et al., 2021; Sumedrea, 2013). The contributions of some relevant authors who have investigated IC are presented below (table 1).

Table 1

ORCID: Https://orcid.org/0009-0000-2569-3710

Main contributions to IC definitions.

Aportaciones a la definición del CI	Autor
Sistemas y procesos que la hacen competitiva.	Steward, 1997
Los activos que no están en los estados financieros pero deberían reflejarse.	Petty & Guthrie, 2000; Roos, 2001 Reed et al. 2006; HernandezBueno et al., 2008
Fuente de futuros beneficios.	Lev, 2001
Necesarios para la innovación.	López et al., 2004; Rideg et al., 2023
Impulsor de la innovación y factor clave en la economía.	OECD, 2006
Combinación de intangibles y tangibles alineados a la estrategia empresarial para generar beneficios.	Bueno et al., 2008
Conocimiento a disposición de la organización para decidir las estrategias.	Aramburu et al, 2015
Creación de valor	Cañibano et al., 2002 Demartinni &Trucco, 2016 Garanina et al., 2021
Motor del desarrollo económico y social	Merino et al., 2018 Suciu & Năsulea, 2018
Creación valor corporativo y generación ventajas sostenibles en economías emergentes	Xu & Wang, 2018
Recursos estratégicos.	García-Flores & Palma., 2020
Motor de la cuarta revolución industrial.	Li et al., 2020
La tecnología es impulsora de las relaciones sociales que posibilitan su difusión.	Briñez, 2021
Rápido crecimiento económico.	Hazan et al., 2021
Efectos en el valor del mercado	Dumay et al., 2016
Mejora el desempeño organizacional	Thum-Thysen et al., 2021 Fernández-Solís et al., 2025

In this study we define IC as intangible values that, managed together with tangible values, contribute to business, economic and social growth.

Just as there is no consensus on the definition of IQ, there is no universally accepted model for its measurement. Over time, various models have attempted to classify the measurement of intangibles, evolving from simpler models such as Skandia (1997) to more complex ones such as the updated Intellectus model (2011).

Among the pioneers in the measurement of IQ, Edvisson and Malone's Skandia Navigator (1997) groups the elements that make up IQ into two dimensions for its study: human capital and structural capital. In contrast, most authors dedicated to the study of IC, there is consensus in grouping the intangibles that compose it into three capitals: human capital (HC), relational capital (RC) and structural capital (SC) (Petty & Guthrie, 2000; Navarro & Medina, 2024). To exemplify this, we set out the classifications into capitals with their elements in Table 2. The first column shows the indicators of Johnson (1999) who contributed to the literature a clear distinction between financial and non-financial indicators in relation to the market value of a company. The second column shows the classification made by Cañibano et al. (2002) based on the MERITUM project[1] promoted by the OECD and the EC; it has been represented because the Institution is framed in this context.

Table 2
Examples of IC Categories and Indicator classifications.

Capitales	Elementos no financieros	Elementos CE y OCDE
Capital Humano (CH)	Habilidades; conocimientos; tareas y motivación	Capacidades, saberes, habilidades y experiencias
Capital Estructural (CE)	Procesos de negocio y renovación, flow de información, productos y servicios; formas de cooperación de procesos	Procedimientos, rutinas organizativas, cultura, sistemas, bases de datos, licencias, etcétera.
Capital Relacional (CR)	Relaciones con los socios, clientes, proveedores e inversores	Relaciones con clientes, proveedores, socios de I+D+i.

For these authors, IC is the combination of the elements that make up the capitals that companies have. However, in the literature review we have also found authors such as Delgado et al. (2008), who prefer to study it by dividing it into five dimensions: human capital, technological capital, organisational capital, relational capital and social capital. Following this last categorisation of IC, one could therefore consider the convenience of extracting social capital from IC and aligning it with the social economy. The objection we raise is that social capital, either as a dimension or as a subdivision of relational capital, does not in itself create value without the interaction of the other two capitals, as we explain below.

To this end, at this point, we define in synthesised form the dimensions into which the elements that make up IQ are usually categorised by academics for their study, and how they are related:

- The human capital (HC) dimension comprises the knowledge established in a company's employees; individuals are capable of generating it (Delgado et al. 2008). It resides in the capabilities, skills, experience (Bueno & Merino, 2007; Bellucci et al., 2021), values and attitudes towards the company and the job. In addition, this capital includes that of employees as they are active sources of useful

[1]Measuring Intangible to Understand and Improve Innovation Management (MERITUM): Joint OECD-EC project to boost research in Europe (1998-2001).

knowledge for the organisation (Merino et al., 2018). The relationship with the other two capitals is manifested both in innovation (Li et al., 2020), as it is the individuals in an organisation who request new ways of doing things (CE) and in the ability to work with others and negotiate, which requires motivation, loyalty and satisfaction (CE, 2006) (CR).

- The structural capital (SC) dimension is constituted for most authors (Chen et al., 2009; Delgado et al., 2008; Dumay et al., 2016; Merino et al., 2018, Oliveira et al., 2020) by assets such as: organisational structure, routines, procedures, processes, databases, manuals, patents and software, which remain in the company when the individuals working in it have finished their work. Some of these are tangible, such as machinery and structure. However, others are intangible such as intellectual property, trademarks, patents, organisational culture (Chen et al., 2009) and image (Merino et al., 2018; Jeffrey et al., 2019). The most notable relationship with the other two capitals is based on the structure of the organisation. This serves as a scaffolding through which processes and procedures are transferred between human and technological capital, creating relationships between *stakeholders* .[2]

- The relational capital (RC) dimension covers the assets generated by the set of relationships between employees, customers, suppliers, shareholders (Bellucci et al., 2021), strategic alliances that generate information and knowledge relevant to the company. The synergy generated with the other capitals can be exemplified by formal and informal relationships between employees in the organisation, as they are key in the transmission and generation of information and knowledge (CH). With the CE, we see it through the fact that this knowledge spreads from one individual to another and is also transformed by remaining in the organisations (De Castro & García, 2003), influencing the economy and society (Garanina et al., 2021). The importance of this relational capital is perceived in the segmentation of customers that companies usually make; creating or decreasing commercial agreements and establishing or strengthening alliances, since not everyone has the same needs or these change over time.

In this way, it is the interaction of the aforementioned capitals that creates value in an organisation. We exemplify it with the generation of knowledge, as it is recognised as key to economic development (OECD, 2006). Information and knowledge is disseminated through human or technological structures (Devenpor & Prusak, 2001; Wang, 2011) or both (CH). We also know that it is accumulated in them through processes, operations, organisational routines, procedures, etc. (De Castro & García, 2003), these are the scaffolding for business and social activities, achieving organisational value (Demartinni & Trucco, 2016) (EC). Well, to a greater or lesser extent, the development of a network is encouraged, promoting schemes of participation, collaboration, development of initiatives and social platforms (CR). However, this network, even in its optimal state, could hinder the flow of knowledge, due to the elements that compose it, such as: having insufficient or bad staff, poor management, or even that

[2] *Stakeholders*. For the pioneer Friedman, *stakeholders* are any type of person who influences or is influenced by a company. The Guardia Civil's stakeholders include citizens, public administrations, civil guards and other organisations such as NGOs, private security, universities and international police forces. They also include people with opposing interests who belong to: criminal gangs, terrorist groups, criminals, etcetera.

the procedures or policies of the company's strategy interfere negatively in it (Merino et al., 2018).

As a theoretical conclusion, there is no doubt that focusing on the real value of a company and determining it was the *driver of* the development of intellectual capital. The aim was to explain the result of the difference found between the value of a company in its financial books and its market value. This value explained to the IC, is due to the interaction of the elements that form it such as: the skills, knowledge and experience of employees together with R&D&I projects; organisational routines; the interaction of internal and external relationships (Briñez, 2021) both at the employee level and with suppliers, shareholders, allies and customers (EC, 2006) [3] . Not forgetting the management of transforming, acquiring and applying them in a changing environment (Nonaka & Takeuchi, 2021).

These characteristics position the IC as a key to economic (Bellucci et al., 2021), social and sustainable growth (Secundo et al., 2020) adapted to a volatile, diffuse, uncertain, ambiguous, complex (Nonaka & Takeuchi, 2021) and technologically disruptive market (Wang et al., 2021). For this reason, in the following section we will empirically explain, through the institution of the Civil Guard, how companies can provide social economic benefits through IC.

2.2. SOCIAL ECONOMY AND THE INSTITUTIONAL BODY OF THE CIVIL GUARD

The social economy[4] is defined as a set of business and economic activities carried out by entities for the achievement of the collective good of its members, the general economic and/or social interest following the principles of the social economy (MITES, 2025). Currently, the concept is consolidated in Spain and is disseminated by the International Centre for Research and Information on the Public, Social and Cooperative Economy. If we relate these terms: public, social, cooperative and public economy, it leads us to think of an organisation that has aligned them in its strategy for more than 181 years of existence: the Civil Guard Institution, by converging economic and social practices in the provision of goods and services. We rely on finding in the Institution, established principles of the social and collaborative economy such as those listed below, by authors such as Díaz-Foncea et al:

- Promote solidarity among employees by facilitating structures, motivating them to show solidarity and cooperation.
- Recognition of solidarity and committed work through the spirit of merit.
- Promotion of equality in a broad sense not only based on gender.
- Inclusion and social cohesion.
- To help and support the most vulnerable groups and those at risk of social exclusion.
- Reconciliation of professional and family life.

[3]EU RICARDIS document (2006). The European Commission relies on this interaction based on the MERITUM project, 2002. It is defined as the combination of human capital, structural capital and relational capital resources and activities of an organisation.

[4]It is currently being promoted by the European Economic and Social Committee, focusing on the interdependence between the economy and society.

- Generate sustainability internally and externally, with clear respect for the environment and the protection of biodiversity.

The competitive advantage of this Institution is to offer superior quality services in order to be a reference in its sector, before the citizens, the State and the European Union. Its mission, within the State Security Forces and Corps, is to "*protect the free exercise of rights and freedoms and guarantee public safety*" (Art. 104, Constitution). It does so by placing people at the centre of its actions, ensuring their safety and integrity, in a close manner. The functions are set out in Table 3.

Table 3

Definition of the Civil Guard's functional competences

Note: The data in this table is based on the Organic Law 8/1986 of 13 March 1986 and the Sustainability Reports of the Guardia Civil, 2023.

Diferentes Cuerpos de Seguridad Artículo 11 (página 26)	Específicos de la Guardia Civil Artículo 12, B (página 27)
• Velar por el cumplimiento de las leyes y disposiciones generales. • Auxiliar y proteger a personas y bienes. • Vigilar y proteger edificios públicos. • Mantener el orden y velar seguridad ciudadana. • Prevenir la comisión de actos delictivos. • Investigar delitos, asegurar las pruebas e instrumentos poniéndolos a disposición del juez. • Prevención de la delincuencia. • Colaborar con Protección Civil, caso grave de riesgos o catástrofes.	• Control de armas y explosivos. • Resguardo Fiscal del Estado (costas, fronteras, puertos y aeropuertos) • Vigilancia del tráfico, tránsito y transporte en las vías públicas interurbanas (exceptuando el País Vasco y Cataluña). • Conservación de la naturaleza y medioambiente, recursos hidráulicos, riqueza forestal y de otra índole relacionada con la naturaleza. • Conducción interurbana de presos y detenidos. • Aquellas otras que les atribuye la legislación vigente.

missions by joining an international organisation such as EUROPOL, the UN or NATO, as well as the Spanish Armed Forces (CG, 2023).

We can say that, with more than 80,000 troops, deployed throughout the national and international territory. It is diversified into specialities: Nature Protection, Judicial Police, Information Services and Maritime Service, among others. Together with the human potential deployed in citizen security, with more than 2,000 territorial units (GC, 2025).

2.2.1. Social value created by the institution.

Social value can be defined as the positive result of the actions developed by an entity on society (Retolaza & Alzola, 2021). This intangible value is contextualised in the commitment of the Civil Guards to go beyond the fulfilment of their mission. They do so as a social contribution, focusing both on improving the lives and support of citizens, as well as being aware of environmental concerns, following one of the principles of the social economy set out by Díaz and Lejarriaga (2019). For example, with regard to the latter principle, it has registered its carbon footprint with the Spanish Climate Change Office (OECC), becoming one of the only police forces to do so worldwide. We also highlight the award granted by the United Nations in 2023, the "Ozone Protection Award for Customs and Police Officers".

These values are enhanced by the Institution through transparency and recognition of its actions, presenting an integrating and collaborative impact, where the communities where its projects are developed have a role in decision-making, on what they consider as value. Therefore, the Institution combines its resources, policies and processes to achieve improvements in the lives of people and society in general, which is what social value is called (Retolaza & Alzola, 2021).

To develop its capabilities, its business model is to disseminate and apply a culture of quality security that is versatile, available and close to the citizen. It does this by transmitting its knowledge and experience to other national and international police forces, citizens, the government and other stakeholders, with professionalism and a benevolent character. The latter is recognised because civil guards work with the knowledge and commitment to do extraordinary things, contributing to what we have called intangibles.

It should be remembered that in the first Service Regulations of 1844, article 32 already stated its charitable and protective nature. At the same time, article 6 of the Guardia Civil's Charter stated that the Guardia Civil should care for the unprotected and be a happy prognosis for the afflicted (GC, 2025). A few years later, in 1929, the Institution was awarded the Grand Cross of the Civil Order of Charity with a black and white badge, which implies personal risk, in recognition of the humanitarian and heroic services performed. Therefore, we can say that solidarity and cooperation are values established in the DNA of the Institution since its creation, becoming the hallmark of the Institute's identity.

The spirit, or benevolent character, is still present today, expressed in its Code of Conduct[5] . Article 21 establishes the provision of assistance to citizens, whether or not its personnel are on duty. It is also found in point 7 of the Guardia Civil members' decalogue, which states that they should always help those who need it most, focusing on people in situations of vulnerability and lack of protection; it is also expressed in their corporate social responsibility reports (MRSC) and in the Guardia Civil's official magazine.

Therefore, this intangible is promoted by the Institution, being considered an organisational asset, promoting it through humanitarian services, volunteering, the fight

[5] Royal Decree 176/2022 of 4 March, approving the code of conduct of the Civil Guard.

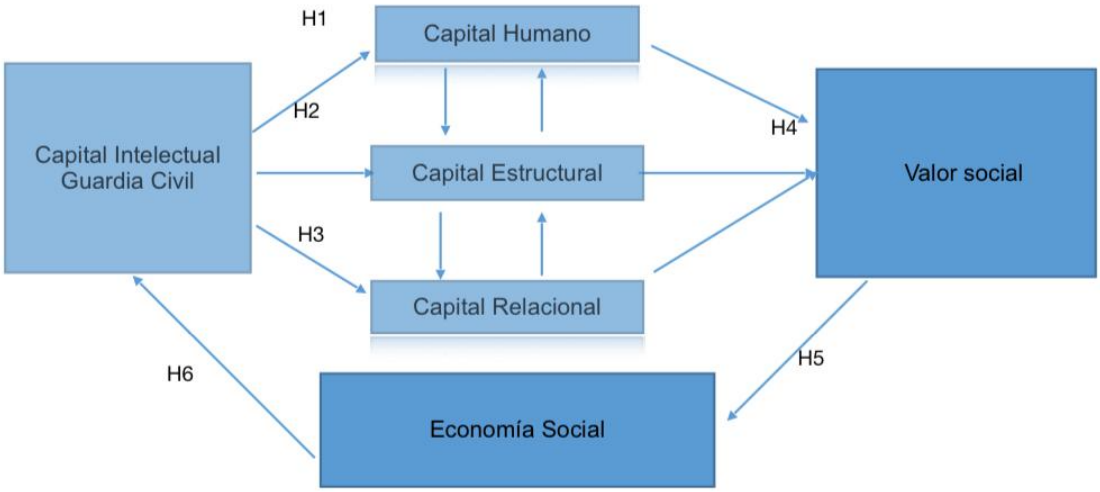
for biodiversity and the environment. It is produced, both at an individual level and in other organisations, as stated on its website #GComprometidos.

Given the above, we can say that the mission of the Civil Guard is not only based on public safety but also includes the welfare of society, which is determined through the dynamism provided by the dimensions of the IC that form it, generating economic growth (Nonaka & Takeuchi, 2021). However, this economic-social value is not taken into consideration or is unknown in academia, since, when we conducted our research, we did not find any studies, research or articles on the subject. Therefore, in the following section we will set out our hypotheses on the contribution of the social economic value of the institution in the research model.

3. METHODOLOGY

Based on the above, we present the research model (Figure 1) where the hypotheses of this study are set out:

Figure 1.
Research model and hypotheses.



H1. Human Capital is identified in the Institution.

H2. Structural Capital is identified in the Institution.

H3. Relational Capital is identified in the Institution.

H4. The interrelation of the three capitals impacts on the creation of social value.

H5. The social value generated influences the social economy.

H6. The social economy influences the intellectual capital of the Guardia Civil.

In order to test our hypotheses, we followed the indications of Codina et al. (2020) by carrying out a literature review using scientific databases such as SCOPUS, Web of Science and Google Scholar. These authors show in their research that these databases, used by the international scientific community, broadly cover all areas of knowledge. The search was carried out both in the fields: article titles, in the *abstract* or by the keywords indicated in this article. However, the search did not return any results, demonstrating the lack of scientific articles on our research topic. For this reason, our data have been obtained from the documentary and bibliographic review of databases of the Ministry of the Interior, as well as the Ministry of Defence and the Civil Guard Institution, where the Institution publishes its financial and non-financial reports. We therefore rely on quantitative and qualitative data from open primary sources.

The technique chosen has been a content analysis[6] as it has been frequently and successfully used in the analysis of IC disclosure reports (Magau 2021; Dumay el al., 2016). It is also suitable for verifying deductively stated hypotheses (Bini & Giunta, 2017). The corpus of the content analysis, are the Civil Guard Social Responsibility Reports (MRSCGC) and Sustainability Reports (MS). Our decision is based on the fact that annual reports are tools used by organisations to communicate to all stakeholders what they consider important, disclosing them in them (Petty & Guthrie, 2000; Bontis 2002; Guthrie & Abeysekera, 2006; Dumay et al., 2016). In line with the current trend for companies to disclose their financial and non-financial statements to stakeholders in these annual reports (Dumay et al., 2016).

This is a longitudinal study covering the period from 2014 to 2023, the date of the last annual information reports published. In addition to determining the consistency of the data, we are able to obtain the institutional trend by analysing them. We intend to answer whether the institution's contribution to the social economy is inherent in it, following our study objective.

The unit of analysis in content analysis is that which indicates the presence or absence of the elements to be investigated (Moreiro et al., 2006). To obtain this unit of analysis, among the conceptual frameworks used to define, classify and record the information disclosed on IC, some authors usually use the model of Sveiby (1997) modified by Petty and Guthrie (2000). However, in this research, in order to obtain our unit of analysis we have adapted the indicators of the Intellectus model[7] (2011) to the Institution, due to its wide national and international repercussion and because it is considered an integrative model for measuring IQ (Merino et al., 2018). The most notable considerations of this model are:

- The creation of a "relevance tree" establishing a structure of the IC, in order to identify the units of measurement that compose it, establishing a hierarchy of components, elements, variables and indicators. On this basis, the categories, elements, their definitions and indicators have been adapted for the identification of the IC in the Institution (See Annex I: tables 4-6).

[6] For Allport (1965), it is a method for studying and analysing communications in a systematic, objective and quantitative way with the aim of measuring variables.

[7] Intellectus Document, nº5 (2003): It was developed by Professor Bueno and the Centre for Research on the Knowledge Society (CIC). It was modified in 2011, giving rise to the Intellectus Model: Measurement and Management of Intellectual Capital, by the IADE (Institute of Business Administration). The adapted indicators are taken from its point 6. Indicator Table (pp. 36-58).

- The elaboration of a Synthetic Index, based on the main components to quantify it. These are represented in a "map of variables and main indicators" which will be used as a quantitative measure of the set of identifiable intangibles. Following this point, we indicate in Annex II the formulas used to obtain the indices.

- The preparation of the IC Report (ICR), for its dissemination. Therefore, following the literature, a review of the documents where the Institution discloses its financial and non-financial reports has been carried out.

We have managed to limit the subjectivity that could occur in obtaining the sampling unit or unit of analysis, adding transparency in categorisation and using consistent decision rules throughout our longitudinal study. In relation to reliability, the coding instrument has been manual without the use of software, avoiding the problems presented by words with multiple meanings which, although they can be reduced by increasing the key words in context, do not detect the meaning of the specific IC of the institution, or the interpretation that is made of it (see Annex III: Phases in the content analysis).

Next, in order to understand the behaviour of our study variables (dimensions of IQ), we have categorised them according to the tripartite division of IQ: human capital, relational capital and organisational capital. We base ourselves on this as it has been established by the European Commission (2006), based on the MERITUM project (Cañibano et al., 2002) cited in section 2.2 (see Annex I: tables 4-6).

Finally, a statistical analysis of the measures of frequency distribution, trends and dispersion has been carried out. The statistical study aims to observe the importance of the elements for the Institution and their comparison and position with respect to the other elements of the IC, throughout the period studied. For this purpose, the statistical programme RStudio, version 2024.12.0+467 for macOS 13+ has been used.

4. RESULTS AND DISCUSSION

The results of our research identify IQ in the institution. In the analysis of our research, adapting the Intellectus model, the categories, elements and indicators, the identification of its component elements is derived from the construction of the categories, elements and indicators. The Institution's IC can be classified by grouping its component elements into human capital, structural capital and relational capital (see Annex I). These results are similar to most academic studies. Consequently, we accept the first three hypotheses of this research:

H1. Human Capital is identified in the Institution.

H2. Structural Capital is identified in the Institution.

H3. Relational Capital is identified in the Institution.

We then go on to verify the remaining hypotheses. With reference to social value, on analysing the subject of the elements that make up the IC capitals and the capitals of the Institution (Appendix I), we can see that the definitions of the elements that make up human, relational and structural capital have a direct impact on social value. In other words, the IC elements are aligned with the identification of social value in the literature, as shown in table 7 below.

Table 7

Relationship between the institution's IQ and social value.

Dimensión Capital Humano			
Elementos	Definiciones	Capital Humano	Valor social
IDENTIDAD MOTIVACIÓN CREATIVO EDUCACIÓN ESPECIALIDAD; UNIVERSITARIO FORMACIÓN EXPERIENCIA DESARROLLO APRENDIZAJE CIVIL CONCILIA LIDERAZGO	Valores, motivación a la excelencia en sus actuaciones, formación especializada y conocimientos. Adaptación y generación ideas novedosas aplicables en el desarrollo del trabajo.	Autores como Nonaka y Takeuchi (2021) puntualiza que las empresas que cuentan con empleados con muchas habilidades y experiencia son capaces de gestionar escenarios cambiantes. Capacidad sin actitud o aptitud generaría una desaceleración o destrucción del valor (Merino et al., 2018)	Valor aportado por las personas a las empresas (Carina et al., 2024). Las creencias personales sobre un propósito social (Díaz-Foncea et al., 2016).
Dimensión Capital Estructural			
Elementos	Definiciones	Capital Estructural	Valor social
CULTURA CLIMA IGUALDAD ESTRUCTURA DESARROLLO RUTINAs RELACIONINT CRIMINAL PROVEEDORES INVERSIONIDi PERSONALIDi INFRAESTRUCTURA EQUIPOPOLICIAL INNGEST COMUNICACIONGC MARCA LICENCIAS SECRETO PATENTES TECNOEXT TECNONEW TECLIC PLEXBIBILIDAD TALENTOS	Cultura institucional, idiosincrásica de la institución. Espíritu benemérito transferido generación a generación a través de acciones solidarias de cooperación, sacrificio y apoyo al necesitado. Seguridad y protección según la legislación vigente. La estructura de la Institución la hace distintiva, por su diversificación tanto geográfica como en especialidades para llegar a todos los ciudadanos. Andamiaje a través del cual el conocimiento, la experiencia y la información se transfiere diversificándose en especialidades aumentando así su valor empresarial. Sin olvidar las políticas e inversión en innovación y desarrollo.	Las empresas deben desarrollar su capital humano con los medios necesarios que apoye la visión sobre lo que las personas son capaces de hacer para generar cambio (Mohdzaini, 2021).	Recursos que los individuos pueden conseguir a través de la estructura de una organización (Sánchez et al., 2018). Sin estructuras sociales es difícil generar el capital social (Nonaka &Takeuchi, 2021).
Dimensión Capital Relacional			
Elementos	Definiciones	Capital Humano	Valor social
CIU LEALCIU QUEJAS PROTCIU ESTADO IADMINISTRACIÓN CAPITALEXTERIOR ALIANZAS ALIANZASESTABLES ALIANZASBENEFICIO CONCOMPETENCIA PRIVADA CERTICAL REDES ADMINISTRACIÓN MEDIOS DEFENSAMBIENTE VERDE MERCADO CODIGOCON ACSOCIAL BUENGOBIERNO	Genera valor a través de las relaciones y alianzas establecidas con todos sus grupos de interés. En el plano internacional, establece relación de cooperación y colaboración con otros países. Es reseñable el apoyo a los más vulnerable y desfavorecidos. La inclusión y la cohesión social. Impulsa proyectos de voluntariado dentro y fuera de la institución. Dedicada a la defensa del medioambiente interna y externamente y la biodiversidad. Cuenta para ello con una red de medios de comunicación internos y externos promoviendo la transparencia y el buen gobierno.	Las empresas generan valor a través de las relaciones creadas con sus grupos de interés (Maqbool,2020) y en la transmisión de ese conocimiento (Rideg et al. 2023; Nonaka & Takeuchi, 2021). Este conocimiento debe ser fluido (Merino et al., 2018).	A través de promover el empleo, la inclusión social, sostenibilidad, innovación y crecimiento económico se consigue impulsar la economía social (cepes, 2023). Las empresas logran sus objetivos sociales promoviendo la transparencia (Sumedrea, 2013). Los programas de inclusión económica tienen un fuerte impacto en las personas más pobres del mundo (Word Bank, 2024).

Once the data had been quantified (Annex II) to find out the behaviour of the elements of our variables and whether they are a constant over the period studied, an analysis of the frequency distribution and trend measures was carried out (Figure 2).

Figure 2
Frequency distribution and trends of IC elements (2014-2023)

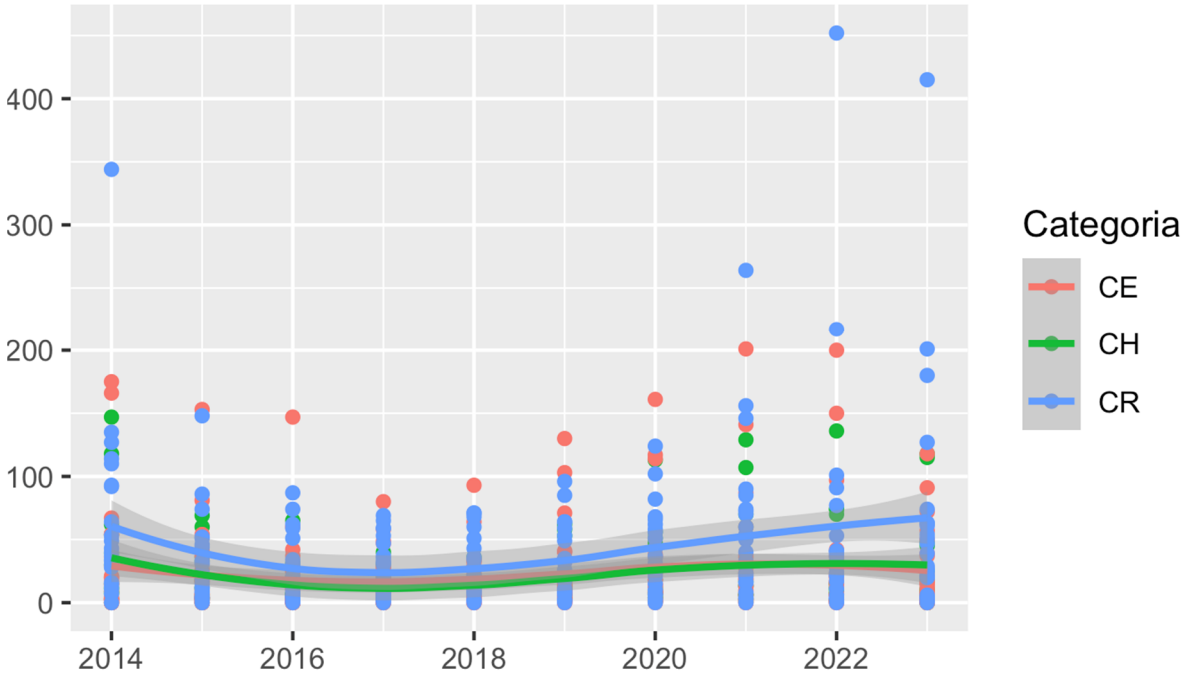


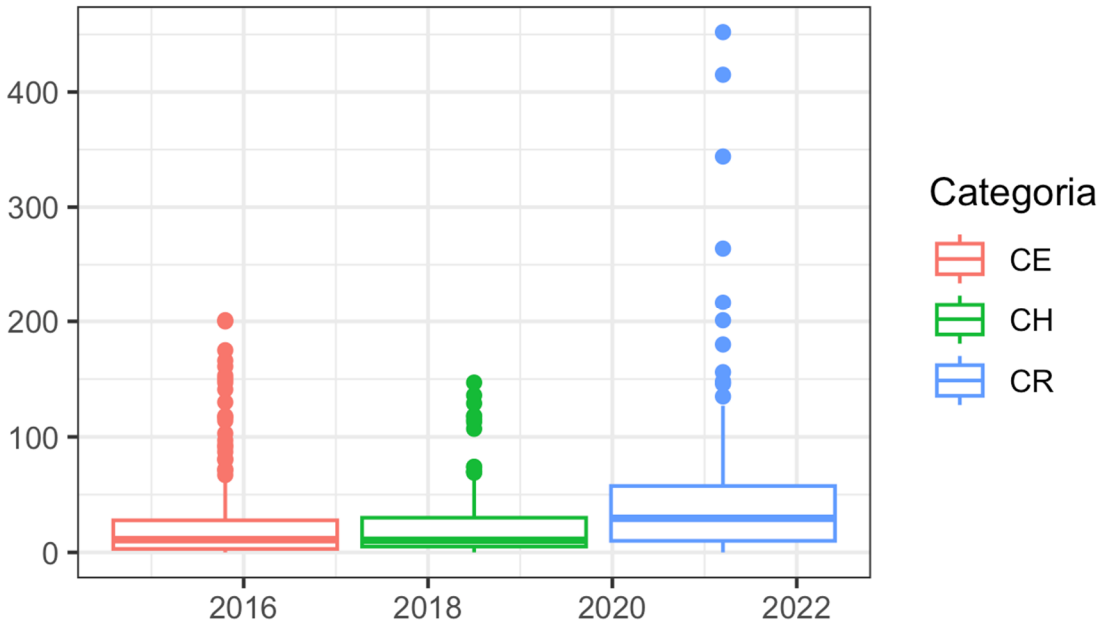
Figure 2 shows how the elements are represented in the period studied, and their distribution in categories. It is noteworthy that, while the dispersion curve of human capital (HC) and structural capital (SC) are almost aligned over the 10 years, indicating the constancy between the frequencies of the elements of both capitals, that of relational capital (RC) remains above them. In addition, the outlier scores of the elements of the latter capital are the furthest apart compared to the other two capitals in recent years, showing the relevance of these elements.

Next, to determine the grouping of these elements, in figure 3, measures of central tendency and position have been used. A box plot has been drawn up to visualise both the measures of central position (mean, median and mode) and the non-central position measures, quartiles, based on our knowledge of the dispersion of the data in figure 2.

ORCID: Https://orcid.org/0009-0000-2569-3710

Figure 3

Plot of measures of central tendency CI dimensions (2014-2023).



Observing (figure 3) the dispersion of the data and the outlier scores, we choose the median as a measure of central position. This graph shows that the median of the relational capital is above the Q3 of the other two capitals, and that its interquartile range is almost double, together with the lines that protrude from the upper margin of the box (whiskers) and the distance between their outlier scores, confirming the dispersion of the data. We observe much higher scores in relational capital in 50% of their scores, higher than the other two capitals, together with the fact that their outlier scores are the highest in the period studied. The latter is interesting as it signifies the importance that the Institution attaches to these outliers. A disaggregated analysis of these outlier scores indicates that they correspond to the elements detailed in table 8.

Table 8

Outlier scores of the elements in the period under study

Elemento	Total 2014	Total 2015	Total 2016	Total 2017	Total 2018	Total 2019	Total 2020	Total 2021	Total 2022	Total 2023
CRALIANZASESTABLES	X								X	
CRALIANZASBENEFICIO	X	X	X	X						
CRPROTCIU		X			X	X	X	X	X	X
CRACSOCIAL	X			X	X	X		X	X	X
CRVERDE		X	X			X	X	X		X
CRDEFENSAAMBIENTE	X							X		X
CECRIMINAL	X	X	X		X	X	X	X	X	
CECOMUNICACIONGC	X	X	X	X	X	X	X	X	X	X
CEIGUALDAD						X	X	X	X	X
CHFORMACION	X	X	X			X				
CHDESARROLLO		X			X	X	X			
CHUNIVERSITARIO						X	X	X	X	X
CHCREATIVO								X	X	X

Table 8 shows the relevance of the elements for having obtained the highest scores: Stable Partnerships, Beneficial Partnerships, Protciu, Social, Green, Defesaenvironment, within the RC. The elements: Criminal, Communications, Equality, within the EC and the elements: Training, Development, University and Creative, within the CH. High scores for the elements: Protciu together with Asocial for 7 years, Criminal for 8 years, and Communication for 10 years.

With these data (table 8) and the sample units (appendix I), we can infer that for the institution, its actions are aimed at security, protection of citizens and the development of social actions through the strength of partnerships and joint services with other identities. In the same vein, its actions are aimed at protecting the environment and biodiversity. For it, "value" is not only considered in financial terms but, in line with Nonaka and Takeuchi (2021), "social and environmental" are also valuable assets, being constant in this. To this end, its human capital is egalitarian and diverse, qualified and developed, adapting and creating new ideas in the performance of the service by transferring its knowledge.

These results show that the definition of social value follows the definition of social value as an outcome generated from the combination of resources, processes and policies that improve people's lives and society as a whole (Sánchez et al., 2018). Therefore, we see that hypothesis 4 is corroborated:

H4: The interaction of these capitals generates social value.

Following our line of research, we are now going to find out how this social value has an impact on the social economy, beyond its main mission as described in section 2: Protection and Social Action to the citizen (table 9), following the principles of the social economy and the definition of social value.

Table 9

Indicators of the elements: protection and social action for citizens.

The data shown above (table 9) are interesting as they indicate that in the last nine years, 1,883,862 humanitarian services have been carried out; 14,689 actions for the benefit of the community and 2,410 voluntary actions. In addition to other solidarity and

	2022	2021	2020	2019	2018	2017	2016	2015	2014
Acciones beneficio comunidad (más allá misiones encomendadas).	1.012	960	1.151	2.659	2.647	2.986	1.956	1.318	1.620
Acciones solidarias (voluntariado nivel individual hay constancia).	1.026	267	347	121	114	140	215	180	62
Actividades de acercamiento a la sociedad	247	499	503	482	340	316	105	904	142
Charlas en centros escolares	34.459	21.328	16.078	34.848	12.970	12.412	16.245	12.814	11.782
Acciones seguridad mayores	3.607	2.740	3.275	3.732	3.816	3.769	9.712	10.364	11.605
Colaboraciones convenios.	261	149	106	114	92	86	96	115	95
Servicios humanitarios	242.575	218.303	215.697	194.923	193.593	193.135	458.360	167.266	SD

protection activities for the elderly and minors. Demonstrating that people are more important than capital in the social economy (Pedreño, 2024).

These data show that humanitarian services and actions for the benefit of society are a plus. Moreover, their financial value is inestimable. To visualise the economic value of these actions, we have summarised it by taking the example of the Asociación Guardias Civiles Solidarios[8] (ASGS). Table 10 shows the economic value of its actions over the last 5 years, data obtained from the ASGC's annual reports.

Table 10
Economic evaluation of "Civil Guards in Solidarity" actions

	Actuaciones	Niños	Adultos	Alimentos (kg.)	Valor económico €
Memorias 2024	60	2.977	2.987	22.540	60.257
Memorias 2023	44	4.771	9.109	44.980	45.396
Memorias 2022	65	1.832	63.396	362.040	367.356, 21
Memorias 2021	54	2.419	5.346	13.210	52.000
Memorias 2020	138	2.017	13.251	8.262	38.482

With the data presented in both tables (8 and 9) we enter into the discipline of the social economy that permeates the traditional economy, the value of the social (Diaz-Foncea et al., 2016) and the institution of the Guardia Civil that sustains it, through its intellectual capital. Thus, it is demonstrated that the value of the services provided has a positive impact on the social economy by pursuing the general economic and/or social interest. Consequently, hypothesis 5 of our research is confirmed:

H5: The social economic value of the institution influences the social economy.

Finally, we have analysed whether the social economy returns to the Institution, thus completing the objective of our research. To this end, we have analysed the trust granted to the Institution by citizens, institutions and various entities carried out by the Sociological Research Centre (CIS) during the period studied. The results are shown in table 11 below.

[8]In 2014, the Asociación Guardias Civiles Solidarios (ASGC) was founded with the aim of channelling the numerous individual actions of volunteer personnel.

Table 11
Valuation of the institution by Spanish society

	2023	2022	2021	2020	2019	2018	2017	2016	2015	2014
Posición entre instituciones más valoradas	SD	FFCCSE	FFCCSE	FFCCSE	1ª	1ª	1ª	1ª	1ª	1ª

As we can see, a positive valuation is passed on to the institution through the loyalty and trust that society places in it. Being recognised as an institution with social value significantly increases its reputation (Jeffrey et al., 2019; Maqbool et al., 2018). Within the institution, the commitment acquired by civil guards to society favours self-esteem and motivation by fighting for human rights and the most disadvantaged (MS, 2023). These actions, programmes or volunteering projects are aligned with the objectives of the institution, such as protecting and helping citizens, thus strengthening it.

In addition, their consolidated structure and diversification not only serves for alliances that generate already established social networks, but also facilitates connections between communities and individuals who are distant from each other (Álvarez & Berni, 2001). Not forgetting that the cohesion and trust generated in them facilitate the internal and external dissemination of knowledge, which is a valued intangible in the economy (Nonaka & Takeuchi, 2021), making it more competitive.

In line with the above, our last hypothesis (H6) is verified, thus concluding our research objective.

H6: The social economy returns to the institution.

5. CONCLUSIONS

A defining characteristic of our times is how companies manage social capital. The Institution responds to the question posed by the new economic perspective where organisations reflect on their contribution of value to society (Retolaza & Alzola, 2021). By analysing this through the IC of the Civil Guard Institution, which belongs to the public sector and is eminently social, we argue that just as capital does not create value on its own, neither do investments in it on their own. It will be the capacities generated by companies in the management of these intangibles that will achieve economic growth (Hazan et al., 2021), through services.

The Institution, in carrying out its security and citizen protection activity, goes further by creating improvements in the lives of individuals and/or society as a whole. According to the data, this is due to the knowledge, relationships, organisational culture, experience and active participation of the people who make up the institution. We deduce, through the results obtained in the research carried out, that it fulfils one of the objectives set out in the report of the World Bank's Partnership for Economic Inclusion (2024), by being able to evaluate its social programmes based on key evidence.

Its actions present an inclusive model, directly reaching those most in need, generating social cohesion through the institutional structure and its diversification. It has a solid structure that is necessary for collaboration with other non-governmental,

community and private sector organisations (García-Flores & Palma, 2019), thus reducing capacity limitations.

The institution's meritorious character, driven by its personnel, is a social value, which is defined in this work by showing the positive impact of its actions on society. By showing it as an active actor, we open a breach in the stereotype of security by going further with its social actions, environmental protection and biodiversity. In this case we have presented an inclusive model that believes that solidarity and cooperation is necessary, removes social barriers, and transforms difficult environments. These assets are valuable to the Institution following Barney's (1991) VRIN criteria as they are difficult to imitate, buy or replace, providing competitive advantage.

We believe that adequate data and measurement tools are essential for the implementation of sound policies on any type of capital. This makes it possible to obtain information and show all interested parties the investment made and the results obtained (García-Porras, 2025), under the prism of transparency. In this research, quantitative and qualitative data have been collected and analysed, continuing open lines of research based on evidence on the different ecosystems that host the social economy, fulfilling one of the objectives of the industrial strategy set by the EU (Carini et al., 2024).

We conclude with the contributions and limitations found in this study. The results show, on the one hand, that institutions belonging to the public sector can be involved with non-governmental and private organisations as a necessary agent of change, promoting the social economy. On the other hand, we contribute to the application of the study of IC management in an institution belonging to the public sector, since the study of IC is more focused on the private sector. We believe that it is novel to investigate social value in an institution that is often studied from a legal or operational perspective.

With regard to the limitations encountered, it should be mentioned that the fact that the data are based on institutional documents could generate a single source bias. In the same vein, the indices of the elements obtained from the IC have not been weighted, which minimises the relative importance they may have for the specific group of experts in social economy. More research in this field would be needed to increase our understanding of this issue. Therefore, a future line of research could strengthen this study by using expert opinions and other external perceptions and by considering the use of weighted indices.

BIBLIOGRAPHICAL REFERENCES

Alvarez, S. A., & Barney, J. B. (2001). How entrepreneurial firms can benefit from alliances with large partners. *Academy Of* Management Perspectives, 15(1), 139-148. https://doi.org/10.5465/ame.2001.4251563

Aramburu, N., Sáenz, J. and Rivera, O. (2005). Knowledge Management: Methodological and empirical aspects. Working paper. San Sebastian, University of Deusto EAST.

Arteaga A. L., Ojeda, J. F., and Alvarez D. G. (2020). Trajectory and strategies of entrepreneurship in women. *aDResearch ESIC International Journal Of Communication Research*, 22(22), 176-195. https://doi.org/10.7263/adresic-022-10

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. Journal of Management, 17(1), 99-120. https://doi.org/10.1177/014920639101700108

Bellucci, M., Marzi, G., Orlando, B., & Ciampi, F. (2021). A review of emerging themes and future trends. *Journal of intellectual capital*, 22(4),744-767. https://doi.org/10.1108/JIC-10-2019-0239

Bini, L., Bellucci, M., & Giunta, F. (2017). Integrating sustainability in business model disclosure: Evidence from the UK mining industry. *Journal of Cleaner Production*, 171, 1161-1170. https://doi.org/10.1016/j.jclepro.2017.09.282

Briñez M. E. (2021). Information technology: An empowering tool for managing intellectual capital? *Revista de Ciencias Sociales 27*(1), 180-192. https://dialnet.unirioja.es/servlet/articulo?codigo=7817690

Bontis, N. (2002). Intellectual capital disclosure in Canadian corporations. Journal of Human Resource Costing and Accounting, 7(1-2), 9-20.

Bueno E. J. and Merino C. (2007). Intellectual capital and the creation of companies in society. *Encuentros multidisciplinares, (9)26*, 37-46. https://dialnet.unirioja.es/servlet/articulo?codigo=2324790

Bueno, E. J., Salmador, M. P. and Merino, C. (2008). Genesis, concept and development of intellectual capital in the knowledge economy: A reflection on the Intellectus Model and its applications. Studies in Applied Economics, 26(2), 43-63. https://www.redalyc.org/pdf/301/30113187003.pdf

Burt, R. S. (2004). Brokerage and Closure: An Introduction to Social Capital.

http://ronaldsburt.com/research/files/B&C_Introduction.pdf

Cañibano L., Sánchez, P., García-Ayuso, M., and Chaminade, C. (2002). MERITUM Project. Guidelines for the management and dissemination of information on intangibles (Intellectual Capital Report). Vodafone Foundation.

https://dialnet.unirioja.es/servlet/libro?codigo=448252

Carini, Ch., Galera, G., Tallarini, G., Chaves, A., Sak, B. & Schoenmaeckers, J., (2024). *Benchmarking the socio-economic performance of the EU Social Economy*. European Commission.

https://eismea.ec.europa.eu/news/study-benchmarking-socio-economic-performance-eu-social-economy-now-published-2024-09-19_en

European Commission (EC, 2006). Reporting intellectual capital to augment research, development *and innovation in SMEs: report to the Commission of the High Level* Expert Group on RICARDIS (European Commission. Directorate General for Research ed.). Luxembourg: Office for Official Publications of the European Communities.

https://op.europa.eu/es/publication-detail/-/publication/60cbf27c-5552-429f-a077-44135a97cc27/language-en

Chen, Y. S. (2008). The positive effect of green intellectual capital on competitive advantages of firms. *Journal of Business Ethics*, (77)3, 271-286. https:// doi.org/10.1007/s10551-006-9349-1

Chen, H., Shih A. & S. Y. Yang, (2009). The Role of Intellectual Capital in Knowledge Transfer. IEEE Transactions on Engineering Management, (56)3, 402-411.

https://ieeexplore.ieee.org/abstract/document/5072284

Codina, L., Morales-Vargas, A., Rodríguez-Martínez, R. and Pérez-Montoro, M. (2020). Use of Scopus and Web of Science for research and evaluation in social communication. Comparative analysis and characterisation. Index.ComunicaciónN/Index Comunicación, 10(3), 235-261. https://doi.org/10.33732/ixc/10/03usodes.

Davenport, T. and Prusak, L. (2001). Knowledge in action. Buenos Aires: Prentice Hall. Argentina.

De Castro, G. and García-Muiña, F. E (2003). Hacia una visión integradora del capital intelectual de las organizaciones. Concept and components. ICE Economic Bulletin, Spanish Commercial Information, 2756, 7-16. https://dialnet.unirioja.es/servlet/articulo?codigo=303756

Delgado, M., Navas, J.E., Martín. G. & López, P. (2008). Technological innovation from the framework of intellectual capital. Cuaderno de Trabajo 04/2008. Complutense University of Madrid.

Demartini, C., & Trucco, S. (2016). Does Intellectual Capital Disclosure Matter for Audit Risk? Evidence from the UK and Italy. Sustainability, 8(9), 867. https://doi.org/10.3390/su8090867

Díaz B. F. and Lejarriaga G. (2019). Presentation of the monograph: Social entrepreneurship and employability. REVESCO. Revista de Estudios Cooperativos, 129, 9-15. https://doi.org/10.5209/REVE.62962

Diaz-Foncea M., Marcuello S. and Monreal G. (2016). Social economy and collaborative economy: Fit and potentialities. Industrial Economics, 402, 27-35 https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/402/D%C3%8DAZ%20FONCEA,%20MARCUELLO%20Y%20MONREAL.pdf

Dumay, J., Bernardi, C., Guthrie, J., & Demartini, P. (2016). Integrated reporting: A structured literature review. *Accounting Forum*, 40(3), 166-185. https://doi.org/10.1016/j.accfor.2016.06.001

Edvinsson, L. and Malone, M.S. (1999). Intellectual Capital. Barcelona: Gestión, 2000.

Fernández , D. J. Guevara, G. D. , Dávila T. L. and Cruz, J. J. (2022). Intellectual capital as a factor of organizational performance in Micro and Small Enterprises. Journal of Research in Communication and Development, 13(1), 63-73. https://doi.org/10.33595/2226-1478.13.1.595

Fernández-Solís, C., González-Ramírez, M. R., and Gascó-Gascó, J. (2025). The adoption intention of human resource analytics and its impact on organizational performance: a theoretical approach. *INNOVA Research Journal*, 10(1), 93-111. https://doi.org/10.33890/innova.v10.n1.2025.2706

Garanina T., Hussinki H., & Dumay J. (2021). Accounting for intangibles and intellectual capital: A literature review from 2000 to 2020, *Accounting & Finance*, forthcoming. https://doi.org/10.1111/acfi.12751

García-Flores, V. and Palma Martos, L. P. (2019). Social innovation: Key factors for its development in the territories. CIRIEC-Spain Revista de Economía Pública Social y Cooperativa, 97, 245-278. https://doi.org/10.7203/ciriec-e.97.14148

García-Flores, V. and Palma Martos, L. P. (2020). Third sector entities and social innovation. Characterising elements and success factors. REVESCO Journal of Cooperative Studies, 136, e71861. https://doi.org/10.5209/reve.71861

García-Porras, B. (2025). Presentation of the statistical report CIRIEC, Euricse and Spatial Foresight. Benchmarking the socio-economic performance of the EU Social Economy. https://ciriec.es/noticias/el-nuevo-informe-de-euricse-ciriec-internacional-y-spatial-foresight-impulsado-por-la-comision-europea-cifra-en-115-millones-las-personas-empleadas-en-la-economia-social-en-la-ue/

Grant, R. M. (1996). Toward a Knowledge-Based Theory of the Firm. Strategic Management Journal, 17, 109-122. https://doi.org/10.1002/smj.4250171110

Guthrie, J. & Abeysekera, I. (2006). Content analysis of social, environmental reporting: What is new?, Journal of Human Resource Costing & Accounting, 10(2), 114-126. https://doi.org/10.1108/14013380610703120

Hazan, E., Smit, S., Woetzel J., Cvetanovski, B., Krishnan, M., Gregg, B., Perrey J. & Hjartar, K. (2021). Getting tangible about intangible. The future of grow and productivity? Mckinsey Global Institute. https://doaj.org/article/faecfbdaace64e669c135ccadc104776

Haarhaus, T. & Liening, A. (2020). Building dynamic capabilities to cope with environmental uncertainty: The role of strategic foresight. *Technological Forecasting and Social Change*, 155. https://doi.org/10.1016/j.techfore.2020.120033

Jeffrey, S., Rosenberg, S. & McCabe, B. (2019). Corporate social responsibility behaviors and corporate reputation. *Social Responsibility Journal,* 15(3), 395-408. https://doi.org/10.1108/SRJ-10.11-2017-0255

Johnson, W.H.A. (1999). An integrative taxonomy of intellectual capital: Measuring the stock and flow of intellectual capital components in the firm. International Journal of Technology Management, 18(5-8), 562-575.

Lev, B. (2001). *Intangibles: Management, Measurement, and Reporting*. Washington DC: Brookings Institution Press. http://www.jstor.org/stable/10.7864/j.ctvcj2rf2

Li, X., Nosheen, S., Haq, N. U., & Gao, X. (2020). Value creation during fourth industrial revolution: Use of intellectual capital by most innovative companies of the world. *Technological Forecasting And Social Change*, 163, 120479. https://doi.org/10.1016/j.techfore.2020.120479

López P., Martín de Castro, G., and Navas, J.E. (2004). An approach to the relationships between elements of intellectual capital in organisations. ICE Economic Bulletin (2817). https://www.revistasice.com/index.php/BICE/article/view/3626/3626

Maqbool, S., Rasool, H., & Ahmad, S. (2018). Corporate Social Responsibility and Financial Performance: An Empirical Analysis of Indian Banks. Future Business Journal, 4(1), 2314-7210. https://doi.org/10.2139/j.fbj.2017.12.002

Magau, M. D., Roodt, G., & van Zyl, G. (2021). A measurement scale for assessing intellectual capital disclosure. *Journal of HumanResource Management, 19,* 1-14. https://doi.org/10.4102/sajhrm.v19i0.1645

Merino C., Alonso, M., González, N., & Plaz, R. (2018). Knowledge management in organisations in the nuclear sector. National University of Distance Education (UNED).

Ministry of the Interior (GC, 2023). Guardia Civil 2023 Sustainability Report. https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/memoria-RSC-Sostenibilidad-de-la-Guardia-Civil/Memoria-sostenibilidad-GC_126230302_pdfWEB.pdf

Ministry of Labour and Social Economy (MITES). Informe de evolución y Tendencias en el ámbito de la Economía Social (2023). Spanish Social Economy Business

Confederation (CEPES). https://www.fundae.es/docs/default-source/publicaciones-y-evaluaciones/publicaciones-econom%C3%ADa-social/1-1-evoluci%C3%B3n-y-tendencias-de-la-ec-social_2023.pdf

Mohdzaini, H. (2021). Technology and the future of work: How artificial intelligence (AI) robots and automation are shaping the world of work, m the ethical considerations and the role of people professionals. CIPD. https://www.cipd.org/uk/knowledge/factsheets/emerging-future-work-factsheet/

Moreiro J. A., Morato J., Sánchez S. y Rodríguez B. A., (2006). Categorization of concepts in content analysis: its signalling from classical Rhetoric to Topic Maps. Investigación Bibliotecnológica: Archivonomía, bibliotecología e información, *20*(40). https://doi.org/10.22201/iibi.0187358xp.2006.40.4097

Navarro González A. and Medina Jiménez, A., (2024). Relación del Capital intelectual con el capital humano, estructural y relacional. Transcender Contabilidad y Gestión, 9(26), 100-127. https://doi.org/10.36791/tcg.v9i26.260

Nonaka, I. & Takeuchi, H. (1995). *The knowledge creating company*. New York: Oxford University Press.

Nonaka, I. & Konno, N. (1998). The Concept of Ba: Building a Foundation for Knowledge Creation. California Management Review, 40, 40-54. https://doi.org/10.2307/41165942

Nonaka, I., & Takeuchi, H. (2021). Humanizing strategy. Long Range Planning, 54(4), 102070. https://doi.org/10.1016/j.lrp.2021.102070

Oliveira, M., Curado, C., Balle, A. R., & Kianto, A. (2020). Knowledge sharing, intellectual capital and organisational results in SMES: are they related? Journal of Intellectual Capital, 21(6), pp. 893-911. https://doi.org/10.1108/JIC-04-2019-0077

Organisation for Economic Co-operation and Development (2006). Creating Value from Intellectual Assets. Meeting of the OECD Council at Ministerial Level.

Pedreño, J., (2024). The social economy and The EU 2024-2029 Objectives. Europe Social Economy. https://www.socialeconomy.eu.org/2024/10/22/great-sucess-of-the-event-the-social-economy-and-the-eu-2024-2029-objectives/

Petty, R., & Guthrie, J. (2000). Intellectual capital literature review. *Journal Of Intellectual* Capital, 1(2), 155-176. https://doi.org/10.1108/14691930010348731

Porter, M. (1996). What is strategy? *Harvard Business Review 74*(6), 61-78. https://iqfystage.blob.core.windows.net/files/CUE8taE5QUKZf8ujfYlS_Reading+1.4.pdf

Retolaza, J. and Alzola, M. (2021). Applying social value in organisations. Bulletin of Economic Studies, 76(232), 19-22. https://doi.org/10.18543/bee.2383

Rideg, András, Szerb, László, & Róza Varga, Anna (2023). The role of intellectual capital on innovation: Evidence from Hungarian SMEs. Tec Empresarial, 17(2), 1-19. https://www.researchgate.net/publication/370608181_The_role_of_intellectual_capital_on_innovation_Evidence_from_Hungarian_SMEs

Roos, J. (2001). Intellectual capital: the intangible value of the firm. Barcelona: Paidós.

Sánchez-Espada J., Martín S., Bel P. and Lejarriaga G. (2018). Education and training in social entrepreneurship: characteristics and sustainable social value creation in social entrepreneurship projects. REVESCO. Journal of Cooperative Studies, 129, 16-38. http://dx.doi.org/10.5209/REVE.62492

Secundo, G., Ndou, V., Del Vecchio, P., & De Pascale, G. (2020). Sustainable development, intellectual capital and technology policies: A structured literature review and future research agenda. Technological Forecasting And Social https://doi.org/10.1016/j.techfore.2020.119917

Stratone, M. (2023). A Bibliometric Analysis of the Role of the Intellectual Capital in the Organizational Agility and Performance. Proceedings Of The International Conference On Business Excellence, 17(1), 1275-1285. https://doi.org/10.2478/picbe-2023-011

Steward, T. (1997). The New Wealth of Organisations: Intellectual Capital Buenos Aires: Ediciones Granica S.A.

Suciu, M., & Năsulea, D. (2018). Intellectual Capital and Creative Economy as Key Drivers for Competitiveness Towards a Smart and Sustainable Development: Challenges and Opportunities for Cultural and Creative Communities. In: Intellectual Capital Management as a Driver of Sustainability. https://doi.org/10.1007/978-3-319-79051-0_5

Sumedrea, S. (2013). Intellectual Capital and Firm Performance: A Dynamic Relationship in Crisis Time. *Procedia Economics And Finance, 6*, 137-144. https://www.sciencedirect.com/science/article/pii/S2212567113001251?via%3Dihub

Teece, D.J., Pisano, G. & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509-533.

Thum-Thysen, A., Voigt, P., & Weiss, C. (2021). Refections on Complementarities in Capital Formation & Production: Tangible & Intangible Assets across Europe. Euopean Commission/EuropeanEconomy[online]https://economy-finance.ec.europa.eu/document/download/3ddd17a1-0d58-4614-a363-90a9e6a12e9c_en?filename=dp152_en.pdf

Wang, C.N., Chang, Y.L., Huang, Q.H. & Wang, C.H. (2011). Assessment on intellectual capital management for Taiwanese pharmaceutical industry: using GRA and MPI. African Journal of Business Management 5(7), 2950-2958.

https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=78a492920f297eb118e7972ef4ad52ce99ec2355

Word Bank Group (2024). Annual Report 2024. https://openknowledge.worldbank.org/bitstreams/91a20260-c3c4-4ed7-a488-d7dd8d419c8a/download

Xu, J., & Wang, B. (2018). Intellectual Capital, Financial Performance and Companies' Sustainable Growth: Evidence from the Korean Manufacturing Industry. Sustainability, 10(12), 4651. https://doi.org/10.3390/su10124651.

Zheng S., Zhang W., Wu X. & Du J. Know ledge-based Dynamic capabilities and innovation in networked environments. Journal of Knowledge Management 15(6), 1035-1051.

ORCID: Https://orcid.org/0009-0000-2569-3710

Annex I

Tables 4-6: Sampling units and definition of IQ dimensions in the Institution

ELEMENTOS DIMENSIÓN CAPITAL HUMANO		
Códigos	Unidad Muestral	Definición
CHIDENTIDAD	Pertenencia y compromiso.	Identificación de las personas como guardias civiles dentro de la Institución.
CHMOTIVACION	Automotivación	Los impulsos conscientes que hacen a los guardias civiles conseguir desempeñar el servicio con excelencia.
CHSATISFACCION	Satisfacción	Forma de participar en el desempeño de su trabajo y comportamientos de los guardias civiles en la Institución. Evaluación desempeño.
CHCREATIVO	Creatividad. Cultura innovadora	Creación de ideas nuevas y aplicables al desempeño del servicio. La forma de impulsar los pensamientos nuevos, ideas y actitudes por la Institución para generar nuevas formas de actuación o una mejora de las existentes.
CHEDUCACION	Educación reglada.	Conocimientos explícitos que posee en general los guardias civiles.
CHESPECIALIDAD	Formación especializada.	Conocimientos específicos de una especialidad concreta o trabajo técnico en la Institución
CHUNIVERSITARIO	Inversión en formación Universitaria.	Centro Universitario Guardia Civil (CUGC).
CHFORMACION	Formación interna.	Conocimientos adquiridos mediante programas, jornadas, talleres, y todos los cursos de formación que comprenden la capacitación y promoción interna en las Academias y en el Centro Universitario de la GC.
CHEXPERIENCIA	Experiencia.	Conocimientos adquiridos mediante el desempeño realizado en la Institución.
CHDESARROLLO	Desarrollo personal.	Conocimientos adquiridos informalmente en la Institución. Personas que promocionan. Promoción interna.
CHAPRENDIZAJE	Aprendizaje	Adquisición de nuevos conocimientos. Jornadas PATIO Y SIO.
CHCIVIL	Colaboración, personal civil.	Capacidad de trabajar con otras personas: compañeros, personal administraciones públicas. Personal civil funcionariado.
CHCONCILIA	Conciliación vida familiar profesional	Favorecer el equilibrio entre la vida familiar y la laboral a los guardias civiles. Compatibilizar la vida profesional y familiar.
CHLIDERAZGO	Liderazgo.	Guiar y mover a los compañeros hacia el desempeño de un servicio con excelencia y otras personas relacionadas con el servicio.

ELEMENTOS DIMENSIÓN CAPITAL ESTRUCTURAL

Códigos	Unidad Muestral	Definición
CECULTURA	Homogeneidad cultural.	Aceptación de los valores de la Guardia Civil.
CECLIMA	Clima social-laboral.	Ambiente generado en la unidad, departamento o equipo de trabajo. Índice de clima social.
CEIGUALDAD	Sensibilidad género. Igualdad.	Introducción de la perspectiva de género en la Institución. Igualdad de condiciones entre hombres y mujeres acceso mismo puesto bajo las mismas condiciones e iguales requisitos
CESTRUCTRURA	Diseño organizativo. Plantilla. Delimitación competencias	Estructura de la Institución que establece las relaciones laborales. Distribución. Competencias funcionales.
CEDESARROLLO	Desarrollo organizativo.	Acontecimientos que propician adaptación a las situaciones actuales. Regulación de Jornadas y horarios en general.
CERUTINAS	Pautas organizativas. Procedimientos establecidos y sistemas.	Procedimientos y rutinas establecidos o nuevas competencias para mejorar la Institución. Mejora de las funciones a desempeñar por los guardias civiles, mejorando su calidad profesional y aumentando su motivación.
CERELACIONINT	Explicación de la estrategia a su personal.	Procesos dirigidos a explicar a los componentes de la Institución su Estrategia, visión, misión e innovación. Introducción de algo nuevo o modificación de lo anterior que provoque un mejor desempeño en el servicio.
CECRIMINAL	Actuaciones, denuncias e infracciones administrativas.	Procesos dirigidos a explicar, numerar y contextualizar las detenciones, denuncias e infracciones administrativas.
CEPROVEEDORES	Contratación proveedores.	Conjunto de procesos de proveedores, alineados a los valores de la Institución. Contratación pública socialmente responsable (CPSR).Orientado a los riesgos laborales, reciclaje y medio ambiente.
CEINVERSIONIDi	Inversión I+ D+ i. Dominios de sus sedes electrónicas.	Inversión económica en investigación y desarrollo. Gastos elaborados por su funcionamiento al desarrollar acciones innovativas, conferidas como espacios virtuales de uso exclusivo por la Institución. Dominios internet.
CEPERSONALIDi	Personal I+D+i.	Plantilla de plena dedicación a investigación y desarrollo.
CEPROYECTOSIDi	Proyectos I+D+i. Programa Marco UE. Programa Horizonte 2020.	Trabajos realizados relacionados con la innovación y el desarrollo. Proyectos generados en concordancia con el proceso innovativo con otras organizaciones o de forma independiente.
CEINFRAESTRUCTURA	Infraestructuras y material.	Mantenimiento de las instalaciones. Inversión en instalaciones e infraestructuras.
CEEQUIPOPOLICIAL	Equipamiento policial. Dotación tecnologías de producción.	Productos y herramientas adecuadas a las necesidades particulares de la Institución. Conjunto de equipos tecnológicos necesarios para el cumplimiento de un servicio.
CEINNGEST	Innovación de gestión. Innovación de modelo de Institución.	Herramientas nuevas y procedimientos compartidos en la Institución que impulsan la innovación. Transformación digital.
CECOMUNICACIONGC	Comunicación interna Relaciones asociaciones. Consejo.	Sistemas informáticos, telecomunicaciones útiles funcionamiento de la Institución. Facilidad y buena actitud en la transmisión de los conocimientos e información para la ejecución de un servicio con las personas adecuadas para ello. Atención al guardia civil.
CEMARCA	Marcas registradas. Imagen de la GC	Marca, logo y emblemas en la Institución. Referencia a los uniformes.
CELICENCIAS	Licencias forenses, subscriptores.	Procesos por el que se comparte una parte de los procesos y conocimientos de la Institución. Convenios con otras administraciones y universidades.
CESECRETO	Protección de datos.	Todos los considerados por la Institución como tales. Protección de datos (ciudadanos).
CEPATENTES	Información patentes.	Base de datos registren cantidad y uso de patentes empleadas por la Institución.
CETECNOEXT	Conocimiento actividad tecnológica competencia.	Bases de datos e información disponible sobre los avances en I+D de los competidores.
CETECNONEW	Información sobre líneas investigación y tecnología emergente.	Bases de datos de información sobre tecnología emergente que afecte a la Institución. Conocimiento posibles asociaciones con empresas para I+D.
CETECLIC	Localización tecnología sobre la que buscar licencias	Fuentes de datos sobre tecnologías útiles para ser desarrolladas en la Institución.
CEFLEXIBILIDAD	Flexibilidad y adaptabilidad.	Comportamiento favorable hacia el cambio por las situaciones derivadas del servicio o de la Institución.
CETALENTOS.	Antigüedad y fidelización de los guardias civiles.	Permanencia de los empleados basada en políticas de retención y atracción de guardias civiles que aportan valor a la Institución. Situaciones.

ORCID: Https://orcid.org/0009-0000-2569-3710

ELEMENTOS DIMENSIÓN CAPITAL RELACIONAL

Códigos	Unidad Muestral	Definición
CRCIU	Base ciudadanos.	Ciudadanos en general.
CRLEALCIU	Lealtad ciudadanos.	Grado de fidelidad que procesan los ciudadanos a la Institución. Primera opción en seguridad.
CRSATISFACCION	Satisfacción ciudadanos. Seguridad pública.	Grado de eficacia que el ciudadano percibe en la cumplimentación de un servicio y en general con la Institución. Felicitaciones atención al ciudadano.
CRQUEJAS	Quejas, reclamaciones y sugerencias ciudadanos.	Quejas recibidas por la prestación de un servicio y sugerencias. Atención a la ciudadanía. Oficina de Información y Atención al Ciudadano(OIAC). Puntos de Atención Especializada (PAEs).
CRPROTCIU	Procesos relación ciudadanos. Protocolos ciudadanos.	Protocolos de actuación y comportamiento con los ciudadanos. Turismo seguro. Trata de seres humanos (TSH). Mayores seguros. VdG. Menores. Víctimas de terrorismo.
CRESTADO	Relaciones Estado y UE. Accionistas e inversiones institucionales.	Grado de inversiones; recursos disponibles; presupuestos.
CRIADMINISTRACION	Relaciones Institución mercado. Relaciones con otros grupos de interés Administración.	Relaciones con otros grupos de interés de la Institución. Administración general ACCEDA; Firma digital. Partidos políticos. Firma convenios administraciones.
CRCAPITALEXTERIOR	Relaciones participación empresarial.	Capital de la Institución en otras entidades.
CRALIANZAS	Base aliados.	Alianzas con otras instituciones dentro de su área de seguridad. Relacionados con la creación de conocimiento, y su transferencia impulsando la innovación.
CRALIANZASESTABLES	Solidez alianzas. Servicios conjuntos. Estabilidad alianzas y formalización.	Formas establecidas de cooperación con policías misma área de seguridad. Innovación internacional. Nuevas formas en otros países que contribuyan al desarrollo o diversificación de la Institución o sus competencias. Misiones encomendadas por el Ministerio de Defensa.
CRALIANZASBENEFICIO	Beneficio alianzas. Resultados obtenidos alianzas.	Generación de beneficios de las alianzas establecidas. Ayuntamientos Seguridad Ciudadana y Seguridad Vial. Protección civil.
CRCONCOMPETENCIA	Conocimiento competidores.	Conocimiento otras policías en la compartición de las competencias de seguridad.
CRPRIVADA	Relaciones seguridad privada.	Grado beneficios obtenido relaciones con otros grupos de interés. Seguridad privada.
CRCERTICAL	Certificaciones y sistemas calidad.	Certificados de calidad otorgados a la Institución. Premios (SEPRONA); Igualdad.
CRREDES	Portal guardia civil exterior. Información divulgada redes.	Canales de comunicación en la Institución basado en la tecnología. Notas de prensa e información comparte Institución en Redes Sociales. Información pública.
CRADMINISTRACION	Colaboración Adm. Públicas. Cooperación para el desarrollo.	Cooperación con otras administraciones nacionales e internacionales de la Institución. Ministerios. Compras públicas innovadoras firma de Convenios con otras administraciones.
CRMEDIOS	Relaciones medios comunicación convencionales.	Exposición de la institución medios de comunicación. TVE; radio; periódicos. Medios más convencionales.
CRDEFENSAMBIENTE	Relaciones instituciones defensa medioambiental.	Grado de efectividad con otros grupos dedicados a la defensa del medioambiente.
CRVERDE	Códigos y certificaciones medio ambientales.	Procedimientos y protocolos establecidos interiorizados por la Institución en la defensa del medioambiente.
CRMERCADO	Relaciones instituciones mercado trabajo.	Relaciones institución con el mercado laboral. Contribución al tejido empresarial Oferta empleo público (OEP).
CRCODIGOCON	Código de conducta.	Nuestro código es normativo. Normas explícitas establecidas de comportamiento recogidas en el Reglamento. Código Penal Militar.
CRACSOCIAL	Acción social al ciudadano. Preocupaciones sociales	Espíritu Benemérito. Comportamiento adecuado y correcto del personal especialmente con los ciudadanos en el desempeño del servicio. Responsabilidad con la sociedad, desarrollo económico, solidaridad e integración social.
CRBUENGOBIERNO	Dirigidos a los ciudadanos. Buen gobierno.	Procesos dirigidos a la catalogación de los ciudadanos, sus riesgos y necesidades. Código buen gobierno de la AGE. Difusión de buenas prácticas. Transparencia, responsabilidad y eficacia con todos los grupos de interés. Compromiso adquirido voluntario por la Institución como forma de rendir cuentas a la sociedad a la que sirve.

Annex II

Examples of calculation of an index of an element, belonging to each category.

Categoría Capital Humano

Elemento: *CHEducación*.

$$\text{I CHEducación } = 1/14 \sum_{i=1}^{14} j = \text{I CHEducación } \textit{cuanti} + \text{I CHEducación } \textit{cualit} + \text{I CHEducación } \textit{gráfico}$$

Categoría Capital Estructural

Elemento: *CERutinas*.

$$\text{I CERutinas } = 1/25 \sum_{i=1.}^{25} j = \text{I CERutinas } \textit{cuanti} + \text{I CERutinas } \textit{cualit} + \text{I CERutinas } \textit{gráfico}$$

Categoría Capital Relacional

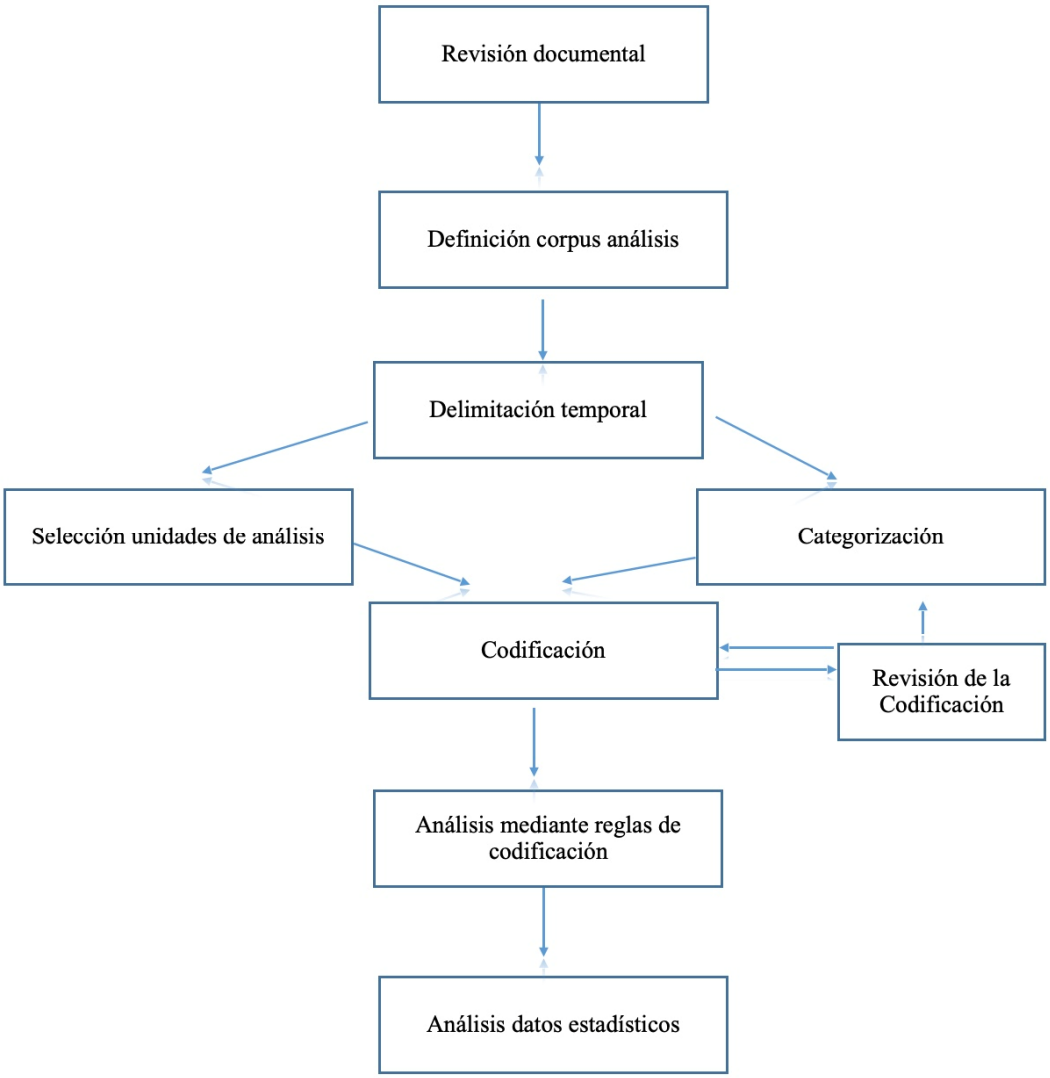
Elemento: CRLealciu.

$$\text{I CRLealciu } = 1/23 \sum_{i=1.}^{23} j = \text{I CRLealciu } \textit{cuanti} + \text{I CRLealciu } \textit{cualit} + \text{I CRLealciu } \textit{gráfico}$$

ORCID: Https://orcid.org/0009-0000-2569-3710

Annex III

Phases developed in the content analysis



Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

III.- CASE LAW REVIEWS

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Case law review

REVIEW OF JURISPRUDENCE 2ND CHAMBER SUPREME COURT

English translation with AI assistance (DeepL)

Javier Ignacio Reyes López
Magistrate of the 46th Examining Magistrate's Court of Madrid
Diploma of Advanced Studies (DEA)
ji.reyes@poderjudicial.es

Received 06/06/2025
Accepted 06/06/2025
Published 27/06/2025

Recommended citation: Reyes, J. I. (2025). Reseña de jurisprudencia Sala 2ª Tribunal Supremo. *Revista Logos Guardia Civil*, 3(2), p.p. 295-320.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

REVIEW OF CASE LAW 2ND CHAMBER SUPREME COURT

Summary: STS 350/2025, of 10 April. Concept of interested party in a home search. 2.- STS 358/2025, of 10 April 2025. Criminal news transferred to Spain by a foreign judicial authority and continuation of the investigation in our country with new investigations. 3.- STS 324/2025, of 07 April 2025. Conservation of communications data. 4.- STS 294/2025, of 28 March 2025. Principle of insignificance and toxicity in crimes against public health. 5.- STS 8/2025, Criminal Section 3ª, of 2 April 2025. Offence of havoc for terrorist purposes. 6.- STS 308/2025, of 2 April 2025. Police investigation in Spain arising from knowledge of an EPO issued by the judicial authorities of another country for another criminal offence. Presence of detainees in a house search. 7.- STS 295/2025, of 28 March 2025. Crime of harassment, "stalking". 8.- STS 284/2025, of 27 March. Sexual abuse of a 17 year old with borderline intelligence. Moral damage.

1.- STS 350/2025, of 10 April. Concept of interested party in a home search .[1]

Factual background.

The Juzgado de Instrucción nº 5 of Marbella opened abbreviated proceedings nº 104/2018 for an alleged crime against public health against Noelia, among others, which, once concluded, was referred for trial to the 1st Section of the Provincial Court of Malaga. The abbreviated procedure nº 1004/2019 was opened on 17 May 2021, and the Court handed down sentence nº 233/2021, in which it declared as proven that, "....Taking into account the evidence, it is expressly and categorically declared as proven that the Urban Crime Group of the CNP Marbella Police Station carried out a surveillance operation in order to detect the sale of substances in area xx of Marbella, which is located between the Ermita Industrial Estate and the Boulevard of Avenida José Manuel Valles and next to a school, a frequent and well-known point for its conflict and for being a point for the sale and consumption of drugs. They became aware of the existence of the "Chatos" clan dedicated to the sale of narcotic substances through properties located in this shantytown, as they were aware that their residents could be involved in the sale of narcotic substances, as there was a daily flow of people making short visits. As a result of the surveillance, exhaustive observation, interception and successive seizure, by means of reports of drugs from people who had specifically come to buy in the homes under investigation, the following reports are collected...and subsequently, based on the police request, by the Court of Instruction no. 5 of Marbella, an order was issued on 4 June 2018 authorising the entry and search, among others, in the various homes in which narcotic substances were seized and the investigated persons were arrested...".

Legal basis.

An appeal in cassation is being lodged with the Supreme Court against judgment number 197/2022, of 14 July 2022, handed down by the Civil and Criminal Division of the High

[1] STS 350/2025, Penal section 1 of 10 April. Published on the website of the Judicial Documentation Centre, CENDOJ, (ROJ: STS 1701/2025 - ECLI:ES:TS:2025:1701), appeal no. 7569/2022. Rapporteur, Mr Eduardo de Porres Ortiz de Urbina.

Court of Justice of Andalusia, Ceuta and Melilla, which rejected the appeal lodged against judgment number 233/2021, of 17/05/2021, of the 1st Section of the Provincial Court of Malaga, convicting of an offence against public health. Of the four persons convicted, only one has lodged an appeal.

The first ground of appeal alleges that the contested judgment violated the right to privacy in the home of Article 18.2 EC and the right to a trial with all the guarantees recognised in Article 24.2 of the Constitution.

She claims that she was in custody at the time of the house searches and could only be present at one of them (the house from which she was leaving when she was arrested) and not at the other houses, in respect of which a criminal connection was attributed to her.

The defence understands that the presence of the interested party is an inexcusable requirement for a home search in accordance with art. 569 LECrim, being null and void any home searches that do not comply with this requirement when the interested party is detained and there is no other reason that makes this impossible, and therefore it is not admissible as evidence for the prosecution, nor are the statements of the police officers who intervened in the searches admissible as evidence for the prosecution.

It considers that, in the present case, the invalidity of the search leads to the impossibility of legally affirming the discovery of the substance and objects from the possession of which the conviction for the crimes against public health and illegal possession of weapons stems, and that this seizure cannot be sanctioned by means of the testimony of the officers present at the search, as their respective testimonies are directly linked to the unlawful action.

This issue was raised in the previous appeal and the arguments for its rejection are ours.

In this procedure, seven simultaneous searches were carried out and in five of them, the search was carried out in the presence of the persons concerned in each of the properties, except in two of them, where no one was found and the search was carried out, as in the others, under the supervision of the Legal Advisor for the Administration of Justice.

The appellant was present at the search of her home and could not have been present at the other homes because the searches were simultaneous and because, in principle, she was not a resident of the other homes and was neither located nor arrested. Her arrest took place precisely at the time of the search.

The article 569 of the LECrim stipulates that the search of a private home will be carried out in the presence of the interested party or the person who legitimately represents them. The case law of this Chamber has been hesitant when it comes to specifying what should be understood by "interested party", since in some judgments this has been taken to mean the person who owns the affected home, as the holder of the right to privacy affected by the interference (SSTS. 18.7.98, 16.7.2004, and 3.4.2009), while other rulings have considered that the person who is the object of the police investigation has this character, insofar as they have a direct interest in the result of the search due to

the procedural and criminal repercussions that may derive from its development (SSTS 27.10.99, 30.1.2001 and 26.9.2006). This last position is the majority one, so that the presence of the interested party is required in the proceedings, even if they are not the owner of the home in the event that the interested party is detained. In STS 771/2010, of 23 September, followed by many others, it was stated that case law is certainly uniform in requiring the presence of the interested party - the person under investigation - in the search in those cases in which they are detained and even in the event that they are different from the owner of the home or the latter is present or refuses to be present at the search. Such presence, if possible, is required due to the contradictory requirements that must surround any evidentiary procedure and even more so due to the characteristics of home searches in which the absence of contradiction in the act of the search itself cannot be fulfilled due to the contradictory activity that makes the debate of the oral trial possible. Therefore, if the interested party is detained, his presence in the search is obligatory, and the exceptions established in paragraphs 2 and 3 of art. 569 LECrim do not apply (SSTS. 833/97 of 20.6, 40/99 of 19.1, 163/2000 of 11.2, 1944/2002 of 9.4.2003).

However, there are cases in which this presence is not possible and there are various circumstances that may make this presence impossible: that the person under investigation cannot be located, that they do not want to attend if they are not detained and that they are physically unable to do so, as occurs in cases of simultaneous searches. In the latter case, this has been recognised by this Chamber in numerous rulings, such as SSTS 947/2006, of 26 September, 771/2010, of 23 September and 199/2011, of 30 March.

In this case the appellant was present at the search of her home and was not present at the other searches because they were carried out simultaneously.

The plea is therefore dismissed and the judgment under appeal is upheld in its entirety.

Conclusions.

On few occasions has the SC maintained such a uniform line on who should be considered to be interested in an entry and search, being the person who, regardless of the formal title held with respect to the home, may be legally affected by its result in the crime under investigation. The practical problems between successive and simultaneous searches are also described, so that the interested party can attend this procedure, unless for exceptional reasons or force majeure it is not feasible to do so.

2.- STS 358/2025, of 10 April 2025. Criminal news transferred to Spain by a foreign judicial authority and continuation of the investigation in our country with new police investigations .[2]

Factual background

In case no. 33/2021 (stemming from PA 25/2021 of the Juzgado de Instrucción nº 3 de Talavera), followed before the Audiencia Provincial de Toledo, Sección 1ª, on 5 May 2022, Evelio was convicted as the author of a crime against public health for drug trafficking, which contains the following proven facts:"...As a result of a communication sent by the Public Prosecutor's Office in Portugal, it became known that there could be an organised group that from South America was responsible for sending cocaine to Europe, at least to Spain and Portugal, and that for this purpose they used boats that called at the port of Oporto. And from that town, at least in part, the cocaine was transported by lorry to the town of Talavera La Nueva, where it was unloaded in an industrial warehouse bearing the Puertas Artevi label. As a result of this information, the Udyco began an investigation which resulted in verifying that the information regarding the arrival of lorries at the warehouse was true, so they began a series of surveillance and monitoring which allowed them to discover that the warehouse was rented by the accused Evelio, born in 1984, with no criminal record, who had also rented a warehouse in the town of Ventas de Retamosa and a storage room, with the number, owned by the company Blue Space, from Leganés. By order of 22 December 2020, the Court of First Instance and Preliminary Investigation number three of Talavera authorised the entry and search of the aforementioned warehouses and the storage room. Seven rectangular packages were found in the storage room, containing a white substance, to which the appropriate reagent was applied, testing positive for cocaine. After the corresponding analysis, the substance turned out to be cocaine, with a total weight of six thousand ninety-six grams and an average richness of 77.88%, and whose value on the illicit market would amount to the sum of two hundred and thirty-eight thousand three hundred and sixty-nine and thirty-one euros, which the accused possessed for distribution among third parties. It has not been proven that the other defendants, Gaspar, born on NUM002 1969, with no criminal record, and Jacinta, born in 1991, who was convicted in the sentence of 16 June 2020 for an offence against public health, were related to the substance seized...".

Legal basis

The appellant seeks the annulment of the order ordering the tapping of the defendant's telephones, and of the order of 29 July 2020, by which it was extended, as well as further tapping, requests which were made for the first time as a preliminary question to the start of the trial, and which were already rejected by the court of first instance on the basis of correct arguments.

The plea, as we have said, coincides with that raised on appeal with the sole difference that it transcribes a paragraph of the STSJ, but with which it does not debate, repeats that the nullity of the aforementioned orders is based on the lack of reasoning and

[2] STS 35872025, of 10 April 2025, published on the CGPJ website by the Judicial Documentation Centre, CENDOJ, (ROJ: STS 1628/2025 - ECLI:ES:TS:2025:1628). appeal: 8375/2022. Speaker: Mr. Ángel Luis Hurtado Adrián.

justification, as they lack purpose and go beyond the provisions contained in the framework of collaboration between the Spanish authorities and the Portuguese authorities, and the irregularity attributed to those orders is because the persons where the drugs were to be stored and hidden were already identified by means of police surveillance carried out on 14, 15, 17 and 19 May, so that, in the appellant's opinion, there is no basis and no legal basis for the request by the police to authorise telephone tapping 25 days later.

It is alleged that the object of the surveillance was the arrival from Portugal of a lorry with a shipment to be deposited in the warehouse on 14 May 2020, and that, having the arrival and unloading under surveillance, it is logical that the police intervention should have been carried out on that day or the following days, and that if it is not carried out, it is because there is no certainty that the drugs came there, If this is the case and 25 days later the telephone tapping is agreed, the signatory of the appeal considers that this is a prospective investigation, because at that time there is no evidence that any crime is being committed or is going to be committed, and repeats once again that, when the order in question was issued, there was no "good reason" or "strong presumption" to justify this intervention, and does so without putting forward any argument to the considerations that, in order to reject such an approach, the first instance judgement and then the appeal judgement gave him, when he is reiterating, once again, a claim with such traumatic consequences as a nullity for considering the investigation prospective, to which he should have given considerably more extension after having rejected it on two previous occasions.

The appellant's approach is based on linking the police action which took place from the 14th, as a result of information received from the Portuguese authorities, with the investigation which is the subject of the present case, and this is apparent from a reading of the proven facts, which refers to the communication sent by the Portuguese Public Prosecutor's Office, which revealed the existence of an organised group responsible for sending cocaine to Europe, which arrived via the port of Oporto and from there was transferred, at least in part, to the industrial building with the label Puertas Artevi in the town of Talavera de la Reina, rented by Evelio, around which an investigation was being carried out in Portugal, which led to the issuing of a European Investigation Order by the Public Prosecutor's Office of Oporto, requesting certain proceedings in our country, and which, as stated in order of 22 December 2020, by order of 29 June 2020, it was agreed to recognise and execute, Among the measures taken was the interception of certain telephones, including that of the aforementioned Evelio, which was extended by the order of 29 July 2020 and was annulled by the order of 18 September 2020, a Portuguese investigation in which there is no record that he had ever been charged.

The police investigations continued in our country, through the Udyco, by means of surveillance and monitoring, establishing that, among other things, the aforementioned Evelio was carrying out security measures, as stated in the order, indicative of a presumed criminal activity related to a drug trafficking offence, different and subsequent to that which could be the subject of investigation in Portugal, since, as the lower court's judgment explains, "there is no evidence that the defendants were prosecuted in the neighbouring country, so that the investigation could not be limited solely to the identification of the possible perpetrators who in Spain committed the acts which are the subject of criminal proceedings in Portugal".

In any case, the initial information, even if it came from Portugal, provided elements which justified the adoption of measures taken by the examining magistrate, including the one limiting fundamental rights, such as the agreed telephone tapping, which therefore cannot be considered to have been given in the course of a prospective investigation, but at the same time it was useful in order to investigate the presumed criminal activity being committed in Spain, and to maintain the contrary, as argued by the M.F., is "reasoning which is difficult to maintain, insofar as the appellant seems to claim that in the investigation of a crime of which there is prior knowledge, one has to renounce investigating the existence of other possible participants in a crime, is "difficult reasoning to maintain, as the appellant seems to claim that in the investigation of a crime of which there is prior knowledge, it is necessary to renounce investigating the existence of other possible participants in a crime as serious as in the present case".

This is precisely explained in the judgment under appeal, which sets out the reasons why the facts investigated in Portugal must be disassociated from those which were to be investigated in our country, even though in both cases they were related to drug trafficking offences, because the rupture between the two is evident, and each one, making our own the words we have just transcribed from the M.F., should give rise to its own investigation, The judgment under appeal also explains this, which differentiates between the Portuguese and Spanish investigations, when it says that "the investigation did not have to be limited only to the identification of the persons and the place where they were hiding drugs, because it was not a matter of collaboration with the Portuguese authorities with regard to facts that were the subject of criminal proceedings in Portugal, nor is there any record of criminal proceedings against the accused in that country, but rather it was a question of information sent by the Portuguese Public Prosecutor's Office to the Spanish police on facts from which the possible commission of a crime in Spain could be deduced, incorporating objective data indicative of criminal activity in our country, such as the arrival of a ship, the loading of coils, the transport companies and, above all, the destination in Spain of the material loaded in Portugal".

In short, given that the examining magistrate had sufficiently plausible indications to assess the presumed commission of a drug trafficking offence in our country, even if they were provided by information from Portugal, it is not possible to speak of a prospective investigation, because this information is what provided him with these elements, in line with which he adopted the investigative measures he considered appropriate, including the tapping of the telephone of one of those presumably involved in it, which he justified at sufficient length in his order of 29 June 2020 and also in the extension order of 29 July 2020.

The appeal is dismissed in its entirety and the appellant's conviction is upheld.

Conclusions.

The SC assesses the scope of an OEI formally sent from the Portuguese judicial authority to the national judicial authority, as an instrument of cooperation that entailed some measures restricting fundamental rights. When that line of investigation did not prosper and was not completed, nor was an independent criminal procedure followed in Portugal on the same facts, the Spanish Judicial Police added to that information new data on the persons under investigation and possible criminal acts committed in Spain, and initiated

a procedure which, on the basis of the first, made it possible to dismantle a criminal group dedicated to the commission of serious crimes.

3.- STS 324/2025, Penal section 1 of 07 April 2025. Retention of communications data .[3]

Factual background

The Provincial Court of Barcelona, 7th Section handed down sentence no. 173/2023 of 3 March, arising from summary proceedings no. 1/2021 of the Sant Boi de Llobregat Court of Instruction no. 1, followed for a crime against public health, which contains among others the following proven facts:"...they are proven facts, and it is thus declared, that since at least in the month of August 2018 the defendants Jenaro, Humberto, Fermín, Lucas and Emiliano formed a personal, material, corporate and logistical framework placed at the service of a common plan which was to get hold of cocaine hidden in a container from Brazil that would arrive at the port of Barcelona in mid-December, to proceed to its distribution in the latter province. Jenaro was at the top of the network, providing it with financial cover and contacts to obtain the drugs; Humberto was in charge of management and coordination. Fermín was in charge of the corporate and business structure capable of getting hold of the shipment by passing it off as a legal purchase and sale of Din-A4 sheets of paper, Lucas was in charge of the logistics, especially the organisation of the transport of the substance, which Emiliano would be in charge of, delegating it to third parties.

In execution of this criminal plan, the company Campderros Salvans S.L., acquired, through Fermín, 1.600 boxes of DIN-A4 sheets of paper from the company Precisión Comercio Internacional LTDA, based in Pinheiro-Maceió (Brazil), which was scheduled to arrive at the Port of Barcelona in December 2018; goods that were distributed in two containers with 800 boxes of DIN-A4 sheets each, containers numbered APZU3035695 and APZU3807079 chartered on board the ship of the shipping company CMA-CGM RIO GRANDE, sailing from the Port of ltaguaí (Rio de Janeiro-Brazil) bound for the Port of Barcelona, on 21 November 2018...." The account of proven facts continues saying that, "...At 13:40 hours on the aforementioned date, during the work of loading and redistribution of the packages of folios in the truck that Herminio was driving, accidentally fell from the mechanical forklift employed by one of the workers of Campderros Salvans S.L., Nemesio, a box of foil coming out of the container with number APZU 3035695, which, when broken, revealed several rectangular packages that turned out to contain the aforementioned narcotic substance. When police presence was requested, a team of Mossos d'Esquadra officers arrived on the scene and, after duly inspecting all the boxes of foil, located inside them 1,410 rectangular packages with the following identifying characteristics...".

Legal basis

In a long judgement, the SC goes through the numerous challenges made by the defendants' defence lawyers in an attempt to dismantle the correctness of the conviction,

[3] STS 324/2025, Penal section 1ª of 07 April 2025, published on the CGPJ website by the Centro de Documentación Judicial, CENDOJ, (ROJ: STS 1487/2025 - ECLI:ES:TS:2025:1487). Appeal: 10408/2024. Speaker: Mr Manuel Marchena Gómez.

even highlighting that one of the appellants criticises the investigating judge for not having added to the interference that the telephone tapping represents other measures that reinforce the State's intrusion into the circle of exclusion defined by the right to privacy. It makes no sense to claim the invalidity of a judicial act of interference in the private life of a suspect by reproaching the judge for not having authorised even more severe restrictions than those which were considered necessary and proportionate.

Rarely, as in the present case, any complaint of a possible prospective investigation or contrary to the principles of proportionality, necessity or exceptionality - Art. 588 bis a - must necessarily be dismissed.

From the moment the drug was found by chance due to an accident during unloading, the work of the State Security Forces and Corps aimed at finding out who had acquired this extraordinary shipment of cocaine for clandestine distribution was fully justified. This work, moreover, was subject to the restrictive control of the examining magistrate no. 1 of Sant Boi de Llobregat and the supervisory intervention of the Public Prosecutor (art. 306 of the LECrim).

We now turn to the challenge to the retention of communications data.

The plea incorporates an allegation concerning the Mossos' request to telephone operators to retain data beyond the 1-year expiry period imposed by Law 25/2007 of 18 October 2007 on data retention, with a marginal reference to the judgment of the Court of Justice of the European Union of 8 April 2014, which declared the nullity of the directive 2006/24/EC.

The defence argues that the request for the preservation of this data - which was not formally incorporated into the case - was not authorised in advance by the examining magistrate.

The judgment under appeal criticises the appellant for seeking that nullity by means of a generic allegation in which it is not stated which of the intercepted orders or lines would be affected". And it reasons that judicial authorisation is implicit in the enabling decisions which imply, by their very nature, the need for the data linked to those communication processes to be retained.

In any event, the Chamber considers that such judicial authorisation to require operators or any other natural or legal person to retain the data is not mandatory.

This can be deduced from the provisions of art. 5 of Law 25/2007, 18 October, on the conservation of data relating to electronic communications and public communications networks. And this is also inferred from art. 588 *octies* of the LECrim, which regulates the advance order for the conservation of data as a security measure.

The first of these provisions is addressed to operators that provide electronic communications services available to the public or operate public communications networks, under the terms established in Law 32/2003, of 3 November, General Telecommunications Law", a criterion reiterated in art. 1 of the current Law 9/2014, 9 May, General Telecommunications Law.

The second - art. 588 octies of the LECrim - incorporates the same duty to secure and preserve data when the depositary is a natural or legal person and explicitly excludes the need for judicial authorisation: "the Public Prosecutor's Office or the Judicial Police may require any natural or legal person to conserve and protect specific data or information included in a computer storage system at their disposal until the corresponding judicial authorisation is obtained for its transfer in accordance with the provisions of the preceding articles".

Therefore, both the Public Prosecutor and the State Security Forces and Corps are empowered to issue, without the need for judicial authorisation, such a preservation order, which, logically, only makes sense in the framework of an investigation in which the subsequent need to incorporate these data into the criminal proceedings initiated is foreseeable.

The non-requirement of judicial authorisation is clear not only from the wording of this precept, but also from the explanatory memorandum of LO 13/2015, 5 October, which introduced art. 588 octies, when it said that, finally, and with regard to technological investigation proceedings, the reform contemplates as a security measure the data preservation order, the purpose of which is to guarantee the preservation of specific data and information of all kinds that are stored in a computer system until the corresponding judicial authorisation is obtained.

Conclusions

This STS clearly distinguishes between a data conservation measure and other technological measures, distinguishing between when judicial authorisation is required and when the FCSE can act directly. Technological measures provided for in art. 588 bis and subsequent articles of the LECrim, which in some cases have not been updated, such as the use of drones, the use of AI...

4.- STS 294/2025, of 28 March 2025. Scope of the principle of insignificance and toxicity in crimes against public health .[4]

Factual background.

The Court of Instruction nº 11 of Palma de Mallorca, opened preliminary proceedings nº 649/2020, once concluded it was sent to the Criminal Court nº 2 of Palma de Mallorca, for trial in the abbreviated procedure nº 11/2022, who dictated Sentence nº 111/2022, dated 28 March 2022, which contains the following proven facts: "...SOLE. It is hereby proven and declared that the accused Lázaro, of legal age, with no criminal record and deprived of liberty for this cause on 9 July 2020, at around 00:15 on 9 July 2020, at around 00:15 on 9 July 2020:15 hours on the 9th of July 2020 he was in Calle General García Ruiz in Magalluf, contacting a British tourist to whom he offered cocaine in exchange for 50€ , handing him a wrapper with said substance, receiving the amount of 50€, a fact which was observed by a local police force of Calviá who stopped their vehicle and went to where the British subject had gone together with a friend, They found them sitting there

[4] STS 294/2025, Penal section 1ª of 28 March 2025, published on the website of the CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ: STS 1335/2025 - ECLI:ES:TS:2025:1335), appeal: 6755/2022. Speaker Excma. Ms. Susana Polo García.

sniffing the substance and told them that they had just bought cocaine from a young man of colour and that they had paid 50€, trying to hide the cocaine that was left in the wrapper with their feet. They then went in the opposite direction and proceeded to intercept Lázaro, intercepting 50€ in his wallet and 50€ more in the fabric of his trousers where he was wearing a drawstring as a belt. The substance that remained in the wrapping, once analysed, turned out to be cocaine with a purity of 19.15% and a retail value of €4.83...".

The judgment of the Criminal Court was appealed on appeal to the Provincial Court, which dismissed the appeal. The SC upheld the appeal and handed down a judgement of acquittal.

Legal basis.

Case law admits the atypical nature of trafficking conduct when, due to its absolute insignificance, the substance no longer constitutes, due to its effects, a toxic drug or narcotic substance, but a harmless product due to its precarious toxicity (SSTS 527/1998, of 15 April; 985/1998, of 20 July; 789/99, of 14 April; 1453/2001, of 16 July; 1081/2003, of 21 July; and 14/2005, of 12 February). The principle of insignificance would call for impunity when the quantity of the drug is so small that it is incapable of producing any harmful effect on health. There is a lack of material unlawfulness due to the absence of a real risk for the protected legal right (SSTS 1441/2000, 22 September; 1889/2000, 11 December; 1591/2001, 10 December; 1439/2001, 18 July; and 216/2002, 11 May).

On the other hand, it should be pointed out that our most recent case law has qualified the use of the term "insignificance", preferring to speak of "toxicity". What does not fall within the scope of the offence is the transmission of substances which, due to their lack of harmfulness, would not entail a risk.

This doctrine must be applied exceptionally and restrictively, but with certainty. In this context, this Chamber continues to operate with the criteria established in the Plenary Session of 24 January 2003. This is confirmed by numerous precedents (SSTS 936/2007, of 21 November; 1110/2007, of 19 December; 183/2008, of 29 April; and 1168/2009, of 16 November) (see STS 587/2017, of 20 July).

Now, with regard to the concept of psychoactive minimum, and its penal repercussions in the subjective element of the offence, STS 1982/2002, of 28 January 2004, tells us that the psychoactive minimums are those parameters offered by an official body of recognised scientific solvency, such as the National Institute of Toxicology, which suppose a degree of affectation in the central nervous system, determining a series of effects on people's health, These are, of course, harmful, as they contain a minimum level of toxicity, and also produce an addictive component, which means that their lack of consumption leads to compulsion. These are therefore drugs that cause harm to public health, understood as the health of the individual members of the community, and whose penalties are designed by the criminal legislator, depending on whether or not the harm is serious. These minimums assume that the quantity transmitted is some type of narcotic, toxic or psychotropic substance included in the international conventions on the matter, by means of the lists to that effect. They therefore fulfil the objective nature of the offence, and affect both formal and material unlawfulness. Such minimums have been offered by the report of the National Institute of Toxicology, and within the margins allowed by such

expertise, they can be interpreted, without necessarily requiring any judicial automatism (STS 580/2017, of 20 July).

In other words, any narcotic substance that exceeds the minimum psychoactive dose, generates the damage to health that the typical rule sanctions and, consequently, if it is seriously harmful to health due to its nature and classification, it continues to be so, whatever the quantity and purity (or degree of adulteration, if preferred), once the minimum psychoactive dose has been exceeded (STS 723/2017, 7 November).

In any case, because on this matter we must remember our jurisprudential doctrine, which originated in the Non-Jurisdictional Plenary Session of 24 January 2003 which, in relation to cocaine, established that its active ingredient operates from 50 milligrams (0.05 grams); This criterion was accepted by the Chamber and taken up in the Non-Jurisdictional Plenary Session of 3 February 2005, in which it was agreed to "continue to maintain the criterion of the National Institute of Toxicology regarding minimum psychoactive doses, until such time as a legal reform is produced or another criterion or alternative is adopted".

Indeed, as the appellant points out, the factual account does not include the quantity of cocaine seized, moreover, according to the report of the Health Department of the Government Delegation of the Balearic Islands, the substance seized by the police was 0.093 grams of cocaine. Therefore, if, as stated in the proven facts, the purity is 19.15%, we have a total of 0.017 grams of net cocaine, i.e. 17 milligrams, which is clearly less than the 50 milligrams above which there is a risk to public health.

Although it is true that the factual account incompletely relates an event which could constitute, as a whole, an act of trafficking, the fact is that in the end only the occupation of the alleged buyer - unidentified, although the police say they spoke to him - of an infinitesimal quantity of drugs, 0.093 grams, with a purity of 19.15%, is declared proven, therefore, We therefore find ourselves with a total of 0.017 grams of net cocaine -17 milligrams-, an amount lower than the minimum psychoactive dose, without expressly considering the occupation of other narcotic substances by the accused to be accredited, so that it cannot reasonably be inferred, from this minimal amount, that he was involved in trafficking and, above all, it must be considered that it lacks criminal relevance due to its harmlessness for public health.

Conclusions.

Despite the clarity of the account of the proven facts, an act of retail drug trafficking in which the role of the buyer and seller is detailed, this STS adds nothing new to the line of jurisprudence already followed for years and which remains unchanged, on the principle of insignificance which is now extended with the qualifier of toxicity, when it comes to applying the INTCF criterion on the minimum psychoactive doses to assess the criminal nature of the offence.

5.- SAN 8/2025 of 2 April 2025. Criminal offence of terrorist-related havoc . [5]

Factual background.

The present judicial proceedings were initiated by virtue of communication via fax from the Secretary of State for the Interior, TEPOL, informing of the explosion of a controlled explosive device at the "El Altet" Airport in Alicante, with the Central Court of Instruction number 2 of Madrid issuing an order to initiate preliminary proceedings on 31 July 1995, and after the corresponding investigation, an indictment was issued on 19 May 2010 against Melisa for the crimes of terrorist destruction in the degree of frustration.

Legal basis.

This judgement of the National High Court states that in the body of evidence in the proceedings we find, firstly, a report from the Guipúzcoa Civil Guard Headquarters of 10 May 2001, folio 294 et seq. of volume I of the proceedings, which informs the Central Preliminary Investigation Court that the defendant, in other proceedings (26/01), also acknowledges expressly that she had placed the device at Alicante Airport, in which the Central Investigating Court is informed that the defendant, in other proceedings (26/01) also from the said Command, expressly acknowledges that she had placed the device at Alicante Airport together with another person (who is not being tried) inside a bag and inside a wastepaper basket. These statements are contained in his second statement made at the Guardia Civil on 31 March 2001 (folio 163 of volume I of the proceedings), also stating that it was on the same day that he placed another device in the tourist office in Denia....

At the trial, and after commendable work by the Guardia Civil, there is an incomprehensible evidential vacuum which the members of the Court themselves denounce and which reads as follows, "...Notwithstanding the above, and despite the efforts made by the Public Prosecutor's Office, we understand that there is an important evidential vacuum which means that we must declare the acquittal of the defendant. An evidentiary vacuum that stems from the lack and absence of proof of a transcendental piece of information, such as the authorship of the handwritten letter that the Public Prosecutor's Office attributes to Melisa, and for which no evidence has been produced. This evidentiary vacuum is due to the failure of the police officers who issued the handwriting expert report, which is included in the proceedings in the so-called "Documentation Annex", and where the documents found in France, including the "kantada" attributed to the defendant, are analysed in detail. This handwriting expert report dated 20 May 2008 and drawn up by police officers with professional licence numbers NUM005 and NUM006, was ratified in the investigation phase before the Central Investigation Court, but subsequently the Public Prosecutor's Office did not propose them as expert evidence, and therefore, as they had not been "brought" to trial, and not having been subjected to contradiction between the parties, it cannot be taken as evidence against the defendant, having been expressly challenged by her defence, a defendant who, on the other hand, in the plenary session clearly and patently stated that she did not recognise the document in question as hers and that she had not written it. On the other hand, report 7/2015, a report that could be called an "intelligence report" which

[5] SAN 8/2025, Penal section 3ª of 02 April 2025, published on the website of the CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ: SAN 1662/2025 - ECLI:ES:AN:2025:1662). Appeal: 132/2010. Speaker: Mr Jesús Eduardo Gutiérrez Gómez.

analyses the existence and components of the ETA commando known as Ibarla, its activity, and data on the attacks committed by this terrorist commando, and its comparison with the documents found in France, This report, which could have shed light on the possible authorship of the placement of the explosive at Alicante Airport, as opposed to the defendant's denial of the facts, has not been the subject of evidence in the plenary session either, as the authors of the report were not proposed as experts. Therefore, the statements of the witnesses who appeared at the trial have no probative value as evidence for the prosecution and as proof of the defendant's authorship, since it has been wrongly "presumed" and assumed that the "kantada" was the only solid evidence for the prosecution (the statement of the accused), (the police statement has no value as evidence for the prosecution as it has not been verified or ratified by the defendant in the Central Preliminary Investigation Court) had been written by the defendant, so that proving the possible discrepancies between this document and the police statement is of little use to us, as the requirement or precondition, that the authorship of this document has been accredited, is lacking.

Consequently, and without assessing the other evidence, the defendant should be acquitted with all the necessary conditions for acquittal...".

Conclusions.

This is a shocking testimony in this SAN nº 8/2025 Section 3, when the police work is impeccable and the work in the pre-trial phase was more than complete. The Public Prosecutor's Office made a serious mistake by not proposing in the plenary session the testimony of the agents who analysed the defendant's documentation and of the authors of the intelligence expert's report. There was no other option but acquittal.

6.- STS 308/2025, of 2 April 2025. Police investigation in Spain arising from knowledge of an EPO issued by the judicial authorities of another country for another criminal offence. Presence of the detainees in a house search . [6]

Factual background.

Coín Examining Court no. 1 opened abbreviated proceedings 22/2022 for offences against public health and illegal possession of weapons against, among others, Clemente, David and Eliseo, which, once concluded, was referred for trial to the Malaga Provincial Court, 3rd Section. Having initiated abbreviated proceedings 54/2022, on 23 November 2022, it handed down Judgement no. 362/22, which contains, among others, the following proven facts: "...It is proven and thus declared that the police authorities in Malaga were aware that Clemente, of legal age, with no computable criminal record, of British nationality and subject to an international arrest warrant issued by the United Kingdom authorities, might be residing in this province, specifically somewhere in the Guadalhorce Valley or Coín. Following the appropriate investigations, the investigating officers came to the conclusion that he may be residing at address xxx in the town of Coín. For this reason, police surveillance was carried out on 3, 4 and 5 May 2022, on the aforementioned property at address xxx in Coín, where police officers finally learned with certainty that Clemente was living together with other men. Specifically, on the days indicated, the

[6] STS 308/2025, Penal section 1ª of 02 April 2025, published on the website of the CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ: STS 1482/2025 - ECLI:ES:TS:2025:1482), appeal: 11312/2023. Speaker: Mr. Pablo Llarena Conde.

aforementioned Clemente, of legal age and without a criminal record, together with David and Eliseo, all of them of legal age and without a criminal record, and Fidel, of legal age and without a computable criminal record, who entered the aforementioned property at some point between the night of 3 May, when he was released from prison, and 20.35 hours on 5 May, when he was seen leaving the property to go to a sports centre, were inside the property. Of all of them, it was David and Eliseo who left the property to make the necessary purchases, and they did so using a Volkswagen Polo vehicle with English number plates, adopting security measures when driving to check if they were being followed, such as driving around roundabouts or not parking the vehicle at the door of the property but in the immediate vicinity of the house.

On 5 May at around 20:35 hours, Clemente, Fidel, David and Eliseo left the house together, Fidel locking the door of the house, who at the time was carrying a black rucksack on his back, which he handed to Clemente on the way. The four aforementioned persons went to the BlueLife Sportclub and Spa Gymnasium, located in the La Trocha Shopping Centre in Coín, at which point the police officers intervened to arrest the four aforementioned men. At the time of the arrest, the black rucksack that Fidel was carrying on his back at the exit of the house was placed at the feet of Fidel and Clemente. Inside the backpack, upon inspection, a 9mm Parabellum calibre Ruger P89 pistol, model P89, with ammunition and without safety catch, with the serial number removed, was found. After the pertinent analysis, it was in a correct state of conservation and its mechanical and operational functioning was also correct in both single and double action, being suitable for firing. Neither Fidel, Clemente, David nor Eliseo were in possession of a licence for this weapon.

On 6 May 2022, the Coín court issued an order authorising the entry and search of the house at address xxx in Coín by order of 6 May 2022, in which a large quantity of narcotics was found...".

Legal basis

It is surprising that the defendants' defence did not raise the possible nullity of the actions carried out by the Judicial Police, when, knowing of the existence of a European arrest warrant, they initiated an investigation and did not proceed to the immediate arrest of the requested person. Nothing is said in the judgement, and better, because it endorses all the police work, which is immediately reported to the examining magistrate, who even agrees to the entry and search of the home for the act carried out in Spain. As we shall see, the ruling of the Malaga Provincial Court was condemnatory and the Supreme Court dismissed the appeal in cassation.

This is the information from the case that is transferred to the Coín Court and which we see so often in practice, for example, the existence not only of OEDE but of searches and seizures at national level, which would make us think of the immediate need to arrest when this is not always the case, as we see in this STS.

The appellants claim that the search and entry procedure carried out on 6 May 2022 at the house located at address xxx in the town of Coín is null and void as a matter of law, because being the habitual residence of the four accused and all of them being in custody, the police officers only took Fidel to be present at the search and entry procedure. They therefore consider that the results of this investigation are null and void and that they

cannot be used as legitimate prosecution evidence, and that they must be acquitted because there is no other evidence to establish the appellants' responsibility.

In the judgments handed down by this Chamber 420/2014, of 2 June, or 508/2015, of 27 July (Malaya case), citing other precedents, we summarised our doctrine on the requirement of the presence of the interested party in the practice of the entry and search of the home.

We said in them that the basis for the requirement of the presence of the interested party or his representative at the entry and search of the home ordered by the judicial authority in criminal proceedings lies, firstly, in the fact that this procedure affects a personal right, of a constitutional nature, which is the right to personal privacy, since the constitutionally protected home, as a person's dwelling or habitation, is closely linked to their sphere of intimacy, since what is protected is not only a physical space but also the emanation of a physical person and their private sphere (STC 188/2013, of 4 November, in relation to art. 18 2nd EC and art. 8 ECHR). Secondly, it affects the right to a fair trial, because the result of this procedure will constitute evidence in the trial against the accused whose home has been searched, which means that the search must be conducted in such a way as to ensure the validity of the search as pre-constituted evidence.

The procedural law therefore foresees, as a requirement for the practice of the search, the presence of the interested party or person legally representing them (art. 569 LECrim). And the interested party referred to in article 569 of the LECrim is not necessarily the owner, in the sense of owner or tenant of the property. What is decisive is not who the owner is, who may be unknown, not reside in the home, or even be a legal person, but who is the resident in the home, as it is their privacy that is going to be affected.

Ordinarily, the person interested in the search is the defendant, as the outcome of the search will affect his or her defence, although it does not always necessarily have to be the defendant who is present at the legally authorised search. The accused or the person against whom the proceedings are directed may be unaccounted for or simply outside the home and untraceable at the time of the search. The entry and search of a home authorised in the course of legal proceedings for a criminal offence is, by its very nature, an urgent procedure that cannot be delayed while waiting for the accused to return home or to be located by the police. For this reason, the law authorises the interested party to be dispensed with "when he is not present", which clearly refers to the accused, and in these cases the search can be carried out in the presence of any of his family members of legal age, with the jurisprudential doctrine considering, taking into account a social reality in which groupings of homes are no longer necessarily carried out by families in the strict sense, that this rule is applicable to all the inhabitants of the home, of legal age, even if they are not family members in the strict sense of the term.

However, what is required is the presence of the accused in the search when he or she is detained or under police or judicial custody, as in these cases there is no justification for prejudicing his or her right to contradict, which is better guaranteed by the effective presence of the accused in the search.

In any case, we also recalled in these judgments that this rule is not applicable to cases of force majeure, in which the absence of the accused, despite being at the disposal

of the police, is justified. We cited as an example cases of hospitalisation of the accused, or arrest in a place far away from the home, or in the case of searches carried out simultaneously in several homes. And also when the impossibility of their presence is of a legal nature, for example when the investigation has been declared secret (STS 143/2013, 28 February).

And when there are several residents in the residence, in our SSTS 336/2017, of 11 May or 913/2023, of 13 December, recalling SSTS 698/2002, of 17 April, 1108/2005, of 22 September, 352/2006, of 15 March, 684/2014, of 2 October or 79/2015, of 13 February, we emphasise that the validity and effectiveness of the entry and search procedure is not affected when one of the residents is present, provided that the attendee does not have interests that conflict with those of the other defendants. Without prejudice to the fact that, in these cases, despite the validity of the search and in order to guarantee respect for the right to contradiction, which is part of the broadest right of defence, the search cannot be considered as pre-constituted evidence and it will be necessary that, beyond the mere reading of the record drawn up during its execution, the witnesses who approached or witnessed its practice appear to give evidence in the oral trial.

The pleas in law are therefore dismissed.

Without prejudice to the fact that in the present case the driving and custody of all those deprived of their liberty would have affected the availability of the police personnel assigned to the small town where the appellants carried out their criminal activities and where they were detained, as a large number of officers would have been required for the transfer and surveillance of the four defendants and for carrying out the investigation, an objective analysis of the concurrent circumstances provided the investigators with the basis that there was no contradiction of interests between the persons under investigation. Specifically, the police surveillance system, set up over three days to monitor the inhabitants of the house for a long period of time, made it possible to establish that they were all residents of the house and that they were all acting in concert. In particular, David and Eliseo, when they left the house by car, took security measures to check if they were being followed. And both they and the other detainees sometimes acted in concert and even exchanged objects such as a rucksack. And this presumed absence of conflicting interests was confirmed by the significant quantities of narcotic substances seized and the number and location of the weapons seized, as the witness evidence, which was contradicted in the plenary session, shows that the drugs were visible to all the inhabitants of the house and were not hidden in any room intended for the exclusive use of any of them, thus ruling out the possibility of one person responsible trying to shift sole responsibility to the other residents. And so the three pistols were also seized, which led to their conviction as perpetrators of the offence of illegal possession of weapons.

Conclusions.

After endorsing the investigation in a case that was based on police knowledge of an EPO issued by the judicial authorities of the United Kingdom for a different criminal act, and without the Defence having challenged the possible omission of the duty to prosecute crimes by the FCSE by not immediately arresting the person covered by the EPO in force, and thus avoiding the investigation initiated in the Court of Coín, this STS 308/2025 makes a phenomenal and didactic description of who has the concept of interested party in an entry and search of the home of a person who is the subject of an entry and search

of a person's home, and thus avoiding the investigation initiated in the Court of Coín, this STS 308/2025 provides a phenomenal and didactic description of who enjoys the concept of interested party in an entry and search of a home, whether or not the person is detained, establishing a general rule and the exceptions in extraordinary cases. It also delimits the possible conflict of interests between those affected.

7- STS 295/2025, Penal section 1ª of 28 March 2025, crime of harassment, "stalking".[7]

Factual background.

The Court of Violence against Women nº 1 of Medio Cudeyo, opened urgent proceedings nº 36/2021, once concluded it was sent to the Criminal Court nº 5 of Santander, for trial in the fast track trial procedure nº 125/2021, who issued Sentence nº 285/2021, dated 25 November 2021, which contains the following proven facts: "..."It has been proven that the accused Basilio, of legal age, and without a criminal record computable for the purposes of recidivism, who maintained a sentimental relationship for a year with Concepción, with address in Iruz (Santiurde de Toranzo), which ceased in July 2020, since October of that year called her on the phone, sent WhatsApp messages and letters insistently, asking for her forgiveness and asking her to resume the relationship, saying "my life has no meaning, that I was thinking about the best way to disappear, what am I going to do now, that life has no meaning for me", having been found at 09:00 on 15 December.00 hours on the 15th of December he was found sitting on a chair in his garden semi-conscious with his eyes rolled back in his head and had to be evacuated to hospital, coming on the 1st of January 2021 to his home knocking on the door, and then constantly calling him and sending him a letter a month, all with the intention of seriously altering his life, despite having knowledge that Concepción does not want to maintain any kind of relationship with him...".

The 3rd Section of the Provincial Court of Santander upheld the appeal of the convicted person and acquitted him, and the victim's representative lodged an appeal in cassation, which was upheld, again convicting the accused.

Legal basis.

Given the striking nature of judicial pronouncements, conviction at first instance, acquittal on appeal and conviction again on appeal, the case law of the ECtHR allows for the review of acquittals when the Supreme Court acts within the margins of the infringement of the law, reviewing purely legal issues. In other words, when this Chamber limits itself to correcting errors of subsumption and to establishing uniform interpretative criteria to guarantee legal certainty, the predictability of judicial decisions, the equality of citizens before the criminal law, and the unity of the criminal and criminal procedure system, without altering any factual assumptions.

Article 172.3 of the Penal Code, in force at the time of the commission of the acts - since the precept has been reformed by LO 1/2023 of 28 February - expressly punishes

[7] STS 295/2025, Penal section 1ª of 28 March 2025, delito de acoso, "stalking", published on the website of the CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ: STS 1348/2025 - ECLI:ES:TS:2025:1348), appeal: 7251/2022. Speaker Excma. Ms. Susana Polo García.

anyone "who harasses a person by insistently and repeatedly carrying out, without being legitimately authorised to do so, any of the following conducts and, in this way, seriously alters the development of their daily life". The aforementioned article, which defines the offence of harassment, was introduced into the Criminal Code in O.L. 1/2015 of 30 March 2015. 1/2015, of 30 March, whose Explanatory Memorandum states that "it deals with "all those cases in which, without necessarily involving the explicit or non-explicit announcement of the intention to cause harm (threats) or the direct use of violence to restrict the victim's freedom (coercion), there are repeated conducts by means of which the victim's freedom and sense of security is seriously undermined, who is subjected to constant persecution or surveillance, repeated calls or other continuous acts of harassment".

In such terms, the Jurisprudence has been pronounced since the Judgment of the Plenary 324/2017, of 8 May, and 554/2017, of 12 July, the latter with express reference to the previous one, where it is stated, among other things, that, therefore, it can be said that in an insistent and repeated manner it is equivalent to saying that there is a repetition of actions of the same nature - a continuum - which is repeated over time, in a period not specified in the type, it can be affirmed that in an insistent and reiterative manner it is equivalent to saying that we are faced with a reiteration of actions of the same nature - a continuum - which is repeated over time, in a period not specified in the criminal type, and that we are in the presence of a criminal type that is very "attached" to the specific profiles and circumstances of the case being prosecuted. In other words, the analysis of each specific case, in view of the actions carried out by the agent with insistence and reiteration, and on the other hand, in view of the suitability of such actions to seriously alter the life and peace of mind of the victim, will lead us to the existence or not of the crime of harassment, and it is up to this Court of Cassation, as the appeal is based on the double instance - sentence of the Criminal Judge and the appeal sentence issued by the Provincial Court - to determine whether or not, given the proven facts, the elements that form the backbone of the crime exist.

On the other hand, apart from the legal definition, there are definitions of the phenomenon in the scientific community, basically in the field of psychology and psychiatry, which as a general rule define it as behaviours that one individual inflicts on another by means of intrusions or unwanted communications, identifying intrusion with the fact of persecuting, prowling, hovering, watching, approaching, and communicating with behaviours such as sending letters, making phone calls, sending e-mails, graffiti or notes on the car, or associated behaviours such as ordering services in the name of the victim, making false accusations etc., always requiring that these behaviours be repetitive or reiterative.

Article 172 ter describes the criminal offence, in general terms, using the verb "to harass", a term on which there is no consensus in our legal system regarding its definition, especially in terms of the need for as many acts as are necessary, but we cannot ignore the fact that sexual harassment and harassment on grounds of sex do not require repetition or persistence, according to the concept of the same in the article. 7.1 and 7.2 of the Organic Law 3/2007, of 22 March, for the effective equality of women and men, and the introduction in our criminal law of the crime of stalking, is a further response to the fight against gender violence and compliance with international regulations and more specifically with the Istanbul Convention.

It should also be borne in mind that the legislator, rightly, in our view, does not determine the number of occasions on which the harassing conduct should take place, nor the time frame in which it should take place, and as for the serious alteration of daily life, we have said that the offence does not require planning, but does require a methodical sequence of actions that force the victim, as the only way out, to change their daily habits. In order to assess the suitability of the sequenced action to alter the victim's daily habits, the standard of the "average man" must be taken into account, although this is qualified by the specific circumstances of the victim (vulnerability, psychological fragility, etc.) which cannot be completely ignored (STS 639/2022, of 23 June).

We anticipate that the appeal will be upheld, with the consequent annulment of the acquittal and its replacement by a conviction.

The account of proven facts describes the conduct of the accused, who over a period of at least three months, repeatedly phoned his ex-partner, sent her WhatsApp messages and letters, insistently according to the account, in all of them asking for forgiveness and asking his former partner to resume the relationship that had ceased months earlier, saying "my life has no meaning, that I was thinking about the best way to disappear, what am I going to do now, that life has no meaning for me", one day the victim even found him sitting on a chair in his garden "semi-conscious, with his eyes rolled back in his head and he had to be evacuated to hospital", going to Concepción's home 15 days later, knocking on the door, and then constantly phoning her again and sending her a letter a month, with the aforementioned intention of resuming the relationship despite knowing that Concepción did not want to maintain any kind of relationship with him.

The offence of stalking protects individual freedom and the right to live in peace and without anxiety. The messages, appearance at the victim's home showing her suicide attempt in order to make her responsible for it, together with the calls and messages sent, are in themselves capable of disturbing the habits, customs, routines or way of life of any person, taking into account the standard of the "average man/woman", the Criminal Court reflecting in its reasoning that the above obliged the victim to receive psychological support, a fact that is not disputed. The same acts of the proven facts, -cover the requirements that this Chamber has been demanding of the type of art. 172 ter CP, namely, insistence, reiteration, repetition, reflection of the same pattern or systematic model, existence of a will to persevere in these intrusive actions, far exceeding the purely episodic or circumstantial and lack of legitimisation, or authorisation to act in this way. Because of the period of time during which they are sent and their content, the disvalue they contain is of a very high level, sufficient to trigger a criminal reaction.

In this case, we are not dealing with a simple annoying behaviour, the actions described in the factual account are capable of altering the victim's life and peace of mind in any way, affecting or altering the victim's future in any way in her private life, work or relations with third parties. In short, Concepción was subjected to emotional blackmail, understood as a form of communication that seeks to manipulate one person over another by using fear, obligation and especially, in this case, guilt.

We are dealing with facts that imply a clear psychological submission, in which the accused psychologically subjugates his ex-partner with the idea that he will not stop until he returns to him, even making him responsible for his own life with the self-harming attempt in the garden of the victim's home, which provokes fear in the victim, seriously

altering her daily life, which is subject to psychological treatment, without it being necessary to provide expert psychological evidence at the trial to prove that the victim's psyche has been affected by this situation of harassment or stalking, and that this determines an alteration in her life, when, as in this case, it is clear from the factual account itself, as the events necessarily generated an emotional impact on the victim - fear for her safety and that of her surroundings - and an impact on the normal development of her daily life, with the need to undergo psychological treatment.

As we have said in STS 843/2021, of 4 November, the essence of the criminal type, and above all, related to acts of gender violence, such as harassment in the situation of a former partner, must be contemplated with a gender perspective, as a situation of harassment between strangers or acquaintances is not the same as in the relationship of a partner or former partner, where the interpersonal ties that have been created intensify the harasser's demands for domination or humiliation of the victim who is, or has been, his or her partner in order to create physical and psychological ties that demonstrate the submission that the harasser wants to transfer to his or her victim so that she does not resist the harassment and returns to him or her.

Consequently, the facts described are suitable for forcing the victim to change her way of life, with sufficient force to constitute a crime of harassment as defined in Article 172 ter of the Criminal Code, therefore, the appeal should be upheld and the accused should be sentenced as the perpetrator of the aforementioned crime, to the same penalties imposed by the Criminal Court, and the aforementioned sentence should be reinstated.

Conclusions.

Important terminological and factual precision of this type of crime, which as STS 295/2025 rightly states, does not quantify the number of acts of harassment necessary to integrate the criminal offence, but which environmentally and evaluating all the evidence as a whole, not in isolation, does allow its appreciation because the victim's way of life was altered, and more so in cases of violence against women.

8.- STS 284/2025, of 27 March. Sexual abuse of a 17 year old with borderline intelligence. Moral damage.[8]

Factual background.

Criminal Court no. 6 of Las Palmas de Gran Canaria in the case coming from the PA with the number 247/2020, instructed by the Court of Instruction no. 1 of Telde, for a crime of sexual abuse against Maximino issued a sentence that contains the following Proven Facts: "...SOLE. It is hereby proven and declared that the accused, Maximino, born xx1984, on 1 May 2017 in the afternoon, without being able to specify the time, guided by the desire to satisfy his sexual instincts, persuaded the 17 year old minor, Socorro, to accompany him to the building located at the address xxx, and once there, he touched her buttocks and thigh, taking advantage of her, knowing that she was a minor and that her level of intellectual functioning was on the borderline of normal intelligence, making her

[8] STS 284/2025, Penal Sección 1ª, of 27 March published on the website of the CGPJ, Centro de Documentación Judicial, CENDOJ. (ROJ: STS 1469/2025 - ECLI:ES:TS:2025:1469), appeal: 7022/2022. Speaker: Mr. Antonio del Moral García.

highly vulnerable to becoming a victim. The legitimate representative of the minor claims...".

On appeal, the Provincial Court partially upheld the appeal for undue delay and the Supreme Court upheld the Provincial Court's conviction.

Legal basis.

On the one hand, the appellant argues that the facts are atypical on the basis of the victim's consent. The description of the act does not allow for a finding of mental disorder. The judgment speaks of a level of intellectual functioning on the borderline of normal intelligence. Being on the borderline and not below the borderline - it is typographically emphasised - it would not be possible to speak of abuse of disorder.

The reasoning is not clear. On the one hand, it seems to be reasoning that the accused was not aware of this circumstance. This contradicts the proven fact that he took advantage of this characteristic, which implies knowledge. This renders the claim unviable.

It could also mean that, being at the limit of normality, one could speak of normality, which would deprive the absence of consent of support.

This second possible argument plays with language, ignoring the fact that the locutions, borderline intelligence or borderline intellectual functioning, are well-coined concepts that express something more than what would be derived from their strict literal meaning. People with these characteristics lack what is considered to be an average intellectual level. They are - and this belongs to the common cultural heritage: this is not psychiatric, let alone legal technicalities - people who are able to develop life processes, to function and to understand the world, but they need appropriate support, as their low IQ requires it. They have difficulties in decision-making and conflict resolution; their social skills are diminished. The World Health Organisation establishes that the average intelligence is between 85 and 115. People with borderline intelligence are those who are just below these figures: between 70 and 85. Nor can one speak of intellectual normality. From a criminal law perspective, they are covered by the normative concept of art. 25.1 CP.

The proven facts, moreover, as is made even clearer in some parts of the factual reasoning, do not mention any consent of the minor to the touching with sexual implications. It is not said that she consented to them. They were imposed on her until she managed to escape, but without the use of violence or intimidation. In fact, the judgement does not cite Art. 181.2 (abuse of mental disorder).

The performance of sexual acts without the consent of the other person is typical in itself, regardless of the intellectual level of the victim. If, in addition, the victim has intellectual deficits that make him/her particularly vulnerable, the act will be aggravated.

The second line of appeal seeks to expel this aggravation by considering it to be inherent to the abuse of a mental disorder or beyond the defendant's knowledge.

Only by twisting the proven facts can it be argued that the accused was unaware of the special vulnerability arising from the borderline intelligence he exploited. For the rest, the sequence of the facts and the way in which they are recreated in the legal grounds are extremely expressive.

If it were a case in which the consent, express or externalised by conclusive acts, of the victim is obtained, and the typical nature is based on dealing with a non-free consent due to the absence of capacity to give it and with the perpetrator taking advantage of the cognitive deficit to obtain it, the problem of the compatibility of art. 181.2 above (abuse of mental disorder) or art. 178.2 in force (abuse of a situation of vulnerability of the victim) with the specific aggravation (especially vulnerable due to... age, illness, disability or situation: art. 180.1.3º and 181.5 in the legislation applied; or special vulnerability due to... disability or any other circumstance: art. 180.1.3º after LO 10/2022). But this is not the case.

On the one hand, there is an absence of consent. We are not dealing with a consent that is not free because it was obtained abusively. On the other hand, it appears that the victim has a diminished intellectual capacity that makes her particularly vulnerable.

The criminalisation has therefore been correct.

And what stands out from the STS is the concept and scope of non-pecuniary damage, which is so difficult to see in the daily practice of our courts.

So much so that art. 193 CP contains a prescription, in convictions for crimes against sexual freedom, in addition to the pronouncement corresponding to civil liability, there will be, where appropriate, those corresponding to filiation and maintenance, which represents a legal presumption (based on a maxim of shared and undoubted experience) of moral damages in this type of crime (vid SSTS 327/2013, of 4 March; 1033/2013, of 26 October; 733/2016, of 5 October; 812/2017, of 11 December; 393/2020, of 15 July; 1040/2021, of 26 October or 1209/2021, of 2 December).

The appellant is in no doubt that compensation would also be awarded in the civil courts if the action had been reserved for that area.

Although it is not applicable as it was not in force at the time of the facts, it is relevant to refer to the regulation of this issue in Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, as it endorses, with novel additions, the inexcusability of this compensation by breaking down concepts in which moral damage and damage to dignity are highlighted.

This is stated in art. 53 of the aforementioned Law, under the heading Indemnification.

"1. Compensation for material and non-material damages corresponding to the victims of sexual violence in accordance with the criminal laws on civil liability derived from the crime shall guarantee the economically assessable satisfaction of at least the following concepts:

(a) physical and psychological harm, including moral harm and harm to dignity.

(b) Loss of opportunities, including opportunities for education, employment and social benefits.

(c) property damage and loss of income, including loss of profit.

d) Social damage, understood as damage to the life project.

e) Therapeutic, social and sexual and reproductive health treatment.

2. The compensation shall be paid by the person or persons civilly or criminally liable, in accordance with the regulations in force".

Conclusions.

This STS 284/2025 deals with two questions of interest. On the one hand, the perfect fit of an aggravated figure in crimes against sexual liberty, when there has been a lack of value in the aggressor's action which is not only objective, acts of touching, but also has a relevant subjective perspective, knowingly taking advantage of the victim's vulnerability. On the other hand, the almost forgotten concept of moral damage, which although existing previously in numerous judicial pronouncements, has had its express recognition in the controversial LO 10/2022 of integral guarantee of sexual freedom.

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
GUARDIA CIVIL

Revista Científica
del Centro Universitario de la Guardia Civil

Revista Lógos Guardia Civil

CENTRO UNIVERSITARIO GUARDIA CIVIL