Transforming intelligence through innovation

IJ 3-B

INTELLIGENCE JOURNAL



MINISTERIO
DE DEFENSA



Transforming intelligence through innovation

IJ 3-B

INTELLIGENCE JOURNAL 3-B



MINISTERIO
DE DEFENSA

Catálogo de Publicaciones de Defensa
publicaciones.defensa.gob.es

Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

© Autores y editor, 2025

NIPO 083-25-273-1 (edición impresa)
ISSN 3101-6685 (edición impresa)

NIPO 083-25-274-7 (edición en línea)

Depósito legal M 27654-2025
Fecha de edición: abril de 2026
Maqueta e imprime: Imprenta Ministerio de Defensa

Las opiniones emitidas en esta publicación son de exclusiva responsabilidad de los autores de la misma.
Los derechos de explotación de esta obra están amparados por la Ley de Propiedad Intelectual. Ninguna de las partes de la misma puede ser reproducida, almacenada ni transmitida en ninguna forma ni por medio alguno, electrónico, mecánico o de grabación, incluido fotocopias, o por cualquier otra forma, sin permiso previo, expreso y por escrito de los titulares del copyright ©.

En esta edición se ha utilizado papel procedente de bosques gestionados de forma sostenible y fuentes controladas.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica». No se puede modificar. No se puede utilizar con fines comerciales.

publicaciones.defensa.gob.es
cpage.mpr.gob.es

Index

Foreword 11
Carlos Alberto Ramírez Sánchez

Article one

The transformation of intelligence in European security and defence: challenges and opportunities in the digital era 15
Carlos Hugo Fernández-Roca Suárez
1 Introduction 15
2 Impacts of the Fourth Industrial Revolution on intelligence defence 15
3 Artificial Intelligence as a transformative factor 16
4 Europe's institutional responses: from the ReArm Europe Plan to the Defence Industrial Strategy 18
5 Cases of technology application in intelligence and defence 21
6 The quest for European technological sovereignty 23
7 Regulatory aspects in the digital transformation of security and defence in Europe 25
8 Prospective scenarios towards 2040: the future of European digital intelligence 27
8.1 The first scenario: Autonomy and integrated European intelligence 27
8.2 The second scenario: Persistent dependency 28
8.3 The third scenario: Conditional cooperation 28
9 Conclusions 29
Bibliography 31

Article Two

***Conductual Explorer*: an autonomous solution to the cognitive environment challenge** 35
Pablo Caneda González
María Porrar Santisteban
Álvaro Álvarez Álvarez
1 Introduction 36
1.1 Motivation: solving internal needs with creativity and reduced costs 37
1.2 Context of the project and its importance 38
1.3 Objectives and scope of the programme 38
2 Need for an analyst and creation of the database 40

2.1 Analysis of the area: data collection and structuring 40
2.1.1 Defining the scope of the study 40
2.1.2 Selection and filtering of information sources 41
2.1.3 Identification of key actors 41
2.2 Tools used in the initial analysis 43
2.3 Building a database 44
3 Codes developed and how they work 46
3.1 Code 1: Sentiment analysis of the information environment 46
3.1.1 Objective and rationale behind the analysis 46
3.1.2 Techniques used: natural language processing (NLP) and taxonomy-based classification 47
3.1.3 Practical example and expected results 47
3.2 Code 2: Classifying Social Networks and Means of Mass Communication with machine learning 50
3.2.1 Definition of categories and classificatory approach 50
3.2.2 Implemented algorithms and models 52
3.2.3 Expected results of a practical scenario 52
3.3 Code 3: Multi-stage classification of TikTok content 53
3.3.1 Filtering by hashtags and taxonomies in the video description 53
3.3.2 Filtering by comment analysis 54
3.3.3 Frame filtering by deep learning for image processing 54
4 Conclusions and lessons learned 55
4.1 Impact of the programme on the organisation 55
4.2 Main lessons learned and contributions 55
4.3 Next steps and proposed improvements 56

Article Three

Post-normal intelligence: risk management in the grey zone 59

Jesús Hernández Álvarez

1 Introduction 60
2 Post-normal science 62
3 From the intelligence cycle to risk management 66
4 Intelligence and cognition 70
4.1 Cognitive biases 71
4.2 Linear vs. systemic thinking 72
4.3 Mental models vs. conceptual models 75
4.4 Situation awareness 76
5 Evolutionary systems 77
6 A new paradigm in Intelligence 79
7 The cognitive domain as an asset to be protected 80
8 Conclusions: innovation scenarios 81

Bibliography 84

Article Four

A real-world experience of AI usage: the analysis factory of the Analysis and Foresight Centre of the Spanish *Guardia Civil* 87

Enrique Ávila Gómez

Lorenzo Luna Zambrana

1 Introduction 88

2 The Centre for Analysis and Prospective of the ***Guardia Civil*** (CAP) 89

3 Pre-scenario: language, detection, validation and timing 90

4 The talent problem 100

5 Hallucinations and Other Issues: A Practical Approach 102

6 Conclusions 109

Bibliography 110

Article Five

ECySAP and situational awareness in multi-domain warfare operations 113

Antonio Legaz

Juan Tejero

José Francisco Suárez Mulero

1 Fundamentals of Cyber Situational Awareness (CySA) 114

1.1 From Coup d'Œil to Cyber Situational Awareness: transforming the military paradigm 114

1.2 Historical evolution of situational awareness: from Sun Tzu to the digital environment 114

1.3 Theoretical framework of Cyber Situational Awareness: Endsley's model in cyberspace 115

1.4 Contemporary operational context: multi-domain warfare and mosaic approach 116

2 ECySAP: a comprehensive platform for Cyber Situational Awareness 117

2.1 Functional architecture of ECySAP: from perception to projection 117

2.2 ECySAP applications in operational planning and courses of action 118

2.3 Risk management and incident assessment through ECySAP 119

2.4 Artificial Intelligence integration: boosting ECySAP capabilities 120

2.5 ECySAP in the context of Mosaic Warfare: enabling Multidomain Situational Awareness 121

2.6 ECySAP as an enabler of synchronised operations in multi-domain environments 121

3 Doctrinal and regulatory framework 122

3.1 The cyber defence doctrine 122

3.2 Regulatory framework 123
4 Use case 125
4.1 Historical context: Mosaic war and the annexation of Crimea 125
4.2 ECySAP analysis layers within the Crimea-Russia context 126
4.3 Protection against disinformation 127
4.4 Critical infrastructure protection 128
4.5 Protection of physical military assets 129
4.6 Conclusions of use case 129
5 Conclusions 130
Bibliography 131

Article Six

Technological innovation in the area of cyber threat intelligence and, by extension, cyber defence 137
Juan Adolfo Montero
1 Introduction: cyber threat intelligence as a basis for the transition from cybersecurity to cyber defence 138
1.1 Why is traditional cybersecurity no longer enough? (Rodriguez, 2023) 138
1.2 Key differences between cybersecurity and cyber defence 139
1.3 Military analogy: cybersecurity as basic defence 140
2 The "operationalisation" of Cyberspace 140
3 Cyber defence: a holistic and intelligence-led approach to cyber threats 141
3.1 Advantages and disadvantages of the attacker and the defender 141
3.2 Cyber defence: from reaction to anticipation 141
3.2.1 The threat 142
3.2.2 The mission 142
3.2.3 Cyberspace to be defended 142
3.3 Application of tactical, operational and strategic intelligence 143
3.4 The IPB model applied to cyberspace (Cyber-IPB) 143
3.4.1 Cyber-IPB: goals and benefits 145
3.5 Cyber defence plans (Corletti Estrada, 2017) 146
3.5.1 Advanced Detection Plan 146
3.5.2 Obstacle Plan 147
3.5.3 Impact Mitigation Plan 147
3.5.4 Reaction Plan 147
3.5.5 Recovery Plan 147
4 Technological challenges of Cyber Defence 148
4.1 The need for national and strategic solutions 148
4.2 The need for agile development and procurement 149
4.3 Technological gaps 149
4.3.1 Situational Awareness (CySA) 149
4.3.2 Cyber threat modelling 150

5 Technology initiatives promoted by the Joint Cyberspace Command (MCCE) .. 153
5.1 PICO Platform 153
5.1.1 What does PICO offer? 153
5.2 ECySAP / ECySAP EYE 158
5.2.1 ECySAP v1.0 158
5.2.2 ECySAP v2.0 (ECySAP EYE) 161
5.3 SCOMCE: Cyberspace Combat System 162
6 Advanced technological requirements for SCOMCE 163
6.1 Data lake technology 163
6.1.1 Sources of information and data to be integrated 164
6.1.2 Structure of the data lake 165
6.1.3 Challenges in implementing a data lake 165
6.2 Ontology 166
6.3 Application of Artificial Intelligence (AI) 167
6.4 Application of simulation techniques 169
6.4.1 Simulation as a strategic tool 170
7 Conclusions 171
Bibliography 172

Article Seven

Cross impact matrices and the structural method: a partial review of tools for future scenario building 175

Licesio J. Rodríguez-Aragón

1 Introduction 176
2 Modelling and prospective simulation 178
2.1 Modelling 179
2.2 Simulation 180
3 Cross-impact matrix methods 181
4 Structural analysis of impact matrices 183
5 Influence Dependence Graph 186
6 Multiplication of the Cross-Impact Matrix Applied to Classification (*Matrice d'Impacts Croisés Multiplication Appliquée à une Classification*-MICMAC) .. 188
7 Conclusions 192
Bibliography 193

Article eight

Technology at the service of deterrence 197

Emilia José Peña Ruiz

1 Introduction 198
1.1 The need for a safeguards system 200
1.2 The role of geographic information systems in the safeguards system 202

2 A practical example: the case of North Korea 206
3 Conclusion 209
Bibliography 209

Article Nine

Transforming the JISR cycle in the digital age: technological innovation for information superiority 213
Begoña Rojo Carralero
1 Introduction 214
2 Basics of the ISR process 215
3 JISR in multi-domain operations and the transparent battlefield 216
4 NATO and European initiatives related to the intelligence cycle 218
5 Transformation of the JISR process: from the classical to the digital and multi-domain model 219
6 The impact of emerging technologies on the JISR process 221
6.1 AI and edge computing 222
6.2 Expansion and diversification of sensors 223
6.3 Use of unmanned platforms 224
6.4 Quantum technologies 225
6.5 Space / Satellites 226
6.6 Hypersonic systems 227
6.7 Cross-cutting trends in emerging SRI technologies 227
7 Possible improvements at each stage of the JISR process 228
7.1 Tasking – Resource planning and allocation 228
7.2 Collection – Information gathering 229
7.3 Processing – Processing and classification of data and information 230
7.4 Exploitation – Data and information analysis 230
7.5 Dissemination – Distribution and use of information 230
7.6 Lessons learned and conditions for success 231
8 Interoperability and the “one data” philosophy 231
9 Technological innovation as a threat to the JISR process 233
9.1 The importance of cybersecurity in the JISR Process 233
9.2 Biases and vulnerabilities of Artificial Intelligence in the JISR process 234
10 Conclusions 235
Bibliography 237

Article Ten

Adapting new technologies in the JISR community. Specific characteristics of the maritime domain 239
Alfonso Herrero Pita
1 The information revolution and the intelligence community 240

2 Vectors of change 240
3 Adaptation of traditional structures 241
4 JISR as an innovation paradigm 241
5 Challenges in adapting technology to JISR capability 242
5.1 Original environment 242
5.2 Technology tools for ISR, ISR = I+SR? 243
5.3 The maritime environment 245
5.4 Interoperability Standards. MAJIIC2. Thwarted projects? 246
5.5 Interoperability standards; organisational impact (normality) 247
5.6 Interoperability standards; impact on operations - the case of the MCC 248
6 Conclusions 249
Bibliography 249

Article Eleven

Narrative intelligence in the age of AI: analysing Russia's anti-Ukraine disinformation 251

Viktoriia Romaniuk

Yevhen Fedchenko

1 Introduction 252
2 Narrative Intelligence: interdisciplinary perspectives and definitions 253
3 Narratives against Ukraine 257
4 Artificial Intelligence and the promotion of anti-Ukrainian narratives in Kremlin disinformation campaigns 258
5 Deepfakes as a means of disseminating disinformation 261
5.1 Case 1: Commander-in-Chief of the Ukrainian Armed Forces, General Valerii Zaluzhnyi (2021-2024) 263
5.2 Case 2: Commander-in-Chief of the Ukrainian Armed Forces, Oleksandr Syrskyi 264
5.3 Case 3: Michael O'Flaherty, Commissioner for Human Rights of the Council of Europe 265
6 Conclusions 266
Bibliography 267

Article Twelve

What does the growth of OSINT mean for military intelligence analysts? 273

Marcel Plichta

Edwin Dudley-Taylor

1 Introduction 274
2 What is OSINT? 274

3 Military and civilian intelligence priorities 275
4 Advantages of OSINT for military analysts 276
5 The use of OSINT to improve and verify information gathering 278
6 Use of OSINT in transparency and intelligence sharing 279
7 Challenges for military analysts 279
8 Legal restrictions and privatization of information gathering 282
9 Conclusion 283
Bibliography 284

Scientific Committee and Editorial Board 287

Rules for shipment of items 291

Foreword

Carlos Alberto Ramírez Sánchez

The third edition of the Intelligence Journal maintains the continuity and development that has been a hallmark of previous issues.

Back in 2023, the first issue attempted to outline the birth of a publication that was launched to fill an almost empty space in intelligence publications by focusing, above all, on the little-known and enormously complex area of military intelligence.

The second issue sought to open up the broad range of intelligence to all civilian and military agencies that make up the rich ecosystem dealing with threats to National Security on a daily basis.

This third issue reaffirms a fundamental premise: intelligence is not the exclusive resource of any one organism. Rather, its value lies in its ability to adapt to the specific needs of each entity or organisation, providing effective advice to decision-makers.

Based on this perspective, the concept of the "Extended National Intelligence Community", which proposes a comprehensive synergy of all state intelligence capabilities to address threats and challenges in a cohesive and effective manner, takes on especial relevance.

This issue once again grants a voice to all aspects of intelligence (military, civilian, police, academic, business, etc.) with the conviction that, over time, what unites these actors will overcome their differences.

The Intelligence Journal number three is titled *Transforming intelligence through innovation*. It was decided to centre this issue on innovation applied to intelligence in an attempt to reveal the enormous transformations that are currently underway in intelligence as technology advances.

Concepts such as "transparent battlefield" no longer sound like science fiction. At the same time, the news from conflict zones astonishes us as to how effective military operations become when intelligence enhanced by new technologies gives decision-makers a distinctive advantage over their opponents: to strike earlier and more accurately.

The growing interest of the business sector in integrating intelligence into their strategies has prompted the creation of specialised departments, which operate in coordination with government agencies. At the same time, the academic sphere has experienced a notable consolidation of its postgraduate programmes on intelligence in both number and quality, projecting a not-too-distant future when universities will award degrees in intelligence studies.

This academic drive, coupled with the strength of businesses, gives Defence Intelligence the opportunity to advance and evolve into an advantageous capability that facilitates effective defence against today's increasingly dynamic and surprising threats.

Intelligence that merely reacts to technological progress would be insufficient to fulfil its mission. Instead, an intelligence that is consolidated as a proactive and innovative discipline will provide the freedom of action required to mitigate tomorrow's risks in all areas.

The following topics are covered in the Intelligence Journal number three:

— The European Union's determined move towards technological sovereignty in order to fully guarantee its strategic autonomy, and for which progress is being made in intelligence-enabled technologies.

— A Spanish Armed Forces' solution to the challenge of keeping abreast of the cognitive environment and its threats.

— Post-normal science will be explored as a conceptual framework for addressing problems with uncertain facts, conflicting values and urgent decisions, as well as the evolution from the traditional intelligence cycle towards a risk management approach, integrating intelligence and governance functions in the search for a shared vision of the security issue to be managed.

— It will address how generative AI transforms the detection, selection and analysis of information, enabling faster and broader access to diverse sources.

— Situational awareness in multi-domain warfare operations will also be studied in detail.

— It will analyse the emergence of Cyber Defence, which, thanks to the development of advanced technologies, can integrate cyber threat intelligence to plan and execute defensive operations.

— Another interesting work seeks to present some of the tools that are used when working with impact matrices and which allow us to analyse indirect relationships and to classify system variables, revealing hidden variables that gain relevance through indirect relationships.

— A comprehension of how new technologies applied to means of information gathering can help in the face of the challenge posed by certain proliferating countries whose nuclear activities appear to be moving away from a peaceful course will be sought.

— The impact of new technologies at each stage of the JISR process (TCPED), as well as the challenges arising from their use, will be examined.

— Transferring technological changes to the execution of ISR operations in the maritime domain, detailing the particularities it offers due to the unique organisation of a naval force in a Maritime Component Command, is the objective of another article.

— We will dive into Narrative Intelligence (NARINT), a crucial tool for understanding and countering information warfare, focusing on the context of Russia's war against Ukraine since 2014.

— Finally, the impact of new technologies on analysts, who are bombarded by massive amounts of information from open sources, will be reviewed.

To conclude this foreword, it is only fair to express our gratitude to all the experts who, with their contributions, help to consolidate this publication as a reference platform from which to promote the development and effectiveness of intelligence.

The transformation of intelligence in European security and defence: challenges and opportunities in the digital era

Carlos Hugo Fernández-Roca Suárez

1 Introduction

European security and defence are undergoing a profound transformation driven by unprecedent technological advances in the digital world. The accelerated Fourth Industrial Revolution —characterised by significant advances in digitalisation, automation, large-scale data management, and Artificial Intelligence (AI)— is altering the way intelligence is stored, analysed, and utilised in the military and strategic spheres. These technological developments, alongside a challenging geopolitical environment, especially following Russia's aggression against Ukraine, compel Europe to urgently strengthen its strategic capabilities in a coordinated and effective manner (European Council, 2022).

Governments in the European Union (EU) have acknowledged that investing in emerging technologies and the defence industrial base is essential to enhance European capabilities, increase its share in transatlantic security, and reduce critical dependencies on arms and technology (Fiott, 2024). Within this context, European institutions and Member States are developing reforms and ambitious plans to bring intelligence in defence up to date, implementing AI and other disruptive technologies while fostering European technological sovereignty as a common goal, which reinforces and does not oppose identity and national interests.

This article analyses the aforementioned transformation of intelligence in Europe, encompassing the impact of the Fourth Industrial Revolution, AI's primary role, institutional responses —such as the ReArm Europe plan—, specific technological application examples, and the pursuit of technological autonomy.

2 Impacts of the Fourth Industrial Revolution on intelligence defence

The so-called Fourth Industrial Revolution (4IR) has been described as a disruptive shift of an era, blurring the lines between what's physical and what's digital, the civil and military, and the realms of peace and conflict (Fojón, 2018). As previous industrial revolutions shaped battlefield driving,

the 4IR is introducing advanced technologies —such as autonomous systems, big data, the Internet of Things, and machine learning—, posing both opportunities and challenges for defence. In the military intelligence and defence scope, these changes entail the processing capability of diverse-sourced massive real-time data volumes —remote sensors, social media, commercial satellite imagery—, as well as the algorithmic automatization of ordinary analytic tasks.

The armed forces and the European intelligence agencies must adapt to this new technological landscape to maintain informational superiority and anticipation capability. Therefore, a transformation in the traditional doctrines and intelligence procedures is required. For instance, the proliferation of cutting-edge sensors and uncrewed platforms is increasing the amount of data collected exponentially —signals, imagery, communications—, which demands new AI-powered data fusion and analysis tools to extract relevant information. At the same time, non-state actors and rival powers also have access to cheap double-edge technologies —such as drones and cyberattack software— which "democratise" access to disruptive power, forcing European agencies to accelerate their innovation (Fojón, 2018). The 4IR is ultimately shaking the foundations of intelligence in security and defence, rendering traditional methods obsolete and demanding investments in new technical, organisational, and human capabilities.

An illustrative example is the concept of "algorithmic warfare" initially developed by the US Department of Defence. Algorithms were used to multiply the options and accelerate the decision-making on the battlefield (Fojón, 2018). Pioneer initiatives such as the American Project Maven —using machine learning to analyse imagery intelligence (IMINT) and target detection— have been used as a reference on how intelligent automation can upgrade the effectiveness of military intelligence.

Europe has taken note of these trends; Spain has considered Maven lessons to contemplate similar applications for the Spanish Armed Forces (Fojón, 2018). The implementation of derived-4IR tools poses ethical and doctrinal questions on the degree of autonomy allowed in intelligent arms systems or the reliability of a machine-made decision. These debates are very present in Europe, where a human-centred approach to AI use prevails (Csernatoni, 2023).

3 Artificial Intelligence as a transformative factor

Among 4IR technologies, AI stands out as the main transforming driver in security and defence. AI —understood in general terms as computer systems capable of performing tasks that normally require human intelligence, learning from experience (Fiott and Lindstrom, 2018)— has become a frontline strategic tool for the military and defence (Csernatoni, 2023).

Powers like the US and China have already implemented AI in their defence doctrines. These powers consider AI as a key element of technological superiority and warn of a potential new arms race in this field (Csernatoni, 2023). Despite AI having developed at a slower pace in Europe, there is an increasing belief in its revolutionary potential in the defence sector. On the one hand, it offers significant advantages in intelligence —such as automated threat analysis, scenario simulation, and decision-making support—; on the other, it raises ethical and security concerns —including algorithmic bias, lethal autonomy, and cyber vulnerabilities— that demand a balanced regulatory framework adapted to emerging challenges.

In the military intelligence scope, AI pursuits the acceleration and optimization of the whole intelligence cycle from the data collection —through algorithms capable of tracking open sources or managing swarms of sensors— to analysis —including the intelligent filtering of relevant information, the automatic recognition of patterns in images or intercepts, and anomaly detection— and finally to the distribution and exploitation of intelligence, via decision-support systems that provide analysts and commanders with optimal options generated from the processing of large volumes of data.

For instance, deep learning algorithms applied to satellite imagery can identify movements of adversary military groups much faster than human analysts, providing earlier warnings. By the same token, natural language processing tools can automatically classify and translate intercepted communications, enhancing the efficiency of signals intelligence (SIGINT).

These capabilities could enhance threat detection, as well as protection and preparation of emerging risks (Fiott and Lindstrom, 2018), reinforcing collective European security.

Nevertheless, AI implications are not unequivocally positive nor entirely known. There is some consensus that AI will act, at least in the short term, as a strategic facilitator rather than a total substitute for human intelligence (Fiott and Lindstrom, 2018), meaning that the autonomy of AI systems will continue to be limited and the human factor will remain essential in the supervision of algorithms and ultimate decision making.

In fact, the EU has highlighted the importance of maintaining a “significant human control” on autonomous weapon systems and military Artificial Intelligence, considering ethical and legal implications (European Parliament, 2020). As AI is making progress, Europe faces the challenge of leveraging its advantages without committing unacceptable risks, such as ensuring that AI systems do not lead to bias or systematic errors in intelligence analysis and that they preserve their operational integrity against manipulation attempts, such as attacks designed to deceive recognition algorithms.

On the other hand, Artificial Intelligence is not only a tool, but a strategic goal and a new field of confrontation. Its progressive militarisation —encompassing offensive applications such as cyberattacks, AI-driven disinformation, or armed unmanned vehicles— compels European intelligence services to develop specific detection, prevention, and response capabilities. This dilemma underscores the importance for Europe not to fall behind in the application of AI to defence, while also paving the way for its responsible use in accordance with international law (Csernatoni, 2023).

Currently, UE institutions acknowledge that AI is a double-edged sword. It can reinforce security, for instance, in surveillance tasks and early warnings, but it also poses threats if used maliciously or beyond human control (Csernatoni, 2023). For this reason, the EU advocates for "reliable, ethical and secure" AI even in military affairs, implementing these principles in their policies and research projects related to defence.

4 Europe's institutional responses: from the ReArm Europe Plan to the Defence Industrial Strategy

Aware of the scale of the technological challenge, the European institutions have proposed a series of strategic responses and political initiatives to transform their capabilities in intelligence, security and defence in recent years. An important milestone was the endorsement of the UE Strategic Compass in March 2022, which outlined a common vision of security and defence for the next decade, highlighting the need to improve, among other aspects, a shared forward intelligence (Council of the European Union, 2022).

The Compass particularly highlighted the mechanism creation, such as the Single Intelligence Analysis Capacity (SIAC), which focused on enhancing the implementation of the information of Member States and providing an assessment of major threats at the EU level (Council of the European Union, 2022). This strategic approach paved the way to subsequent plans specialised in capabilities and technology.

In the wake of the invasion of Ukraine in 2022, the EU has stepped forward, acknowledging that it should be rearmed and strengthening its defensive position for 2030. The President of the European Commission, Ursula von der Leyen, called for the mobilisation of resources on an unprecedented scale to provide Europe with credible deterrence before the end of the decade. As a result of this political will, the European Commission (2025) presented the plan initially known as ReArm Europe, an ambitious programme aimed at concentrating and coordinating defence investment by the Member States, with the support of European funds.

This initiative has now adopted the designation "Readiness 2030", due to the reservations expressed by some countries, including Spain and Italy,

regarding the original term, which was considered too bellicose or politically and socially sensitive. The plan foresees the mobilisation of more than €800 billion in cumulative defence investment by 2030. Its objective is to reduce divergences among Member States and to harness the economies of scale of the common market.

Some of the ReArm Europe specific goals are the following: to raise to 50% the share of military procurement expenditure allocated to European providers —thus strengthening the European Defence Technological and Industrial Base (EDTIB)— and to ensure that at least 35% of new capabilities are acquired jointly by several Member States, compared to the current low level of 18% (Fiott, 2024).

A significant increase in the exchange of weaponry and components among European countries is also envisaged. Were these objectives achieved, Europe would not only advance in its technological autonomy, but would also address long-standing structural deficiencies in key areas —such as secure communications, space surveillance, air defence, and cyber defence— many of which depend directly on advanced intelligence capabilities. In my view, however, it would be necessary to introduce the concept of strategic sovereignty of the nations that constitute Europe as sovereign states more clearly.

In parallel with the ReArm Europe plan, the EU has deployed financial and industrial instruments to support technological innovation in defence. Particularly noteworthy is the European Defence Fund (EDF), operational since 2021, with a budget of around €8 billion until 2027, dedicated to fostering collaborative military research and development projects (Fiott, 2023).

The EDF represents the first time that the Union, through its common budget, has directly invested in defence capabilities, already making it one of the largest funders of R&D in this field at the European level. Of this total, approximately €2.7 billion are allocated to innovative research —including disruptive technologies such as Artificial Intelligence, microelectronics, and advanced materials, among others— and €5.3 billion to prototype development and the consolidation of industrial capabilities (European Commission, 2021a).

The EDF is pursuing a dual goal: fostering cooperation among companies and Member States in developing new defence systems, thereby avoiding the fragmentation of national efforts, and strengthening the European Defence Technology Industrial Base (EDTIB) so that Europe can rely on its own supply with reduced European dependence on non-European providers.

This is a key point; previous analyses have shown that more than 60% of the defence procurement expenditure of EU countries between 2007

and 2016 was directed towards military imports from outside the Union, primarily from the United States (European Commission, 2022). The war in Ukraine once again highlighted this dependency, as an even greater proportion of the urgent arms purchases made in 2022-2023 were carried out with non-European suppliers, especially regarding U.S.-manufactured weapons and missile systems. The Union's institutions have warned that this situation is unsustainable if Europe aims for true strategic autonomy (European Commission, 2022).

Therefore, in addition to the EDF, complementary measures have been launched, such as the European Defence Industry Reinforcement through Common Procurement Act (EDIRPA), as well as regulatory proposals aimed at incentivising the acquisition of European products —for instance, tax exemptions applicable to collaborative projects within the single market.

Another relevant institutional component is the European Defence Industrial Strategy, published in March 2024. This is the Union's first comprehensive strategy focused on its defence industry, emerging as a direct response to the lessons of the war in Ukraine (Fiott, 2024). The Industrial Strategy places particular emphasis on military readiness and on the development of next-generation capabilities, many of which rely on emerging technologies.

Its main lines of action include consolidating European aggregate demand through joint procurement, promoting innovation in areas such as Artificial Intelligence, quantum computing, and space, and guaranteeing that the industrial base can rapidly scale up its production in the event of a crisis (Fiott, 2024).

Despite the strategy representing a positive step that proves a European vision, experts note that it also raises questions about the effective implementation and coordination with national efforts (Fiott, 2024). Still, it shows the growing priority of technology in defence within the European agenda.

Additionally, the EU and its Member States have strengthened NATO collaboration in terms of innovation, looking for synergies and task division —for example, NATO has launched its Defence Innovation Accelerator for the North Atlantic and an Innovation Fund, while the EU focuses on industrial projects and regulation.

In summary, Europe has, in just a few years, moved from a lagging position to a decidedly proactive stance in the face of the technological revolution in the defence field. Initiatives such as the ReArm Europe plan, the activation of the European Defence Fund, and the promotion of new industrial strategies reflect a clear determination to modernise both military capabilities and intelligence systems through the incorporation of AI and other advanced technologies.

All of this also responds to a fundamental strategic objective: safeguarding European technological sovereignty. From our perspective, however, this aspiration must be accompanied by a firm commitment to respecting the national interests of each sovereign state. The construction of shared technological autonomy cannot and must not take place at the expense of national sovereignties; instead, it must be grounded in forms of cooperation that acknowledge and respect the specific priorities of each nation.

5 Cases of technology application in intelligence and defence

This technological transformation can be observed in various projects and practical cases where AI and other innovations are already being applied in the field of European security and defence intelligence. One of the most direct examples is the *Artificial Intelligence for Defence* project (hereafter, AI4DEF), which was funded in 2020 under the European Defence Industrial Development Programme (EDIDP) —the precursor to the EDF. AI4DEF is a multinational project aimed at demonstrating the benefits of AI across various military functions, particularly in enhancing situational awareness, intelligence, surveillance, and reconnaissance (ISR), as well as the optimisation of operational planning (European Commission, 2021a).

More specifically, AI4DEF is developing a cloud-based platform that integrates Artificial Intelligence algorithms to, for instance, analyse imagery captured by unmanned aerial vehicles (UAVs) in real time and identify targets of interest. This project illustrates how AI can adopt an integrated and adaptable approach in the field of defence, being applied across land, air, and maritime domains to challenges such as the automated detection of mobile threats, three-dimensional terrain segmentation for urban operations, or the intelligent fusion of data from heterogeneous sensors (European Commission, 2021a).

Another key technological application lies in the advanced processing of satellite and reconnaissance imagery. The EU has the European Union Satellite Centre (hereafter, SatCen) at its disposal, located in Spain, which provides geospatial analysis to Member States and missions under the Common Security and Defence Policy. Given the growing volume of Earth observation imagery available —including that from the EU's Copernicus programme and commercial providers—, SatCen and the European Defence Agency have promoted studies to integrate AI into Imagery Intelligence (IMINT) processes, to automate object identification, change detection in infrastructures, and border surveillance. For instance, computer vision algorithms can analyse thousands of satellite images in search of patterns —such as unusual concentrations of vehicles or signs of military preparation— with a speed and accuracy far superior to that of a human team, thereby allowing analytical efforts to focus solely on those alerts with the

highest likelihood of relevance. Such tools have gained particular importance in recent conflicts such as the one in Ukraine, where open-source intelligence (OSINT) and commercial satellite imagery have played a fundamental role in monitoring military movements. Building on this experience, European agencies aim to equip themselves with AI-based platforms capable of filtering noisy data and extracting useful, actionable knowledge from the vast volume of open data available.

European countries have also begun to apply AI in support of counterterrorism and counter-organised crime intelligence. One example is the use of algorithms to analyse Internet and social media communications to detect early signs of radicalisation or attack planning. There are pilot projects, often in collaboration with domestic security agencies, that combine multilingual natural language processing with social network analysis techniques to identify potentially dangerous profiles, always in compliance with data protection laws. Although this is a sensitive field, the use of Artificial Intelligence for predictive functions could enable European intelligence units to prioritise investigations and prevent violent acts based on indications that would otherwise remain hidden among vast volumes of data. Organisations such as Europol have already explored such tools to screen online extremist content, and at the national level, several intelligence services are investing in advanced big data analysis capabilities. This technological evolution illustrates how the boundaries between internal and external security tend to blur —a dynamic recognised by the Strategic Compass (Council of the European Union, 2022)— and requires a closer inter-agency cooperation.

In the armed forces of European nations, adopting Fourth Industrial Revolution (4IR) technologies is also evident. Robotics and unmanned systems are increasingly common in reconnaissance and intelligence missions. For instance, several NATO countries deployed in the Sahel region have employed mini drones for tactical aerial surveillance, thereby reducing risks for personnel and obtaining real-time intelligence on insurgent movements. In complex urban environments, where GPS may fail and obstacles are abundant, AI-based solutions are being explored to enhance the autonomous navigation of drones. In 2018, France, through the CEA-List organisation, specialised in AI, funded several projects aimed at solving the precise three-dimensional localisation of unmanned aerial vehicles (UAVs) in densely built-up urban environments by combining computer vision and deep learning (Ministry of the Armed Forces, 2019).

This type of technical challenge, such as detecting and avoiding obstacles in narrow streets or identifying hidden human figures among buildings, is being addressed through algorithms trained to interpret video images in real time. The progress achieved not only strengthens military recognition

capabilities, but also shows significant potential for dual-use applications, for example, in disaster management or in the field of civil security.

It is also worth highlighting the ambitious Franco-German-Spanish project of the Future Combat Air System (FCAS), conceived as a "system of systems" that will integrate a sixth-generation manned fighter with swarms of combat drones and a "combat cloud" that will connect sensors and operators in real time. Although still at the conceptual stage, the FCAS explicitly incorporates the use of AI and cloud computing technologies to enable massive data fusion and the dynamic allocation of targets across platforms.

This programme, led by France, exemplifies how the European vision for air superiority toward 2040 and beyond is closely dependent on leveraging advanced AI capabilities —for cooperative management of unmanned systems, cognitive electronic warfare, *inter alia*— and ensuring the full interoperability of autonomous systems. If FCAS were to be successful, it would equip Europe with a highly sophisticated distributed intelligence and command architecture, significantly reducing its operational dependence on US assets in future scenarios.

To sum up, the above-mentioned cases —AI4DEF, AI-powered SatCen, counter-terrorism big data analysis, autonomous drones, and FCAS— prove the range of domains in which technology is transforming the work of European intelligence and defence. From the tactical to the strategic level, AI, robotics, and digital tools are amplifying the scope and speed with which Europe can obtain and exploit information of military value.

However, this technological revolution requires a political and strategic vision guaranteeing its feasibility, which is linked to the concept of technological sovereignty discussed below.

6 The quest for European technological sovereignty

The European drive to implement AI and emerging technologies in defence is tightly linked with the aspiration of achieving a major technological sovereignty. This concept refers to Europe's capacity to decide and act autonomously in the technological sphere, by controlling critical supply chains and reducing excessive dependencies on external powers in strategic domains (Ministry of the Armed Forces, 2019). In recent years, "technological sovereignty" and "strategic autonomy" have become key themes within the EU discourse, driven by challenges such as the US-China trade and geopolitical rivalry, supply chain disruptions —e.g., semiconductors— and the European defence dependency on non-EU suppliers.

In the realm of security and defence, technological sovereignty means that Europe can develop and produce its own critical technologies —from AI and cybersecurity to satellites, advanced military platforms, or secure

5G networks— without being subject to external vetoes or vulnerabilities. Ursula von der Leyen has defended this idea during her term of office at the helm of the Commission, aligning it with the vision of a "Geopolitical Commission" capable of furnishing the EU with the tools to be a strategic actor in its own right (Csematoni, 2023). The pursuit of technological sovereignty has spurred initiatives such as the identification of "Important Projects of Common European Interest" (IPCEI) in fields like microelectronics and the cloud, the European Chips Act to boost semiconductor production in Europe, and the aforementioned mobilisation of defence investments to strengthen the EDTIB. Specifically in defence, the March 2022 Versailles Declaration —signed by the EU's heads of state and government— explicitly outlined the need to reinforce the European defence technological and industrial base and to correct strategic dependencies, listing key sectors where Europe must ensure control.

AI is precisely considered one of these critical sectors. The French Government even stated in its 2017 Strategic Review of Defence and National Security that expertise in AI would be a matter of sovereignty in the future (Ministry of the Armed Forces, 2019). In line with this, France and other countries have advocated for the EU to treat military AI and deep tech as a domain for priority investment, in order to avoid falling behind the United States or China.

The discourse on technological sovereignty also permeates the narrative on data and intelligence: there is a persistent insistence that Europe must be able to store, process, and extract value from its data —including intelligence data— on secure European infrastructure, avoiding dependencies on foreign cloud services that could pose risks of access denial or disruption. This is an argument in favour of initiatives like GAIA-X —an open data infrastructure— or of reinforcing indigenous capabilities in quantum encryption and cybersecurity.

However, achieving technological sovereignty does not mean isolation: the EU recognises that international cooperation remains important. For instance, a balance is sought whereby Europe can "stand on its own two feet" in defence technology yet still interoperate fully with NATO allies. Nor do all EU countries share the same emphasis on autonomy. While France traditionally pushes a vision of a "Europe puissance" capable of autonomous action, other nations view this autonomy as complementary —not a substitute— for the Transatlantic Alliance.

In any case, the concept of technological sovereignty has served to guide concrete policies: the EU has made funding from the EDF conditional on the majority participation of industries from Member States, preventing control by companies from outside the EU. Similarly, supply vulnerabilities are being mapped; for example, Europe imports reconnaissance drones

from Israeli or American suppliers, which has spurred projects to manufacture European drones. The European strategic discourse now clearly links technological superiority to strategic independence: whoever controls the critical technologies will primarily control their own security and defence destiny.

Facing this strategic priority, several challenges emerge. Developing cutting-edge technologies requires enormous investment, coordination, and the attraction of talent, in a context where Europe is competing with more dynamic innovation ecosystems like Silicon Valley or Shenzhen. Similarly, imposing a "Buy European" approach in defence could drive up costs or delay capabilities if European industry cannot produce certain equipment at the required pace —for example, armed drones, where until recently there was no established European alternative.

Therefore, technological sovereignty is being approached as a goal to be achieved gradually, combining cooperation between EU Member States —to achieve critical mass— with selective external collaboration where necessary. In this context, France's role has been crucial, as will be elaborated in the following section, as it has acted as a catalyst for European technological autonomy, driving common industrial projects and leading by example through ambitious national policies in AI and defence.

7 Regulatory aspects in the digital transformation of security and defence in Europe

The digital transformation of European security and defence requires a structured legal framework that regulates both disruptive technological developments and the protection of strategic infrastructure. In recent years, the EU has deployed a series of regulatory instruments aimed at establishing a regulated, coherent, and secure environment for the digitalisation of essential services, including those with implications for intelligence and technological sovereignty.

One of the most significant developments is (EU) Directive 2022/2555[1], known as NIS 2, which replaces and expands the original NIS Directive (2016/1148/EU). This new regulatory framework establishes stricter requirements for entities in key sectors —including transport, energy, public administration, and certain digital infrastructures— and introduces obligations concerning risk management and incident reporting. Although activities strictly related to national defence are excluded from its scope

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (OJ L 333/80, 27.12.2022).

(Art. 2.3), the directive indirectly affects strategic operators that may collaborate with the defence sector or handle sensitive information.

Among the most significant new features is the establishment of the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) in Article 16, which facilitates operational coordination between Member States in the event of serious cybersecurity incidents with potential cross-border effects. The effective application of this directive depends on its transposition by the Member States. In the case of Spain, this adaptation finds an already advanced foundation in Royal Decree 311/2022, which reforms the Spanish National Security Framework (Esquema Nacional de Seguridad [ENS])[2] and anticipates principles of active protection, continuous supervision, and response to threats, in line with community standards.

In parallel, the EU has formulated a comprehensive legal approach for regulating AI through the proposal for a Regulation laying down harmonised rules on Artificial Intelligence, known as the Artificial Intelligence Act[3]. This regulation, still undergoing parliamentary approval, introduces a classification system based on the level of risk posed by an AI system, establishing proportional restrictions according to its potential impact on the exercise of fundamental rights, public safety, or institutional integrity.

AI systems classified as high-risk —such as those used in critical infrastructure, biometric surveillance, or the administration of justice— will be required to comply with strict obligations regarding data quality, technical documentation, human oversight, and traceability. Although the regulation formally excludes military and defence applications from its scope (Art. 2.3), its impact is significant in contexts of dual-use or civil-military cooperation, particularly concerning systems used by public authorities or contractors operating in sensitive environments.

The regulation also envisages the creation of a European Artificial Intelligence Office, conceived as a supervisory and coordination body responsible for ensuring the correct application of the rules across the Union's territory. This body is established as a key element to ensure the ethical and controlled development of automated technologies, including those that can directly impact essential state functions.

Collectively, the European regulatory framework reflects a legal architecture designed to ensure a controlled digital environment, compliant with high technical standards and the fundamental principles of European law. The interplay between regulations such as NIS 2, the future AI Act, and

[2] Royal Decree 311/2022, of 3 May, regulating the [Spanish] National Security Scheme. BOE no. 106, of 4 May 2022.

[3] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (COM/2021/206 final).

sector-specific digital proposals constitutes an essential axis for the strategic evolution of intelligence and defence capabilities in the technological age.

8 Prospective scenarios towards 2040: the future of European digital intelligence

Looking ahead to 2040, several possible scenarios for European intelligence and security can be foreseen, depending on how current opportunities and risks are managed. The following three prospective scenarios outline plausible futures for the role of digital intelligence in Europe, considering technological, geopolitical, and regulatory variables.

8.1 The first scenario: Autonomy and integrated European intelligence

In this future, the EU successfully realises its transformation plans. By 2040, Europe possesses a fully interoperable and sovereign digital defence infrastructure: next-generation European satellites provide ubiquitous surveillance; secure European 5G/6G networks connect sensors and command centres in real-time; and Member States share intelligence through a common, robust, and protected platform, an evolution of the current SIAC.

This progress has been made possible by an approach that respects and upholds the sovereignty of nations. Governments have succeeded in building a future where national interests are not diluted but instead converge and are mutually reinforced within a framework of voluntary cooperation. Far from representing a cession of sovereignty, European collaboration has become a tool to strengthen national capabilities and project them more effectively in a complex international environment.

AI, developed in accordance with these ethical principles, is routinely used to anticipate crises, detect hostile disinformation campaigns, and coordinate multinational deployments. The EU has established a permanent European Intelligence Centre, where analysts from all member countries work together with access to common databases, while respecting classification levels. Thanks to sustained investment in R&D, Europe has mitigated its strategic dependencies by producing critical chips and sensors locally, competing on an equal footing with the US and Asia in areas such as cybersecurity, robotics, and military AI (Csernatoni, 2023).

From a political standpoint, the EU gains regulatory influence and successfully sees its “trustworthy AI” approach adopted globally in the armaments sector, thereby helping to prevent an uncontrolled race towards the development of autonomous weapons. In this scenario, European digital intelligence acts as a security multiplier: it anticipates hybrid threats,

facilitates rapid responses to crises, and underpins European strategic autonomy in international decision-making.

Current initiatives, such as the Strategic Compass and PESCO, are successfully implemented, strengthening solidarity among Member States in the face of external threats and consolidating the EU's role as a key factor in international security.

8.2 The second scenario: Persistent dependency

In this scenario, integration efforts in defence advance only to a limited extent, partly because several Member States choose to reassert their sovereignty in the realm of security and defence. In the wake of the crisis in Ukraine, a logic of national action prevails, whereby each country strengthens its capabilities according to its own strategic assessments, establishing bilateral alliances and contracting directly with international suppliers based on its specific needs.

By 2040, European intelligence will remain structured primarily around national capabilities, and the EU will have failed to consolidate a common operational core. The CIIU maintains a symbolic and basic coordination function but does not evolve into a fully integrated platform. This configuration allows Member States to retain control over their sensitive information, but it hampers rapid collective responses to shared crises (Csernatoni, 2023).

On the technological front, Europe has advanced cautiously in the development of Artificial Intelligence for military applications, partly due to an overly cautious ethical approach, which has reduced its competitiveness compared to powers like China, which is projected to achieve military AI supremacy by around 2035 (Csernatoni, 2023).

This situation has reinforced its strategic dependence on the United States, limiting Europe's ability to execute complex operations in a fully autonomous manner. Consequently, its diplomatic room for manoeuvre is reduced, and certain vulnerabilities persist in the face of international actors with more assertive agendas (Csernatoni, 2021).

8.3 The third scenario: Conditional cooperation

This scenario, the most likely to happen, places Europe in an intermediate position. By 2040, the EU will have achieved notable progress in technological and intelligence integration, although certain structural limitations will persist. Common security is upheld through mechanisms like the Strategic Compass, renewed every five years, yet Europe continues to depend partially on imports for critical technologies.

The development of AI in Europe advances primarily in defensive applications, avoiding an uncontrolled race towards autonomous weaponry. This approach is made possible by international agreements promoted by the EU itself, which have succeeded in establishing strict regulations for these technologies (Calderón and Pedemonte, 2023).

Transatlantic cooperation remains solid, albeit adapted to a new equilibrium: the US continues to provide strategic intelligence on a global scale, while Europe contributes regional stability and specialised capabilities in local intelligence. NATO, for its part, incorporates European ethical standards into the development of AI, thereby reinforcing operational trust among allies (Calderón and Pedemonte, 2023).

On the industrial front, although the US retains supremacy in key sectors, European firms lead in strategic niches such as cybersecurity and intelligent non-lethal drones. In this context of contained competition, the EU wields significant influence in the international regulation of AI, helping to prevent accidental conflicts arising from unsupervised algorithms.

Europe will be ultimately stronger in 2040 than in 2025, yet it will maintain certain selective dependencies. Its digital intelligence will have reached a considerable level of effectiveness, though it will still require the support of allies to achieve full sovereignty.

These scenarios —analytical approximations— highlight that the future of European intelligence will depend heavily on the decisions made today. How Member States balance cooperation and autonomy, joint investment and national priorities will be decisive in shaping the direction of that future.

The decisive variable will be the political willpower of the Member States to sustain investment, uphold their principles, and articulate forms of cooperation that are compatible with their national interests. Digital intelligence would become either a strengthening or an exposure factor in security matters, depending on how it is managed. Therefore, envisioning these futures is not a purely speculative exercise, but a strategic tool for the present: Europe must not resign itself to having others define its destiny; it must resolutely assume the responsibility of building it from the sovereignty of its nations.

9 Conclusions

The transformation of intelligence for European security and defence within the digital age is a complex and dynamic process, responding directly to the challenges posed by the Fourth Industrial Revolution and the growing sophistication of hybrid and conventional threats. The widespread adoption of AI, big data, and autonomous systems is redefining

the operational capabilities and procedures of European armed forces and intelligence agencies, offering exceptional opportunities to significantly enhance the effectiveness, speed of response, and precision of operations.

Both the EU and its sovereign nations have clearly identified these potential benefits, but also fully recognise the involved technological, ethical, and political challenges. This has translated into the implementation of multiple strategic initiatives and investment programmes, notably including the Strategic Compass, the Defence Industrial Strategy, the European Defence Fund, and key projects such as ReArm Europe, Eurodrone, and the Future Combat Air System (FCAS). These efforts aim to consolidate European strategic autonomy by reducing its technological and operational dependence on third countries, especially in critical areas like AI, cyber defence, satellite technologies, and unmanned vehicles.

Nevertheless, Europe continues to face decisive challenges. The differences between sovereign nations —a result of historical trajectories, strategic structures, and legitimate national priorities— constitute a structural reality that directly influences how security and defence cooperation is articulated. Far from being an impediment, this can become a factor of strength if managed through mutual respect and a willingness to collaborate. The goal is not to impose uniformity, but to foster cooperation based on respect for national sovereignty.

Today, the EU has yet to articulate a clear and coherent doctrine on the military use of emerging technologies like Artificial Intelligence. This failure threatens to generate fragmented, ineffective strategies constrained by bureaucratic logic detached from national realities. In a rapidly evolving technological environment, an agile and coordinated response among sovereign states is imperative —one guided by national interest, not external agendas— to guarantee defence and security from the foundation of a genuine Europe of nations.

Furthermore, it will be essential to manage strategic relationships with key allies like the United States appropriately. The strategic autonomy that Europe seeks should not be interpreted as distancing, but as a pursuit of balance, strengthening its own capabilities to complement those of NATO. This approach necessitates constant dialogue, close cooperation, and reinforcing European influence in the ethical regulation and international normative framework governing the use of military AI.

Europe possesses fundamental assets to confront these challenges from a position of strength: it boasts first-rate scientific talent, competitive technology firms, a consolidated single market, and a significant tradition of security and defence cooperation. The political commitment and active involvement of countries like France, Germany, Italy, and Spain provide

a firm foundation for continuing to drive this transformation, building on national capabilities which, when combined voluntarily and in a coordinated manner, strengthen the whole.

Looking ahead to 2040, digital intelligence could acquire a strategic significance comparable to the role played by nuclear weapons in the 20th century, redefining global power balances and strategies. Europe aspires for this digital intelligence to serve as an effective tool for safeguarding peace, promoting democratic values, and preventing it from becoming an instrument of totalitarian control or uncontrolled conflict. To achieve this, it will be crucial to maintain a human-centric approach, ensuring mechanisms for democratic oversight and transparency to the greatest extent possible without compromising legitimate security needs.

In conclusion, this transformation —situated within the digital age— represents an exceptional opportunity to strengthen both the collective security and the strategic autonomy of Europe's sovereign nations. While considerable challenges persist, the progress achieved demonstrates a Europe in constant evolution, where cooperation is built on the foundation of respect for national sovereignty. If political will is maintained, sustained investment in research and development is guaranteed, and a common vision for the responsible use of technology is consolidated, Europe will be in a position to reach 2040 with significantly reinforced intelligence capabilities, prepared to effectively protect its citizens, as well as its principles and values, in an increasingly dynamic and uncertain international environment.

Bibliography

Ash Center. (2024). *AI, digital sovereignty, and the EU's path forward: A case for mission-oriented industrial policy* [online]. Harvard Kennedy School. [Accessed: 2025]. Available at: https://ash.harvard.edu/resources/ai-digital-sovereignty-and-the-eus-path-forward-a-case-for-mission-oriented-industrial-policy/

Calderón, I., and Pedemonte, C. (2023). NATO's AI strategy focuses on responsible use: AI chief [online]. *NATO News*. [Accessed: 2025].

Council of the European Union. (2022). *Strategic Compass for Security and Defence* [online]. Brussels: Council of the European Union. [Accessed: 2025]. Available at: https://www.consilium.europa.eu/es/policies/strategic-compass/

Csernatoni, R. (2021). *Security 2040: Perils and promise over the near horizon* [online]. Carnegie Europe. Available at: https://carnegieeurope.eu/2021/03/25/security-2040-perils-and-promise-over-near-horizon-pub-84124

Csernatoni, R. (2023). Weaponizing innovation? Mapping artificial intelligence-enabled security and defence in the EU [online]. *Non-proliferation and Disarmament Papers*. Stockholm, SIPRI. 84. [Accessed: 2025]. Available at: https://www.sipri.org/publications/2023/eu-non-proliferation-and-disarmament-papers/weaponizing-innovation-mapping-artificial-intelligence-enabled-security-and-defence-eu

European Commission. (2021a). *EDIDP 2020 – Artificial Intelligence: Project AI4DEF (Factsheet)* [online]. Brussels, DG DEFIS. [Accessed: 2025]. Available at: https://defence-industry-space.ec.europa.eu/system/files/2021-06/EDIDP2020_factsheet_AI_AI4DEF.pdf

European Commission. (2021b). *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence* (COM/2021/206 final) [online]. European Union. [Accessed: 2025]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

European Commission. (2022). *Joint communication to the European Parliament and the Council on defence investment gaps analysis and way forward* (JOIN(2022) 24 final) [online]. [Accessed: 2025]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022JC0024EUR-Lex+1EUR-Lex+1

European Commission. (2025). *White paper on European defence – Readiness 2030 (ReArm Europe Plan)* [online]. Brussels, European Commission. [Accessed: 2025]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_793

European Council. (2022). *The Versailles Declaration* [online]. Brussels: European Council. [Accessed: 2025]. Available at: https://www.consilium.europa.eu/es/press/press-releases/2022/03/11/the-versailles-declaration-10-11032022/Consilium

European Parliament. (2021). *Report on artificial intelligence in a digital age – Civil and military* (2020/2266(INI)). Brussels.

European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union, L 333/80*.

Finabel. (n. d.). *A shift towards sovereign EU military capabilities? The Eurodrone project awaits final signature* [online]. [Accessed: 2025]. Available at: https://finabel.org/a-shift-towards-sovereign-eu-military-capabilities-the-eurodrone-project-awaits-final-signature/

Fiott, D. (2021). The European front-runners: France, Germany, Italy and Spain in PESCO. *European Foreign Affairs Review*. 26(Special Issue), pp. 87-110.

Fiott, D. (2023). *Investing and innovating? Spain and the European Defence Fund* [online]. Elcano Royal Institute. [Accessed: 2025]. Available at: https://www.realinstitutoelcano.org/en/analyses/investing-and-innovating-spain-and-the-european-defence-fund/

Fiott, D. (2024). *Beyond strategy? Industrial strategy and the future of European defence* [online]. Elcano Royal Institute, ARI 57/2024. [Accessed: 2025]. Available at: https://www.realinstitutoelcano.org/analisis/mas-alla-de-la-estrategia-estrategia-industrial-y-futuro-de-la-defensa-europea/

Fiott, D. and Lindstrom, G. (2018). *Artificial intelligence: What implications for EU security and defence?* (EUISS Brief No. 10) [online]. Paris, European Union Institute for Security Studies. [Accessed: 2025]. Available at: https://www.iss.europa.eu/publications/briefs/artificial-intelligence-what-implications-eu-security-and-defenceiss.europa.eu

Fojón, E. (2018). *La cuarta revolución industrial, el "algoritmo de guerra" y su posible aplicación a la Defensa española* [online]. Elcano Royal Institute, ARI 23/2018. [Accessed: 2025]. Available at: https://www.realinstitutoelcano.org/analisis/la-cuarta-revolucion-industrial-el-algoritmo-de-guerra-y-su-posible-aplicacion-a-la-defensa-espanola/

Global X. (2023). *Rearming Europe boosts defense tech* [online]. Mirae Asset. [Accessed: 2025]. Available at: https://www.globalxetfs.com/research/rearming-europe-boosts-defense-tech/

Liboreiro, J. (2023). Brussels rebrands 'Rearm Europe' after backlash from Italy and Spain [online]. *Politico*. [Accessed: 2025].

Ministry for Europe and Foreign Affairs. (2022). *A strategic compass to strengthen the security and defence of the European Union by 2030* [online]. [Accessed: 2025].

Ministry of the Armed Forces. (2019). *L'intelligence artificielle au service de la défense – Rapport de la Task Force IA*. Paris, Ministry of the Armed Forces.

OpenAI. (2024). *ChatGPT* (GPT-4 model) [The text has been reviewed with the support of AI-based tools to improve clarity and coherence] [online]. [Accessed: 2025]. Available at: https://chat.openai.com/

PESCO. (n. d.). *Joint EU Intelligence School (JEIS)* [online].

Spain (2022). Royal Decree 311/2022, of 3 May, regulating the National Security Scheme. *Official State Gazette*. 106.

Jorge Ricart, R. (2024). Waking up slowly: Defense AI in Spain [online]. In: Borchert, H., Schütz, T. and Verbovszky, J. (eds.). *The very long game*. Springer. [Accessed: 2025].

Conductual Explorer: an autonomous solution to the cognitive environment challenge

Pablo Caneda González
María Porrar Santisteban
Álvaro Álvarez Álvarez

Abstract

In the hyper-connected age in which we live, the means by which people communicate are mainly digital and accessible to any network user. This puts a wealth of subjective opinions and publications at one's fingertips available with one's device. In the cognitive domain of influence and intelligence, it is a challenge to harness this flow of information, as these are not quantities of data that can be processed by one or more human resources in a reasonable amount of time.

To this end, the initiative has arisen within the Spanish Armed Forces and, more specifically, in the area of operational-level influence and intelligence, to develop autonomously, without the support of external agents and with limited resources, a technological solution that has been christened Conductual Explorer, which allows the vast amounts of data obtained from digital media or social networks in a defined geographical or social environment to be managed.

The analysis and storage of all this information makes it possible to monitor the target information environment over time, being able to detect trends and narratives and their evolution over the envisaged time periods. The processing of this information shall be of great use in supporting decision-making at the level at which the Spanish Armed Forces operate.

Keywords

Social networks, Open sources, Influence, Intelligence, Artificial Intelligence.

1 Introduction

> *"On taking office, Caesar was the first to establish that, in the future, a record would be kept of all the acts of the senate and of the people, and that this record would be made public."*

According to Suetonius, in 59 B.C., Julius Caesar ordered the publication of the *Acta diurna populi Romani*, which were periodically displayed in public places and were intended to provide Roman citizens with a more accurate channel of information than the gossip and hearsay that travelled by word of mouth through the intricate networks of the complex Roman social life.

Considered by many as the first written medium and by others as the first official publication in the form of the original official state bulletin, it soon established itself as a tool for influencing public opinion. As Emperor Augustus, Caesar's successor, stated, its usefulness as a propaganda tool in the service of the State was undeniable.

Since then, the relevance of the ability to influence audiences has grown in parallel with the complexity and size of human organisations and more markedly so today, with the irruption of new technologies.

Today, traditional media are integrated with new forms of information dissemination, new applications and social networks allowing millions of users to participate in the generation and dissemination of content in a decentralised way. This vast production, together with the hyper-connectivity generated in digital environments, is capable of rapidly producing or modifying currents of opinion that must be taken into account in the study of the new meta-geopolitics.

In the current context of hybrid conflicts, the "grey zone" has been established as a space of strategic dispute where narratives, misinformation and manipulation of public opinion play a crucial role. The proliferation of digital platforms has transformed the information environment into an unconventional battlefield, where state and non-state actors employ cognitive warfare tactics to influence perceptions of reality. In this scenario, the ability to analyse sentiment in social networks and media, as well as to classify a large volume of data efficiently, becomes a key resource for both national defence and security.

According to Spanish military doctrine, intelligence encompasses a series of activities that make it possible to obtain a comprehensive and up-to-date vision of the environment in which operations are carried out. The need to obtain a comprehensive vision of the multi-domain makes it necessary to include in intelligence capabilities tools for analysing new areas such as, for example, the growing cognitive domain.

The study and knowledge of the social and cultural conditions of a given environment will make it possible to find indicators in the cognitive domain that will serve as an alert to possible crises or security threats.

In order to preserve its role, military intelligence must innovate and adapt to a new context, as Julius Caesar did when he established the diurnal minutes in ancient Rome

In the field of defence, the enormous potential of the observation of open sources is widely known. It can enable one to quickly obtain the information needed to produce basic intelligence on any part of the world and it can support a deep understanding of the operating environment, as well as detect trends and currents of thought in a part or the whole of a society.

Upgrading to new capabilities brings some challenges. The sheer volume of information to be handled poses a challenge for analysts, the need to filter out incorrect, intentional or biased misinformation requires experienced and specifically trained staff, which translates into considerable human and time resources.

To mitigate these drawbacks, a close collaboration becomes necessary between the analyst, who knows the product necessary to determine trends and currents in a social environment, and the data processing expert, who is familiar with the techniques that make it possible to obtain, store and process large amounts of data.

In the development of Conductual Explorer, both technical aspects and the needs and points of view of the analyst have been taken into account, trying to adapt the potential of the tool to the needs in terms of analysis as much as possible.

1.1 Motivation: solving internal needs with creativity and reduced costs

In the specific case to be developed in this article, in order to meet the challenge of processing large amounts of information from open sources, there is a need to develop tools that allow the dynamics of the information environment to be interpreted both systematically and efficiently. Traditional methods of analysis have limitations in terms of scalability and speed, making it difficult to obtain usable intelligence in real time. The solution presented here responds to this problem through an innovative and low-cost approach based on automation and the use of Artificial Intelligence for the extraction and classification of data and for the extraction of statistics and metrics illustrative of the analysis of the information environment being carried out.

This code, developed entirely in Python, has been developed with the approach of being an OSINT (Open-Source Intelligence) tool. It is designed

to facilitate the work of security and defence analysts and researchers. Its purpose is to offer an accessible and adaptable alternative to the specific requirements of different operational contexts, without relying on expensive infrastructure or proprietary commercial solutions. By combining advanced natural language processing (NLP) techniques, Artificial Intelligence models of machine learning and deep learning, as well as traditional programming techniques, the tool allows not only to analyse the prevailing sentiment in the digital environment, but also to structure and categorise large volumes of information from both Social Media and the Media in general, with a high degree of accuracy, and to expose the results in an easily understandable way. At the same time, it is an example of the application of advanced programming technologies as a solution to a specific problem, using the appropriate technical resource to solve each aspect of the problem. The latter underlines the idea that programmatic solutions are a means and not an end, and that the most modern solution is not always the most appropriate one to address a problem.

1.2 Context of the project and its importance

The use of digital information in grey zone scenarios has proven to be a determining factor in shaping military, diplomatic and security strategies. Grey-zone conflict is characterised by the absence of direct confrontation, with information dominance being central to the struggle for influence and legitimacy. In this context, the ability to anticipate trends, detect patterns of misinformation and analyse discourses in real time enables government and private actors to make informed and strategic decisions.

This project was born out of the need for a flexible and efficient tool to enable analysts to manage the growing volume of data in cyberspace. Its implementation offers advantages in the early detection of threats, the monitoring of influence campaigns and the evaluation of the impact of narratives on different target audiences. Furthermore, its modular nature allows it to be integrated with other OSINT tools, thus optimising the intelligence gathering process in high-volatility and high-risk environments.

This initiative aims to strengthen analytical capacity in the field of security by providing an effective and accessible solution for the study of the digital information environment in conflict zones.

1.3 Objectives and scope of the programme

The main objective of this program is to provide an OSINT tool capable of collecting, analysing and classifying data from both social media and the media in general in areas of conflict or interest in order to optimise strategic security and defence decision-making. For this purpose, the tool is based

on Natural Language Processing (NLP) techniques, allowing an automated assessment of the prevailing sentiment in the digital environment and an efficient segmentation of the data according to specific criteria.

Specific objectives

- Sentiment analysis automation: implementing NPL models to identify and categorise emotions and trends in digital discourse.
- Advanced data classification: developing Artificial Intelligence models to segment information from social media and the media in general according to importance and reliability.
- Presenting the results in an understandable way, with statistics and metrics that make it easy to understand the results of the analysis and draw conclusions.
- Real-time monitoring: design a continuous updating structure to detect changes in the digital narrative and assess their impact.
- Adaptability and scalability: create a modular system that can be adjusted to different operating environments and specific requirements.
- Integration with other OSINT tools: facilitate interoperability with existing databases and analysis systems to maximise operational efficiency.

Scope of the programme

The programme has been designed with a flexible and modular approach, allowing it to be implemented in different scenarios and levels of operation. It is aimed at both government agencies and private organisations interested in monitoring digital information in crisis or conflict situations.

The programme may be used for:

- Disinformation and propaganda analysis: identifying influence campaigns and information manipulation strategies on digital platforms.
- Narrative impact assessment: determining how certain discourses affect public perception and audience behaviour.
- Strategic decision support: providing structured data and predictive analytics to improve response to emerging threats.
- Tracking conflict dynamics: monitoring the development of crises in real time through digital content analysis.

This comprehensive approach seeks to provide intelligence analysts with a tool that not only simplifies the management of large volumes of information, but also provides advanced predictive and strategic analysis capabilities to understand the desired information environment.

2 Need for an analyst and creation of the database

The use of open source intelligence (OSINT) tools has become increasingly important in the field of data analysis, providing significant support to the analyst, without replacing the essential work of the human factor. While automation makes it possible to process large volumes of information quickly and efficiently, contextual interpretation and the definition of search criteria still require human intervention to ensure the accuracy and reliability of the data collected.

Prior to the implementation of an OSINT tool, it is necessary to establish a methodological framework to ensure the quality of the analysis. The initial phase involves delimiting the information environment, defining the search objective and structuring the information to be exploited in a robust database. The absence of one or more of these steps increases the margin of error and may lead to incomplete or inaccurate results.

In this chapter, the essential procedures for data collection and structuring are detailed, highlighting the importance of the analyst in building a database that facilitates the processing of information and obtaining valid results. In addition, case examples are provided for each stage of the procedure.

2.1 Analysis of the area: data collection and structuring

The delineation of the information environment is the first step in OSINT analysis, and clear criteria for data collection must be established. This phase involves the identification of spatial and temporal parameters, the selection of relevant sources and audiences, and the identification of key actors within the target digital ecosystem.

The data collection methodology is organised in three key stages.

2.1.1 Defining the scope of the study

The delimitation of the analysis must address a number of key factors that ensure the accuracy and pertinence of the information collected. Firstly, it is essential to establish the spatial and temporal parameters, clearly defining the object of study and the period of observation, which allows the data obtained to be properly contextualised.

It is also necessary to determine the sector of interest, identifying the thematic area in which the analysis will be carried out. This can be situated in political, social, economic or security dimensions, depending on the objective of the research.

Finally, the selection of relevant platforms and media is an essential aspect of the process. The identification of primary and secondary sources, such as social networks, forums, blogs and specialised digital media, allows for the collection of information representative of the information ecosystem analysed.

2.1.2 Selection and filtering of information sources

The proper functioning of the OSINT tool developed depends, to a large extent, on the accuracy and reliability of the data feeding its analysis base. Although information gathering is a complex process, its effectiveness lies in the prior work of the analyst, who must define clear selection criteria and ensure that sources are verifiable and representative of the information environment. Without this initial phase, the margin of error increases, directly affecting the programme's ability to process and classify data accurately, delivering results that may differ from reality.

To optimise its performance, the OSINT tool integrates data from media, social media and open sources, prioritising those that meet reliability standards. In addition, it uses automatic filters and standardisation techniques to minimise information noise, detect communication patterns and structure information in a coherent way. In the case of social media, discursive trends, use of symbols and hashtags, and, where possible, geolocated data are analysed to improve contextualisation.

Flexibility in data selection is key to adapting the tool to different scenarios, allowing parameters to be adjusted according to the availability and quality of the information. In this sense, the work of the analyst not only defines the starting point of the process, but also optimises the performance of the programme, ensuring that the predictions and classifications generated are as accurate and useful as possible.

2.1.3 Identification of key actors

Within the digital ecosystem, certain actors play a decisive role in the dissemination and amplification of information, influencing the construction of narratives and the public perception of events. The identification of these actors is an essential step in OSINT analysis, as it allows one to understand how discourses are propagated, who generates them and what impact they have within the information environment.

To this end, the OSINT tool implements a process of segmenting users by level of influence, differentiating between government actors, media, opinion leaders and digital communities. This classification facilitates the detection of key sources within each category and allows for an analysis of their role in the dissemination of information, whether as primary broadcasters, amplifiers or counter-narrative agents.

In addition, an interaction and scope analysis is carried out, assessing the capacity of each actor to generate reactions within the digital ecosystem. This process considers metrics such as the frequency of publication, the number of interactions (comments, shares, reactions) and the content scope. Through these indicators, the tool can identify dissemination patterns and detect emerging trends, which is essential to anticipate the impact of certain discourses and assess their level of penetration in different audience segments.

The combination of these methodologies allows the OSINT tool not only to map the flow of information within the digital ecosystem, but also to optimise the accuracy of the analysis, distinguishing between actors with real influence and those whose presence is circumstantial or of lesser importance.

Applied example: analysis of the perception of the Spanish Military Emergencies Unit (UME) and the Spanish Army in the Autonomous Community of Valencia after the DANA (hurricane)

In this case, the analyst must collect data on how the intervention of the UME and the Spanish Army has been perceived in the aftermath of the DANA crisis.

Geographical and sectoral delimitation

To ensure the accuracy of the analysis, the geographical area and scope of the study has been delimited according to the area of operation and the thematic area of interest. In this case, the research focuses on the Autonomous Community of Valencia, with emphasis on the media and social perception of the intervention of the military forces, differentiating the coverage and discourse surrounding the Military Emergencies Unit (UME) and the Spanish Army in the context of the DANA.

Sources of information

The data collection was based on digital sources representative of the Valencian information ecosystem. The following channels have been selected to ensure a comprehensive view of media and citizen discourse:

— Digital media: articles and reports published in *Levante-EMV*, *Las Provincias*, À *Punt and Información Alicante* were analysed, due to their importance in the regional news coverage.

— Social network X: posts from citizens, journalists and political actors have been collected in order to assess the digital conversation and its impact on public perception.

— Telegram: posts from key accounts have been extracted in order to analyse and classify their messages.

— Community platforms: discussions and opinions in Facebook groups and local forums have been examined, allowing the identification of citizens' perceptions outside conventional media channels.

Data Filtering and Standardisation

Given the large volume of information collected, it has been necessary to implement a data filtering and standardisation process in order to ensure the relevance and quality of the analysis. This process has involved the following stages:

— Elimination of irrelevant publications: content that is not directly related to DANA or to the intervention of military forces has been discarded, reducing information noise.

— Data standardisation: dates, formats and categories have been standardised, ensuring the coherence of the information and its compatibility with the developed OSINT tool.

2.2 Tools used in the initial analysis

Once the analyst has conducted an accurate search for key sources and actors, these are fed into specialised tools for automated data extraction, optimising the collection process. Commercial and open access solutions are used to obtain structured information from a variety of platforms.

These tools include web scraping techniques, which allow content to be extracted from websites of interest; social media application programming interfaces (APIs), which facilitate the collection of posts and metadata from platforms such as Telegram or TikTok, and news aggregation platforms, which centralise information from different media.

While the construction of the database is done manually, the analyst can rely on advanced spreadsheets, data management software and automatic tagging systems, which facilitate the organisation and segmentation

of the collected information, ensuring its consistency and usefulness for further analysis.

Applied example: use of tools to analyse the perception of the Spanish Military Emergencies Unit (UME) and of the Spanish Army

In this case, once the analyst has identified the key sources, specialised tools are used for data extraction and subsequent analysis. For this purpose, the following can be used:

— Web scraping techniques: automated data extraction methods have been applied to compile digital media articles on the DANA in the Autonomous Community of Valencia, thereby permitting an exhaustive analysis of the news coverage.

— Social network APIs: application programming interfaces (APIs) have been used to identify mentions and discursive patterns on platforms such as Telegram, with the aim of analysing the digital conversation around the UME and the Spanish Army. This methodology makes it possible to access publications in real time and to evaluate the interaction of users with certain discourses.

— News aggregation platforms: specialised tools have been used that centralise information from various media, facilitating the detection of news trends and the identification of predominant narratives in the context of the DANA.

2.3 Building a database

Once the information has been collected, it is essential to structure and consolidate it in a robust database that ensures its secure storage and facilitates its efficient exploitation in OSINT analysis. The quality and organisation of this database will largely determine the accuracy of the results obtained by the tool, as poor screening can lead to misinterpretation, bias or loss of relevant information.

In order to optimise its functioning, the database must meet a number of organisational criteria that allow for an efficient management of the data collected. First, the storage structure should provide for a detailed categorisation based on date, source, type of content and level of relevance. This allows for filters to be established to speed up access to information and to facilitate the identification of patterns within the dataset.

Information labelling is another key aspect of storage optimisation. The use of keywords, *hashtags* and categories helps to improve the segmentation and search of data within the storage repository, allowing for a more accurate indexing of the available items. The integration of multiple

formats is also a prerequisite, as the information collected can be presented in a variety of file types, including text, images, videos and audio files. The ability to store and process these formats ensures that the tool can analyse heterogeneous data without structural limitations.

In addition to organisation, the security and maintenance of the database is a critical factor in ensuring its reliability and operational continuity. Data protection is a priority, so measures are implemented to prevent manipulation of information and avoid accidental loss. This involves the implementation of authentication protocols, access control and regular audits to verify the integrity of records.

The database should also have a system of continuous updating, allowing for the incorporation of new sources of information and the elimination of obsolete data. This process ensures that the analysis performed by the OSINT tool is always based on up-to-date and relevant information, avoiding biases caused by the use of outdated or irrelevant data.

Together, these criteria enable the construction of a structured, secure and adaptable database, ensuring that the tool can process information efficiently and provide accurate analysis based on quality data.

Finally, storing the data collected from open sources in a structured way, as well as the results obtained from the analyses and classifications performed by the programme or the analyst, will be crucial when generating or refining AI models, as these models require considerable amounts of labelled data. These models perform fundamental tasks in carrying out the analyses, as will be detailed below.

Applied example: construction of the database on the perception of the UME and the Spanish Army in the Autonomous Community of Valencia

The analyst must design a structured database that ensures efficient organisation of the information and facilitates its exploitation in subsequent phases of the OSINT analysis. To this end, the database must include:

— A list of key users of social networks and media relevant to the analysis.

— A register of media mentions, incorporating key data such as date of publication, source and category of information, which will allow an assessment of media coverage and its evolution over time.

— Analysis of publications on social networks, with a systematic collection of content associated with relevant hashtags, words and emoticons used or interaction metrics, making it possible to identify trends and the impact of certain discourses in the digital conversation.

— Categorisation by public perception, segmenting content according to its positive, negative or neutral tone, with the aim of assessing the predominant orientation in the media and social narrative.

A densely populated and well-structured database is essential for the implementation of advanced analytical tools, as it allows for the detection of opinion patterns, trend analysis and the assessment of the impact of specific narratives in the information ecosystem.

3 Codes developed and how they work

3.1 Code 1: Sentiment analysis of the information environment

3.1.1 Objective and rationale behind the analysis

Sentiment analysis is a fundamental technique in information processing in digital environments, used to assess the perception and attitude expressed in social media posts and mass media. Its application in the OSINT tool developed is primarily aimed at determining the emotional and narrative orientation of the analysed content, providing a structured view on how certain events, actors or topics are perceived within a news ecosystem.

The purpose of sentiment analysis in this context is to classify and quantify the prevailing tone of publications associated with a specific operation or study. To do this, advanced NLP models are used to assign values to publications according to their emotional charge, segmenting them into three main categories:

— Positive: content with a favourable perception of the topic analysed.

— Negative: publications with a critical, adverse or hostile tone.

— Neutral: information with no obvious emotional charge or with a balanced tone.

The underlying logic of this analysis lies in the need to understand the dynamics of digital discourse, identifying trends, patterns of polarisation and possible attempts at information manipulation. Thanks to this methodology, it is possible to detect changes in public perception, assess the impact of certain narratives and establish correlations between specific events and the reaction of the digital ecosystem.

Moreover, this approach not only allows for real-time monitoring, but also provides strategic information for decision-making, facilitating the adaptation of messages, the identification of communication risks and the development of evidence-based response strategies.

3.1.2 Techniques used: natural language processing (NLP) and taxonomy-based classification

The sentiment analysis implemented in this code is based on advanced NLP techniques, allowing the algorithms to understand, process and classify natural language text in a structured and accurate way. In principle, a trained deep learning model has been used to determine the sentiment of a text.

To carry out this analysis, the text is first pre-processed by removing special characters, emojis and punctuation marks that could generate noise in the results. In addition, the text is converted to lower case to avoid discrepancies due to capitalisation and "stopwords", i. e. words that do not provide relevant information, such as articles and conjunctions, are removed.

Once the text has been cleaned up, it must be transformed into a numerical representation that is understandable for the analysis models. For this purpose, techniques such as TF-IDF (Term Frequency-Inverse Document Frequency), which weights the relevance of words in a set of texts, are used.

For the sentiment classification phase, the text is processed using a trained sentiment classification model based on the BERT text classification model. BERT is a deep learning model which has been tuned for the desired classification in this case. In this way, it is possible to assign a category to the processed text of each publication: positive, when the content conveys a favourable perception; negative, when the tone is critical or adverse; and neutral, when there is no predominant emotional charge.

The results of the analysis are presented in a variety of visual representations to facilitate the interpretation of the data. Bar charts are used to show the volume of publications in each category, as well as pie charts that reflect the relative proportion of each type of sentiment, and heat maps that position key actors within the information ecosystem according to their favourability or hostility, and their level of relevance are also employed.

3.1.3 Practical example and expected results

The developed system classifies all publications and news items according to criteria predefined by the analyst, which have great weight when training the text classification model used, determining the degree in which it is favourable or unfavourable towards the objective of the operation being analysed.

Sentiment analysis in publications

In the first image provided, the distribution of sentiment of the publications analysed can be seen. Two representations are presented in this graph:

— Bar chart: shows the absolute number of positive, negative and neutral publications. The graph shows that the majority of publications are neutral, followed by negative and, to a lesser extent, positive publications.

— Pie chart: expresses the percentage share of each category. In this case, 77.4% of the content is neutral, 13.2% negative and only 9.4% positive.

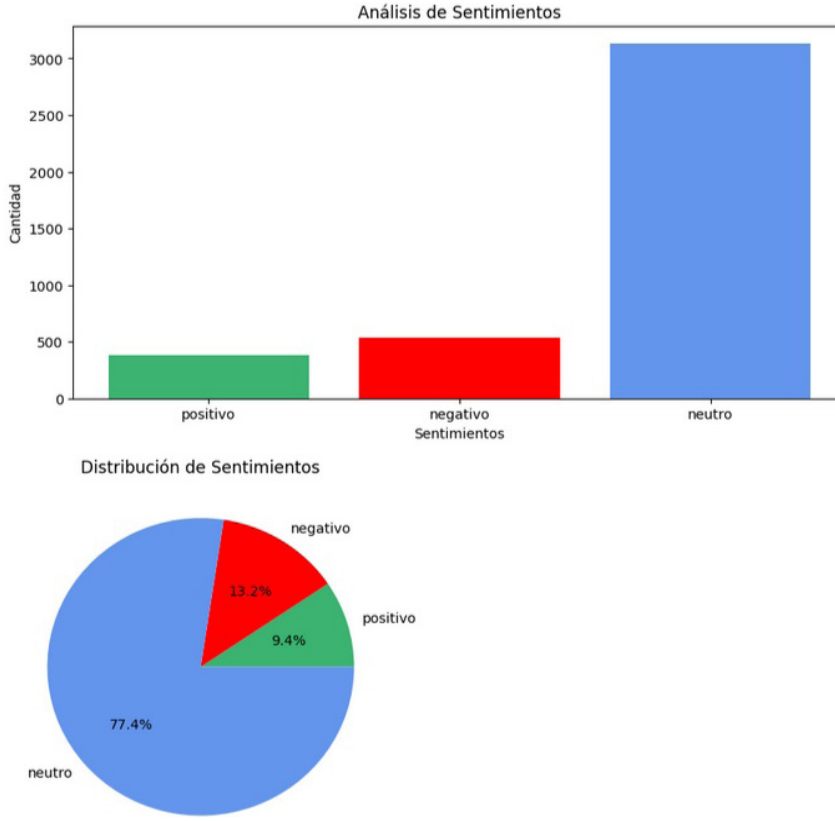


Figure 1. Graphs of sentiment analysis results. Self-elaboration

In the second figure, a stacked bar chart is presented, analysing specific keywords determined by the analyst, which have been found in the publications using traditional programming algorithms and their association with a given sentiment. In this analysis, the following are highlighted:

— The volume each term is mentioned in the publications analysed.

— The proportion of sentiment (positive, negative or neutral) for each keyword.

This type of analysis makes it possible to identify terms with a high negative emotional charge, which may signal the presence of conflict or controversy. It also facilitates the evaluation of the perception of key concepts within the information ecosystem, allowing for a deeper analysis of their impact. It also contributes to the detection of strategic opportunities to influence the digital narrative through targeted communication actions.

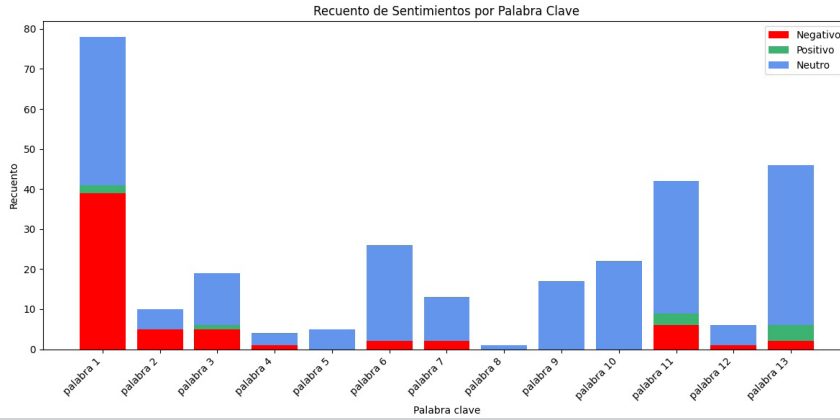


Figure 2. Bar graph of sentiment analysis results by keywords. Self-elaboration

Finally, the heatmap used in this analysis positions the key actors according to two fundamental variables: their hostility or favourability towards the topic of interest under analysis, represented by their position on the x-axis, and their importance within the information environment, represented by their position on the y-axis. This graphical representation makes it possible to identify patterns of polarisation and to prioritise those actors with the greatest impact on the digital conversation. Each medium is represented by a label with a number.

To prevent differences in importance between media and social network users from distorting the visualisation, the y-axis representing this value is scaled logarithmically. Given that in digital environments the distribution of importance is often highly uneven —with some actors reaching massive audiences while others have considerably less visibility— the logarithmic scale allows to smooth out these discrepancies and to represent in a more balanced way the weight of each actor within the analysed environment.

In the case of media, importance is measured by the number of weekly or monthly views, extracted by web scraping techniques on websites that openly offer these data. For social media users, the metric utilised is engagement, which includes interactions such as comments, shares and reactions, providing a more accurate indicator of their impact on the dissemination of narratives.

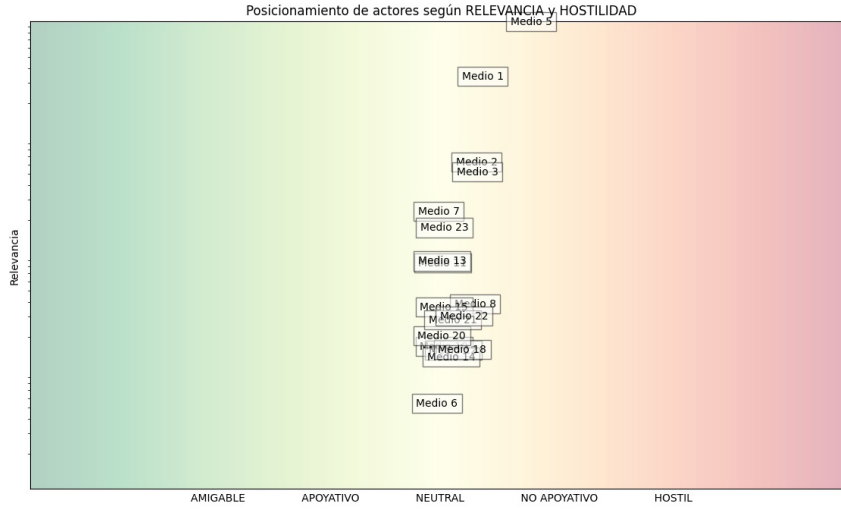


Figure 3. Heatmap, y-axis indicates relevance, x-axis position indicates level of hostility. Self-elaboration

The arrangement of the actors on the map allows for a clear interpretation of their alignment and level of influence. Those located in the zone of greatest hostility and importance imply a significant information risk, as they have a high capacity to disseminate content contrary to the narrative of interest. In contrast, actors with high importance and a neutral or favourable stance may represent strategic allies or spheres of opportunity to influence the digital conversation.

This type of visualisation is essential for strategic decision-making in information monitoring and digital reputation management operations, as it provides a detailed analysis of the actors shaping public perception and facilitates the development of communication strategies adapted to the dynamics of the digital ecosystem.

3.2 Code 2: Classifying Social Networks and Means of Mass Communication with machine learning

3.2.1 Definition of categories and classificatory approach

The second module of the OSINT tool focuses on the automated classification of digital content in social networks and media, using advanced machine learning techniques. This process allows large volumes of data to be segmented in a structured way, facilitating the identification of narratives, trends and potential influential campaigns within the analysed information environment.

Given the exponential growth of information flow on digital platforms, the ability to analyse and classify content in an automated way is essential for strategic decision-making. The implementation of machine learning algorithms overcomes the limitations of manual analysis, providing the system with greater scalability and precision in the detection of discourse patterns.

The effectiveness of the classification process depends on a preliminary phase of analysis in which the analyst determines key criteria such as:

— Selection of key sources: traditional media, alternative platforms, social networks and specialised forums.

— Identification of relevant actors: influential profiles, high impact media, digital communities and anonymous users with significant activity.

— Definition of the target audience: users affected by the analysed narrative and potential recipients of information or disinformation campaigns.

— Contextualisation of the analysis: delimitation of the area of interest, the political, social or economic situation and the strategic purpose of the study.

These factors allow a classificatory taxonomy to be established, ensuring that the machine learning model is trained with data aligned to the objectives of the analysis. Segmentation is done according to different categories, which can be organised under different approaches, such as:

— Thematic content: classification according to areas such as politics, security, conflict, economics or disinformation.

— Communicative intent: differentiation between purely informative content, opinion pieces, propagandistic speeches or manipulative strategies.

— Type of source: distinction between official media, alternative communication platforms, social networks and specialised forums.

— Importance and reach: evaluation of the influence of each source within the digital environment, considering metrics such as engagement, web traffic and level of interaction.

The implementation of these criteria allows the machine learning model to accurately identify the structure of digital discourse in the area of interest, differentiating between legitimate content, emerging narratives and possible attempts at information manipulation.

The pie chart presented in the figure reflects the segmentation of the content according to the predefined categories. Each segment represents a

proportion of the total volume of publications classified within each topic of interest and allows the analyst to visualise the thematic distribution of digital discourse.

3.2.2 Implemented algorithms and models

To achieve the classification of publications based on the taxonomies defined by the analyst, a machine learning model has been trained with a large amount of data to automate the categorisation process. This required prior work to manually tag batches of publications relating to the digital environment under analysis. This model has been refined as more data have become available for training and its results are always monitored by the analyst to determine whether the classification of publications is correct.

In this way, a tedious process of manual sorting of large numbers of publications can be automated.

Once the model has been run on a batch of publications and the results have been checked and adjusted, if necessary by the analyst, they are stored in the database, with the certainty that they are completely reliable. Thus, the model can be further refined by training it with more batches of labelled data so that, over time, the accuracy of the model can converge to a value approaching 100%.

3.2.3 Expected results of a practical scenario

Once the publications are classified with the support of the machine learning model, the tool graphically displays the results to obtain a

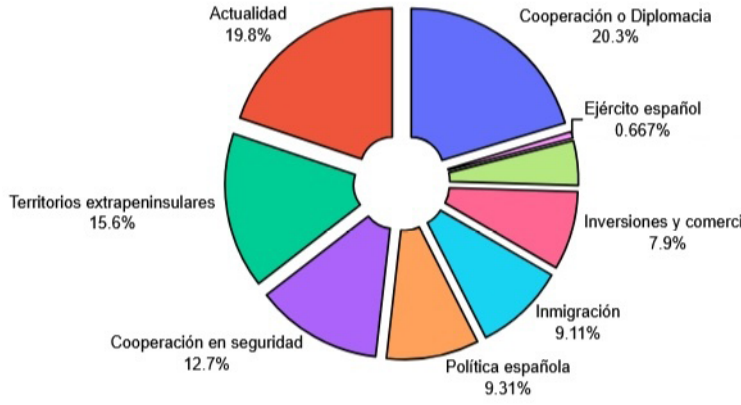


Figure 4. Classification results graph in taxonomies. Self-elaboration

visualisation of the topics covered in the target digital environment based on the taxonomies devised.

In this case, they are displayed in a pie chart as shown in the figure below. No conclusions should be drawn from the results, they are only shown to expose the capabilities of the tool.

3.3 Code 3: Multi-stage classification of TikTok content

The classification of the content in TikTok within the developed OSINT tool is structured in three phases or filters, which correspond to different stages of data extraction and processing. These filters allow content to be segmented and analysed in a progressive manner, ensuring an efficient classification adapted to the objectives of the operation.

Before applying these filters, a database with previously selected users is loaded into the tool. The selection of this sample may vary depending on the focus of the analysis, and may be a biased or specific sample, if one wants to focus on a specific niche, or a more representative and random sample, always maintaining minimum criteria of relevance.

To carry out the processing of this information from TikTok, web scraping methods were used to extract the description, comments and video location data from each of the selected users' posts. In addition, the video has been downloaded and processed using a deep learning model for object detection in images.

Each content classification phase developed below corresponds to a progressive filter in the detection of relevant content in TikTok.

3.3.1 Filtering by hashtags and taxonomies in the video description

In the first phase, the tool analyses the description of the videos posted by the selected users, searching for hashtags or keywords predefined by the analyst. This initial classification allows a first segmentation of the content according to the tags that the creators themselves use to categorise their publications. The result of this analysis is a table showing the username, the URL of the post, the description and the keywords found in the description of the post, including those appearing as hashtags.

The information contained in this table can be represented in graphs, as has been done with the results of the previous analyses, or it can be used to identify the publications that are most interesting for analysing the environment under study. At this stage, no specific graphical representations that can be presented in this article have been developed for this information in the tool.

3.3.2 Filtering by comment analysis

In the second phase, the comments of the videos identified in the first phase are analysed, looking for mentions of hashtags or keywords that are not necessarily in the description, but that can contextualise the content. This phase allows to extend the detection range and to capture significant content that has not been explicitly tagged by the video creator.

The result of this analysis consists of a new column in the table mentioned in the previous section indicating which keywords and in what quantity have been found when processing the comments of the publication.

It is important to note that the three phases are not mutually exclusive. If no results are found in one phase, the tool continues to process the video in the following filters until the analysis is complete. Exclusion only occurs when, after applying the three steps, no match with the established criteria is detected.

3.3.3 Frame filtering by deep learning for image processing

In the third phase, the emoticons of interest that are present in the video of the publication are detected. To do this, a deep learning model has been trained to detect certain emoticons in images. More specifically, the flag of Spain and of the European Union. For each case, a model must be trained to detect the desired emoticons.

In order to process the video from the TikTok post, the tool first obtains the location of the video using web scraping techniques and downloads it. It then separates the video into frames and processes them one by one with the emoticon detection model, writing in a new column of the table mentioned above if it has found the emoticons of interest.

The result of the processing of a video frame by the deep learning model is visually shown in the following figure.



Figure 5. Result of object detection processing. Self-elaboration

The figure shows that a Spanish flag emoticon has been detected with a detection accuracy of 91.2%. This datum will be stored in the row corresponding to the publication together with the word analysis of the description and the comments.

This procedure makes it possible to detect messages embedded in videos on the social network, a practice that is quite common in this environment.

Finally, with regard to this analysis of the post's video, it should be noted that the training of the model to detect emoticons in video frames requires prior work on image labelling to train the model. The collection and labelling of these images for training is the most critical step in order to have an accurate and functional detection model.

4 Conclusions and lessons learned

4.1 Impact of the programme on the organisation

The development and implementation of the OSINT programme based on NLP techniques, Artificial Intelligence and traditional programming has proven to be a very efficient tool for the analysis of the information environment in digital scenarios. Its integration within intelligence processes has allowed optimising the monitoring and classification of large volumes of data, facilitating the automated detection of trends and narratives.

One of the main impacts of the programme has been the reducing the time required to process large amounts of open source information, which has improved responsiveness and strategic decision-making, as well as allowing better use of the unit's human resources. Furthermore, its modularity and adaptability have made it possible to implement it in a variety of operational contexts, making it a flexible and scalable solution.

In addition, the combination of analytical methodologies and the expertise of analysts has made it possible to refine the results and improve the accuracy of the analysis, minimising biases and ensuring that the information obtained is useful and relevant for decision-making.

4.2 Main lessons learned and contributions

The development of the programme has provided a number of key learnings in the field of open source intelligence and automation of information analysis:

— Importance of methodological design: the effectiveness of the programme depends to a large extent on the correct structuring of the data collection, filtering and analysis process. Defining clear criteria from the outset is essential to ensure the quality of the results.

— Interdisciplinary collaboration: the integration of analysts with data processing experts has been instrumental in fine-tuning models and improving their accuracy. The synergy between operational and

technical expertise permits the development of more robust tools adapted to specific needs.

— Challenges in automated classification: the ambiguity of language in social networks and the constant evolution of terms and expressions require continuous updating of classification models and sentiment analysis. The implementation of hybrid approaches has proven to be an effective solution to address this challenge.

— Scalability and adaptability: the flexibility of the programme has allowed it to adjust to different environments and scenarios, which shows the importance of designing modular technological solutions that can evolve along with operational requirements.

— Strategic impact of data analysis: the ability to identify patterns, trends and key players within the information ecosystem has reinforced the usefulness of OSINT in decision-making. Early detection of disinformation campaigns or changes in public perception are a valuable resource in crisis management and security operations.

— Combining different technologies: the development of this tool serves as a good example of using different technologies to solve different parts of the problem one faces. In this way, the most suitable solution has been chosen according to the needs, with the tool coexisting in both Artificial Intelligence models of machine learning and deep learning and web scraping techniques or keyword filtering carried out by traditional programming algorithms.

4.3 Next steps and proposed improvements

To maximise the potential of the programme, the following lines of improvement and development could be explored:

— Improvements in the accuracy of sentiment analysis: implementation of more advanced models, for more accurate and context-adaptive classification.

— Integration with additional data sources: expansion of the programme's reach by incorporating new digital platforms and media, improving the coverage of the analysis.

— Automation of the update process: development of a system that allows the automatic update of taxonomies, key terms and classification patterns according to emerging trends.

— Performance optimisation and scalability: improved data storage and processing infrastructure to enable efficient management of growing volumes of information.

— Continuous training of staff: promoting training programmes for analysts and data experts, ensuring constant updating of analytical and information processing techniques.

In addition, one can try to combine different modules of the programme with the aim of reaching more advanced analyses, such as using the model that classifies text sentiment with comments from TikTok posts accessed through web scraping.

In conclusion, this programme represents a significant advance in the application of OSINT in strategic environments, providing an effective tool for analysis and decision-making in crisis and security contexts. Its development and continuous improvement will strengthen its impact and broaden its applicability in different operational areas. Thus, this development with limited resources demonstrates that technological solutions are accessible and can be exploited autonomously if the available human resources are properly aligned.

Article Three

Post-normal intelligence: risk management in the grey zone

Jesús Hernández Álvarez

Abstract

This article questions the traditional paradigm of intelligence, which emerged during the Cold War, analysing its transformation within the context of a rapidly changing global environment characterised by uncertainty and the complexity of post-normal times, arguing for a new, more adaptive, multidisciplinary and cooperative paradigm, integrating open sources and an extended intelligence community.

Post-normal science is explored as a conceptual framework for addressing problems with uncertain facts, conflicting values and urgent decisions, as well as the evolution from the traditional intelligence cycle towards a risk management approach, integrating intelligence and governance functions in the search for a shared vision of the security issue to be managed.

It also stresses the importance of understanding and mitigating cognitive limitations such as biases, encouraging systems thinking and AI-assisted complex modelling to improve situation awareness. Finally, it highlights the need to protect the cognitive domain as a crucial asset in the face of hybrid strategies in the grey zone, outlining possible innovation vectors for State Intelligence and Information Services in a post-normal environment, which would give rise to several evolutionary scenarios.

Keywords

Innovation, Intelligence services, Information services, Evolution, Governance.

1 Introduction

When it comes to innovation in security and defence, one is often quick to think of technological innovation. In this sense, it is true that innovation, which requires a combination of incremental advances and emerging technologies with disruptive capabilities, is currently focusing on big data and advanced analytics, Artificial Intelligence (AI), autonomous systems, quantum technologies, space technologies, hypersonic weapons, biotechnologies and human enhancement technologies, and advanced materials and new manufacturing techniques (Martin, 2023).

Moreover, in an environment of geopolitical tensions, conflict should be highlighted as a driver of change, especially in five areas: sociological, technological, doctrinal, political and economic change. In this sense, conflict could be understood as the result of maladaptation to previous changes, in a continuous cycle of maladaptation-conflict-adaptation (Frías, 2023)

Within this context and with regard to intelligence, this article focuses more on doctrinal, conceptual and methodological aspects than on technological aspects, which may be relevant in the transformation of the processes and structures of the State Intelligence and Information Services.

The 2021 National Security Strategy focuses on a number of transformational vectors that have accelerated significantly in recent years and have changed the strategic environment. It notes that the global order and the liberal socio-economic paradigm are in a period of change, with the new landscape of the international system not yet clearly defined. The main transformational vectors identified are: the geopolitical context, the socio-economic environment, the digital transformation and the ecological transition.

Similarly, the European Union's strategic foresight system identifies fourteen megatrends that are shaping the world at the time of drafting this article. These include accelerating technological change and hyper-connectivity, worsening resource scarcity, the changing nature of work, a reconfiguration of the security paradigm, climate change and environmental degradation, continuing urbanisation, diversification of education and learning, widening inequalities, expanding influence from the east and south, rising consumption, growing demographic imbalances, increasing influence of new governance systems, the relevance of migration, and changing health challenges.

While these global trends and transformational vectors may seem distant, their effects are palpable in everyday life, sometimes dramatically so. It is enough to recall certain significant events of the last five years: the pandemic in 2020, the withdrawal of Western troops from Afghanistan and the Taliban's return to power in 2021, the Russian invasion of Ukraine

in February 2022, the launch of the ChatGPT generative AI in November 2022, the attack by Hamas in October 2023, the missile exchange between Israel and Iran in 2024, Donald Trump's victory in the US elections in November 2024, the increasing ideological polarisation of the new European Parliament in late 2024, the fall of the Syrian regime in December 2024 and the US President's rapprochement with Russia in 2025.

The concentration of these events and circumstances of international significance within such a short period of time makes us direct witnesses of a rapidly changing world. This structural change in the international system is shaking the tectonic plates of our reality, which, though seemingly solid, have been sliding unnoticed into an uncertain future.

The widespread uncertainty produced by these events only reinforces the ordinary person's perception that the world is too complex to understand and impossible to analyse 'rationally'. However, intelligence organisations, whose primary mission is to sort out these same uncertainties and complexities in order to provide the best courses of action, are also to a greater or lesser extent overwhelmed by the task.

Against this backdrop, a major strategic concept has gained momentum, the *Grey Zone*, a space within the spectrum of conflict that lies between peaceful competition and war, characterised by ambiguity, multidimensional (hybrid) strategies, substantial stakes and the gradual implementation of strategies to achieve long-term objectives (Jordán, 2018). This space is an area of the conflict spectrum where actions outside the principle of good faith between states (*bona fide*) predominate, and which, despite significantly altering the peace, do not cross the thresholds that would allow or require an armed response (Ministry of Defence, 2018).

This confrontational scenario is already identified by the 2021 National Security Strategy to a greater or lesser extent, as it links hybrid strategies to risks and threats at various levels of correspondence: very high for strategic and regional tension, espionage and interference from abroad, disinformation campaigns, threats to critical infrastructure, cyberspace vulnerability, economic and financial instability and, finally, energy vulnerability. At a lower level of connection with hybrid strategies, we have terrorism and violent radicalisation, vulnerability of maritime space, vulnerability of aerospace, organised crime and serious crime, and finally the proliferation of weapons of mass destruction.

Within this context of grey-zone confrontation in which the fundamental components of National Security, namely National Defence, Public Security and External Action, are so interlinked, a question arises: is any kind of innovation required by the State Intelligence and Information Services, in accordance with the scope of their powers, in order to continue to provide

permanent support to the National Security System, providing elements of judgement, information, analysis, studies and proposals required to prevent and detect risks and threats and contribute to their neutralisation? (art. 9 of the National Security Act).

The ease of formulating this question contrasts with the difficulty of answering it, something that this article does not attempt to do on a rigorous basis, rather it seeks to introduce a series of elements to encourage strategic reflection.

2 Post-normal science

It is well known that the Intelligence Cycle shares with the scientific method its systematic and analytical approach, but they differ in objectives and application. While science seeks universal truths through the initial formulation of falsifiable hypotheses and subsequent reproducible experimentation, Intelligence generates practical knowledge for urgent decisions, working with incomplete data and prioritising action over methodological perfection. Both use structured processes, but the Intelligence Cycle is more flexible, allowing for leapfrogging in emergencies.

In terms of context and rigour, the scientific method requires strict controls and reproducibility, while intelligence operates in dynamic environments where uncertainty is inherent. For example, a scientist would discard unverifiable data, but an intelligence analyst could use it to prevent an immediate threat by taking certain risks. In essence, Intelligence adapts scientific rigour to realities where speed and operational utility are of the essence.

However, the gap between intelligence and science seems to be narrowing in recent years. The context of change faced by intelligence organisations on a daily basis has also been the subject of scientific discussion not so much from a technical, but from an epistemological point of view. In recent decades, theoretical and methodological approaches have emerged which question the usual way of doing science, such as Mode 2, post-academic science and post-normal science (Jiménez-Buedo and Vielba, 2009).

Over the last three centuries, science has been progressively placed at the centre, with the ability to provide quantitative, objective and neutral evidence, as well as increasing explanatory power. The traditional model of problem-solving assumed a strict separation between facts (the territory of science) and values (the territory of governance), and a process conceived of in which, having obtained the truth, political action was taken for the common good. The idea was simple: a) any practical-political problem can be translated into a technical-scientific problem and b) the resolution of the technical-scientific problem solves the practical-political problem. (Hidalgo and Funtowicz, 2024)

However, in 1993, Silvio Funtowicz and Jerome Ravetz coined the term post-normal science (PNS) to refer to a new way of dealing with scientific problems in concrete situations, placing their approach somewhere between science and governance. PNS is defined by four main characteristics: *the facts are uncertain; there are multiple values, usually in conflict; the stakes are potentially very high; and decisions are urgent*. As may be seen, these assumptions characterise many of the operating environments faced by intelligence and information services for years.

In this approach, the focus shifts from the search for a single truth defined by science to the quality of the processes of knowledge creation in relation to a socially and politically determined purpose. In this sense, PNS recognises the knowledge created outside the scientific sphere as equal, including practical knowledge, experience, assuming that it is not enough just to 'know what', but that it is also necessary to 'know how'. From this perspective, and in the field of security and defence, PNS may be interpreted as placing scientists and intelligence analysts on the same level in terms of quality knowledge production.

This equalising conception of knowledge would materialise, according to the authors, in an 'extended community of peers' or 'extended community of evaluation', which extends the evaluation of knowledge quality beyond the experts in each of the scientific disciplines. In post-normal contexts, participation, inclusion and diversity of voices contribute to knowledge quality assessment.

The challenge is how to create this extension of the community of peers in situations of real conflict, recognising that social transformations emerge from these processes. PNS proposes a reform where the democratic extension of the right to knowledge is not only ethically and politically effective, but also 'enhances the quality of technical and scientific evidence' for action for the common good.

Ultimately, PNS argues that the modern model of problem-solving based on prediction and control is obsolete. This requires taking on board the impossibility of predicting and justifying political action solely on predictions and moving towards a 'science of responsible anticipation' that is concerned with the quality of the processes by which institutions function. Thus, ultimately, given the inevitability of error or the occurrence of unexpected events, the focus should be on managing failures 'with political-institutional legitimacy'.

The assumption of a certain inevitability and the impossibility of science to make reliable predictions in the face of highly complex problems was already pointed out in 2007 by Nassim Nicholas Taleb, who revitalised the concept of the 'black swan' to refer to rare and unpredictable events that

have a significant impact, arguing that these events are inevitable and that our perception of them changes after they occur, tending to believe that they were more predictable or inevitable than they actually were at the time they occurred (hindsight bias). Additionally, and similar to PNS, this author noted in 2012 that social effort should be directed at boosting our capacity to withstand the unpredictable, coining the concept of 'anti-fragile' to describe systems that not only resist chaos, but also benefit from it, improving with each iteration of coping with adversity.

However, it should be noted that the metaphor of the 'black swan' is compared with that of the 'black elephant', which describes problems that are obvious and known to all, with potentially devastating consequences, but which are ignored, so that the lack of action or will to address them turns their impact into an inevitable crisis—can we identify our own black elephants?

So far, certain partial conclusions could be drawn by applying the conceptual framework proposed by PNS to the context of the functioning of Intelligence and Information Services: a) strengthening the capacity to generate knowledge by creating an extended community of theoretical and practical experts; b) focusing on the quality of knowledge generation processes while assuming the difficulties in predicting the evolution of certain environments; and c) that the detrimental effects of complexity and uncertainty have reached such levels that they have been the subject of scientific study, demonstrating the point of transformation at which the world around us finds itself.

Complementing the conceptual framework of PNS is the *Theory of postnormal times* (Sardar, 2019), which defines in greater the situations where PNS may be applied, characterising them by the four Ss and the three Cs:

— 4S: speed (everything accelerates), scale (events take on a global dimension), simultaneity (crises occur at the same time) and scope (penetrating even the remotest parts of the globe).

— 3C: complexity (interconnected and interdependent systems), contradictions (competing demands and conflicting interests) and chaos (small events can trigger huge and unpredictable changes).

Postnormal times, according to the author, are manifested in various spheres. In politics, we see the rise of populism, polarisation and the crisis of governance. In the economy, unbridled capitalism leads to growing inequality and radical uncertainty. Technology, while offering opportunities, also presents risks such as manipulation, loss of privacy and increased chaos. Society faces the erosion of trust in institutions, fragmentation and the spread of post-truth. Even religion experiences new forms and tensions in this context.

This theory focuses on three concepts: uncertainty, ignorance and time horizons (the so-called Three Tomorrows), so that each type of uncertainty is intrinsically associated with a specific category of ignorance, which helps to better understand the nature of the unknown at each time horizon:

— *Surface Uncertainty*, characteristic of the *Extended Present*, is linked to *Plain Ignorance*. At this horizon, while the general direction of change may be foreseeable, the exact magnitude and likelihood of events is unknown. This ignorance is plain or simple in the sense that it refers to the absence of knowledge regarding specific aspects, but may be overcome through information gathering, research and learning. This is the domain of traditional science.

— *Shallow Uncertainty*, characteristic of *Familiar Futures*, is related to *Vincible Ignorance*. Here we face a wide range of possible futures and the direction of change is less clear. Ignorance is vincible because even if one does not know what questions to ask in the present, one recognises that the answers to those questions can only be found in the future, as one experiences the consequences of current trends and developments. This is the area of application of knowledge adapted to each situation by professional consultants.

— *Deep Uncertainty*, which defines *Unthought Futures*, is associated with *Invincible Ignorance*. On this horizon, the nature, direction and impact of change is completely unknown, and our own understanding of the world may be inadequate. This ignorance is invincible because it represents the ignorance of our own ignorance, that which is not known and which is outside conventional frameworks of thought. Addressing this ignorance requires a fundamental rethinking of our assumptions and worldview, and is the domain of post-normal science, which recommends fostering knowledge generation by extended communities of experts which focus on the quality of knowledge generation, rather than the predictability of the environment.

In short, the depth of uncertainty reflects the degree to which our ignorance prevents us from understanding the future. As we move from the Extended Present into the Unthought Futures, uncertainty becomes more profound and the ignorance we face becomes more fundamental, requiring ever more radical strategies for understanding and managing it.

To supplement the partial conclusions listed above, it may be stated: a) that post-normal science is a kind of ‘extension’ of traditional science; b) that a good definition of the characteristics of problems is key to determining how to approach them, placing intelligence work between the boundaries of expert consultancy and post-normal science; c) attempting to use

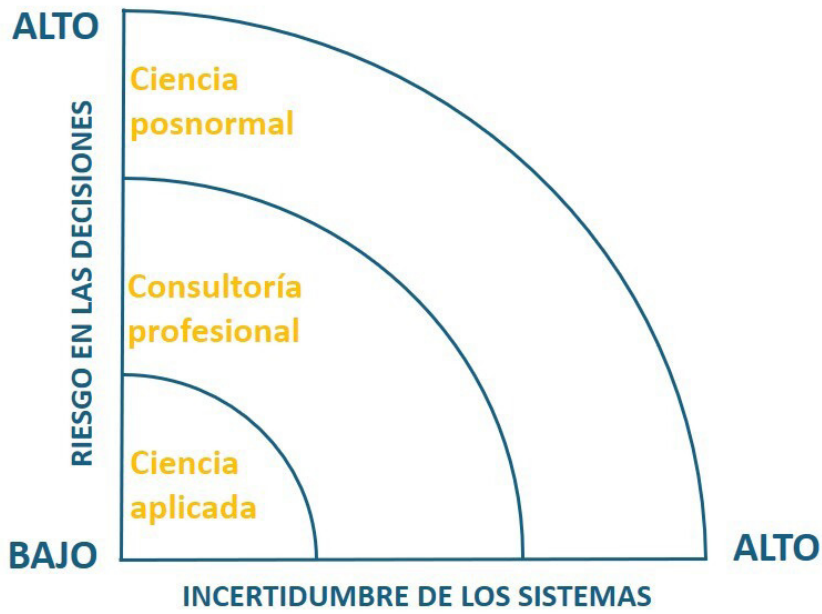


Figure 1: Uncertainty-risk relationship. Self-elaboration

procedures from applied science in post-normal situations may not be the best approach.

3 From the intelligence cycle to risk management

For a critical review of the intelligence cycle, the main conceptual framework for understanding the process of intelligence production in security and defence, one may consult Javier Jordán (Jordán, 2016). His analysis recognises that the cycle model, though simple, logical and easy to understand and remember, and with some level of correspondence with the internal organisation of intelligence services, is criticised for oversimplifying reality and not accurately reflecting the actual process of intelligence production. The text points out several inconsistencies between the ideal model and actual practice, which include: a) in the steering phase, objectives are not always clear and it is often the technicians who drive the process; b) the obtaining and processing phases are not strictly sequential, but operate in parallel and interactively; c) in their dissemination, raw information may reach decision-makers without prior analysis; and d) processed intelligence may be ignored if it contradicts the ideological framework of the policymaker.

Additionally, each phase of the cycle faces specific constraints, such as budgetary restrictions, data processing problems, legal limitations

and difficulties in coordination. Jordán points to alternative models such as Treverton and Gabbard's model, which introduces the notion of 'short-cuts' between phases; Lowenthal's multi-strata model which stresses the importance of continuous feedback throughout the cycle; and finally, he describes Clark's Target-Centric approach to Intelligence, which proposes a networked approach where all participants collaborate in building a shared picture of the target. The three alternative models reflect the complexity and non-linear nature of the actual Intelligence process. In conclusion, while the traditional Intelligence Cycle model has pedagogical value, more flexible approaches that incorporate constant interaction and feedback between the different stages must be considered in order to better understand the actual functioning of intelligence services.

On the other hand, it must be said that the four basic phases of the cycle do not take into account the decision-making process itself, since it ends with the communication of Intelligence to the decision-maker. From a conceptual point of view, there would be a clear gap between the knowledge generated to solve an intelligence problem, the decisions made to solve it, and the impact of the decisions on the problem itself. Following Clark's proposal, a shared picture of the intelligence problem cannot be created without a conceptual framework that encompasses all actors involved, including decision-makers.

From a law enforcement perspective, the 4-I Model (Intent, Interpretation, Influence and Impact) proposed by Jerry H. Ratcliffe, develops the conceptual framework to explain dynamics between key actors in the production and application of criminal intelligence, highlighting the interaction between analysts, decision-makers and the criminal environment (OSCE, 2020).

However, it should not be forgotten that the Intelligence Cycle is ultimately subordinate to a larger security and defence management process. It is precisely at this point that Funtowicz and Ravetz's post-normal science proposes a new way of dealing with post-normal times, right at the intersection between scientific/technical knowledge and governance. Thus, the question is not so much whether the Intelligence Cycle correctly describes the activity of the State Intelligence and Information Services, but how to establish a conceptual framework that integrates their activity with the activities of security and defence problem management

An approach that links scientific/technical knowledge with governance criteria may be offered by the conceptual framework established by the *UNE-ISO 31 000 standard for Risk Management*. The standard presents general guidelines for the management of any risks by public or private organisations, proposing a process map.



Figure 2. Model 4i (adapted from Ratcliffe)

Applying this map to the National Security System's (SSN) management of the risks contemplated in the National Security Strategy and, understanding that the State Intelligence and Information Services are a subsystem of the SSN, would provide a conceptual framework that would integrate the Intelligence subsystem as well as the decision-makers and measures implemented to reduce these risks, making it easier for all participants to share the same vision of the security problem to be solved, as Clark pointed out.

Below is the process map (adapted by the author) based on the proposal of the UNE-ISO 31 000 standard, displaying the iterative interrelation of processes and their adaptation to the functioning of the SSN:

— *Definition of the context*: it defines the scope of risk management, its geographical and temporal scope and the domain where the effects materialise, considering factors both internal and external (strategic environment) to the NSS, establishing risk criteria (tolerance thresholds) to assess its importance, as well as the definition of applicable standards and values, also the NSS actors involved in any of the management processes of that particular risk. This process would include the Intelligence Cycle Management phase.

— *Communication and consultation*: it involves both internal SSN and external parties related to the collection and iterative exchange of relevant information applicable to the risk in question. This process would be similar to that of Obtaining the Intelligence Cycle.

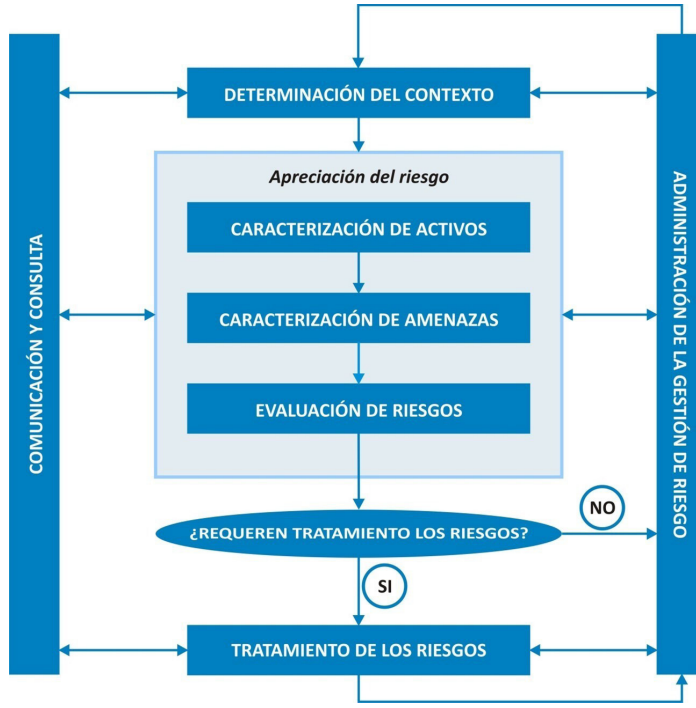


Figure 3: Risk management process map (adapted from UNE-ISO 31000)

— *Risk assessment*: measures to identify, analyse and evaluate the risk that may be involved:

- Characterise assets: identification, analysis and valuation of assets at risk. It involves determining their criticality or relative importance, as well as their vulnerabilities, resulting in a map of assets to be protected.
- Threat characterisation: identify, analyse and assess the threats that generate risk. It would involve the determination of their danger, capability and intention to materialise the risk, resulting in a threat picture.
- Risk assessment, which would involve establishing relevant assumptions that relate the risk in question to threats and assets. Risk assessment with regard to SSN criteria allows prioritisation of actions by identifying the risks that can be assumed and those that need to be addressed.

This process would be similar to the Development phase of the Intelligence Cycle and would be closely linked to intelligence production for dissemination to those responsible for the next process.

— *Risk Management and Administration*: a process in which those responsible for risk management and administration monitor and review risks according to their different perspectives, making the relevant decisions supported by the intelligence reports received.

— *Risk processing*: the process of establishing the conditions for implementing measures, as well as their implementation, both operational and strategic, aimed at preventing or avoiding the occurrence of risk, the protection of assets, the neutralisation of threats, as well as measures to reduce the effects or impact of risk in the event of its occurrence.

From the point of view of public management, the definition of a single process map for the entire SSN opens the door to establishing clear quality policies for the functioning of each process, regardless of the actors involved in each of them, which would undoubtedly result in the quality of the knowledge generated, in turn pointing in the direction indicated by post-normal science.

It is important to remember that the process map is a generic model that is applied to specific risks with their own characteristics, so that the necessary process maps may be defined to manage the sixteen risks and threats prioritised in the National Security Strategy.

However, from the perspective of generating extended communities of peers, it remains to be determined which actors should be incorporated into the process map, which will be addressed below. In any case, and especially in a growing hostility in the grey zone where National Defence, Public Security and Foreign Action intermingle, it seems a priority to boost collaboration between all Intelligence and State Security Services.

4 Intelligence and cognition

Another field in which scientific development has favoured innovation in terms of intelligence production has been the cognitive sciences. The analogy of the computer, widely used for decades, compares the functioning of the human mind to that of a computer, suggesting that both systems process information in a similar way. This analogy which has been questioned from some perspectives, has served as a conceptual model for numerous advances in the cognitive sciences which, in the field of Intelligence, have had a special impact on the Development phase. Some reflections are made below, pointing to certain avenues for improvement, which have already been initiated in general terms. To this end, a brief mention will be made of cognitive biases, systems thinking, mental models, and situation awareness.

4.1 Cognitive biases

Following the doctoral thesis of Claudio Payá (Payá, 2017) on the cognitive biases of intelligence analysts, it may be stated that cognitive biases are systematic and predictable errors in the processing of information, inherent to the structure of the human mind and which can affect the objectivity of the analysis. These biases are not simply random errors, but patterns of thinking that can lead to erroneous conclusions, even when the analyst is aware of their possible influence.

It is important to highlight the work of Herbert Simon and the concept of 'bounded rationality', which challenged the limits of human rationality, demonstrating that people do not always opt for the choice that maximises their interests. Simon argued that, in the face of the complexity of the world, human beings cannot achieve an ideal of perfect rationality and that, instead, people use a variety of strategies to simplify their environment. Subsequently, Kahneman and Tversky's work on heuristics and biases delved into the limits of rationality by proposing two systems of reasoning:

— *System One*: intuitive, quick and unconscious, based on heuristics and emotions, operating automatically, proposing quick responses to System Two and prone to systematic errors or biases.

— *System Two*: deliberate, slow and conscious, based on logic and cognitive effort. Although more precise, it is also limited by mental capacity. A lazy System Two directly rationalises the automatic proposals generated by System One.

Within the context of intelligence analysis, these biases can have a significant impact. They can lead to premature closure, where analysts reach conclusions quickly without exploring all possibilities. The presence of uncertainty, the possibility of deception by adversaries and the tendency to seek information that confirms pre-existing assumptions (confirmation bias) are factors that exacerbate the influence of biases. Time pressure and the need for precision can also exacerbate these cognitive limitations.

To mitigate the negative impact of cognitive biases in intelligence analysis, *Structured Analytic Techniques* (SAT), which have been widely disseminated since 2011 thanks to the work of Richards J. Heuer and Randolph H. Pherson, are often used. These techniques are designed to make analytical arguments, assumptions and intelligence gaps more transparent, helping to prevent automatic responses that may compromise the robustness of the analysis. The techniques, which have different applications, provide a structured framework and are designed to: break down complex problems into smaller, more manageable problems of analysis; make the analysis process explicit to so it is collaborative; challenge working hypotheses, forcing conscious justification of conclusions, forcing the incorporation of

alternative hypotheses; stimulating the ability to anticipate and imagine the unexpected, encouraging consideration of new perspectives and ideas to avoid single-minded thinking, and so on.

While it is true that SATs have come to provide a good toolbox for intelligence analysts, it is no less true that no matter the level of expertise, a bricklayer still needs an architect to provide the big picture of the project that is underway. This global vision is provided by systems thinking.

4.2 Linear vs. systemic thinking

Another limitation of the human cognitive system is the tendency towards linear thinking. However, within this context of increasing global complexity, how problems are addressed and solved has become critically important. Linear thinking, characterised by a sequential and analytical approach, has been the dominant paradigm for decades. However, systems thinking, which considers interrelationships and emerging patterns, has gained prominence as a more holistic and comprehensive alternative. The results indicate that linear thinking is more effective in well-defined problems of limited scope, while systems thinking displays significant advantages in solving complex and interconnected problems, especially when there is a transdisciplinary approach (Lorenzo-Penalva, 2023).

General Systems Theory, the basis of systems thinking, was developed by Ludwig von Bertalanffy in the 1940s and formalised in 1969, proposing a holistic view of natural and social systems. This Austrian biologist devised an interdisciplinary approach that considers systems as sets of interrelated elements, emphasising the emergent properties that arise from these interactions: the system is more than the sum of its parts.

The modelling of a system begins by establishing its structure, first identifying its elements analytically (breakdown), and then establishing the relationships between them in an effort at synthesis (integration). These relationships are often represented by a diagram of influences, positive or negative, to the extent that almost everything around us may be understood as a system, and even as a system within a larger system (nested systems).

By looking closely at a system, feedback loops, whether positive or negative, can be identified. A feedback loop is simply a closed chain of influences that start and end at the same variable. A positive feedback loop tends to destabilise the system until it encounters some kind of limit, usually a negative feedback loop, which tends to stabilise the system. This non-linear vision of systems allows us to begin to comprehend their complexity, to which we may add the delay of the impacts of some variables on others (Aracil J, 1995).

This methodology has been applied to the analysis of security issues, such as counter-terrorism (Pajares de Mena, 2010). For example, taking the 'political opportunity' variable defined by Sidney Tarrow to explain the emergence and strengthening of terrorism as an explanatory variable (Tarrow, 1994), a basic system of terrorist-anti-terrorist confrontation may be defined in which the variables that shape terrorist capabilities constitute the positive feedback loop that destabilises the system given that: more destabilisation (political opportunity for terrorists)→ more radicalisation→ more terrorist capability→ more attacks → more destabilisation. On the other hand, the negative feedback loop, formed by the variables that support counter-terrorist capabilities, basically states that: more destabilisation (political opportunity for terrorists)→ more counter-terrorist capabilities→ less terrorist capabilities→ fewer attacks→ less destabilisation. In the case of ETA, the output variable, number of fatalities, would show the state of the system characterised by a sigmoidal curve, initially ascending when the positive terrorist loop prevails and descending when the negative counter-terrorist loop prevails (Penalva Lucas, 2023).

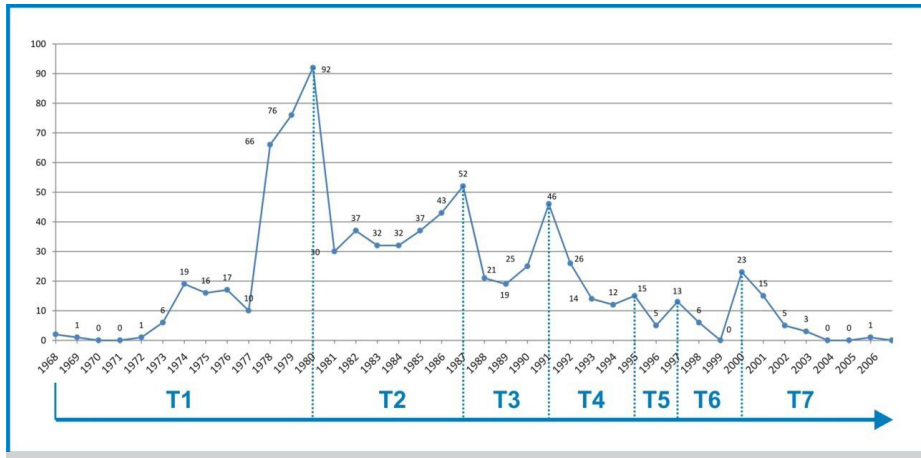


Figure 4: ETA fatalities. Self-elaboration

On the other hand, system dynamics, especially unstable balances between positive and negative feedback loops, provide the methodology to explain why the Arab uprisings that started in late 2010 created a window of opportunity for the emergence of DAESH, the most lethal terrorist group known to date. The emergence of a new 'political opportunity', in Tarrow's terms, brought about by these uprisings meant that the terrorism-counter-terrorism balances achieved to date in some countries of the Arab world were rapidly altered.

The disappearance, transformation or reduced capabilities of the security apparatuses of some of these countries meant that the limits containing

latent terrorist activity in the area disappeared. In addition to the social and political instability generated by the uprisings in these countries, terrorist groups added their own destabilisation, fuelling the system to the point of chaos to the point of civil war in some of them. In turn, the security apparatuses of these countries, unable to compensate for the dynamics already generated, had to be supported by the international community to contain the terrorist insurgency, especially in Syria/Iraq.

Delays in decision-making and strategies, the lack of initial international commitment due to the amount of resources required to effectively manage the different crises, as well as the incorporation of international actors with their own conflicting dynamics such as Iran-Saudi Arabia, the US and the EU, have all contributed to the crisis. The US and Russia gave international jihadism sufficient time (delay) to configure itself and adapt to a new reality, resulting in the emergence of DAESH.

On the other hand, action-reaction logic, which is relatively simple in the case of a terrorist/counter-terrorist system, is to some extent conducive to predicting the evolution of the system. However, if one seeks to determine the structure of a more complex system and to predict to some extent its future behaviour, it is important to establish the rules governing the relationships between its parts, as well as the existing constraints. A good example is the systemic relations that may be found in *international relations*, where the driving force of the dynamics of the international system will be conditioned by the relative power relations between the different actors within it. Following Kenneth Waltz's neorealist thesis, the system will remain stable to the extent that actors' strategies are stable because there is no incentive to change them, considering the actions of others. The principles that would govern the system of international relations (Jordan, 2022) are basically:

1. Anarchy: the absence of a central authority is the organising principle of the international system. This means that there is no authority to regulate relations between states, leading to an environment of self-defence where each state must ensure its own survival.
2. Functionally Similar Units: States are functionally similar units, as they do not specialise in specific functions as they do in hierarchical systems. This is because no state wants to depend on others for its survival.
3. Distribution of Capabilities: the structure of the international system is also defined by the distribution of capabilities among states. This distribution can be bipolar, multipolar or unipolar, which affects the stability of the system.
4. Security as a Primary Objective: states seek to ensure their survival and security above all other objectives. This limits cooperation and creates competition for security.

5. Balance of power: states tend to balance power among themselves in order to maintain stability in the international system.
6. Regardless of the existence of other models of international relations, Waltz's model helps to exemplify the modelling of complex systems from which security problems can arise, but which are underpinned by a prior conceptual framework that determines the rules of operation of the system established by scientific research. In this regard, modelling based on sound conceptual models is essential.

4.3 Mental models vs. conceptual models

In relation to the previous section and from a cognitive point of view, we must take into account *mental models*, which are internal and personal representations of external reality that individuals employ to understand the world, reason and make decisions. They are idiosyncratic, incomplete, unstable and basically functional constructs based on individual perception and are influenced by factors such as the analyst's experience, prior knowledge, beliefs and emotions. Their main objective is functionality, which often takes precedence over accuracy. Conversely, *conceptual models* are external, well-defined, bounded representations, defined and shared by a scientific community. They are consistent with the accepted knowledge of that community and are distinguished from mental models by their objective and consensual nature.

In intelligence analysis, analysts inevitably develop and use mental models to simplify the complexities of reality. However, this very feature can become a significant source of error, since the subjective and incomplete nature of mental models can lead different analysts to develop different representations of the same phenomenon. Additionally, resistance to change in these models can make it difficult to adapt to new information, causing data that does not fit the pre-existing model to be ignored or interpreted in a biased way. This confirmation bias can lead analysts to overestimate information that confirms their models and to discount information that contradicts them. Ultimately, the use of incomplete, limited or inadequate mental models can lead to erroneous assumptions, estimates and predictions, which can result in intelligence failures with serious consequences.

It is therefore crucial that analysts are aware of their own mental models and how these can influence their analysis. In this sense, the proposed solution focuses on training to recognise one's own mental models, understanding how they influence information processing, keeping an open mind, questioning beliefs, valuing different perspectives (Martínez-Sánchez, 2014) and, above all, incorporating solid conceptual models generated by the scientific community and sharing them with the Intelligence Community.

4.4 Situation awareness

As a last reference to the cognitive domain after biases, systems thinking and mental models, situation awareness (SA) is the one that mainly affects decision-makers. For this purpose, Mica Endsley's model is followed (Endsley, 2000) which defines it as 'the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future', so that SA is a crucial state of knowledge for effective decision-making in dynamic environments. However, it must be said that SA is a state of knowledge separate from decision-making, as it is possible to have perfect SA and yet make a wrong decision, or vice versa. Nevertheless, good SA increases the likelihood of making good decisions. It must also be stated that the real challenge lies in finding the information required when required, assuming that more data does not equal more information.

While it is true that the concept of SA is widely used in tasks with a high component of motor skills and performance in highly dynamic environments, such as pilots, air traffic controllers and medicine, the intended application of SA here is more focused on SA for decision-makers who have to solve security problems. SA is organised into three interdependent levels where cognitive elements play a major role:

— Level 1: perception of the elements in the current situation. This level involves the detection and monitoring of relevant information from the environment by the decision-maker, which is not free from bias.

— Level 2: understanding the current situation. This level extends beyond simple perception and involves the integration, interpretation and evaluation of the meaning of the perceived elements in relation to the goals and targets of the decision-maker.

— Level 3: projection of future status. The highest level of SA involves the ability to anticipate future events and dynamics based on a current understanding of the situation, which would allow for timely decision-making in the present, while anticipating its effects in the immediate future.

At the heart of Endsley's model are mental models, which, as mentioned above, are knowledge structures stored in long-term memory representing an individual's understanding of a system or environment and the relationships between its components. In addition to steering attention (Level 1) and facilitating the distinction between signals of interest and noise, mental models provide a framework for the interpretation and integration of perceived information, facilitating understanding (Level 2) by helping to

determine the relevance of information in relation to goals. Mental models are also essential for projection (Level 3), as they allow permit the envisioning of future states of the system based on its current state and understanding of its internal dynamics.

However, efforts should be directed at continuously improving the SA of decision-makers by addressing these cognitive factors and supporting the internalisation of accurate and adaptive conceptual models. But we must be aware that the task will be particularly complex, if not impossible, in post-normal circumstances when the facts are uncertain; there are multiple values at play, usually in conflict; the stakes are potentially very high; and the decisions are urgent.

5 Evolutionary systems

At this point, it seems clear that the State Intelligence and Information Services must transform and adapt to the new operating environment as they have been doing for years. Perhaps one of the clearest cases is how Spain has fought against terrorism since its beginnings in the 19TH century, evolving to confront the terrorist waves identified by Rapoport that have affected our country: the anarchist (19th-20th centuries), the new left (second half of the 20th century) and the religious (21st century).

However, the characteristics of post-normal times, such as the speed, scale, simultaneity and scope of change (4S), as well as the accompanying complexity, contradictions and chaos (3C), cast doubt on the scope and speed of the transformation required to adapt to such an uncertain environment.

In the face of this accompanying uncertainty, it may be useful to follow Jan Huston's *Evolutionary Systems Theory* (Huston, 1992, 2005) which postulates that all evolving systems, such as biological or social systems, undergo changes and transformations following a fundamental sequence of five stages:

1. *Emergence*: the start or appearance of a new system.
2. *Development*: a period of growth and internal organisation of the system.
3. *Maturity*: the stage in which the system reaches a state of optimal operation within its existing parameters.
4. *Destabilisation*: a stage characterised by increasing internal complexity and growing difficulty in maintaining stability. It identifies *critical* situations, where the system is increasingly sensitive to change, and *super-critical* situations, where the system experiences excessive and unmanageable complexity.

5. *Transformational Breakdown*: a critical point where the system is transformed, which may result in its extinction or the emergence of a new and different system. Transformation options are limited to three levels: upper (with potential for a new evolutionary sequence), lateral and lower (both leading to extinction at different rates).

In this case, it is assumed that the State Intelligence and Information Services, understood as a subsystem of the SSN, are emerging from a phase of Maturity towards a phase of Destabilisation caused by the new strategic environment, marked by a reorganisation of the International System and a growing geopolitical tension that is affecting the security, defence and intelligence systems at European and the global level.

Prior to its transformational breakdown, a destabilised system goes through critical and super-critical phases, becoming increasingly sensitive to internal and external changes until it experiences excessive complexity. During the super-critical phase, the predominant type of actions determines the outcome of the transformation:

— *Optimisation Actions*: focusing on exploiting the performance of the existing system with the same conservative actions that led to super-criticality. This limits transformational options to lateral or lower levels, eventually leading to extinction.

— *Amplification Actions*: involving the exploration of new or novel actions to enable options to reach a higher level, characterised by new organisational structures and the simplification of processes that are capable of absorbing complexity.

In evolving systems, processing information is vital for adaptation: increased analytical capacity enables anticipating change and designing flexible responses. When a system reaches a critical threshold (information overload or incompatibility with existing structures), it destabilises, generating chaos that forces its reorganisation into a more complex order. Disruption is not a failure, but a stage of innovation where the system evolves by being able to integrate and efficiently manage more and more information.

Some authors aim to conceptualise threats to National Security as complex social systems, proposing the use of structured analytical techniques (SAT), systems modelling and artificial intelligence (AI) as the main tools for their study (Gil, 2024). Considering that the threats of today are characterised by dynamism, interdependence, technological complexity and hybrid strategies, the author calls for a paradigm shift in intelligence from qualitative systems modelling that use SAT to mixed modelling using AI-assisted modelling and multidisciplinary teams to meet the challenges of the 21st century.

At this point, several questions arise: What kind of actions should the State Intelligence and Information Services take to evolve towards higher states of efficiency in order to ensure their adaptation? *Optimisation* actions, i.e. more of the same through small incremental advances? *Amplification* actions through more disruptive and bold changes? Do we know which measures are of one type and which are of the other? Is it sufficient to integrate AI into work processes? More SAT? Better conceptual models? Better modelling of complex systems? A new risk management process map? Restructuring the State Intelligence and Information Services?

6 A new paradigm in Intelligence

Outside the field of post-normal science, several voices have been long calling for a revision of the conceptual framework on which traditional intelligence has been based (Lahneman, 2010; Arcos and Antón, 2010) although recently these and other contributions have been taken up (Ivars, 2023), in order to highlight proposals for a new paradigm of intelligence, however, this presentation will especially follow Lahneman.

In the field of security and defence, Intelligence has historically been a crucial tool for states to ensure their survival and achieve political goals. However, the threats to states have evolved significantly over time, influenced by historical developments, technological advances and momentous events such as the end of the Cold War and globalisation. This situation has led several authors to conclude that the traditional paradigm of intelligence is obsolete and a new one is required.

Traditional Intelligence or the Old Paradigm was developed to a significant extent during the Cold War and analysts' work resembled puzzle-solving with a focus on uncovering secrets, and limited interest in open-source information. Threats, originating from state adversaries with symmetrical and clear-cut behavioural patterns, made military intelligence predominant.

However, the current context, due to its complexity, contradiction and chaos, differs substantially from the Cold War period. The concept of security has broadened to include economic, migratory, informational, energy and other factors. Threats have become transnational and multi-causal, with state, non-state and even institutional actors, making it difficult to distinguish between internal and external threats. The speed of change is high and predictability is low, requiring intelligence methods to be adapted.

Faced with this new scenario, Lahneman proposes a New Intelligence Paradigm, based on the adaptive interpretation of information, in a more proactive, multidisciplinary and cooperative approach. This implies building complex models with information mainly from open sources, which would require expanding the Intelligence Community and the inclusion of various

actors from public administration, civil society and the business world, in order to achieve a holistic and integrated approach in the analysis of reality, which would imply a high level of voluntary information exchange and mutual trust. The author advocates the integration of the two main streams of information, traditionally secret information provided by the Intelligence Community and another stream of open but assessed information, such that they result in reliable, high-value information. In short, Lahneman highlights the dilemma between the secrecy of the traditional paradigm and the openness required for an adaptive interpretation of a rapidly evolving reality that leaves a large trail of useful information available to all.

Other authors have merged Lahneman's ideas with the concepts of post-normal times (Serra and Sardar, 2017), resulting in an interesting synthesis that provides a clear conclusion, the need to expand the number of actors involved in intelligence production. If on one hand, post-normal science recognises knowledge created outside the scientific domain, including practical knowledge, as equal, Lahneman on the other hand advocates broadening the Intelligence Community by merging information from open sources with high added value.

7 The cognitive domain as an asset to be protected

Finally, a last element of discussion is introduced in terms of the need to transform the State Intelligence and Information Services: *the cognitive sphere*. The new operating environment is characterised by the incorporation of the cognitive domain into the operations domains, adding to land, aerospace, maritime and cyberspace. In essence, the multi-domain may be considered an innovative concept developed by the US to adapt to new operational scenarios, in which the effects of different military capabilities at different levels or domains must be coordinated to achieve operational or strategic advantages (Gutierrez, 2023).

For its part, the doctrine of the Armed Forces conceives of the cognitive sphere as:

> '[...] the intangible sphere inherent to human beings, considered individually, socialised or organised, and is consubstantial with their capacity for judgement and decision-making. This area covers the wills of all those affected by conflicts and artificial intelligence systems, and thus permeates all other areas. Its main limitation is that it deals with intangible aspects that are difficult to evaluate, such as values, perceptions, awareness, attitudes and prejudices. Perception is understood as the subjective interpretation, personal creation or mental representation resulting from the internalisation of information and stimuli received from the environment. This area enables the Armed Forces to achieve objectives that are beyond the reach of others, using communication techniques, psychological science and other social sciences'. **(**Ministry of Defence, 2018).

Its introduction into this discussion does not address the need to develop military operations in the cognitive realm, for which one can follow Donoso (Donoso, 2020) but rather the need to adapt the capabilities of the SSN to protect it, given that the belief and value system of a democratic society is one of its main assets. The cognitive realm, a strength of liberal democracies, has become vulnerable in the context of the digital revolution, which is being exploited by hostile actors in a context of grey zone confrontation. Thus, it is crucial to adapt the State Intelligence and Information Services to this new environment; effective strategies must be formulated to manage the risks of disinformation, radicalisation, polarisation, political disaffection, loss of confidence in institutions, scientific denialism, etc., all in a context of ideological freedom typical of a liberal democracy, which makes it a real post-normal challenge to our security.

8 Conclusions: innovation scenarios

The article commenced by asking whether any kind of innovation is required of the State Intelligence and Information Services, in accordance with the scope of their powers, in order to continue to provide permanent support to the National Security System, providing elements of judgement, information, analysis, studies and proposals necessary to prevent and detect risks and threats and to contribute to their neutralisation. In my humble opinion, which represents only my own and not that of the institution to which I belong, several avenues for improvement have been identified in the course of the article, many of which are complementary.

Given the growing hostility in the grey zone, where National Defence, Public Security and Foreign Action intersect, it appears to be a priority to boost collaboration between all Intelligence and State Security Services.

A minimum acceptance of post-normal approaches could strengthen the capacity for knowledge generation through the creation of an extended community of theoretical and practical experts; focusing on the quality of knowledge generation processes while acknowledging the difficulties in predicting the evolution of certain environments; and learning to identify the types of uncertainty we face in order to adjust the strategies that are to be followed. In this sense, it would be interesting to explore the potential role of the National Scientific Advisory Office (ONAC), although it would have to be complemented by collaboration with the security and intelligence departments of strategic sectors, many of which are private.

From a process management point of view, it would be interesting to find a link between intelligence activities (Intelligence Cycle) and the management of security issues (governance), focusing on the quality of knowledge production processes. In this sense, the risk management approach

may be an avenue open to exploration, enabling the modelling of a system of interrelated risks that would favour situation awareness.

As far as Intelligence and cognition are concerned, reducing the impact of cognitive limitations would come from the use of SATs; improvements in systems modelling, especially with the help of AI and; the incorporation of solid conceptual frameworks that may be shared by the State Information and Information Services. All of this would be aimed at improving not only intelligence production, but also the building of situation awareness in decision-makers, thus favouring more appropriate decision-making in each situation.

As far as the evolutionary status of the Spanish Intelligence Community is concerned, it is clear that all its components are trying to adapt to a new strategic environment. In this sense, innovation through incremental advances seems a viable strategy under normal circumstances, but there is a risk that post-normal times will catch us with our homework half done and with little time to react. On the other hand, risky and disruptive changes are not appropriate in the public administration, where continuity and stability are a sure value that guarantees the long-term functioning of the state. In any case, beyond the adaptations of each actor, SSN's global response can only be systemic and must take into account the increasing interaction of the fundamental components of National Security in a context of growing hostility that has not been witnessed in Europe for eighty years.

In terms of the closed-open information balance, the use of open sources to produce both operational and strategic intelligence, has increased dramatically in recent years, although the proposal to augment the intelligence pool with experts from outside the Intelligence Community, generating an open flow of reliable information, is interesting.

Finally, given the growing importance of the cognitive domain in the hybrid strategies being developed in the grey zone, the protection of the cognitive domain in a context of digital revolution is proposed developing strategies adapted to a liberal democratic society that allow the risks of disinformation, radicalisation, polarisation, etc. to be adequately managed.

At this point, it is possible to summarise a number of innovation vectors that can steer the future transformation of the State Intelligence and Information Services:

— Integrating intelligence and governance processes: risk management as a conceptual framework for public security policies.

— Focusing on what can be done (black elephants) and not so much on what is difficult to predict (black swans): quality and resilience of Intelligence processes.

- Strong conceptual frameworks shared by the Intelligence Community.
- Managing uncertainties (surface, less deep and deep) in the most appropriate way: applied science vs. post-normality.
- Integrating cognitive sciences: SATs, systems modelling, etc.
- Integrating processes and improving the situation awareness of decision-makers.
- Extended Intelligence Communities.
- Simplification and efficiency of Intelligence structures.
- The cognitive domain as a new area of confrontation: improving analytical skills and action strategies in democratic environments.
- Merging Intelligence capabilities in the grey zone: coordination and collaboration of the key components of National Security.
- Technological innovation: especially AI integration into routine processes, systems modelling, etc.
- Information flows: knowledge generation through reliable open sources.

Many of these innovation vectors are already part of the State Intelligence and Information Services' lines of action, while others are possibly not. The combination of these vectors, either incrementally or through disruptive leaps, can lead to three scenarios (Curry and Hodgson, 2008):

1. Horizon 1. Dominant system: represents the present and majority practices already in place in the SSN and its Intelligence sub-system. It is characterised by a high degree of stability and strategic effectiveness, although over time it may become less suited to the post-normal environment, facing adaptation difficulties.
2. Horizon 2. Transition and innovation: this is an intermediate period between Horizons 1 and 3. It is characterised by the coexistence of elements of the dominant system with disruptive innovations. This horizon is ambiguous and turbulent, full of experimentation, creativity and debates regarding change. Certain innovations may be absorbed by the dominant system, while others can pave the way for deeper transformations.
3. Horizon 3. Transformative future: represents a transformative vision and a new paradigm that, where appropriate, replaces the current dominant system. This horizon emerges as a response to the shortcomings of Horizon 1, incorporating the successful innovations of Horizon 2. Although initially a barely perceived possibility, it eventually establishes itself as the new dominant system due to its ability to better adapt to the changing environment.

In any case, the very path of transformation of the Intelligence sub-system is one of less deep uncertainties that only time can tell.

Bibliography

Aracil, J. (1995). *Dinámica de sistemas*.

Arcos, R. and Antón, J. (2010). *Reservas de Inteligencia: hacia una Comunidad ampliada de Inteligencia*.

Curry, A. and Hodgson, A. (2008). Seeing in Multiple Horizons: Connecting Futures to Strategy. *Journal of Futures Studies*.

Donoso, D. (2020). Aspectos psicológicos en el ámbito cognitivo de las operaciones militares. *Implicaciones del ámbito cognitivo en las Operaciones Militares*. Pp. 21-45.

Endsley, M. R. (2000). *Situation Awareness Analysis and Measurement* [online]. Lawrence Erlbaum Associates. [Accessed on: 2025]. Available at: https://www.researchgate.net/publication/292771806

Frias Sánchez, C. (2023). Conflict as a driver of change. In: Ministry of Defence (ed.). *XXX Curso Internacional de Defensa. Los motores de cambio de la seguridad y la defensa*. Madrid, Ministry of Defence. Pp. 153-162.

Gil Armario, J. M. (2024). La comprensión de las amenazas a la Seguridad Nacional como sistemas complejos sociales. Aplicación de las técnicas analíticas estructuradas, modelado de sistemas e inteligencia artificial. *Cuadernos de Inteligencia*. 2, pp. 49-74.

Gutierrez de León, B. (2023). Las operaciones multidominio. In: Ministry of Defence (ed.). *XXX Curso Internacional de Defensa. Los motores de cambio de la seguridad y la defensa*. Madrid, Ministry of Defence. Pp. 131-152.

Hidalgo, C. and Funtowicz, S. (2024). Epistemología política. Ciencia con la gente [online]. *Revista iberoamericana de ciencia tecnología y sociedad*. 19(55), pp. 215-228. DOI: https://doi.org/10.52712/issn.1850-0013-454

Huston, J. (1992). *What are the greatest challenges for evolutionary theory in our times?*

—. (2005). *Which Way is Up?*

Ivars Pérez, J. (2023). Una aproximación teórica al viejo y nuevo paradigma de inteligencia para la seguridad [online]. *Disjuntiva. Crítica de les Ciències Socials*. 4(1), p. 39. [Accessed on: 2025]. DOI: https://doi.org/10.14198/disjuntiva2023.4.1.3

Jiménez-Buedo, M. and Vielba, I. R. (2009). ¿Más allá de la ciencia académica?: Modo 2, ciencia posacadémica y ciencia posnormal [online]. *Arbor*, pp. 721-737. [Accessed on: 2025]. DOI: https://doi.org/10.3989/arbor.2009.738n1048

Jordán, J. (2016). *Una revisión del ciclo de Inteligencia* [online]. [Accessed on: 2025]. Available at: http://www.seguridadinternacional.es

—. (2018). The international conflict in the gray zone: A theoretical proposal from the offensive realism perspective [online]. *Revista Española de Ciencia Politica*. 48, pp. 129-151. [Accessed on: 2025]. DOI: https://doi.org/10.21308/recp.48.05

—. (2022). *Teorías realistas para comprender la política internacional* [online]. *Global Strategy Report*. 4. [Accessed on: 10 March 2025]. Available at: https://global-strategy.org/teorias-realistas-para-comprender-la-politica-internacional/

Lahneman, W. J. (2010). The Need for a New Intelligence Paradigm [online]. *International Journal of Intelligence and CounterIntelligence*. 23(2), pp. 201-225. [Accessed on: 2025]. DOI: https://doi.org/10.1080/08850600903565589

Lorenzo-Penalva, J. (2023). Inteligencia estratégica, transdisciplinariedad y sistemas complejos adaptativos. *Cuadernos de Inteligencia*. 1, pp. 51-61.

Martín Palma, R. J. (2023). Las tecnologías del futuro de la seguridad y la defensa. In: Ministry of Defence (ed.). *XXX Curso Internacional de Defensa. Los motores de cambio de la seguridad y la defensa*. Madrid, Ministry of Defence.

Martínez-Sánchez, J. A. (2014). *The Use of Mental Models as a Source of Error in the Analysis of Intelligence*.

Ministry of Defence. (2018). *PDC-01 (A) Doctrina para el empleo de las FAS* [online]. [Accessed on: 2025]. Available at: https://publicaciones.defensa.gob.es/

OSCE. (2020). *Guía de la OSCE sobre actividad policial basada en la inteligencia* [online]. [Accessed on: 22 February 2025]. Available at: https://www.osce.org/es/secretariat/455536

Pajares de Mena, M. D. M. (2010). *Dinámica de organizaciones terroristas domésticas*.

Paya Santos, C. (2017). *Aproximación transversal a los sesgos cognitivos del analista de inteligencia*.

Penalva Lucas, J. (2023). Análisis de modelos matemáticos aplicados a la lucha contra el terrorismo y los extremismos violentos [online].

Revista Política y Estrategia. 140, pp. 35-62. [Accessed on: 2025]. DOI: https://doi.org/10.26797/rpye.vi140.1008

Sardar, Z. (2019). *The Postnormal Times Reader* [online]. [Accessed on: 2025]. Available at: https://www.cppfs.org/

Serra, J. and Sardar, Z. (2017). Intelligence in Postnormal Times [online]. *World Futures Review*. 9(3), pp. 159-179. [Accessed on: 2025]. DOI: https://doi.org/10.1177/1946756717709277

Tarrow, S. (1994). *El poder en movimiento: Movimientos sociales, acción colectiva y política*.

Article Four

A real-world experience of AI usage: the analysis factory of the Analysis and Foresight Centre of the Spanish *Guardia Civil*

Enrique Ávila Gómez
Lorenzo Luna Zambrana

Abstract

This paper examines the use of artificial intelligence (AI) in open-source intelligence analysis, focusing on the experience of the Analysis and Foresight Centre (*Centro de Análisis y Prospectiva-CAP*) of the Spanish Guardia Civil.

It addresses how generative AI transforms the detection, selection and analysis of information, enabling faster and broader access to diverse sources.

However, there it also highlights the challenges, especially AI 'hallucinations', and explores strategies to mitigate these risks, such as the use of knowledge graphs and human validation.

The text highlights the importance of human talent in reviewing and verifying information, as well as the need to adapt to technological change to improve accuracy and efficiency in strategic decision-making.

It also emphasises the need for a holistic and multidisciplinary approach to intelligence analysis, incorporating diverse cultural models to reduce bias.

Keywords

Foresight, Analysis, AI, Hallucinations, Biases.

1 Introduction

This article will descend into tactical-operational territories in the world of AI applied to intelligence analysis processes oriented towards strategic decision-making, abandoning the perennial tendency towards the description of strategic levels that do not allow one to approach this new technological challenge in a holistic manner and with the aim of practical applicability in diverse sectors, amongst which, of course, is the Defence sector, occupying an increasingly central place in a complex and changing geopolitical environment and with the need for tools that allow it to adapt quickly to the scenario.

The social, political and economic structures of our societies are becoming increasingly complex. Each technological advance has introduced, in a layered model, a new layer of complexity. The superstructure generated has, in our opinion, been a barrier to understanding a system which, moreover, requires continuous attention, whose interconnection causes unknown and often undesired effects between the various layers and in which, even more seriously, an important part of the understanding of the functioning of this superstructure has been lost due to the intellectual impossibility of human beings to handle this level of complexity, both on an individual and at a collective level.

The emergence of artificial intelligence (not only generative intelligence) has opened up an array of possibilities, often inaccessible until recently, to the open source information analysis teams that produce the reports that will help decision making at the strategic decision-making levels, i.e. to interpret this complex reality in an appropriate way so that the decision maker can carry out the latter's main mission.

The existing limitations, until recently, both in terms of time and access to the specialised talent available in the phases of detection of information assets of interest and, even more so, in the phases of analysis and dissemination of information were increasingly evident for any open-source intelligence analysis unit. The enormous dynamism and complexity of today's world undoubtedly determined a structural limitation to both the quantity and quality of the analyses that should serve as a basis for strategic decision-making.

No less important was the progressive barrier that automated dissemination systems introduced by often flooding the decision-maker with supposedly relevant (and probably relevant) information, leading to a progressive 'disengagement' of the decision-maker from access to processed information.

This article describes the practical experience that has been developed by the Analysis and Foresight Centre (CAP) of the *Guardia Civil* to configure

an ecosystem for the detection, selection, analysis and dissemination of information of interest to the Strategic Management in matters of Homeland Security, practically in real time, with minimal human intervention and specifically oriented towards the validation of content in the phases of selection and final verification of content which, it is considered, will be the main future task of many professions, among them, that of analysts.

An attempt has also been made to generate a model of access and dissemination of the information generated that allows segmentation of the receiver of the information, limiting (but not eliminating) the decision to access the information assets received through the usual technological tools in this model and which, on too many occasions, caused a collapse due to flooding.

2 The Centre for Analysis and Prospective of the *Guardia Civil* (CAP)

Thirty-one years ago, in an innovative agreement between the academic world and the *Guardia Civil*, *the Centro de Análisis y Prospectiva* of the *Guardia Civil* was created (García López, 2010: 45-60). It is unprecedented in Spain's history for a State Security Force to detect the need to anticipate emerging threats by using foresight and, from a proactive position, to try to develop a design of futures (probable, plausible or possible) based on an exhaustive knowledge of the present, using the technological and conceptual tools available at any given moment.

From that moment of genesis to the present time, the Centre has gone through several models of Strategic Management, more or less oriented towards the generation of scientific-technical products, following classic models of detection of information of interest, classification, analysis, generation of a documentary base and dissemination of this, through the circuits defined internally and externally by the Institution.

The explosion of the Internet and global access to sources of interest for the elaboration of open-source intelligence generated the need to equip itself with a set of technological tools. This would configure an information processing ecosystem that would allow, fundamentally, to adapt to the increasingly rapidly changing times in which it is necessary to have pertinent information for its processing and conversion into internal knowledge and oriented, in the case of the CAP, to strategic decision-making.

At the same time, the CAP has been a centre for the detection (and sometimes subsequent recruitment via competitive examinations) of special talents. Configured as an element of connection with higher education in Spain, its internship programmes, considered of an excellent level by the collaborating universities and by the students who have gone through this

experience, have made it possible to incorporate visions, experiences and skills developed by the new cohorts of university-level citizenship.

The temporary incorporation of young talent, with ideas from outside the Institution, brilliant, often with international experience, has been configured as an excellent framework for work and for the generation of analytical capacities that, among other positive externalities generated, allow us to orient the future of the individuals who finish their internships towards intelligence niches that are not limited to the State, but are extended towards Spanish productive sectors that, for some time now, have made intensive use of these capacities in their competitive intelligence and economic intelligence processes.

Some of the first individuals who did part of their professional training at the CAP are now, part of the intelligence units that have been deployed, above all, in the niche of the large national corporate structures.

Finally, the CAP is tasked with generating a 'culture of security'. Focused on improving social resilience through interaction with citizens, using various channels, both analogue and digital, and adapting content to impact on specific population groups, over the last five years, it has participated in activities with universities, generated documents and created and maintained channels of interaction with academia, the private sector, other institutions and citizens themselves, incorporating technologies such as metaverses, metahumans or Artificial Intelligence for direct interaction with specifically selected groups of interest (Soliman, 2024).

Once the CAP's mission is known and the tools available to carry it out have been described, we enter the process of configuring the ecosystem that is currently being deployed to improve the quality and response times for the generation of intelligence products adapted to the needs of the strategic decision-maker.

3 Pre-scenario: language, detection, validation and timing

The current mission of a unit dedicated to open-source analysis is truly a living hell. Detecting, assessing, analysing and disseminating the infinite amount of information generated at any given moment is beyond human capacity, regardless of the number or quality of human resources dedicated to this mission.

Not so long ago, the skills to be developed by analysts in the first phase of the process of detecting significant information or information of interest for decision making were, fundamentally, that of knowing the repositories of sources of interest (a handful of scientific journals, a few selected libraries, a report from a more or less validated and well-known source, etc.).

This type of capacity was transformed, over time and with the support of basic information labelling and classification technology and, hopefully, the use of a document management system with content indexing capacity (we are talking about not much more than two years ago, the time limit in which an analyst's capacities would be considered the most valuable for the analysis of open source documents), into a more or less automated process of classification and retrieval of documents of interest by the person or group interested in some aspect related to Spain's Homeland Security.

Basically, intelligence products were generated from limited sources, considered, due to their insertion in certain indices, to be of absolute validity and without the need for analysis as to their quality. This methodology, of proven validity, did not, in any case, prevent the appearance of biases or incomplete information, given that access to other schools of thought dismissed by the academic world itself was lost.

The results, as we say, were often probably biased (yes, we now talk about biases in AI, but one does not take into account the biases induced by small analysis teams, with very limited multidisciplinary capacities and with little access to experts with knowledge not directly related to the matter of interest being analysed, etc.) (Mosqueira-Rey *et al*, 2023). Not to mention the limitations of approach induced by the limitations of access to other geopolitical and cultural areas due to language problems. Thus, the results, could be considered optimal given the resources available at the time, but clearly insufficient to understand, let alone operate on, the complexity and immediacy of the decision-making processes required in today's world.

In 2013, through a research project of the IUISI (Instituto Universitario de Investigación de Seguridad Interior – University Institute for Homeland Security Research) , now sadly defunct, this initial problem in early access to information of interest, both within and outside the mainstream, was detected and a study was made of the one-way journey that had taken place from the world of Strategic Intelligence to that of Competitive and Economic Intelligence, which had allowed the development of new methodologies and the application of advanced technological tools by corporations with economic capabilities comparable to those of States.

In this way, and with the aim of planning a return journey towards the models of Strategic Intelligence, at State level, of the methodologies and tools that the large corporations had developed for the generation and use of their own Intelligence, with sectorial and eminently economic objectives, we incorporated the processes of Technology Watch into our own model of knowledge[1].

[1] Technology Watch is a systematic process that enables organisations to detect, select, analyse and disseminate significant information on technological and scientific advances.

During the development of this research process, we did not focus so much on the generation of documentary or, even less, academic knowledge, but rather on the design and deployment of a technological ecosystem for the acquisition, validation and analysis of information of interest based on the definition and evolution of a system of sources aimed at the early detection of emerging threats related to dual-use technologies (in fact, it could be said that all of them, although at that time we focused on dronics and instrumental biotechnology developed by biohacking groups).

The existence of a free software technological platform was discovered, developed with the support of public administrations, which made it possible to automate the acquisition of sources of interest from the Internet, store part of the information locally, validate its interest in a simple way by the analysis teams, expand it thanks to subsequent in-depth analysis work and disseminate it in an automated way, making use of newsletter systems through subscription by the recipients interested in a specific area of knowledge.

The HONTZA platform2 was designed for the execution of a complete cycle of Competitive Intelligence which covered from the initial design of the organisation's strategies and the detection of relevant sources for it, to the final automated dissemination of the information, making use of news lettering by subscription, passing through the processes of transforming the information into Intelligence, with the activity of the teams of analysts developing in an internal social network ecosystem and including the coordination and management of networks of experts from outside the organisation, as well as a system of proposals and project management associated with a given detection of interest during the technology watch process.

With a research team formed by Lieutenant Colonel Arturo Crespo Arranz, Lieutenant Colonel Santiago Alonso Pradillo and the researcher and expert in Intelligence Services María Cuiñas Insúa, we have opted for the development of an ecosystem oriented towards the training of intelligence analysts and the intensive exploitation of open-source information of interest, supported by this platform.

This process is essential to anticipate emerging threats and make informed, strategic decisions.

[2] The HONTZA platform allows work teams to collaborate efficiently, automating technological surveillance processes and facilitating the management of pertinent information. Features include the ability to import information channels, generate collaborative documents, and analyse news developments. The idea of HONTZA was born to offer an alternative to closed-source technology monitoring software, which is often expensive and limits customisation and collaboration between users. The project was promoted by business associations in the Basque Country and funded by the Basque Government's Society for Competitive Transformation (SPRI).

This is the basis of a modern intelligence-generating ecosystem: being able to detect and acquire, in an automated way and in real time, information of interest for the elaboration of knowledge and intelligence on matters of strategic (or tactical) interest to the organisation.

This was happening in 2013-2014 and, of course, over the next ten years, the tools for this type of process have improved in terms of access, detection, indexing and multimodality capabilities. It was no longer only textual elements that were worked with, but technology allowed access to multimodal knowledge of all kinds: unstructured information, audio, video, etc. (AENOR, 2018)

It is from the end of 2023 when we enter a new scenario: generative artificial intelligence services start to be released which, initially on a textual documentary basis, but little by little, with multimodality capabilities, begin to make it possible to automate several of the analysis processes, radically changing the pre-existing model (Storey, 2025).

What problems were found in the previous model? Basically, there are four: time, the sheer number of sources available, language and the multidisciplinary talent that can be accessed by any organisation. And the first, that of time, moreover, is strongly influenced by all the others.

Language has always been a bottleneck for any given body that generates reports for a strategic decision-maker. In the case of intelligence development, moreover, the failure to incorporate various multidisciplinary, multi-language and multi-cultural approaches into the analysis leads to a set of biases that prevent the availability of adequate knowledge for the management of increasingly complex situations. Even more so in a highly globalised and interdependent society in which the impact of different cultural models on decision-making processes may have to completely turn the outcome of a given analysis upside down. A practical example of this assertion can be found in the Intelligence Practitioner's Handbook (New Zealand Institute of Intelligence Professionals, 2024), which introduces elements of the Maori culture into the intelligence analysis processes featured in this interesting book[3].

This dysfunction often severely limits the possibility of making sound recommendations to the decision-maker. Trying not to fall into this error means, in a classic model, going through cumbersome processes of translation and cultural interpretation, using human capacities, often unavailable,

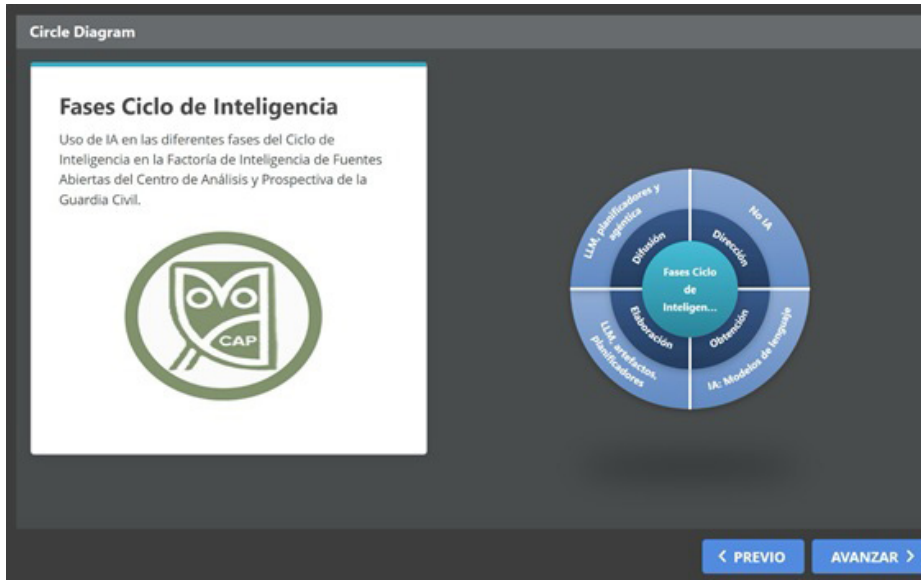
[3] For an analytical access to the content of this one one can use this URL: https://www.ciberinteligencia.eu/new-zealand-intelligence-principles-and-practice/ which also provides a practical example of the analysis model being deployed in the CAP, including the products generated for strategic decision-makers.

which, thanks to automatic translation tools, have made it possible to mitigate, in part, this first barrier.

But it is at the point where generative AI makes its appearance that the access focus of an intelligence team opens up to a model that could be called 360º.

Language barriers disappear and time barriers are drastically reduced when analysing multiple sources, in different languages, in a new process of dialogue with documentary sources that different experts in different subjects can access in a simple way and using natural language for their 'dialogue' with this set of sources.

This is the point at which work begins on introducing the AI tools that are being developed in the different phases of the classic Intelligence Cycle. Below is a graph that attempts to illustrate this implementation. For direct access to the interactive graphic one can use the URL: https://ciberinteligencia.eu/interacciones/ciclo/.



The problem of available talent and the new skills to be developed for its progressive adaptation to the new technological scenario will be dealt with later, because it is a problem that is difficult to solve immediately and requires substantial modifications in matters related to specialised training, culture or limited rotations.

Over the last two years, our Centre has been studying and testing artificial intelligence services that have been considered of interest to improve the efficiency of our task, with the aim of, as far as possible, transforming the Intelligence Cycle process into a model that is as automated and

industrialised as possible, always oriented towards offering strategic decision-makers the intelligence they need, at the right time, to be incorporated into their decision-making processes and, of course, preserving the necessary space for human intervention in the last step of content validation.

Services that have been used include the following:

— NotebookLM by Google. Widely used in the academic world, it generates material of interest for analytical processes such as:

- Documents generated from unstructured documentary sources that are difficult to analyse using traditional methods:
  - o Audio and video sources: there is no longer a need for a human operator to watch/listen to one or more sources for hours on end. An automatic transcription and generation of the basic products of this system is carried out:
    a) Summary document;
    b) Frequently asked questions;
    c) Audio summary file in podcast format.
- The materials generated serve as a starting point for the "dialogue" with the source system, so that, once the necessary knowledge about the subject of interest has been acquired, the analyst, through this process of 'dialogue' with the documentary base, is able to target the prompting in an appropriate manner through adequate contextualisation and orientation towards a specific target audience.
- The final product is a textual document base, of no more than three pages, which delimits the problem and informs the decision-maker of the issues of interest that should be integrated into the decision process.

— Google AI Studio. This platform incorporates the company's new deep reasoning models. Its capabilities for planning, reasoning and searching for information, pinpointing sources and allowing the analyst to define changes in research planning processes make it an invaluable tool for a team of analysts. The possibility of generating intelligence products in both classic documentary and other more accessible and comprehensible, even interactive formats is, in our opinion, a very advanced preview of a set of AI agents that will displace the human being from the centre of the analysis processes[4].

[4] To see a 'life proof' of this controversial assertion, one can access this example of raw analysis, which brings reason to the news: https://edition.cnn.com/2025/06/03/business/trump-tariffs-china-pharmaceuticals-intl-hnk. From this threat detected by

— Microsoft Copilot. Its capabilities for integration with processes through the inclusion of agents and, of course, with standard office tools have undoubtedly been of enormous value in the integration and creation of products of interest for intelligence analysis, with a high impact on training processes and generating the materials for a deployable training activity on an e-learning platform has become an activity that takes hours rather than months. Two internal e-learning courses for analysts, on open-source intelligence analysis and on futures design, have been generated in less than a week. Based on an outline generated from a deep-thinking model, the use of Copilot for the generation of presentations and other training content products, to be deployed, in SCORM format, on the corporate e-learning platform has proved to be a highly efficient experience. Any knowledge is accessible. Any knowledge can be quickly transformed into a structured training action.

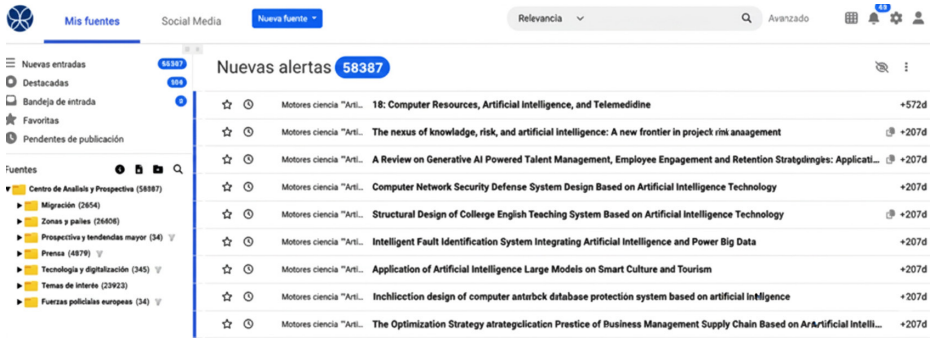
— Deepseek. This model has been incorporated to provide answers generated from other datasets from other geopolitical areas. Being able to compare the approaches, quality of response and ideological spectrum of the model has allowed us to understand a complex context, as well as to detect certain emerging threats related to biases and entity determination. This model is computationally usable with limited resources, so that it is possible to isolate containers of information to be protected and not exposed to systems in the cloud over which control can be lost. Its open-source code allows fine tuning activities to adapt the semantic field to the needs of the organisation, minimising the possibility of unwanted hallucinations.

— Qwen3. This model is characterised by its powerful multi-channel and diverse product generation capabilities including audio, video, images, artefacts or code, among other functionalities. The analysis of unstructured multimedia information has been our main use as we have found its quality to be superior to that of the other models.

— Manus. This is not a language model but a multi-agent system with the ability to interact with the operating system. That is, it can not only generate a plan but also execute it in the form of complex tasks. We were particularly interested in the concept. The agentic ability to perform complex tasks is, in our view, a turning point. Even more so in environments requiring near real-time detection, analysis and response modes of operation. For example, those in the theatre of operations. It is a model that is defined as still experimental but is evolving rapidly.

a global environment, we proceed to use the Gemini 2.5 Pro model and its in-depth reporting utility to obtain the following output: https://www.ciberinteligencia.eu/informe-impacto-amoxicilina/.

The early stage of detection of content of interest already uses AI services to facilitate the generation of a coherent and target-oriented source system as described by the analyst. This activity was historically one of the main sources of error and discussion by the analyst team. Nowadays, it is transformed into a process semi-followed by a planning agent to whom, through natural language, one informs what one's information needs are in order to, from that level, go deeper in the selection of the sources of interest. The analyst becomes a validator of the planner's decisions and, to do so, has to be armed with cultural tools that enable the analyst to make such decisions.



The analysis phase through 'dialogue' with the target sources, contextualising the objectives and the target audience to which the analysis will be directed, making use of various artificial intelligence tools to, in a final phase, analyse the result of the products obtained as new sources of information on which, if necessary, the teams of human analysts can work again, directly. (Bosso and Ruberto, 2025).



The professional analyst will make an initial radical critique of this model, no doubt based on arguments related to professional experience and the need for precision in the response. He will also argue about the possibility of error that all technology introduces into processes that are considered

critical and highly intellectualised, in which it is often professional experience that allows for that 'moment of inspiration' that seems to characterise human beings and place them on an even higher level than technology.

An interesting debate could be held on the harmful consequences of these 'moments of human inspiration' throughout history, as well as their fallibility, which goes beyond the objectives of this document, without entering into the 'interests' that may mediate the recommendations of an analysis group.

However, it can be noted that the fallibility of human inspiration, which is closely connected to our biases, is a key element in shaping analytical teams, as well as in developing their new capacities (Kahneman, 2012)is a fundamental element in shaping analytical teams, as well as in developing their new capacities. Let us see what Gemini has to say about this (IA, 2025):

— 'Cognitive biases: Inspiration often arises from intuitions and hunches, which may be influenced by cognitive biases. These biases, such as confirmation bias (seeking information that confirms our pre-existing beliefs) or the halo effect (letting a single positive characteristic influence our overall perception), can distort our assessment of the situation and lead us to make decisions based on incomplete or misleading information.

— Lack of objectivity: Inspiration can be subjective and emotional, which can make it difficult to be objective in analysis. When we get carried away by passion or enthusiasm, we may overlook important details or ignore potential risks.

— Overconfidence: Inspiration can lead to overconfidence in one's ideas and judgements. When one is convinced that one is right, one might be less likely to listen to others or to consider different perspectives. This overconfidence can lead to risky or unwise decisions'.

In any case, we can only partially agree with this type of criticism from intelligence professionals when it comes to using the tools described above, from a strictly classical intellectual point of view. However, the huge change of scenery imposed by artificial intelligence applied to intelligence analysis induces the need to position oneself critically (constructively) against the considerations of a 'classical' working model.

These would be the arguments considered essential to defend our position in favour of the use of AI in the phases of the intelligence cycle:

— Don't human beings make errors in perception and evaluation response when performing analyses? I believe that our individual and collective bias in assessing situations of interest is indisputable.

Individual biases (educational, ideological, gender) impact on our analyses. But so do the group ones through leadership and power relations in the teams.

— Is the understanding of the current complexity of any human system within the reach of one person (or a team), with limited access to all the knowledge needed to make a correct assessment of a complex threat? One cannot aspire to understand structures as complex as those that shape today's realities. We have neither the individual nor the collective intellectual capacity to achieve this. AI offers a simplification opportunity for understanding complexity.

— Does the time required for understanding and assessing a threat in today's world match the analysis time of a team and, above all, the time required for the strategic decision-maker to respond? Certainly not. Much of today's decision-making processes have already been adapted to algorithmic reality. And it will continue along this path because there is no alternative possibility. It will not stand in the way of complexity and the use of technology to try to make decisions, in real time, about that complexity.

The authors believe that the answer to the three questions posed is negative, which is why we at the Centre for Analysis and Prospective Studies have taken a different approach.

For these reasons, human capacities, limited in quantity and time, are used in only two of the phases of intelligence product development:

— Detection, validation and maintenance of the automated source acquisition system.

— In the validation phase of the product obtained, just before it is disseminated.

We have trained our analysts to perform story structure checks and source verification in order to detect, at an early stage, what we know as 'hallucinations' of artificial intelligence—nothing that any analyst has not experienced on multiple occasions in the course of the latter's career.

It should be noted, however, that the risk has been found to be higher for certain parameters related to the use of general-purpose generative artificial intelligences such as:

— Everything related to entities of different types (people, places, times).

— Up-to-date information on a particular niche issue.

This being true, we have encountered an unexpected ally during the last development phase of our Intelligence Factory in the second half of 2024 and first quarter of 2025: geopolitical (or geo-economic) competition.

After the end of 2024, and especially so far in 2025, we have witnessed a global competition to be leaders in artificial intelligence. Until not so long ago, at least in generative artificial intelligence services, no one had any doubt that the US was the winner... until China positioned itself. And its models (two, with deep reasoning capabilities today, DeepSeek and Qwen) provide differently oriented answers when asked a question of strategic decision interest (Khan, 2024).

Our analysis teams have the mission to operate with different types of AI in order to have a more holistic view of any problem submitted for analysis, as well as to have a parallel system of verification of the information that raises alerts about the existence of a particular hallucination.

The parallel use of several generative AI services, in our experience, improves and enriches the content of the analyses and, above all, provides a vision that is often radically opposed to the one that our teams of analysts handle by cultural and geopolitical model.

This last reflection connects us to talent, its availability, its quality, its multidisciplinary nature.

4 The talent problem

The CAP, currently configured as a civilian unit within the *Guardia Civil*, has as one of its main missions the relationship with universities.

Our internship programme is considered to be of an excellent standard by the universities and training specialisations we work with on a regular basis.

Historically, the vast majority of our trainees have come from degrees in Translation and Interpreting, International Relations, Law, Criminology or Communication. Four years ago, we identified the need to nurture our programmes with capacities in Mathematics, Chemistry, Physics, Engineering and related specialities that would allow us to develop our own capacities related to the most advanced technologies that, at that time, were beginning to emerge on the market.

The training offered to these students is that of a basic level intelligence analyst and, during their stay, they are offered work and problems to help us in our process of continuous improvement of skills.

In the new scenario for the development of their competences, the focus is on critical capacity and the development of cultural skills of a transversal nature, with frequent meetings for debate that generate the necessary 'collective intelligence' oriented towards objectives (Rey, 2022). These sessions are recorded and transcribed so that, using artificial intelligence systems, the knowledge generated can be incorporated into the semantic ontologies of the ecosystem developed.

Setting up stable, multidisciplinary Open-Source Intelligence analysis teams requires access to talent and organisational capabilities comparable to those deployed by the Intelligence units of large corporations, in our case, with the added problem of high turnover and the need for exhaustive control of the information of our trainee teams.

The team's training process begins with the completion of two online courses that allow them, on the one hand, to get to know the environment and the context in which the analysis work will be carried out: the *Guardia Civil*. A Public Security Institution. This is of strategic importance given that students, who come mainly from an 'urbanite' environment, have limited knowledge not only of State security and citizen security, but also of the *Guardia Civil* itself, which they immediately connect with their traffic competencies, and are unaware of its real missions and capabilities.

This fact induces the need for prior training in the knowledge of the aforementioned missions and the appropriate 'semantic model' for the teams to be able to communicate among themselves and with the strategic decision-maker through their reports.

The training is aimed at shaping a 'shared general culture' model in the two areas of knowledge and competence for the KAP: intelligence analysis and the design of future scenarios. Two complementary and fundamental tools for configuring a decision support structure geared to the needs of today's VUCA environment.

Once this initial training has been completed, in which, as we reiterate, the appropriate semantic field has been constructed, we proceed to apply the available tools through specific examples, through which we train the capacities to generate the appropriate prompting to define a context, objectives and a determination of sources and research planning appropriate to the objective set.

In a recursive way and making constant use of DELPHI methodology for the improvement of the final product, either from the optimisation in the generation phase or in the final phase of approval of the product that passes to the dissemination phase.

The experience, once the knowledge structures and information flows have been generated, can be described as optimal, since all these cohorts of students are characterised by a knowledge and use of technological capabilities that can be described as outstanding.

A graphical representation of the process that can be followed, interactively, from the URL: https://ciberinteligencia.eu/interacciones/analistas/.

For all the above, the circle is closed and, our mission being to train these students in basic analysis and futures design skills, their talent is dedicated



to the final review of the products generated almost automatically by the artificial intelligence tools that we make available to them for the generation of reports for strategic decision-makers. Moreover, their own contributions, as outlined above, become part of the shared knowledge both within each cohort and for subsequent cohorts, which, in the end, is one of the best positive externalities achieved: The persistence of knowledge, independent of people. All the knowledge generated automatically becomes part of the CAP knowledge ontology, in such a way that it can be used, at a later stage, to carry out a recursive fine tuning of the model, so as to minimise the possibility of 'hallucinations' in the analysis process.

Diversity (and not just multidisciplinary skills) is therefore seen to have its full meaning in the case in point. Age, gender, ideology, diverse knowledge etc. undoubtedly enriches the quality of the analysis product and, therefore, the ability to detect possible hallucinations in the product generated by the AI.

5 Hallucinations and Other Issues: A Practical Approach

Generalist AIs, while making rapid progress in deep thinking, still have serious problems in handling certain information related to specific entities. Most of us have taken the test of asking AI what it knows about ourselves and have been aware of the disastrous result it has presented, although, admittedly, accuracy is advancing at an undeniable rate.

Let us imagine a similar result when valuing am individual or legal entity, a geolocation or a vehicle, to give an example of interest for Homeland

Security. Such 'hallucinations' would make it unfeasible to use automation processes in a police investigation or, worse, in a theatre of operations of any kind.

Language models trained with general objectives have, among others, this fundamental, one might call it, shortcoming. This would make them practically useless tools for intelligence generation because of their imprecision or, even worse, because of the evident tendency to answer by making up the answers.

Fortunately, in addition to the exponential improvement in their capabilities and accuracy already outlined above, there are possible solutions, so far partial and subject to revision, to mitigate this problem.

How can we improve the quality and timeliness of the data that must feed the answers of language models for them to be reliable?

The generation of specific models, specialised agents, adapted semantic ontologies or knowledge graphs can improve the accuracy of generative AI responses and mitigate the possible hallucinations of generative AI on a sectoral basis.

We will go into detail on this set of technologies, in our opinion, just these are the fundamental elements to be able to make an intensive and precise use of generative artificial intelligence systems in the processes of intelligence generation, in the case of CAP, from open sources.

The paper Ontology Learning for Hybrid Threats (Bosso and Ruberto, 2025), which recommends the use of the HYBOLT tool is described as:

> 'a tool for ontology learning applied to hybrid threat analysis. It is proposed to use large language models (LLM) and knowledge graphs (KG) to extract reliable information from open sources, mitigating problems such as LLM hallucinations. The methodology focuses on extracting subject-action-object triplets to construct a KG, simplifying the information to improve accuracy. HYBOLT's performance in tasks such as location and quantity extraction of affected individuals is assessed, showing high accuracy and resistance to hallucinations'.

This paper offers, in our view, the basic guidelines to be explored in order to achieve the desired results.

After 'dialoguing' with a system of sources related to knowledge about semantic ontologies and other associated strategies applied to intelligence analysis, sufficient knowledge has been obtained to try to develop a set of guidelines with the objective of generating a consistent ecosystem of mitigation of risks associated with possible hallucinations of generative AI during the process of generating Intelligence reports within our Analysis and Foresight Centre, oriented to Homeland Security.

In order to improve the accuracy of sector-specific generative AI from generalist generative AI services, the following strategies have been considered:

— Using formal knowledge bases (Knowledge Graphs – KG) to correct the limitations of Large Language Models (LLM) (Dieter, 2020). LLMs can suffer from delusions, biases and lack of knowledge, especially in specific fields such as hybrid threat analysis. Knowledge bases, such as knowledge networks (KGs), provide structured and verified information to improve the quality of LLM responses. These knowledge bases would draw on established open sources and, on a recurring basis, on their own validated and correctly labelled products. It would therefore enter a process of continuous improvement of the quality of the information handled and used to generate new knowledge.

— Implement a system that transforms unstructured text into structured data. This system includes an ontology learning tool, designed to infer a specific KG of the Homeland Security domain from text and populate it with high quality data. The CAP is currently evaluating the Protegé service[5], from Stanford University, for the generation of a semantic ontology specific to Homeland Security. Generation has been initiated from specific subdomains since the task of generating a semantic ontology for Homeland Security would require resources and equipment that are currently unattainable for our team.

— Build on LLM core capacities. Instead of relying on field-specific knowledge or complex logical reasoning, basic LLM capabilities such as grammatical pattern recognition (subject, action, object) can be used to extract information and create KGs. This minimises biases and hallucinations, as only basic language skills are required. Relying on the LLM's own capacities to generate KGs is the basic tool to ensure the efficiency of the process. KG generation is a complex and costly process that undermines the resources needed to carry it out, making use of the very generative artificial intelligence tools available[6].

— Atomise entities to create simpler and more informative knowledge graphs. This process involves simplifying entity names and adding additional information such as attributes, which makes the graphs more readable and easier to analyse. Correct labelling of entities

[5] See: https://protege.stanford.edu/

[6] A visually attractive example is available at the Spanish Constitutional Court's website. Constitutional Law domain at the URL: https://hj.tribunalconstitucional.es/es/Descriptor/Index?vista=1.

and coherent design of their attributes is a key element in the successful implementation of the ecosystem. To carry out this action requires the incorporation of specific talent. Offers of traineeships have been extended to the areas of expertise needed to work in the above direction.

Allow an example to better understand the concept.

Imagine an open-source news item of research interest.

'Entrepreneur Juan Pérez, CEO of technology company Neuronix, met in Madrid with representatives of the Ministry of Science to discuss a possible collaboration on artificial intelligence'.

A process of entity extraction, entity atomisation and generation of simple and representative knowledge graphs would be executed as follows:

Step 1: Entity extraction (without atomisation)

Initially, the entities detected will be extracted as follows:

— Juan Pérez.

— Neuronix.

— Ministry of Science.

— Madrid.

— AI: artificial intelligence.

But this can lead to an unclear graph if the relationships between entities are not well defined.

Step 2: Atomisation of entities

Atomising means breaking down complex entities into simpler, more specific components. In this way, the relationships between them can be represented much more clearly.

Atomised entities:

- Individual: Juan Pérez.
- Role: CEO.
- Organisation: Neuronix.
- Location: Madrid.
- Government institution: Ministry of Science.
- Theme: AI: artificial intelligence.
- Event: Meeting.

- Relationship: Potential collaboration.

Step 3: Constructing the knowledge network

With the entities atomised, the network will be constructed from these relationships between entities:

- Juan Pérez → holds the role of → CEO.
- CEO → of → Neuronix.
- Juan Pérez → participated in → meeting.
- Meeting → location → Madrid.
- Meeting → with → Ministry of Science.
- Meeting → topic → Artificial intelligence.
- Ministry of Science → interested in → collaboration.
- Neuronix → interested in → collaboration.

This would structure the knowledge in such a way as to feed our ontology in a much safer and firmer way, with structured knowledge that would minimise the possibility of error on the part of the LLM.

— Use a human-in-the-loop approach. Although part of the ontology learning process can be automated, it is important that an expert reviews and adjusts the output generated by AI. Our current validation circuit should be able to implement peer review of the final product. For the time being, this review is assigned to a single analyst who checks the consistency of the document without going into elements of precision, except for the detection of hallucination, which induces an undesirable set of risks. We assess the underlying residual risk as appropriate, on a time-dependent basis.

— Building ontologies semi-automatically. An LLM can be used to generate competence questions for ontology development and convert natural language sentences into OWL axioms, reducing the effort associated with manual creation (W3C, 2025) axioms, reducing the effort associated with manual creation. The LLM's own support in this task is essential for obtaining results and, above all, in maintaining the accuracy of the system. The aforementioned *protégé* is a valuable tool to undertake this automation process.

— Implement knowledge validation strategies. The LLM answers can be compared with the background information of the knowledge networks, verifying the consistency and veracity of the output. Knowledge graphs can also be used as input to multi-step inference processes, further limiting the risk of hallucination. This activity will

be integrated into the process of auditing the quality of responses, in a process of continuous improvement, which is likely to be automated in the future. The SAC is currently studying the possibility of dedicating part of the available resources to training these capabilities to validate, in a more refined way, the quality of the analyses obtained.

— Use a smaller language model, with fewer parameters. Smaller models can be run locally without the need for external computational resources, saving energy and allowing the possibility of using the complexity of the model for future needs. This action needs to be complemented by specific knowledge bases, with high quality data, which, in a way, allow the model to be "sectorised". The possibility of creating specific agents to minimise response times, oriented to specific tasks related to certain decision-making processes or to obtaining limited information on a given issue or entity, is being studied.

— Use the grammatical structure of the text for knowledge extraction. The system can identify and extract elements such as subject, action and object using a few-shot prompting strategy[7].

— Decompose entity names into smaller components. The system can use LLM to split entity names into main name and attributes, allowing the creation of simplified and enriched entities, more manageable for incorporation into other more complex processes. In the CAP, we have tested the extraction and atomisation of entities in certain documents in order to generate KGs on which to work on improving the efficiency and accuracy of the response. Whilst still in the refining process, the results are very promising.

— Ensure consistency of entities. The system can compare the atomised entities with the original ones to ensure that the same entity is not converted into different entities with similar names. Consistency must be ensured so that accuracy does not suffer.

— Implement different strategies to build a coherent knowledge base. This can be by means of high- or low-resolution strategies in the validation of text entities with entities from an existing knowledge base. In our specific sector, Homeland Security, this action is essential to mitigate the risk of hallucinations. Consistency of the

[7] This is a machine learning technique that allows language models to learn to perform a new task with just a few examples. Instead of training the model on a massive dataset, it is provided with some examples of the task and is expected to generalise from them to perform the task on new inputs.

knowledge base and an accurate semantic ontology are the fundamental tools of hallucination mitigation.

— Improve the quality of the instructions given to the LLM in the prompts. Different knowledge graphs generated by different prompts can be compared to determine which is the most promising. It is part of the capacities that the new analysts must develop: to be able to contextualise a given need from different angles and, therefore, to be able to express this contextualisation in prompts that generate responses of varying quality in order to choose the most appropriate one for the proposed scenario. Training the analyst team to develop these specific skills and, moreover, ensuring that the knowledge acquired in this area is persistent is the "core business" of these new analyst teams. Failure to register the prompts ecosystem properly has been a mistake that has been made during the development of new automated analysis methodologies.

— Implement the Retrieval-Augmented Generation (RAG) method. A vector database can be used to keep track of important knowledge graphs loaded by the user (declarative memory) or previous user-LLM interactions (episodic memory). The implementation of a RAG is a complex and action-dependent project which, although studied, would become part of an evolution of our current capabilities. Fundamentally oriented towards proactive maintenance of the semantic domain.



All the above can be represented graphically as follows:

The content of the interactive graphic can be accessed at: https://ciberinteligencia.eu/interacciones/mitigacion/.

6 Conclusions

Open-source intelligence analysis has a tool, generative artificial intelligence, which has opened a new scenario in this sector.

Multi-language capabilities, multi-modality and multi-model LLM constitute an opportunity for intelligence analysis teams in their goal of early detection and access to open source information of interest for strategic decision making by being able to process from diverse cultural models provided by LLM training, thus making it possible to reduce possible biases and, as a result, improve the accuracy of automated analyses.

The problem of hallucinations, especially those associated with specific entities, constitutes a risk to the reliability of the analyses. In this article, possible methodologies and actions aimed at mitigating this problem have been outlined. Some of these are already being studied for implementation in our open-source intelligence factory, in order to replace some of the manual work of the teams with automated tools and processes that also recursively improve the quality of the analyses.

The continuous development of new agentic capabilities, planning and automated execution of open source research processes by the new deep reasoning models is surprising on a daily basis due to the precision and quality of the products generated, which undoubtedly become the working basis for the start of the final content validation action by the human analyst, exponentially improving the efficiency of the process and response times.

The knowledge generated is also incorporated into the Institution's corpus of specialised knowledge, which allows the development of a specific semantic ontology with which to work recursively in the retraining of models adapted to the Institution's needs. At the same time, it reduces the possibility of errors or hallucinations during the analysis process.

By applying these techniques, it is possible to build more accurate, reliable and domain-specific generative AI systems, which improve the quality of the information extracted and reduce the possibility of errors or hallucinations.

Some of these techniques and methodologies for recursive model improvement are already under consideration for implementation in the process of evolving the CAP's analysis capabilities. They will require the development of specific projects associated with a strategic vision that will determine the objectives and tasks to be carried out by the *Guardia*

Civil's open-source intelligence analysis specialised unit in order for the development and implementation to be able to fulfil the task entrusted to it.

Of course, the allocation of financial resources and the attraction of talent for an intensive and efficient exploitation of these tools is, right now, the main objective of the CAP in the short and medium term.

We are learning, sometimes, through error and, of course, thanks to error. There is no need to be afraid of making mistakes. We are in a process of methodological exploration in which the rewards promise to be at a very high level. The process of improving the accuracy of analysis using artificial intelligence tools is evolving and subject to the possibility of partial failure, but the results we are obtaining undoubtedly anticipate the availability of a body of knowledge and tools that will make dealing with complexity no longer an unattainable dream.

Let us not resist change because it is precisely that change that opens up opportunities for success in the future.

Bibliography

AENOR. (2018). *Gestión de la I+D+i: Sistema de vigilancia e inteligencia competitiva* (UNE 166006:2018). [online]. AENOR. [Accessed: 2026]. Available at: https://en.tienda.aenor.com/norma-une-166006-2018-n0059973

Dieter Fensel, U. Ş. (2020). *Knowledge Graphs: Methodology, Tools and Selected Use Cases*. Springer.

Bosso, F. and Ruberto, S. (2025). *Ontology Learning for Hibrid Threats* [online]. EU Science Hub. European Commission. [Accessed: 2026]. Avialable at: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC140863/JRC140863_01.pdf

García López, J. (2010). Creación y evolución del Centro de Análisis y Prospectiva de la Guardia Civil. Revista Española de Seguridad. 25(3), pp. 45-60

Guldenmund, F. W. (2000). The nature of safety culture: A review of theory and research. *Safety Science*. Pp. 215-257.

IA, G. (2025). *Fuentes de error en la inspiración humana*.

Kahneman, D. (2012). *Pensar rápido, pensar despacio*. Debate.

Khan, M. A. (2024). Impact of Artificial Intelligence on the Global Economy and Technology Advancements. *Artificial General Intelligence (AGI) Security*. pp. 147-180.

Mosqueira-Rey, E. et al. (2023). Human-in-the-loop machine learning: A state of the art. *Artificial Intelligence Review*. 56, pp. 3005-3054.

New Zealand Institute of Intelligence Professionals. (2024). *Intelligence Practitioner's Handbook*. New Zealand Institute of Intelligence Professionals. [Consulta: 2025]. Disponible en: https://nziip.org.nz/wp-content/uploads/2024/01/nziip-practitioners-handbook.pdf

Rey, A. A. (2022). *El libro de la Inteligencia colectiva*. Almuzara.

Soliman, M. M. (2024). Artificial intelligence powered Metaverse: Analysis, challenges and future perspectives. *Artificial Intelligence Review*. 57, Art. 36.

Storey, V. C. (2025). Generative Artificial Intelligence: Evolving Technology, Growing Societal Impact, and Opportunities for Information Systems Research. Information Systems Frontiers.

W3C. (2025). *OWL Standard* [online]. w3.org. [Accessed: 2025]. Available at: https://www.w3.org/2007/09/OWL-Overview-es.html

Article Five

ECySAP and situational awareness in multi-domain warfare operations

Antonio Legaz
Juan Tejero
José Francisco Suárez Mulero

Abstract

This article analyses the role of ECySAP (Enhanced Cyber Situational Awareness Platform) as a comprehensive platform for generating cyber situational awareness (CySA) within the context of multi-domain military operations. Based on a conceptual evolution from Clausewitz's *coup d'œil* to Endsley's model adapted to cyberspace, it demonstrates how ECySAP makes it possible to perceive, understand and project threats in complex environments, facilitating decision-making, operational planning and risk management. It describes its functional architecture, its potential integration with Artificial Intelligence and its role as an enabler of mosaic warfare, where interoperability and cross-domain synchronisation are key. Through a hypothetical use case based on the annexation of Crimea, it illustrates how ECySAP could have contributed to mitigating risks, detecting disinformation campaigns and protecting critical infrastructure, while aligning with NATO doctrines and European regulatory frameworks.

Keywords

Situational awareness, Multi-domain warfare, Mosaic warfare, Cyber defence, Artificial Intelligence.

1 Fundamentals of Cyber Situational Awareness (CySA)

1.1 From Coup d'Œil to Cyber Situational Awareness: transforming the military paradigm

The concept of *coup d'œil*, as defined by Carl von Clausewitz, refers to a leader's ability to intuitively and quickly perceive the truth in a complex situation. Clausewitz described this action as an exercise based on instinct and a sense of the truth, unsupported by quantifiable data or extensive analysis. Within the context of traditional battlefields, characterised by linear structures and relative clarity of operations, intuition combined with discernment and foresight enabled commanders to make timely and effective decisions. However, the nature of conflict has evolved dramatically with the advent of the cyber domain, which has redefined the methods and challenges of decision-making.

Today's cyber environment is characterised by its complexity, dynamic nature and high degree of uncertainty. Unlike traditional conflicts, this domain is marked by global interconnectedness, speed of events, and the involvement of multiple actors, which limits the effectiveness of decision-making based solely on individual intuition. Decision-making in cyberspace faces a denser "fog of war" than ever before, with threats evolving rapidly and adversaries using increasingly sophisticated tactics. Within this context, Cyber Situational Awareness (CySA) emerges as an urgent need for comprehension and effective action in this scenario.

1.2 Historical evolution of situational awareness: from Sun Tzu to the digital environment

The concept of situational awareness has acquired a fundamental relevance in many disciplines, especially in the military. Although the term is relatively recent, the essence of this cognitive ability —the perception, understanding and projection of the environment for effective decision-making— has been recognised and applied in military strategy and tactics since ancient times.

Military leaders have always recognised the importance of a clear perception of the environment for planning and executing operations. In *The Art of War*, written by Sun Tzu in the 5TH century BCE, the need to know both the enemy and one's own self is emphasised as an essential principle for victory. The statement "If you know the enemy and you know yourself, you need not fear the outcome of a hundred battles" illustrates an early idea of situational awareness, based on understanding the context and anticipating the adversary's actions.

In the 18th and 19th centuries, European military literature reflected this same concern regarding awareness of the environment. In the treatises on battle strategies of the Napoleonic era, the importance of terrain reconnaissance, the observation of weather conditions, and the gathering of information on enemy positions was emphasised. During Napoleon's campaigns, for example, the use of scouts and reconnaissance units allowed commanders to adjust their strategies based on up-to-date information, demonstrating an implicit understanding of what is now termed situational awareness.

With the First World War, the concept extended to combat in the skies. The term "situational awareness" came into use to describe the ability of fighter pilots to remain aware of their surroundings and enemy movements, a crucial skill for survival in aerial combat. Later, in conflicts such as the Korean War and the Vietnam War, US Air Force pilots identified this capability as the "ace factor", i.e. the ability to anticipate and react effectively to the adversary's manoeuvres.

1.3 Theoretical framework of Cyber Situational Awareness: Endsley's model in cyberspace

Situational Awareness (SA) is defined as the perception of elements within the environment within a volume of time and space, understanding their significance and the projection of their status into the near future (Endsley, 1988). This concept has naturally evolved to cover the cyber domain. Cyber Situational Awareness (CySA) emerges in response to the need to apply these principles to the complex contemporary digital environment, characterised by diffuse and constantly evolving threats (Franke and Brynielsson, 2014).

The adaptation of this concept to the cyber domain has not been trivial. While perception is mainly through human senses in physical environments, in cyberspace this perception depends mainly on technical systems and monitoring tools (Barford *et al*., 2010). This conceptual transition has required a rethinking of classical models in order to incorporate the unique aspects of the digital environment.

Endsley's widely recognised model establishes three hierarchical levels for CySA. The first level, perception, involves collecting data from the cyber environment through sensors, monitoring devices and intrusion detection systems (Endsley and Connors, 2008). This phase is crucial, as it is the informational basis on which any subsequent understanding of the cyber scenario is built.

The second level, comprehension, involves analysing and interpreting the data collected to form a coherent picture of the current situation.

This process requires not only technical skills, but also contextualisation and correlation of seemingly disparate events to identify meaningful patterns (Tadda and Salerno, 2010). Proper comprehension lets us distinguish between false positives and real threats, thus optimising the allocation of defensive resources.

Finally, the third level, projection, represents the ability to anticipate the future evolution of the cyber scenario based on the current understanding of the situation (Onwubiko, 2016). This predictive capability is essential for strategic planning and proactive implementation of defensive measures before the materialisation of potential threats.

CySA shares an intrinsic relationship with the concept of *ground truth*. *Ground truth* represents the objective reality of the cyber environment, regardless of the perceptual or interpretative limitations of the analysts (Jajodia *et al*., 2010). Achieving effective situational awareness involves getting as close as possible to this fundamental truth, recognising that the complexity of cyberspace imposes inherent limitations on this aspiration (McGuinness and Foy, 2000).

1.4 Contemporary operational context: multi-domain warfare and mosaic approach

Modern warfare is no longer only about the most firepower or the best armour, but also about superior situational awareness, the ability to process information quickly and make decisions faster than the opponent (Pulido, 2021). The concept of the OODA (Observe, Orient, Decide, Act) loop has become essential to the planning and execution of military operations (Boyd, 1976). It emphasises the importance of speed and agility in decision-making to gain an advantage on the battlefield.

The transition to multi-domain operations arises from the military's need to be able to operate simultaneously in all these domains, recognising that actions in one can have cascading effects in the others (Fojón, 2020). Multi-domain operations are not limited to armed conflict, but encompass a more holistic view of military strategy. This implies the need to coordinate efforts in different dimensions, such as land, sea, air, cyberspace, aerospace and the electromagnetic spectrum.

This need for coordination and to operate in a complex environment has given rise to the concept of mosaic warfare, which is based on the idea that large military platforms can be divided into a number of functions that can be carried out by individual yet interconnected components (Jordán, 2023). Each of these components would be equivalent to a piece of a mosaic, operating together to achieve a common goal. Thus, mosaic warfare seeks to overcome the limitations of monolithic systems and create a more adaptable and flexible fighting force.

Mosaic warfare is characterised by the disaggregation of functions, where sensors, decision-makers and implementers of actions become separate entities that communicate and collaborate within a network (Pulido, 2021). The importance of information and connectivity in this new paradigm is central, as all "shooters" must be able to use information from all sensors, creating a "kill web" (López Díaz, 2020). This non-hierarchical and distributed architecture allows for greater adaptability and resilience.

2 ECySAP: a comprehensive platform for Cyber Situational Awareness

ECySAP functions as an integrated and modular platform that facilitates the transfer of information on cyber incidents, threats, risks and impacts to different mission effects and objectives. This is in line with the concept of a Cyber Common Operational Picture (CyCOP), which seeks to integrate and contextualise numerous data streams and data points to accelerate cyber situational awareness (Kim *et al*., 2023: 1).

This comprehensive multi-sector planning and mission support tool allows the information generated to be effectively integrated into planning processes, thereby optimising the speed and accuracy of decision-making (Indra, 2021). Situational awareness (SA), although linked to human cognition, is essential for perceiving the environment (Schaberreiter *et al*., 2022: 149, cited in Kim *et al*., 2023: 2) and ECySAP makes a significant contribution to this purpose.

Given the increasing level of interdependence between the physical and digital domains, military and security operations must adopt a holistic approach to achieve an accurate representation of the operational environment. ECySAP not only focuses on the identification and mitigation of cyber risks, but also facilitates the analysis, identification and validation of key elements in multiple operational domains.

2.1 Functional architecture of ECySAP: from perception to projection

ECySAP is based on a multi-tier architecture designed to optimise decision-making in complex operational environments. Its structure is divided in two main layers (figure 1):

— Mission Layer: it includes the mission objectives and tasks, representing the strategic and tactical level of the operation.

— Communications and Information Systems Layer or CIS Layer: contains the CIS services and systems responsible for providing the technological infrastructure need to implement the mission.

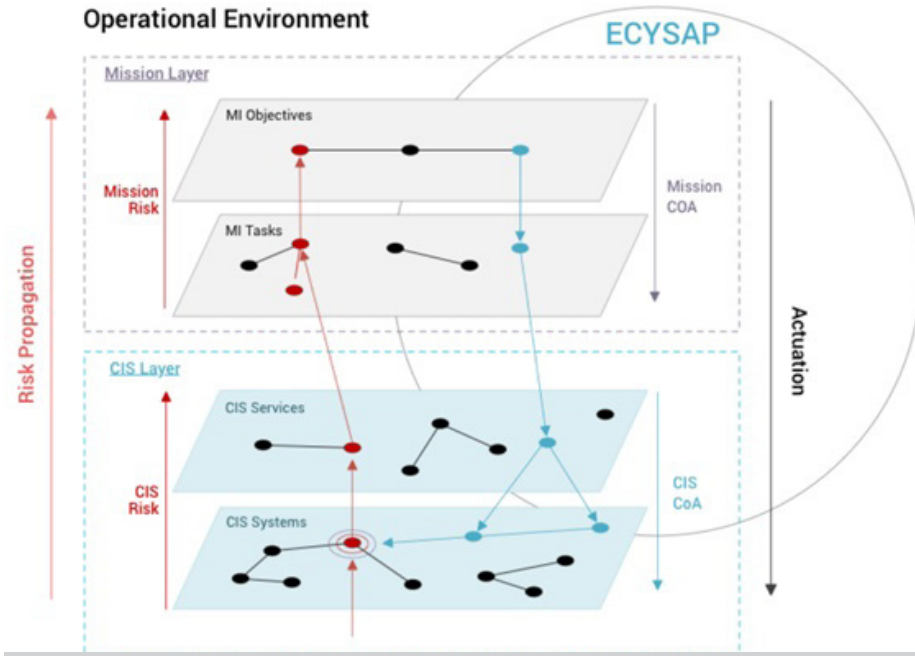


Figure 1. Source: ecysap.eu

One key aspect of the ECySAP architecture is risk spillover from CIS systems to mission objectives. Risks in the CIS layer, that originate in CIS systems and affect CIS services, can spill over into the Mission Layer, affecting mission tasks and objectives. These errors or vulnerabilities in information systems can compromise critical services, leading to adverse impacts on the execution of tasks and the achievement of strategic objectives.

To mitigate these risks, courses of action (CoA) are applied at the mission layer and countermeasures are used at the CIS layer. ECySAP can assist in decision-making to establish an optimal CoA by presenting detailed information at both cyber and mission levels. This facilitates risk management and boosts operational resilience to cyber incidents.

2.2 ECySAP applications in operational planning and courses of action

The information provided by ECySAP on the materialisation of threats and incidents, risks and impacts, and their repercussion on missions, is essential for decision-making. This information serves as a vital input for comprehending the situation in cyberspace in terms of impact (Official Demonstration Communication, 2025), which is essential for mission planning and defining Courses of Action (CoA), as described in the context of NATO's operational planning process (NATO Allied Command Operations, 2010: 4-31).

Operational planning involves mission analysis and development of CoAs (NATO Allied Command Operations, 2010: 4-15). A CyCOP, such as the one developed by Universitat Politècnica de València, aims to generate cyber hybrid situational awareness (CyHSA), merging information from the cyber domain with geo-referenced information from command and control systems in the physical domain, providing a comprehensive view for decision-making (Esteve *et al*., 2016).

By providing relevant information on the cyber situation, ECySAP, can act as a basis for integration with decision support systems, allowing mission commanders or heads to develop strategies and tactics in cyber defence missions within a decision-making space based on accurate and appropriate situational awareness.

This platform also develops and implements advanced analytical tools to detect and assess risks in the technological environment, analysing their possible propagation and impact on operational objectives. In the future, it is envisaged that the system will be able to employ sophisticated techniques to exchange cyber threat information between different actors, boosting their individual and collective response capabilities through the efficient execution of strategies during the mission.

2.3 Risk management and incident assessment through ECySAP

By providing key information on incidents, threats, risks and their impact on missions, ECySAP facilitates and offers functions for risk analysis and assessment of the consequences of incidents (Llopis and Lopes, 2024). This approach responds to the need to assess the damage of cyber-attacks (Kim *et al*., 2022: 59270-59276, cited in Kim *et al*., 2023) and extends beyond the simple identification of incidents, enabling a deep understanding of the operational context in which information systems' capabilities are developed and their impact on missions (NATO Standardization Office, 2024: A-3).

In this sense, the concept of situational risk awareness becomes relevant, as it seeks to assess the hazards and vulnerabilities of complex socio-technical systems (Chatzimichailidou *et al*., 2015, cited in Kim *et al*., 2023: 6).

To approach this analysis in a structured manner, ECySAP follows a number of key steps in the risk and consequence assessment:

1. Identification of critical assets: essential elements, such as servers and firewalls, and their relation to the mission are determined.
2. Risk and vulnerability assessment: threats are analysed using quantitative metrics, considering both the technical and operational contexts and the ongoing mission.

3. Cyber resilience analysis: ECySAP provides the raw data necessary for the analyst to examine the ability of systems to withstand attacks and minimise their impact.
4. Mission impact assessment: scenarios are projected to optimise decision-making at different operational levels.

This holistic approach enables ECySAP to provide relevant information in military environments, facilitating mission planning and defining courses of action (U.S. Army, 2023). A concrete case of this process would be identifying a mail server as a critical asset for communication in a military operation. In this scenario, the assessment would not only consider the technical vulnerability of the server to denial-of-service attacks, but also the potential impact of the disruption of communications on the success of the mission (Indra, 2024).

2.4 Artificial Intelligence integration: boosting ECySAP capabilities

Artificial Intelligence (AI) is deemed a key tool for improved decision-making, as it can analyse large volumes of data quickly, provide dynamic support to decision makers and generate strategic proposals (Llopis and Lopes, 2024). In this sense, AI facilitates information visualisation by automatically refining representations according to risk levels, which improves the understanding of complex situations (Llopis, 2023).

One of the main uses of AI is the automation of malware detection and incident management. Machine learning algorithms, such as Ensemble Machine Learning and Self-Adjusting Memory K-Nearest Neighbors, permit the analysis of data streams in real time to identify malicious patterns (Llopis, Esteve and Mees, 2023). These systems can detect anomalous behaviour indicating an infection or an attack in progress, enabling a rapid and efficient response. Additionally, automation reduces the workload of analysts, freeing them for more complex tasks, while AI-based systems can automatically apply countermeasures, such as blocking malicious IP addresses or isolating infected machines.

Similarly, AI is used to study attacker behaviour and profile cyber-attacks, identifying the tactics, techniques and procedures (TTPs) used by cyber-criminal groups (U.S. Army, 2021). This ability facilitates the anticipation and prevention of potential threats. AI also contributes to real-time decision-making by rapidly analysing large amounts of data, providing concrete recommendations and simulating the impact of different strategies, thus allowing commanders to make better informed decisions.

In the context of ECySAP, the platform will benefit significantly from AI, specifically from machine learning algorithms. At present, ECySAP does not have integrated AI, but the ECySAP EYE project is being developed for

future implementation. This evolution will enable ECySAP to significantly improve its efficiency by enabling a more comprehensive analysis of the data collected and transforming raw data into actionable intelligence for decision making.

2.5 *ECySAP in the context of Mosaic Warfare: enabling Multidomain Situational Awareness*

Within the context of mosaic warfare, the relationship between the ECySAP platform and the networks of effects is essential to understanding the dynamics of modern military operations. Mosaic warfare is characterised by the disaggregation of forces, adaptability and the creation of multiple dilemmas for the adversary, instead of relying on large monolithic platforms and direct confrontation (López Díaz, 2020). Within this framework, the ECySAP platform plays a crucial role in providing the situational awareness required to coordinate and synchronise actions in different domains, which in turn allows for the effective generation of networks of effects (Maestre *et al*., 2022).

The ECySAP platform facilitates this holistic view by providing an in-depth understanding of cyberspace, a domain that has a cross-cutting impact on all other domains in mosaic warfare. ECySAP integrates information from various sources, including physical and logical sensors, to build a complete picture of the operational situation (Maestre *et al*., 2022). This ability to integrate information is fundamental to the creation of networks of effects, as it allows the identification of vulnerabilities in the adversary's system and the critical points that can be exploited for maximum impact.

In this sense, ECySAP not only provides information on cyberspace activity, but also provides insight into how such activity affects other domains. For example, a coordinated cyber-attack can degrade enemy communications, disrupt their command and control systems, and affect the accuracy of their guided weapons, creating a domino effect in other domains. By providing this multi-domain vision, ECySAP becomes an essential enabler for planning and executing networks of effects seeking to disrupt adversary capabilities.

2.6 *ECySAP as an enabler of synchronised operations in multi-domain environments*

The effectiveness of multi-domain operations is critically dependent on the ability to synchronise actions in different battle spaces, generating mutually amplifying effects. ECySAP transcends its role as a mere cybernetic analysis platform to become a backbone of cross-domain integration (Maestre *et al*., 2022). This capability is realised through various functions

that facilitate the transition from the traditional paradigm of segmented operations to a truly integrated approach.

One of the most significant contributions of ECySAP to multi-domain operations is its ability to establish correlations between cyber events and their potential manifestations in other domains. For example, the detection of reconnaissance activities in military networks can be correlated with electromagnetic surveillance data and troop movements, providing early indicators of impending actions in the physical domain (López-Muñiz, 2023). This multidimensional correlation makes it possible to identify patterns that would remain undetected when analysing each domain in isolation.

The platform incorporates predictive analytics and simulation capabilities that allow commanders and staffs to explore simulated scenarios and anticipate cross-domain effects. These functions are aimed at assessing how incidents in cyberspace —such as attacks against industrial control systems (SCADA) or the degradation of satellite positioning services (GPS)— can affect military logistics or the effectiveness of guided weapons systems. These exercises help develop operational intuition regarding interdependencies between domains, preparing decision-makers to manage the complexity inherent in modern operations.

Perhaps the most significant value of ECySAP in the multi-domain context lies in its contribution to the acceleration of the OODA (Observe, Orient, Decide, Act) loop. By providing an integrated view of the operating environment which transcends artificial divisions between domains, the platform enables commanders to identify opportunities and threats that would go unnoticed under traditional compartmentalised approaches. This acceleration of the decision-making process is a decisive advantage in scenarios characterised by the high speed of events and the constant evolution of the tactical situation (Pulido, 2021).

3 Doctrinal and regulatory framework

3.1 The cyber defence doctrine

NATO's doctrinal evolution in cyber defence reflects the transformation of the global threat landscape. Since the first cyber-attacks against Estonia in 2007, the Alliance has progressively developed a robust doctrinal corpus, incorporating cyberspace as a critical dimension of Euro-Atlantic security. The Lisbon Summit (2010) marked the first formal recognition of cyber threats in the Strategic Concept, but it was the Warsaw Summit (2016) that consolidated the Cyber Security Pledge, where allies committed to boosting their national capabilities as an essential contribution to Collective Defence (NATO, 2016).

Developments continued at the Brussels Summit (2018) with the establishment of the Cyberspace Operations Centre (CyOC) in Mons and in London (2019) with the creation of the NATO Cyber Security Centre (NCSC). Both structures operate under the NATO Communications and Information Agency (NCIA) and ensure robust defensive capabilities and the protection of critical C3 networks for command and control (NATO, 2019). The Madrid Summit (2022) deepened this commitment by establishing the Enhanced Strategic Framework for Cyber Defence, which integrates cyber deterrence, defence and resilience into the Alliance's overall posture (NATO, 2022).

The document MC 0665 *NATO Military Concept for Cyberspace Operations* defines the Allied military approach to cyberspace operations and set out three main functions: network protection, defensive operations and support for kinetic operations (NATO Military Concept for Cyberspace Operations, NATO, 2018). This concept is implemented in the AJP-3.20 doctrine, which provides detailed guidelines on the planning, execution and assessment of cyber operations, defining processes for the integration of cyberspace with land, maritime, air and space operations (NATO Standardization Office, 2020).

The *Cyber Coalition* and *Locked Shields* exercises have allowed NATO to test and improve doctrine by providing realistic scenarios to validate operational concepts. The *Crossed Swords* exercise focuses primarily on offensive techniques within the international legal framework, enabling the development of advanced capabilities to counter emerging threats (NATO Cooperative Cyber Defence Centre of Excellence, 2023).

The application of Article 5 to the cyber domain follows a threshold approach, where the determination of an "armed attack" depends on the assessment of scale, effects, intent and attribution (NATO, 2022). This approach, endorsed by the Tallinn Manual 2.0, provides strategic flexibility while establishing credible red lines *vis-à-vis* potential adversaries (Schmitt, 2017).

ECySAP implements these doctrinal principles through multi-source intelligence fusion capabilities, advanced threat analysis and coordinated response tools, aligning with NATO's *Federated Mission Networking* concept to ensure interoperability and operational consistency in multinational environments.

3.2 Regulatory framework

The regulatory framework underpinning European cybersecurity is a complex and multi-level ecosystem that is constantly evolving. The NIS2 Directive (2022/2555) represents its cornerstone, considerably extending the regulatory scope to eighteen critical sectors and introducing

stricter oversight with penalties of up to EUR 10 million or 2% of annual global turnover. It establishes three-step incident reporting mechanisms (24h/72h/1 month) and requires technical and organisational measures that are proportionate to the risk (European Commission, 2023).

The Cyber Resilience Act (2024/1313) complements this framework by addressing connected products, establishing security requirements from design and obligations for manufacturers throughout the product lifecycle. Its security by design approach represents a paradigm shift towards proactive responsibility (European Union, 2024). In parallel, the DORA Act (2022/2554) establishes a specific regime for the financial sector, including advanced penetration testing (APT) and critical third-party provider risk management (TPRM), recognising the interconnection between financial stability and cybersecurity (European Parliament, 2022).

The Cybersecurity Act (2019/881) strengthens ENISA's mandate and establishes the European cybersecurity certification framework, creating sectoral schemes such as EUCC for ICT products and EUCS for cloud services (ENISA, 2023). The CER Directive (2016/1148) addresses critical infrastructures, while the eIDAS Regulation 2 (2023/2084) updates the digital identity framework, incorporating the European wallet and strengthening the requirements for qualified trust services (European Commission, 2023).

At the national level, Spain transposed the NIS2 Directive by Royal Decree-Act 3/2024, creating the National Cybersecurity Office and reinforcing the capacities of the CCN-CERT —National Cryptologic Centre (BOE, 2024). France implemented the *Loi de Programmation Militaire* (2019-2025) with specific provisions on cyber defence and offensive capabilities under the Commandement de la Cyberdéfense (COMCYBER) (Ministère des Armées, 2022). Germany adopted the IT-Sicherheitsgesetz 2.0, granting extended powers to the BSI to audit critical infrastructures and establishing the *KRITIS-Dachgesetz* to standardise sectoral protection (Germany - Federal Government, 2024). Italy developed the *Perimetro di Sicurezza Nazionale Cibernetica* by Decree-Act 105/2019, establishing the Agenzia per la Cybersicurezza Nazionale (ACN) as the national authority (Italy, 2021).

The ISO/IEC 27001:2022 (security management), ISO/IEC 27032:2023 (cybersecurity), and ISO/IEC 42001:2023 (IA governance) standards provide globally recognised technical frameworks, while the NIST Cybersecurity Framework 2.0 offers a complementary role-based approach (identify, protect, detect, respond, recover) widely adopted by European organisations (ISO/NIST Standards, 2023).

ECySAP implements this complex regulatory framework through a modular architecture that ensures multi-level compliance, incorporating specific capabilities for regulatory risk management and agile adaptation

to emerging requirements. Its design facilitates interoperability with national cybersecurity and defence structures, aligning with the principles of European digital sovereignty while maintaining compatibility with NATO standards, thus exemplifying the "Brussels-Washington" approach that characterises modern European cybersecurity (EU Cybersecurity Strategy, 2023).

4 Use case

Russia's annexation of Crimea in 2014 represented a complex multi-domain operation, where actions in cyberspace played a more than important role, as in the case of the attack on the Ukrainian government system using the cyber weapon "Ouroboros", also called Snake, in March 2014 (Ross, 2014) or, according to CrowdStrike, the malware attack on the software used in Ukraine's D-20 howitzers, which led to the destruction of a high percentage of them (Zaks, 2017). We will now perform a hypothetical exercise on how ECySAP could have been used to understand, manage and mitigate the risks associated with this operation.

4.1 Historical context: Mosaic war and the annexation of Crimea

In February 2014, Russia occupied and subsequently annexed the Crimean peninsula, a territory of Ukraine. This operation was a benchmark example of modern hybrid warfare, combining conventional military operations with cyber, information warfare and covert operations. As NATO's official assessment notes, "the illegal and illegitimate annexation of Crimea" represented a flagrant violation of international law and a direct challenge to the European security order (NATO, 2022).

In the case of Crimea, Russia implemented a strategy that combined discrete but coordinated elements: cyber operations against critical infrastructure, disinformation campaigns in traditional media and social networks, deployment of troops without insignia "little green men", and diplomatic actions to legitimise the annexation. This combination of heterogeneous elements acting together exemplifies the principles of mosaic warfare, where the synergy between diverse components creates effects that exceed the sum of their individual parts.

According to the Center for Strategic and International Studies (CSIS), the annexation of Crimea ushered in a new era in the launching of cyber operations as an integral part of broader military campaigns, establishing a pattern that has been replicated and refined in subsequent conflicts (CSIS, 2023). Canada's Cyber Security Agency has documented how, since 2014, Ukraine has had to significantly enhance its cyber defence capabilities in response to persistent Russian threats (Cyber Centre Canada, 2022).

Within this context, a platform such as ECySAP would be especially valuable, as it would provide the ability to integrate information from multiple sources and domains, generating a unified situational awareness to counter mosaic warfare strategies. Just as the concept of mosaic warfare emphasises the flexibility and adaptability of military operations, ECySAP is designed to adapt quickly to a constant threat landscape, providing the tools required to maintain the operational advantage in complex scenarios.

4.2 ECySAP analysis layers within the Crimea-Russia context

Within this context, from ECySAP's perspective, the analysis would begin with an assessment of the mission and information and communication systems (ICS) layers. One of Russia's strategic objectives was to secure control of Crimea, protecting its geopolitical and military interests in the region, including securing the naval base at Sevastopol and projecting its influence in the Black Sea. Operational tasks included the deployment of forces, conducting the referendum and integrating Crimea into the Russian Federation. On the other hand, critical ICS services included telecommunications, Ukrainian government information systems, energy infrastructure and media networks, each subject to risks of cyber-attacks aimed at disrupting communications, spreading disinformation and influencing public opinion.

In the risk analysis and incident assessment, ECySAP would focus on identifying critical assets, such as Ukrainian government servers in Crimea, the telecommunications infrastructure connecting Crimea to mainland Ukraine and the control systems of the energy infrastructure on the peninsula. It would then continue with a risk and vulnerability assessment to analyse exploitable vulnerabilities and possible disinformation campaigns. A cyber resilience analysis would assess the ability of Ukrainian systems to withstand attacks and maintain information integrity. Finally, the impact on the mission would be assessed by projecting views on how cyber-attacks could affect a specific mission, Ukraine's ability to respond to Russian intervention and maintain control over Crimea, as well as the risk of the impact of disinformation on public opinion and the legitimacy of the referendum.

While ECySAP does not have integrated AI for the time being, ECySAP EYE is under development and, with possible future AI integration, it could improve its effectiveness in this scenario. Machine learning algorithms could analyse network traffic in real time to detect malicious patterns associated with Russian activity. AI-based systems could apply automated countermeasures, such as blocking malicious IP addresses or isolating compromised systems. Additionally, AI could study the behaviour of Russian attackers and build cyber-attack profiles, identifying the tactics, techniques and procedures (TTPs) used, which would facilitate the anticipation and prevention of such potential threats.

In the context of mosaic warfare, ECySAP could have facilitated the coordination and synchronisation of actions in different domains, allowing for the effective generation of networks of effects. This would involve multi-domain situational awareness, integrating information from various sources to build a complete picture of the operational situation. In terms of synchronised operations, ECySAP would establish correlations between cyber events and their potential manifestations in other domains, such as the detection of reconnaissance activities in Ukrainian military networks which correlate with Russian troop movements. The platform would facilitate the modelling of multi-domain *kill chains*, where initial actions in cyberspace, such as disabling air defence systems through attacks on their network infrastructure, would facilitate subsequent operations in the physical domain such as air raids.

4.3 Protection against disinformation

In the real-life scenario of 2014, Russia deployed a massive disinformation campaign that laid the groundwork for its military intervention. Russian state media such as RT and Sputnik spread false narratives regarding alleged threats to the Russian-speaking population of Crimea, while covert operations on social media amplified these messages. NATO doctrine recognises disinformation as an integral component of hybrid threats, defining it as "false or inaccurate information spread deliberately to manipulate the opinions and actions of others" (NATO, 2025).

If ECySAP had been operational in 2014, it would have provided critical capabilities to counter this disinformation campaign. The platform could have monitored information flows in real time, identifying anomalous patterns and false narratives through big data analysis and advanced natural language processing. This aligns with the requirement set out in the NIS2 Directive to "develop early threat detection capabilities" (European Union, 2022a).

ECySAP would have analysed the spread of fake news on social media, detecting the sudden creation of thousands of automated accounts (bots) prior to the military intervention, an early indicator of a coordinated operation. The platform would have correlated these disinformation activities with Russian troop movements, establishing patterns that indicated an imminent operation, thus providing what the AJP-3.20 doctrine calls "situational projection capability" (NATO Standardization Office, 2020).

Furthermore, ECySAP could have provided verifiable evidence to Ukrainian authorities and international organisations on the coordinated Russian campaign, facilitating attribution of actions, a critical aspect of NATO doctrine in determining appropriate responses. The platform would

also have generated verified content to counter disinformation, contributing to what the EU's Cyber Defence Policy calls "cognitive resilience" against manipulation campaigns (European Commission, 2022).

4.4 Critical infrastructure protection

During the Crimean crisis, Ukraine experienced numerous cyber-attacks against its critical infrastructure, including denial of service (DDoS) attacks on government websites, disruptions to mobile phone communications, blocked communications between military units and disruptions to essential services. Critical infrastructure protection is a fundamental pillar of both NATO doctrine and the European regulatory framework, with the NIS2 Directive designating eighteen critical sectors as requiring enhanced cybersecurity measures.

The implementation of ECySAP would have provided significant capabilities for the protection of these infrastructures. The platform would have detected, early on, attempts to infiltrate critical Ukrainian networks through network traffic analysis and anomaly detection, fulfilling the requirement set out in Article 21 of the NIS2 Directive to implement "appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems" (European Union, 2022a).

ECySAP would have identified vulnerabilities in SCADA systems of energy infrastructures, anticipated attacks on telecommunications networks based on observed patterns, and continuously monitored electricity grids, water supply and transportation systems for anomalies. This aligns with what the AJP-3.20 doctrine calls "critical information infrastructure protection" (NATO Standardization Office, 2020).

Furthermore, in line with the Common Operational Picture (COP) concept set out in NATO doctrine MC 0665, which emphasises the importance of a shared view of the operational environment for effective action, the system would have provided authorities with a unified view of the state of critical infrastructure. This would have facilitated coordinated decision-making and efficient prioritisation of defensive resources (NATO, 2018).

In the event of confirmed incidents, ECySAP would have automatically alerted analysts of compromised systems so they might be isolated as soon as possible in order to prevent the spread of attacks. Alternative communication channels could also have been established between critical facilities in case of disruption of primary ones, thus implementing the principles of "network segmentation" and "redundancy of critical systems" recommended by the European Union Agency for Cybersecurity (ENISA, 2023).

4.5 Protection of physical military assets

In Crimea, the so-called "little green men", which were Russian soldiers without insignia, took control of strategic military installations, while there was a naval blockade of the Ukrainian fleet, interference with military communication systems, and disabling of radar and air defence systems. NATO doctrine AJP-3.20 recognises and underlines the growing interconnectedness between the cyber and physical domains, stating that "operations in cyberspace can have kinetic effects" (NATO Standardization Office, 2020).

ECySAP would have provided capabilities for the protection of military assets in this scenario. The platform could have warned about electromagnetic interference in navigation and military communications systems by analysing the electromagnetic spectrum and correlating it with cyber activities. It would have detected anomalous communications patterns in the vicinity of Ukrainian military bases, providing early warnings of impending hostile activity.

An especially relevant aspect would have been ECySAP's ability to identify the GPS spoofing used to confuse Ukrainian units, an electronic warfare technique employed by Russia during the conflict. NATO doctrine MC 0665 identifies electronic warfare as a critical component of modern hybrid operations, closely linked to cyber capabilities (NATO, 2018).

The platform would have correlated cyber events with suspicious physical activity around military assets, providing a multi-domain analysis (NATO, 2020) which would have in turn facilitated a holistic understanding of the situation.

Additionally, ECySAP would have provided information required by the command to assess safe routes for the evacuation or reinforcement of critical facilities, maintained secure communications between the Ukrainian central command and units deployed in Crimea, and enabled the remote operation of defensive systems even after the physical occupation of facilities. These capabilities implement the principle of "operational resilience" set out in the NIS2 Directive, which requires "measures to ensure the continuity of critical services even under adverse conditions" (European Union, 2022a).

4.6 Conclusions of use case

The hypothetical use of ECySAP in the annexation of Crimea demonstrates how a comprehensive cyber situational awareness platform could be used to understand, manage and mitigate the risks associated with complex multi-domain operations. In this case, ECySAP could have provided valuable information for decision-making and response planning.

Additionally, while it is stressed that this approach is merely a hypothetical exercise based on the potential capabilities of ECySAP, the Crimean experience highlights five key features of contemporary conflicts that ECySAP would be able to address:

— The line between peace and war is blurred in hybrid conflict scenarios, creating what NATO doctrine calls a "grey zone" where hostile activities take place without escalating into outright armed conflict (NATO, 2020). ECySAP would provide the necessary tools to detect and respond to threats within this ambiguous spectrum.

— In a war environment, attacks start in cyberspace before they are manifested physically, following what the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE, 2023) calls a "preparatory cyber operations model". ECySAP would enable the early detection of these preparatory activities, thereby facilitating preventive responses.

— The ECySAP system would provide capabilities to detect and counter disinformation campaigns. The latter paves the way for conventional military operations, as part of what NATO doctrine MC 0665 identifies as "information operations" aimed at "influencing perceptions, attitudes and behaviours" (NATO, 2018).

— The NIS2 Directive recognises that the integrity of critical infrastructures becomes a priority objective, and it is important to establish enhanced measures for its protection (European Union, 2022a). ECySAP could provide an integrated framework for the protection of this type of infrastructure.

5 Conclusions

Within an international environment characterised by strategic competition and the increasing prominence of cyberspace operations, the development of advanced Cyber Situational Awareness capabilities is no longer an optional advantage but a prerequisite for national security. Military and security organisations that fail to adapt to this new paradigm will be at a significant disadvantage against more technologically advanced adversaries.

The future development of CySA will face a number of challenges, especially with regard to the integration of heterogeneous data sources, the translation of technical indicators into operational implications, and the objective assessment of their real impact. Collaboration between academia, industry and defence organisations will be crucial to overcome these limitations and to maximise the potential of tools such as ECySAP.

Ultimately, the strategic value of Cyber Situational Awareness lies in its ability to reduce uncertainty and accelerate the OODA loop in complex and

dynamic environments. In a world where information superiority is a key factor for operational success, investment in these capabilities is an unavoidable priority for any nation seeking to ensure its security in the complex geopolitical landscape of the 21ST CENTURY.

Bibliography

Barford, P. *et al.* (2010). Cyber Situational Awareness: Issues and Research. *Advances in Information Security*. 46, pp. 3-13.

Boyd, J. (1976). *Destruction and Creation*. U.S. Army Command and General Staff College.

Centre for Strategic and International Studies (CSIS). (2023). *Cyber Operations during the Russo-Ukrainian War*. Washington, CSIS.

Chatzimichailidou, M. M. *et al.* (2015). Seven issues on distributed situational awareness measurement in complex socio-technical systems. In: F. Boulanger *et al.* (eds.). Complex systems design & management. Springer, pp. 89-101. DOI: https://doi.org/10.1007/978-3-319-11617-4_8

Cyber Centre Canada. (2022). *Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine*. Ottawa, Communications Security Establishment.

Endsley, M. R. (1988). Design and evaluation for situational awareness enhancement. *Proceedings of the Human Factors Society Annual Meeting*. 32(2), pp. 97-101.

Endsley, M. R., and Connors, E. (2008). Situation awareness: State of the art. In: *2008 IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*. Pittsburgh, pp. 1-4.

Esteve, M. *et al.* (2016). *Cyber Common Operational Picture: A Tool for Cyber Hybrid Situational Awareness Improvement*. North Atlantic Treaty Organization (NATO) Science and Technology Organization (STO), Technical Report STO-MP-IST-148.

European Commission. (2022). *EU Policy on Cyber Defence. COM (2022) 49 final*. Brussels, European Commission.

—. (2023). *NIS2 Directive: securing networks and information systems*. Brussels, European Commission.

European Union. (2022a). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity throughout the Union, amending Regulation (EU) No 910/2014 and Directive (EU)

2018/1972 and repealing Directive (EU) 2016/1148 (SRI Directive 2). *Official Journal of the European Union*. 27 December, L333.

—.(2022b). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012. (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. *Official Journal of the European Union*. 27 December, L333.

—. (2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council. Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act) [online]. *Official Journal of the European Union*, 20 November. L 2847. [Accessed: 2025]. Available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

European Union Agency for Cybersecurity (ENISA). (2023). *Recommendations for the segmentation of critical networks and systems*. Heraklion, ENISA.

Fojón, E. (2020). *Nuevos paradigmas militares en la era de la Competición Estratégica: el caso de las operaciones anfibias y la guerra mosaico*. Real Instituto Elcano, ARI 13/2020.

Franke, U. and Brynielsson, J. (2014). Cyber Situational Awareness. A systematic review of the literature. *Computers & Security*. 46, pp. 18-31.

Germany – Federal Government. (2024). *Draft KRITIS-Dachgesetz (Framework Act on critical infrastructures) – Comuniqué and documentation* (Official summary of the 2024 legislative process) [online]. [Accessed: 2025]. Available at: https://www.bmi.bund.de

Indra Cyber Defence Unit. (2021). *ECySAP: European Cyber Situational Awareness Project*. Technical White Paper.

—. (2024). *Internal document* (Unpublished document).

Italy. (2021). Decreto-legge 14 giugno 2021, n. 82, convereted to Legge 4 agosto 2021 [online], *Gazzetta Ufficiale* n. 109. [Accessed: 2025]. Available at: https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/SG and https://www.gazzettaufficiale.it/eli/id/2021/08/04/21A04841/sg

Jajodia, S. *et al.* (2010). Cyber situational awareness: Issues and research. In: Jajodia, S. *et al.* (eds.). *Cyber Situational Awareness*: *Issues and Research* (pp. iii-iv). DOI: https://doi.org/10.1007/978-1-4419-0140-8

Jordán, J. (2023). Guerra mosaico: qué es y a qué desafíos se enfrenta. *Revista de Aeronáutica y Astronáutica*. 920, pp. 160-167.

Kim, J. *et al.* (2022). Study on cyberattack damage assessment framework. *IEEE Access*. 10, pp. 59270-59276. DOI: https://doi.org/10.1109/ACCESS.2022.3179977

Kim, K. *et al.* (2023). Study on Cyber Common Operational Picture framework for cyber situational awareness. *Applied Sciences*. 13(4), p. 2331. DOI: https://doi.org/10.3390/app13042331

Llopis Sánchez, S. (2023). *Decision support elements and enabling techniques to achieve a cyber defence situational awareness capability.* Valencia, Universitat Politècnica de València.

Llopis Sanchez, S. and Lopes Antunes, D. (2024). Operation assessment in cyberspace: Understanding the effects of cyber deception. In: *Proceedings of the 19th International Conference on Availability, Reliability and Security.* Association for Computing Machinery, pp. 1-8). DOI: https://doi.org/10.1145/3664476.3672355

Llopis, S. *et al.* (2018). A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military. In: *2018 International Conference on Military Communications and Information Systems* (ICMCIS) IEEE, pp. 1-7.

López Díaz, J. A. (2020). Guerra Mosaico vs Confrontación de Sistemas. *Cuaderno de Pensamiento Naval*. 28, pp. 49-68.

Maestre Vidal, J. *et al.* (2022). Plataforma Europea para adquisición de Consciencia de Situación del Ciberespacio [online]. In: *Actas de las VIII Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2022)*. [Accessed:2025]. Red de Excelencia Nacional de Investigación en Ciberseguridad. 11, pp. xx–xx). Available at: https://2022.jnic.es/Actas_JNIC_2022_v11.pdf

McGuinness, B. and Foy, L. (2000). A Subjective Measure of SA: The Crew Awareness Rating Scale (CARS). In: *Human performance, situation awareness and automation conference; user-centered design for the new millennium*. SA Technologies, pp. 286-291.

Ministère des Armées. (2022). *Commandement de la cyberdéfense (COMCYBER)* [online]. [Accessed: 2025]. Available at: https://www.defense.gouv.fr/comcyber

North Atlantic Treaty Organization. (2016-2025). *Cyber defence, military doctrines and concepts in cyber security.* Warsaw, Brussels and Wales, NATO.

—. (2016). *Warsaw Summit Communiqué* [online]. [Accessed: 2025]. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

—. (2018). *NATO Military Concept for Cyberspace Operations (MCCO)* [online]. [Accessed: 2025]. Available at: https://www.nato.int/cps/en/natohq/

—. (2019). *Brussels Summit Declaration* [online]. [Accessed: 2025]. Available at: https://www.nato.int/cps/fr/natohq/official_texts_156624.htm

—. (2020). *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations (Edition A, Version 1*). [online]. [Accessed: 2025]. Available at: https://iwar.org.uk/wp-content/uploads/2021/06/AJP-3.20-EDA-V1-E.pdf

—. (2022a). *NATO's Strategic Framework for Cyber Defense*. Brussels, NATO.

—. (2022b). *Madrid Summit Declaration* [online]. [Accessed: 2025]. Available at: https://www.nato.int/cps/en/natohq/official_texts_196951.htm

NATO Allied Command Operations. (2010). *Comprehensive Operations Planning Directive (COPD)*. Norfolk: ACO.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2023). *Estrategias de operaciones cibernéticas en conflictos modernos*. Tallinn, CCDCOE.

NATO Standardization Office. (2020). *AJP-320. Allied Joint Doctrine for Cyberspace Operations* (Edition A, Version 1) [online]. North Atlantic Treaty Organization. [Accessed: 2025]. Available at: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

—. (2024). *AJP-6 (Edition B, Version 1) - Allied Joint Doctrine for Communication and Information Systems* [online]. NATO. [Accessed: 2025]. Available at: https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDB_V1_E_2525.pdf

Official Demonstration Communication. (2025). *ECySAP Report: Cyber impact assessment in operations*. Internal project document.

Onwubiko, C. (2016). Understanding cyber situation awareness. *International Journal on Cyber Situational Awareness*. 1(1), pp. 11-30. DOI: https://doi.org/10.22619/IJCSA.2016.100101

Pulido, G. (2021). *Guerra multidominio y mosaico: El nuevo pensamiento militar estadounidense*. Los libros de la Catarata.

Real Instituto Elcano. (2020). *Nuevos paradigmas militares en la era de la Competición Estratégica: el caso de las operaciones anfibias y la guerra mosaico*. Madrid, Real Instituto Elcano.

Ross, A. (2014) Russia's cyber weapons hit Ukraine: How to declare war without declaring war [online]. *The Christian Science Monitor*.

[Accessed: 2025]. Available at: https://www.csmonitor.com/Commentary/Global-Viewpoint/2014/0312/Russia-s-cyber-weapons-hit-Ukraine-How-to-declare-war-without-declaring-war

Schaberreiter, T. *et al*. (2022). A cybersecurity situational awareness and information-sharing solution for local public administrations: The CS-AWARE project. In: Bernal Bernabe, J. and Skarmeta, A. (eds.). *Challenges in Cybersecurity and Privacy – the European Research Landscape*. CRC Press. DOI: https://doi.org/10.1201/9781003337492-8

Schmitt, M. N. (ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press.

Spain. (2024). Royal Decree 443/2024, of 30th April, approving the National Security Scheme for 5G networks and services [online]. *Boletín Oficial del Estado*. 1 de mayo. 106, pp. 49754-49801). [Accessed: 2025]. Available at: https://www.boe.es/buscar/act.php?id=BOE-A-2024-8715

Tadda, G. P., and Salerno, J. S. (2010). Overview of cyber situational awareness. In: Jajodia, S. (eds.). *Cyber Situational Awareness: Issues and Research (Advances in Information Security, Vol. 46)*. Springer. DOI: https://doi.org/10.1007/978-1-4419-0140-8_2

U.S. Department of the Army. (2021). *Field Manual 3-12: Cyberspace operations and electromagnetic warfare* [online]. Department of the Army. [Accessed: 2025]. Available at: https://irp.fas.org/doddir/army/fm3-12.pdf

—. (2023). *ATP 3-12.3, Electromagnetic Warfare Techniques* [online]. [Accessed: 2025]. Available at: https://irp.fas.org/doddir/army/atp3-12-3.pdf

Zaks, D. (2017). Ukraine's military denies Russian hack attack [online]. *RFI*. [Accessed: 2025]. Available at: https://www.rfi.fr/en/contenu/20170106-ukraines-military-denies-russian-hack-attack

Article Six

Technological innovation in the area of cyber threat intelligence and, by extension, cyber defence

Juan Adolfo Montero

Abstract

Traditional cybersecurity focuses on protecting systems from generic threats, which is insufficient in the face of advanced state actors with specific military intentions. To address this challenge, cyber defence, which integrates cyber threat intelligence to plan and conduct defensive operations geared towards specific threats, has emerged.

Cyber defence is based on three pillars:

The mission: ensure that critical systems are protected for operational success.

The threat: assess adversaries, tactics and tools employed.

Cyberspace: identify vulnerabilities, attack routes and strategic areas to establish effective defences.

To improve defensive effectiveness, advanced technologies have been developed such as PICO, a platform integrating cyber threat intelligence and incident management, and ECySAP, which will evolve from a Cyber Situational Awareness System to a cyber operations command and control system.

Additionally, both projects (along with others in development) will be integrated into the SCOMCE programme, which will apply technologies such as data lakes, Artificial Intelligence and simulation to detect patterns, predict attacks and automate responses.

The success of cyber defence will depend not only on these tools, but also on highly trained personnel and a national technology industry that guarantees strategic independence in the protection of military cyberspace.

Keywords

Cyber defence, Cyberspace, PICO, ECYSAP, SCOMCE.

1 Introduction: cyber threat intelligence as a basis for the transition from cybersecurity to cyber defence

For years, cybersecurity has been at the centre of technological developments in cyberspace protection[1]. Research, development and innovation (R&D&I) have been geared towards generating products mainly for the civilian domain, in order to address general and non-directed threats. This approach, which is logical in business or institutional contexts, focuses on the basic protection of systems2 and services against common risks in cyberspace. (Seguritecnia, 2023)

However, when analysing these same products from a military perspective, a major shortcoming is revealed: they do not consider the tactical, operational and strategic aspects of military operations. Nor are they designed to address specific and sophisticated threats that directly affect national defence nor do they respond to operational priorities arising from ongoing missions.

For a long time, the Armed Forces adopted commercial cyber security tools, applying them in military contexts with a similar approach to civilian ones. However, the reality of cyberspace as a new domain of operations has shown that this approach is insufficient. It is essential to integrate a broader model: cyber defence, which complements cybersecurity with an analysis geared to the specific needs of the military environment.

Within this cyberspace context of military interest, conventional cybersecurity systems are not a real obstacle against state actors with large capabilities and resources (technological, economic and human) and clear strategic (geopolitical and military) objectives. These adversaries can use specialised tools to easily evade traditional protection mechanisms (cybersecurity) (Arteaga and Alonso, 2025)

1.1 Why is traditional cybersecurity no longer enough? (Rodriguez, 2023)

— Because adversaries employ advanced technologies that are capable of circumventing conventional cybersecurity systems.

[1] In this article we will refer to cyberspace (or sometimes "systems" in general) as any CIS system, platform or combat system, or weapons system whose components include software, as well as civilian IT/OT-dependent infrastructures and services that support military capabilities or state powers and are therefore critical to National Defence and National Security.

[2] The term "system" in this article refers to any CIS system, platform/combat system or weapons system whose components include software, as well as civilian IT/OT-dependent infrastructures and services that support military capabilities or state powers and are therefore critical to National Defence and National Security.

— Because commercial solutions are designed and configured3 to identify common threats and are not optimised to detect and neutralise specific threats directed at the armed forces.

For this reason, cyber defence based on Cyber Threat Intelligence is positioned as a key element. This approach allows us to:

— Gain situational awareness of cyberspace (CySA).

— Support tactical and operational decision-making and defensive planning for cyberspace from a military perspective.

— -Reconfigure cybersecurity and cyber defence systems to specifically respond to threats4 that directly affect the mission or strategic interests.

This type of intelligence requires a specialised cyber threat intelligence platform (TIP), capable of adapting to the unique characteristics of the environment of military cyberspace operations.

The growing activity of secret services, military cyberspace operations units or proxy groups subsidised and supported by hostile states and nations led NATO to recognise cyberspace as a new domain or field of military operations at the Warsaw Summit in 2016. This statement marked a conceptual shift from reactive and generic cybersecurity (necessary but insufficient) to cyber defence based on planning and cyber threat intelligence (NATO, 2016)

1.2 Key differences between cybersecurity and cyber defence

Cyber defence is not just an evolved form of cybersecurity, but a different approach that incorporates three critical factors:

1. The mission. What are the functions, capabilities, systems or services to be protected?
2. The specific threat. Who is the attacker or potential attacker, how and with what intentions?
3. The weaknesses of the system. What are our vulnerabilities? Where can they attack and impact us operationally?

[3] Cybersecurity systems are designed and configured with detection rules to detect the most common modus operandi for most threats, but it is not specialised, nor does it prioritise detection/reaction capabilities against specific cyber threat actors that the Armed Forces must address. Commercial cybersecurity relies on detecting technical indicators of compromise (IOCs) or anomalous behaviour, but does not provide a tactical or strategic defence against adversaries with clear and persistent intentions against national interests or those of Defence and National Security.

[4] Depending on the mission, geopolitical situation, region or area of operations, etc.

From this perspective, threat analysis becomes a decisive factor. Cyber defence involves planning and conducting predictive and proactive defence driven by cyber threat intelligence.

1.3 Military analogy: cybersecurity as basic defence

"Traditional cybersecurity" may be compared to the basic elements of "immediate protection"5 of an infantry position: barbed wire, minefields, fixed positions. While they are indeed necessary, they are not enough to stop a determined and well-armed enemy with specific targets. These mechanisms act as immediate protection, but have no tactical or strategic vision.

Cyber defence, on the other hand, is based on cyber threat intelligence , planning and adaptation, with the goal of protecting the military cyberspace environment in line with the military mission, anticipating and neutralising the adversary's moves.

2 The "operationalisation" of Cyberspace

The concept of "operationalisation" of cyberspace represents a profound change in the way cyberspace operations are understood. Until recently, actions in cyberspace were approached from a purely technical perspective. However, this domain has begun to be fully integrated into the planning and execution of military operations, applying similar tactical and operational principles as in other traditional domains of military operations (land, sea, air, space) (Ganuza, 2020).

This new approach means that defensive actions in cyberspace are no longer based solely on protecting systems across the board, rather three key factors must now be considered and analysed in detail:

— The specific threat to be faced.

— The mission to be accomplished.

— The vulnerabilities of military cyberspace to be defended.

As a result of this evolution, tools and technologies specifically designed with an operational military mindset begin to be developed, overcoming the limitations of purely technical approaches. The focus is no longer on generic threats, but on specific actors, whose capabilities, motivations and intentions are analysed in light of their geopolitical context, area of influence and strategic objectives.

[5] No tactical purpose, their sole objective being to provide some protection to the combatants.

This transformation has given rise to a much more specialised cyber threat intelligence, one that is capable of integrating aspects such as:

— The region where operations take place.
— The intentions of hostile actors.
— Military and political interests motivating possible attacks.

Consequently, the operationalisation of cyberspace not only shifts the focus, but also incorporates cyber threat analysis as an essential component in designing and executing an effective defence. This inclusion makes cyber defence an area of operations that can no longer be limited to simply preventing or reacting to incidents, but must anticipate them, based on a thorough understanding of the adversary, the operational environment and the military cyberspace on which operations rest.

3 Cyber defence: a holistic and intelligence-led approach to cyber threats

One of the biggest challenges in cyberspace is the clear advantage of the attacker. They can decide what to attack, when and how, using techniques, tools and *malware* at will, and with all the time in the world to plan and execute their offensive. On the contrary, the defender must protect the entire system as a whole, without knowing exactly where, when and how the attack will come from.

3.1 Advantages and disadvantages of the attacker and the defender

The attacker only needs to exploit one vulnerability. The defender, on the other hand, must secure all of them. This asymmetry defines the character of military cyberspace defence: reactive in its most basic form, but with the potential to be proactive and predictive if supported by specialised cyber threat intelligence.

Even so, the defender has certain tools at their disposal:

- Knowledge of the environment to be protected (cyber-terrain).
- Access to cyber threat intelligence, with historical analysis of enemy behaviour.
- Ability to modify military cyberspace, applying defensive configurations, reorganisations and tailored countermeasures.

3.2 Cyber defence: from reaction to anticipation

In the face of advanced threats such as APTs (advanced persistent threats)[6], cyber defence must focus on anticipation, planning, and a pro-

[6] In other words, threat actors with large human, financial, technological and procedural resources. They are usually subsidised and supported by states and with geopolitical, strategic-political and military interests.

active approach. This is achieved through an approach based on a detailed analysis of three key factors.

3.2.1 The threat

It involves identifying and understanding potential adversaries[7]:

— Their capacities and resources.

— Their motivations, intentions and targets.

— Their tactics, techniques and procedures (TTPs, *modus operandi*).

— Tools, malware, the vulnerabilities they exploit, etc.

This knowledge enables the planning of defensive operations driven by specific cyber threat intelligence *(Intel-Driven Defensive Cyber Operations*).

3.2.2 The mission

Defence cannot be generic. It must focus on protecting systems and services that are critical to the success of the military operation. This approach is part of the mission assurance concept. For this purpose, the analysis focuses on:

— Which parts of cyberspace[8] are essential or critical for the mission?

— Which systems, if attacked, could potentially have the most negative impact on the mission?

— What would be the potential impact if they were attacked?

— What services and assets are then a defence priority?

Analysing the operational "Centre of Gravity", critical capabilities, the dependencies of these capabilities on military cyberspace areas, and the vulnerabilities of said areas[9] helps to identify potential adversary targets and priority areas to defend.

3.2.3 Cyberspace to be defended[10]

Once the key assets and services have been defined[11], the following must be analysed:

---

[7] Typically, APTs consisting of state military cyberspace operations units or secret services and criminal groups (proxies) supported and subsidised by hostile states.

[8] Critical cyberspace elements or services that we must, as a matter of priority, defend in order to achieve the mission assurance objective.

[9] These cyberspace areas will consist of services, systems, platforms, etc.

[10] This includes digital assets such as databases, critical applications and operating systems, as well as key infrastructure and mission-critical information and data.

[11] Priority cyberspace areas to be defended in the military interest.

— Their technical and tactical vulnerabilities[12].

— The adversary's possible avenues of approach[13]: potential routes to infiltrate, advance and reach their targets.

— Vulnerable or less protected areas of cyberspace to be defended.

Here, advanced cyber threat intelligence is the key to moving from reactive to preventive and planned defence.

3.3 Application of tactical, operational and strategic intelligence

In order to plan and execute the defence, cyber threat intelligence must be applied at all levels:

— Tactical: analysing defensive vulnerabilities, critical services, possible enemy access routes, intentions and capabilities. It allows defining the defensive plan at the tactical level.

— Operational: studying the actions and effects sought by the adversary to achieve its broader (operational and strategic) objectives.

— Strategic: identifies key cyber threat actors[14], their relationships, structural capabilities, technological and training resources, and links to hostile governments. This will enable strategic-level defensive planning focused on attacking[15] the roots of the adversary's offensive capabilities in cyberspace.

3.4 The IPB model applied to cyberspace (Cyber-IPB)

This approach, taken from the conventional land combat, is adapted to cyber defence by applying terrestrial tactical elements and concepts to cyberspace.

Cy-IPB is the result of a cross-analysis (correlation) of available data and information on: the mission, the threat and cyberspace, provided to cyber warfighters in an organised and easily visible and understandable manner,

---

[12] Such as insecure configurations, outdated software, interconnections and points of vulnerabilities in cyberspace to be defended and which may be exploited by adversaries when attacking.

[13] As a territorial analogy, the aim would be to identify potential valleys and troughs in cyberspace that could potentially be used by the adversary as avenues for approaching, advancing or attacking the targets. These valleys or troughs in cyberspace would consist of the routes formed by the most vulnerable and insecurely configured devices and services.

[14] Depending on the geopolitical situation, missions and operations, etc.

[15] Attacking their human, technological, training, economic and other resources.

so that it supports advice and decision-making in cyberspace operations. (Winterfeld, 2002).

This approach includes conducting a detailed analysis of the environment, similar to the *Intelligence Preparation of the Battlefield* (IPB) process (U.S. Department of the Army, 2009). Some key concepts that have been translated into the realm of cyberspace operations include:

— Basis of departure: these will be the attacker's entry points (such as e-mails, USB ports, connections between systems and services, etc.).

— Targets: these will be critical services or assets that the adversary may intend to attack or target (such as database servers, critical application servers, CORE service servers, COI services[16] and core services, etc.).

— Avenues of approach[17]: these will be the most vulnerable routes within cyberspace to be defended[18] and which may be used by an attacker in advancing towards their targets.

— Hidden or semi-hidden zones: these are cyberspace areas to be defended where adversaries can operate undetected by traditional cybersecurity systems. They may be:

  - Hidden zones: these will be cyberspace areas to be defended that are not monitored by cybersecurity detection mechanisms.
  - Semi-hidden zones: these will be cyberspace areas to be defended, which, although monitored by detection mechanisms, do not have the detection rules or appropriate configuration to detect the TTPs[19] employed by the specific cyber threat actors that we face.

— Covered zones: these will be cyberspace areas to be defended and which do not have cyber defence and cyber security mechanisms in place that would allow us to react directly on the attacker or to modify the cyberspace configuration[20].

---

[16] COI stands for: "Community of Interest." These are functional services such as INTEL-FS, JTS, etc. (formerly called FAS or Functional Area Services).

[17] There may be many potential "Avenues of approach"; therefore it is necessary to perform an analysis and rule out vulnerabilities that are theoretically not exploitable by the TTPs of the cyber threat actors defined for each case. Additionally, these routes will have to be prioritised from a defence planning and blockade point of view.

[18] "Cyberspace to be defended" is understood as the set of IT and OT systems that support military capabilities and thus military operations.

[19] TTP stands for: "Tactics, Techniques, and Procedures." (Tactics, Techniques and Procedures).

[20] For example, by modifying the security settings of devices or rules of access, etc.

— Cyber Key Terrain (CKT[21]): these will be points in cyberspace to be defended (typically where critical and vulnerable routes converge, such as system interconnections, critical servers, satellites or undersea cables), whose control, defence and monitoring provides a defensive advantage.

Cyber Key Terrain (CKT) are those areas of cyberspace that, if properly defended, will make it extremely difficult for an adversary to progress or advance through our cyberspace and for an adversary to successfully attack targets in cyberspace (Multinational Capability Development Campaign, 2017).

This analysis helps to plan a proactive and dynamic defence, anticipating the adversary's moves and closing gaps before they can be exploited.

3.4.1 Cyber-IPB: goals and benefits

Cyber-IPB allows us to:

— Identify who might attack, what they might attack, why and how.

— Detect attack routes and critical areas that may be exploited by the adversary:

- Detect vulnerable routes within cyberspace.
- Detect vulnerabilities in cyberspace that may be exploited.
- Detect insecure configurations that may be exploited.

— Assess potential impacts and risks (technical, tactical and operational).

— Design more effective and efficient defensive, prevention, containment, reaction and recovery plans.

All of the above in order to:

— Pre-empt the adversary.

— Better allocate limited resources:

- Prioritise resources
- Prioritise defensive activities
- Prioritise cyberspace areas where major cyberspace efforts are to be made.

— Reduce the operational impact of a potential cyber-attack.

[21] CKT stands for: "Cyber Key Terrain. Cyber Key Terrain. Equivalent to the concept of "Key Terrain" in the terrestrial domain but transferred to cyberspace.

3.5 Cyber defence plans (Corletti Estrada, 2017)

Based on this Cyber-IPB analysis, a specific Cyber Defence Plan will be drawn up, the objective of which is to:

— Reduce risks in cyberspace.

— Reduce potential impacts.

— Respond to cyber-attacks.

— Ensure operational continuity.

— Ensure the fulfilment of the mission.

Cyber defence plans will be designed and executed at every level of warfare: technical, tactical, operational and strategic. Each of the plans at these levels will address cyber defence from different perspectives:

— Technical level: technical management of risks and potential impacts.

— Tactical level: conducting cyber defence tactically, as a defence of cyberspace as a whole.

— Operational level: supporting the management of the risks and impacts of cyber-attacks on military operations.

— Strategic level: strategic management of cyber defence resources (human, training and technological), strategic attacks on the sources of the adversary's offensive capabilities.

This plan includes the following components.

3.5.1 Advanced Detection Plan

Its purpose is to establish mechanisms to identify malicious behaviour in networks and systems, using cyber threat intelligence.

It focuses on:

— Deploying security sensors in key cyberspace areas (Cy-NAIs[22]), especially at strategic points[23] where an adversary may advance.

— Configuring these sensors with rules to detect tactics, techniques, tools and *malware* commonly used by the threat actors defined, based on tactical and technical cyber threat intelligence.

[22] Cy-NAI stands for: "Cyber Name Areas of Interest.

[23] Generally, these are points of intersection of various avenues of approach by the adversary.

3.5.2 Obstacle Plan

It seeks to hinder the adversary's progress within the system by means of:

— Security mechanisms that monitor, filter and restrict data traffic at key points in cyberspace, preventing the adversary's free movement.

— Pre-defined plans to deactivate vulnerable[24] services that could be exploited as a route for access, penetration and progression of a cyber-attack.

This plan is based on a detailed analysis of possible attack routes (avenues of approach), considering the system's weaknesses (vulnerabilities) and the adversary's capabilities (TTPs and technology).

3.5.3 Impact Mitigation Plan

Designed to minimise damage (effects/impacts) in the event of a successful cyber-attack by the adversary:

— At the tactical level, redundant systems and high-availability configurations will be put in place to keep services up and running despite attacks.

— At the operational level, contingency plans will be implemented with alternative resources, both military and civilian, to ensure the continuity of operations, including outside the digital realm[25].

3.5.4 Reaction Plan

It provides for specific responses to different types of cyber-attacks that are anticipated (Cy-OCOAs[26]), including:

— Rapid Reaction Team Deployment Plans (RRT[27]).

— Detailed incident management plans at technical and tactical levels.

3.5.5 Recovery Plan

It ensures the rapid restoration of critical systems and services through:

---

[24] It would be the equivalent of destroying bridges upon an enemy's advance in the land domain, in order to delay or reroute them.

[25] For example, to make provisions for transporting fuel by tanker trains, in the event that a particular pipeline is attacked.

[26] Cy-OCOA stands for: "Cyber Opposite Course of Action." Potential courses of operational action in the adversary's cyberspace.

[27] Rapid Reaction Team for cybersecurity incidents or cyber-attacks.

— The use of technologies such as virtualisation or hyperconvergence[28] in IT and OT, which allow services to be rebuilt in minutes.

— For data, data recovery plans (DRP) with times (RTO[29]) and recovery points (RPO[30]) defined according to the critical nature[31] of the service for the military operation.

4 Technological challenges of Cyber Defence

The current cyberspace landscape is marked by an accelerating evolution of threats. Zero-day attacks[32], polymorphic viruses[33] or targeted ransomware are advancing at a speed that exceeds the response capacity of traditional cybersecurity tools (Garzón, 2025).

Conventional mechanisms, based on signatures or technical indicators of compromise (IOCs), have become obsolete in the face of highly skilled, sophisticated and, in many cases, hostile state-backed adversaries.

4.1 The need for national and strategic solutions

In the face of this background, it becomes essential to have cyber defence systems that are specifically designed for this highly demanding environment and tailored to the specific needs of our Armed Forces.

Moreover, because of their strategic nature[34], it is essential that these solutions:

---

[28] These are advanced systems that, instead of having separate servers, storage (such as SAN or NAS) and networks, are combined by means of hyper-converged infrastructure (HCI) into modular nodes (such as boxes that have a bit of everything), making it easier to scale and manage the environment.

[29] RTO stands for: "Recovery Time Objective", i.e. the maximum time within which the data must be recovered and the service or system must be able to access the data.

[30] RPO stands for: "Recovery Point Objective", i.e. the maximum amount of data that may be lost, which corresponds to the time between two consecutive data backups.

[31] Potential impact on operations in the event that it is attacked.

[32] A "zero day" is a security vulnerability in software that is discovered by attackers before the software developer becomes aware of its existence. Since the manufacturer has not had time to fix it (because they were unaware of it), there are no official patches or defences available, which makes it especially dangerous. Its name comes from the fact that the software provider has "zero days" to fix it from the time it is discovered publicly or begins to be exploited by potential adversaries or malicious actors.

[33] It can change its form to evade detection.

[34] Cyber defence is an area that cuts across all military capabilities, which gives it a strategic character and therefore requires strategic independence; it cannot be dependent on non-national technology. The cyber defence of our military capabilities cannot depend on an industry under the control of a third country, which may disable these cyber defence capabilities at will, or is able to access information on weaknesses in our cyberspace.

— Are developed nationally, ensuring technological independence.

— Do not rely on foreign technologies or companies that can compromise security or disable defensive capabilities remotely (Kill-Switch[35]).

The national cyber defence industry thus becomes a key pillar in ensuring an autonomous and effective defence of military cyberspace. Without a sovereign technological base, cyber defence becomes a castle on borrowed foundations: stable, as long as the provider of the cyber defence tools agrees to it. Boosting domestic industry is not just an option, it is a strategic necessity (Arteaga and Alonso, 2023)

4.2 The need for agile development and procurement

Cyberspace is a dynamic environment, where attackers and defenders compete in an ongoing technological race. Therefore, cyber defence tools must:

— Keep up with or ahead of the technological pace of attackers.

— Overcome the slow acquisition and development times typical in traditional environments.

— Have highly rapid evolution and deployment cycles[36].

4.3 Technological gaps

Despite progress, important technological gaps remain, especially in three critical areas:

1. Cyber threat intelligence.
2. Situational awareness.
3. Command and control of defensive operations.

4.3.1 Situational Awareness (CySA)

One of the main challenges is to have a clear, complete, accurate and real-time view of what is happening in cyberspace. Without this Situational Awareness, it is difficult to:

— Manage risks in cyberspace.

[35] A kill-switch is a mechanism designed to automatically shut down a system, process or device in case of emergency or when a threat is detected. A kill-switch can remotely shut down an app or device if it is stolen or compromised or at will. For example, certain smartphones allow you to erase all data if they are lost.

[36] In other words, highly agile tool lifecycles and specific cyber defence software.

— Prioritise assets to be defended and actions to be taken.

— Understand the context of a cyber-attack.

— Assess their potential impact and operational effects.

— Make informed decisions under pressure.

This involves monitoring huge volumes of real-time data from multiple sources and transforming it into useful information. To achieve this, we need:

— To integrate data from various systems and sources.

— A single, flexible and scalable repository (data lake).

— Advanced tools for processing and analysing in near real time.

— Interfaces that display information customised[37] to the needs of each combatant in cyberspace at each role and level of command.

4.3.2 Cyber threat modelling

Contrary to generic threats, today's environment requires specialised and targeted intelligence. Threat modelling has become a central element in modern cyber threat intelligence systems and is essential for advanced cyber defence strategy and tactics.

Cyber threat modelling consists of:

— Collecting, storing, analysing and representing all available information on each threat actor.

— Building structured profiles (attributes and parameters) including: tactics, tools, frequent targets, infrastructure, geopolitical relationships, technical capabilities, etc.

— Establishing a kind of "digital mugshot" of each actor, with their fingerprints, *modus operandi* (TTP), relationships, patterns and behaviours.

— Looking for connections and patterns among cyber threat data.

— Graphically represent threat modelling in a way that may be understood by cyber threat intelligence analysts.

Cyber threat modelling applies to:

— Planning: predicting and anticipating the behaviour of cyber threat actors to reduce risks and define contingency plans.

[37] By filtering and selecting the most appropriate display format at any given time and for any given purpose.

— Conducting operations (incident management):
  - o Comparing[38] the characteristics[39] (modelling) of the incident with those of the actor.
  - o Establishing likely attributions.
  - o Leading the investigation.
  - o Proposing adapted tactics and countermeasures.

Threat modelling will enable us to:

— Make technical and tactical attributions regarding the possible authorship of incidents, assigning probabilities based on matches between incident patterns and known behaviours of different cyber threat actors.

— Direct the incident investigation with cyber threat intelligence, defining lines of investigation based on the modes of operation (*modus operandi*) of possible attributions (potential perpetrators) identified in the previous step.

— Anticipate the attacker's next moves, based on profile and historical behaviour.

— Define the most appropriate tactics and techniques to respond to the incident, including detection, containment, mitigation, reaction and recovery actions, with the objective of regaining control of the system and expelling the adversary.

The technical difficulty lies in developing systems that can combine large volumes of data with Artificial Intelligence (AI) techniques (such as Machine Learning [ML] or Deep Learning [DL]) to identify useful patterns and relationships to guide cyber defence (Intel Driven Defensive Cyber Operations).

In the field of cyberspace operations[40], a technologically advanced way is to represent attackers through vector modelling. This technique uses vector databases in which each threat actor is represented as a point in a multidimensional space[41]. Each dimension corresponds to a characteristic

[38] This comparison is done mathematically (automated), by comparing the vectors (in a vector database) representing each incident and actor, where, for example, each actor is represented by a multidimensional vector and where each dimension of this vector space is one of their parameters or attributes.

[39] As an analogy, it is similar to comparing the police investigation file (modelling) of an incident or robbery (with its evidence and clues) with police files (modelling) of the criminals.

[40] Especially in terms of incident management and intelligence analysis.

[41] With multiple dimensions, each representing a parameter or characteristic of the object to be modelled.

or behaviour of the attacker and the aggregate of these data forms a vector describing the attacker.

This approach is not only useful for modelling malicious actors, but can also be applied to other cyberspace elements, such as security incidents or cyber-attacks.

If we represent a cyber-attack as a vector in the same multidimensional space, it can be compared with the vectors of different threat actors.

A comparison between the attack vector and that of the potential perpetrator (threat actor) allows a "difference vector" to be obtained. This "difference vector" reveals the characteristics of the attacker that have not yet been manifested in the potential ongoing cyber-attack, which offers two key advantages:

— Investigation guide: it provides guidance on what evidence, behaviours or details should be sought when analysing the cyber-attack.

— Predict future actions: helps to anticipate the attacker's next moves, based on what they would normally do but have not yet done.

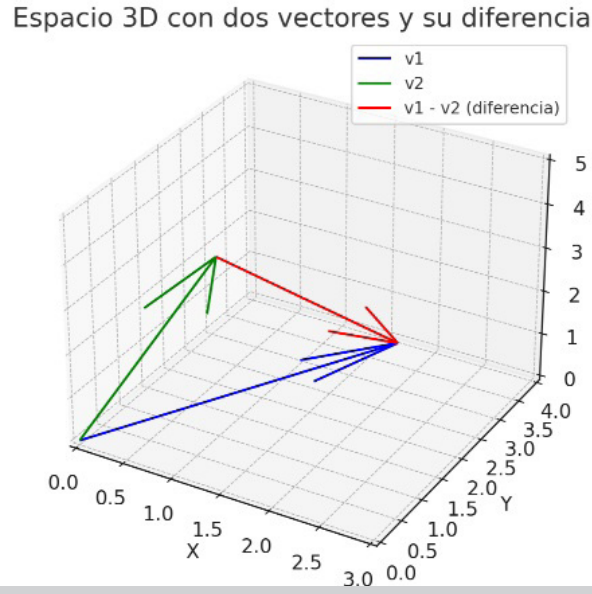


Figure 1. Modeled in three dimensions. Vector representation of two vectorally modeled objects in a three-dimensional cube (with only three parameters) and the vector representation difference from the comparison of the two models. The projections of that vector difference in the axes of that cube will show us the parameters in which both models do not match, and the value of that difference. In a real model, the cube would not be three-dimensional, but n-dimensional. [Image taken from Chagpt]

Additionally, a probabilistic attribution analysis may be performed by comparing the vector of an attack with the vectors of multiple known actors. The closer a vector is to another vector (the smaller the distance between them), the higher the probability that the corresponding actor is responsible for the attack.

Such techniques offer enormous potential not only in cyber defence, but also in other areas where it is necessary to analyse and anticipate complex behaviour.

5 Technology initiatives promoted by the Joint Cyberspace Command (MCCE)

The constant increase of threats in cyberspace has made it necessary to develop specific technological solutions for military cyber defence. However, commercial supply in this area is still scarce, due to the recent nature of the military approach in this domain.

The Spanish Joint Cyberspace Command (MCCE) has therefore promoted a series of projects that seek to fill these technological gaps through technologically and conceptually advanced tools designed to:

— Integrate Cyber Threat Intelligence.

— Provide Command and Control capabilities.

— Improve Situational Awareness.

— Ensure operational Defensive Response.

The main initiatives are presented below.

5.1 PICO Platform

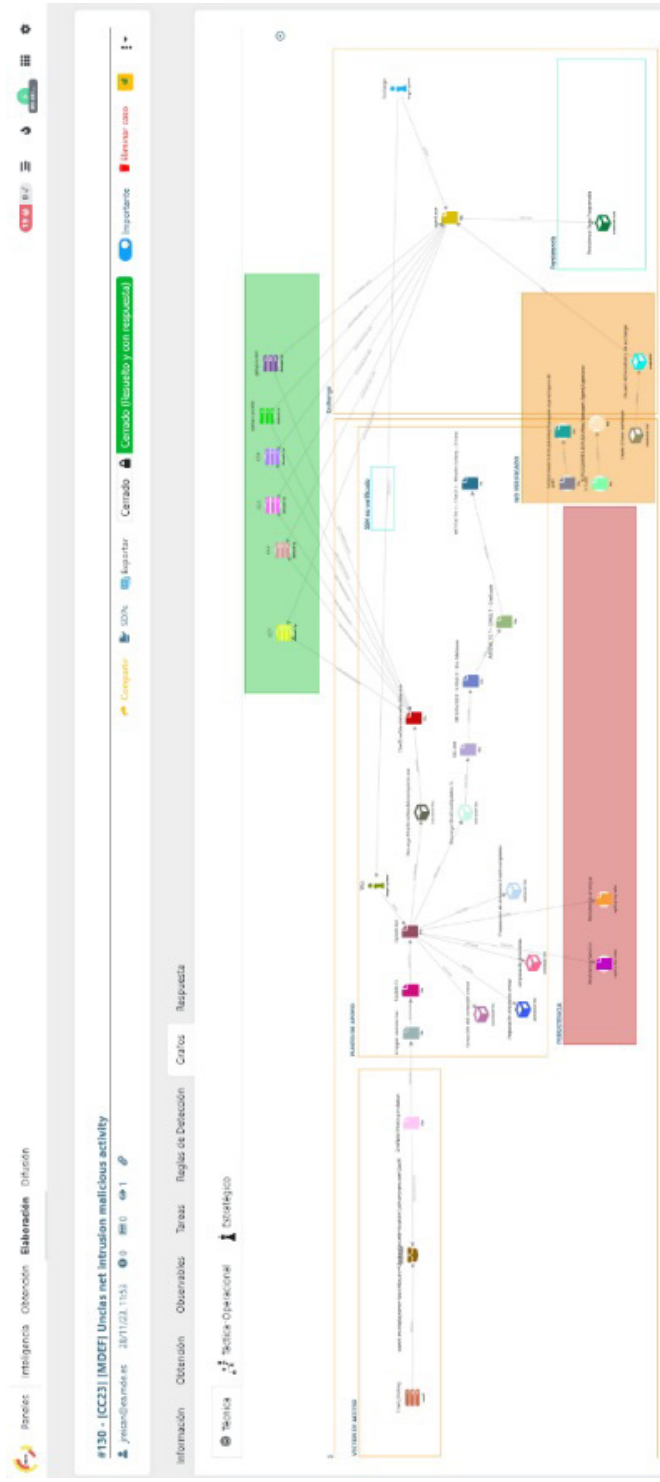
The PICO (Platform for Intelligence to Conduct Cyberspace Operations) platform represents one of the first steps in the acquisition and evolution of specific military cyber defence capabilities within the MCCE.

It is based on CIAT, previously developed[42] by the company Telefónica Soluciones de Criptografía (TELCRYP, Telefónica Group) and has been adapted for military purposes by this company to meet the operational requirements defined and required by the MCCE.

5.1.1 What does PICO offer?

PICO combines two capabilities in one solution:

[42] CIAT stands for: "Global Advanced Cyber Intelligence Platform of Telefónica."


Paneles
Inteligencia
Obtención
Elaboración
Difusión
#130 - [CC23] [MDEF] Uncias net intrusion malicious activity
Cerrado (Resuelto y con respuesta)
Importante
Información
Obtención
Observables
Tareas
Reglas de Detección
Grafos
Respuesta
Táctica
Táctica Operacional
Objetivo/s


#130 - [CC23] [MDEF] Uncias net intrusion malicious activity
Información
Obtención
Observables
Tareas
Reglas de Detección
Gráfos
Respuesta
Cerrado (Resuelto y con respuesta)
Importante
Eliminar caso
Cerrado
Exportar
SDOs
Compartir
Táctica - Operacional
Estratégico
Attack pattern
Campaign
X-mitre-tactic
Tool
Course of action
Uses
Mitigates
TÁCTICAS
TÉCNICAS
SUBTÉCNICAS
HERRAMIENTAS
MITIGACIONES
Campaña

1. Cyber threat intelligence management.
2. Cybersecurity incident management.

This integration allows:

— Modelling of incidents and threat actors.

— Correlation of evidence between the two models (incidents and threats).

— Management of targeted cyber-attacks with cyber threat intelligence.

— Prioritisation, automation and control of tasks in response to cyber-attacks or security incidents.

Additionally, PICO uses the MITRE ATT&CK matrix framework[43] to model (map) the tactics, techniques and procedures employed by attackers, allowing for more accurate attribution and proactive defence planning.

The PICO platform is designed to facilitate comprehensive, coordinated and efficient management of defensive and intelligence operations at the technical (and initially at the tactical) level in the cyberspace domain. These are its main capabilities:

— Unification of tools: enables operations from a single platform, eliminating, to a large extent, the need to use multiple systems at the same time. This provides a centralised dashboard that simplifies management and improves efficiency.

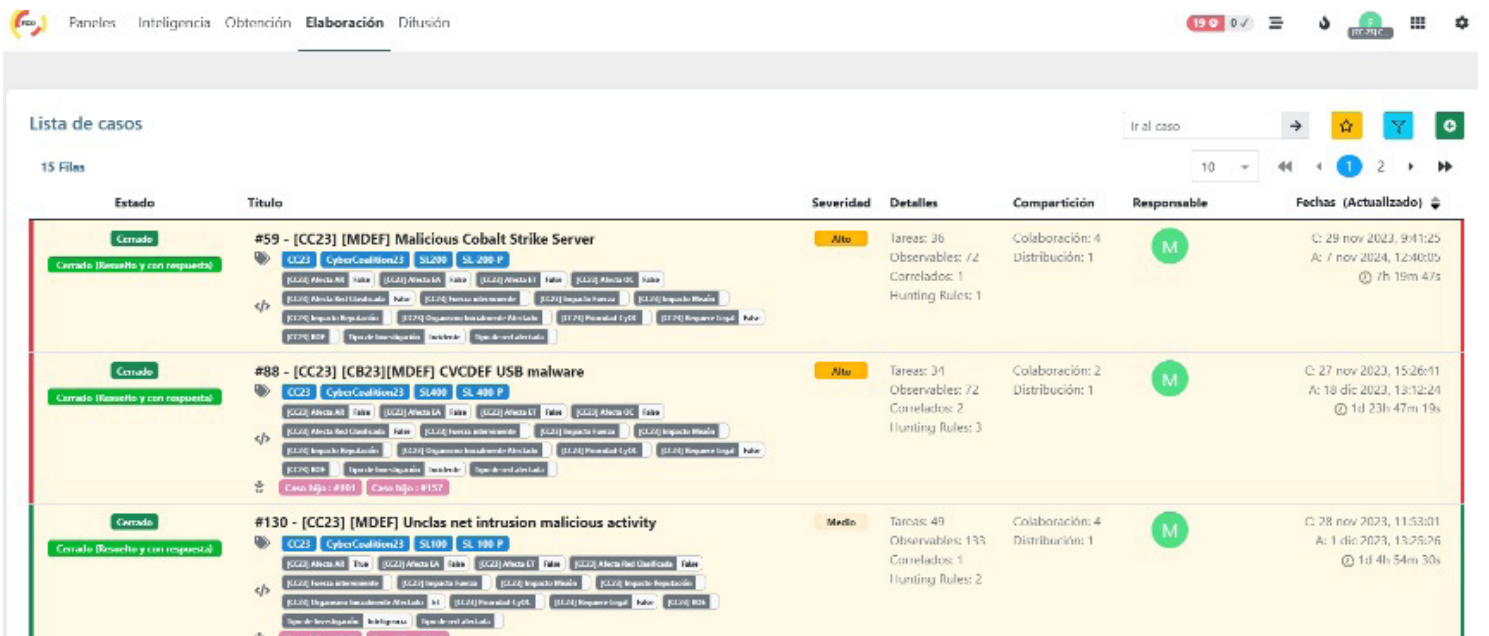
— Centralised management of cyber threat intelligence information: brings together all available data from both one's own environment and potential threats in a single repository[44], facilitating information correlation and improving Situational Awareness to support more effective decision making.

— Automation: streamlines repetitive tasks related to incident management and intelligence analysis and allows operators to focus on tasks of higher strategic value. It also allows the definition of task workflows, with task assignment and control.

— End-to-end surveillance and monitoring: integrates various detection tools within a single platform, enabling continuous surveillance of cyberspace, as well as unified technical/tactical visualisation. All

[43] As an analogy, the Mitre Att&ck matrices are to cyber defence what the periodic table of elements is to chemistry. In other words, Mitre Att&ck matrices are a kind of structured periodic table of all existing or at least identified tactics, techniques and procedures.

[44] It is a relational database. It does not yet include a data lake and therefore does not have the advantages of this type of technology.


Paneles
Inteligencia
Obtención
Elaboración
Difusión
Lista de casos
Ir al caso
15 Files
Estado
Título
Severidad
Detalles
Compartición
Responsable
Fechas (Actualizado)
Cerrado
Cerrado (Resuelto y con respuesta)
#59 - [CC23] [MDEF] Malicious Cobalt Strike Server
Alto
Tareas: 36
Observables: 72
Correlados: 1
Hunting Rules: 1
Colaboración: 4
Distribución: 1
C: 29 nov 2023, 9:41:25
A: / nov 2024, 12:40:05
7h 19m 47s
#88 - [CC23] [CB23][MDEF] CVCDEF USB malware
Alto
Tareas: 31
Observables: 72
Correlados: 2
Hunting Rules: 3
Colaboración: 2
Distribución: 1
C: 27 nov 2023, 15:26:11
A: 18 dic 2023, 13:12:24
1d 23h 47m 19s
#130 - [CC23] [MDEF] Unclas net intrusion malicious activity
Medio
Tareas: 49
Observables: 133
Correlados: 1
Hunting Rules: 2
Colaboración: 4
Distribución: 1
C: 28 nov 2023, 11:53:01
A: 1 dic 2023, 13:25:26
1d 4h 54m 30s

alerts are displayed in a single interface, prioritised according to the threat level identified by cyber threat intelligence and the mission.

— Synchronisation between intelligence and operations: ensures that incident management is intel-driven, enabling a more effective response to cyber-attacks and anticipating potential moves by adversaries.

— Data correlation: the platform automatically analyses large volumes of data to detect patterns and links between incidents, helping to identify connections between seemingly isolated attacks.

— Effective incident management and response: allows incidents to be recorded, classified and prioritised according to their potential impact, resources to be allocated efficiently, and responses to be coordinated quickly, in the style of SOAR systems[45].

— Decision support: generates processed and relevant information so that cyber defence teams can act quickly and accurately, even under pressure.

— Risk reduction: helps to mitigate the effects of incidents and prevent future threats, so that defensive tasks are allocated and coordinated in a structured and effective manner.

Taking this initial version of PICO as a starting point, the MCCE plans to actively support the evolution of this product into a tactical/technical module of the Intelligence System and the Command and Control System within the future SCOMCE[46].

5.2 ECySAP / ECySAP EYE

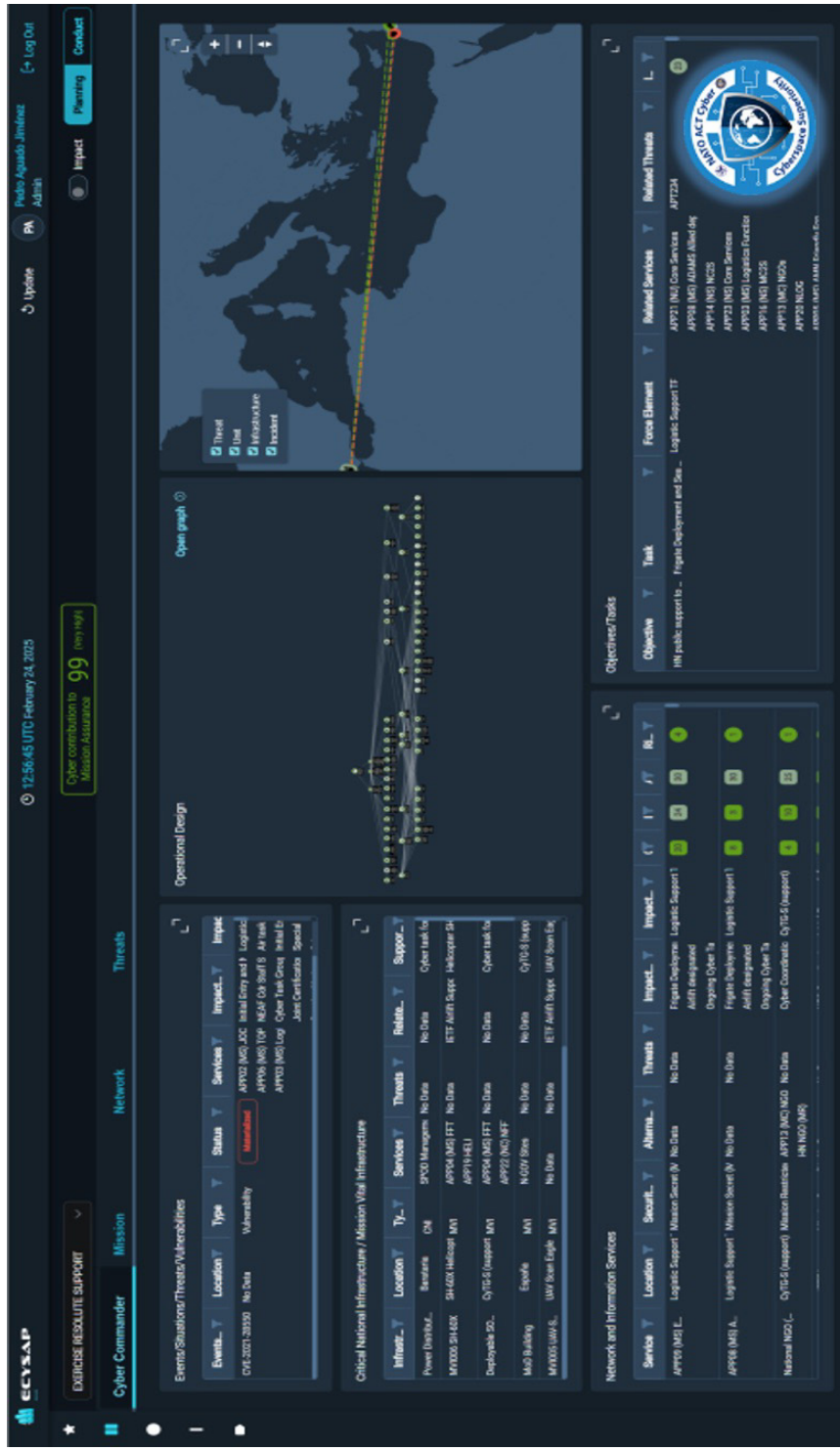
The ECySAP project (European Cyber Situational Awareness Platform) was born from an initiative promoted and subsidised by the EU, with the aim of developing a Situational Awareness (in its version 1.0) and Command and Control platform for cyber defence operations (in its version 2.0).

5.2.1 ECySAP[47] v1.0

It is a tool that focuses on providing Cyber Situational Awareness (CySA).



[45] SOAR stands for "Security Orchestration, Automation and Response." It is a security incident management device with automated response and workflow capabilities.
[46] SCOMCE stands for: "Cyberspace Combat System."
[47] ECySAP stands for: "European Cyber Situational Awareness Project."


ECYSAP
12:56:45 UTC February 24, 2025
Update
Pedro Aguado Jiménez
Adrian
Log Out
EXERCISE RESOLUTE SUPPORT
Cyber contribution to Mission Assurance
99
Impact
Planning
Conduct
Cyber Commander
Mission
Network
Threats
Events/Situations/Threats/Vulnerabilities
Operational Design
Open graph
Threat
Unit
Infrastructure
Incident
Critical National Infrastructure / Mission Vital Infrastructure
Objectives/Tasks
Objective
Task
Force Element
Related Services
Related Threats
Network and Information Services
Service
Location
Security
Alarms
Threats
Impact
NATO ACT Cyber
Cyberspace Operations



- Developed with EU funds.
- Coordinated by INDRA, with the participation of Spain, Italy, France and Estonia.
- The Spanish MCCE (Joint Cyberspace Command) has supported this project from the technical and operational point of view, by delegation of the Spanish Directorate-General for Armaments and Equipment (DGAM) since its inception.
- NATO has expressed an interest in this tool and it was exhibited at this year's EU Annual Conference of Cybercommanders. The Spanish Armed Forces are counting on having a version of ECySAP adapted to the needs of our Armed Forces as an operational and functioning product before the end of the year (2025) in the facilities of the MCCE.

ECySAP has four levels of visualisation, corresponding to the levels of warfare: technical, tactical, operational and strategic.

Each level, in turn, provides four specialised views:

- Mission view: focused on meeting the needs of operations and planning staff.
- Threat view: focused on meeting the needs of intelligence staff.
- Cyberspace view: focused on meeting the needs of CIS/CYBER area staff.
- CYBER view: focused on meeting the needs of the CYBER commander or operations commander.

5.2.2 ECySAP v2.0 (ECySAP EYE)

It is the evolved version of the ECySAP v 1.0 system, and its objective is to become an Integrated Command and Control System for cyberspace operations, incorporating:

- Situational Awareness (CySA).
- Planning and conducting of operations and missions in cyberspace (guided by cyber threat intelligence).
- Wargaming and simulation[48].
- Collaborative workflow.
- Targeting.

[48] Based on "modelling" the different cyber threat actors. These modellings will be used to simulate attacks by cyber threat actors in wargaming modules at the technical level (LIVE simulations) and tactical level (TTX simulations).

This project, also funded by the EU, will be developed by a consortium of eight European countries[49], again led by INDRA, and is scheduled to be completed by 2028, at technology readiness level TRL 6-7[50].

The MCCE (Joint Cyberspace Command) will also support this project from a technical and operational point of view, by delegation of the DGAM.

5.3 SCOMCE: Cyberspace Combat System

As part of its effort to strengthen its combat capability in cyberspace, the MCCE is developing the Cyberspace Combat System (SCOMCE).

The SCOMCE system is the MCCE's most ambitious project to date[51]. It is envisaged as a "system of systems" integrating full capabilities to operate and fight in cyberspace, with the inclusion of the following systems:

— Command and Control System:
  - It provides the ability to direct and monitor operations in cyberspace in real time.

— Intelligence System:
  - It provides cyber threat intelligence capability at all levels of warfare (technical, tactical, operational and strategic).

— Offensive System:
  - It provides the capability to execute active operations in adversary cyberspace and allows for deterrence, neutralisation, etc.

— Defensive System:
  - It provides cyber defence capabilities for our cyberspace through advanced cyber-attack detection, containment, mitigation and recovery measures.

— Cross-Cutting System:
  - It provides cross-cutting capabilities to all the above systems: shared services and support to the other systems.

The inclusion of a dedicated Intelligence System within SCOMCE demonstrates the growing importance of cyber threat intelligence as the backbone of any defensive or offensive operation in cyberspace, as is the case in other areas of military operations.

[49] France, Austria, Italy, Estonia, Poland, Romania, Greece and Spain.
[50] TRL stands for: "Technology Readiness Levels." TRL 6 - Technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies); TRL 7 - System prototype demonstration in operational environment.
[51] As a matter of fact, it is a programme intended to consist of nearly twenty projects.

This system is being designed to serve all levels of command and warfare, from the technical to the strategic level.

6 Advanced technological requirements for SCOMCE

The Cyberspace Combat System requires the integration of the most advanced technologies available in order to meet the operational and strategic challenges of the cyberspace domain or operating environment.

It must be able to:

— Centralise all relevant information in cyberspace.

— Correlate, link and analyse all available information and data in a structured and predictive manner.

— Support real-time decision making.

There are four technologies that are, above all, critical to achieving the capabilities required by the SCOMCE Intelligence System.

6.1 Data lake technology

Data lakes represent a technological evolution over traditional databases, whether relational or non-relational, and provide significantly greater value.

A data lake[52] is a single repository[53] that allows the inputting, storing and pre-processing of large volumes of data from multiple sources and formats, either structured or unstructured.

Its main advantages include the following:

— Flexible and versatile storage: they can handle data in multiple formats and at different levels of structure and can hold:

  • Structured data (such as those stored in relational databases).

  • Semi-structured data (e.g. JSON or XML files).

[52] A data lake is a centralised repository that allows data to be stored in its native format, with no restrictions on structure or size. In the case of SCOMCE, this data lake will integrate (unlike traditional databases) all kinds of information and raw data and will include a layer of specific data processing software to curate (merge, remove duplicates, integrate, cleanse, enrich, link) the data and information according to the analytical requirements of the SCOMCE software module consuming data from the data lake.

[53] It acts as the "single repository of truth", storing all information and data (objects, with their parameters/attributes and semantic relationships) pertaining to operations in cyberspace. The existence of information silos stored in different systems, tools and technical solutions makes it difficult to have a single, clear view of the situation in cyberspace and data correlation: the discovery of relationships, patterns and trends.

- Unstructured data (texts, images, screenshots).
- Loosely structured data (such as sensor data or intercepted communications).

It also allows the same information to be stored coherently in different formats simultaneously (relational, graphic, vector, etc.), which facilitates consultation by Intelligence, Command and Control Systems, or other systems that require different types of analysis.

— Integration of multiple sources: it unifies information that would normally be scattered in separate systems or "data silos." This centralisation favours data correlation from different sources and tools, which helps to identify complex patterns or relationships that would go unnoticed in fragmented systems.

— Intelligent pre-processing: before storing data, data lakes can perform tasks such as removing duplicates, inconsistency correction and standardisation, which improves the quality and consistency of the available information.

— Scalability: they can easily adapt to the growth of data volume without the need to redesign the structure and allow the storage of large historical data, which is key for retrospective analysis or anticipating future trends.

— Centralised access: by concentrating all information on a single platform, it simplifies management and access by cyber defence teams and improves operational efficiency and decision-making.

This data lake will become the repository from which the different SCOMCE systems will consume the data and information and in which they store generated products.

6.1.1 Sources of information and data to be integrated

The data lake must gather detailed and comprehensive information covering three key areas for defence in cyberspace:

— The mission: it should include missions, plans, orders and operational reports from all levels of command and levels of war. This makes it possible to analyse how operations depend on certain capabilities or services in cyberspace and thus identify the risks associated with possible attacks that could affect their performance.

— The threat (organised by levels):
  - Strategic: data on potential actors, their alliances, doctrines, capabilities, funding sources, training methods and cyber weapons development.

- Operational: information on possible intentions, usual targets, the effects they seek to generate, and the members of these groups or entities.
- Tactical: set of employed tactics, techniques and procedures (TTPs), used entry vectors and infrastructures, and available technologies, tools, malware and cyber weapons.
- Technical: more specific details on the used tools and malware, exploited vulnerabilities and the indicators of compromise (IOCs) that may be used to detect their activities.

— Own cyberspace information: it should reflect the status of assets and services, as well as include vulnerabilities, data flows between them, incorrect or missing security configurations, links between components, and the location/configuration of cyber security and cyber defence mechanisms.

The complete integration of this data allows the development of a single, shared view of the cyberspace operations domain (RCyP[54]).

6.1.2 Structure of the data lake

A data lake with these characteristics is normally structured according to the following areas or zones:

— Bronze area: stores raw data as it arrives.

— Silver area: organises data according to a specific ontology of cyberspace (links between assets, threats, missions, etc.).

— Gold area: stores pre-processed data ready to be used by analysis and Artificial Intelligence systems.

6.1.3 Challenges in implementing a data lake

The real challenge in implementing a data lake is not so much technological —integrating different data sources today is not a great technical challenge—, but rather cultural and organisational.

For such a system to be truly effective, it is essential that data from multiple domains be integrated:

— Systems that manage operational cyberspace, controlled by IT and OT service providers.

— Command and Control systems (including planning) at all levels of war and command.

[54] RCyP stands for: “Recognized Cyber Picture.

— Military cyber threat intelligence systems which ideally include information shared by civilian agencies, private bodies and public administrations.

However, this integration is often hampered by a lack of understanding of the strategic value of cyber defence and the importance of centralising all information on a single platform that supports both intelligence and decision making in cyberspace operations.

6.2 Ontology

Unlike other types of repositories, a data lake requires the development of specific data modelling, as it not only defines the key elements (objects or concepts) of the domain, but also their attributes, relationships and rules that describe how they interact with each other. This specific data modelling is called "ontology."

An ontology is a formal, structured representation[55] of knowledge within a specific domain, which allows knowledge to be modelled in a way that can be understood by humans and processed by machines, making it especially useful in areas such as Artificial Intelligence for making inferences, knowledge management, expert systems or interoperability between systems. (Gruber, 1993).

While there is no specific ontology of cyberspace operations as there is in other areas of military operations, there are some elements from which to start:

— With regard to cyberspace:

- The SISO standard[56] CyBERDEM[57] data model aims to facilitate the exchange of cyberspace information between different systems, in particular in the context of simulation, training, analysis and military or cyber-defence operations (Simulation Interoperability Standards Organisation). 2014).
- The OASIS TOSCA open standard[58] developed by the OASIS consortium[59] that enables the definition, deployment and management of applications and services in cloud computing environments in a portable, automated and interoperable way (Kirvan and Bigelow, 2023).

[55] It structurally defines key elements (objects), their characteristics (attributes) and the relationships between them.
[56] SISO stands for: "Simulation Interoperability Standards Organisation.
[57] CyBERDEM stands for: "Cyber Data Exchange Model."
[58] OASIS TOSCA stands for: "Topology and Orchestration Specification for Cloud Applications."
[59] OASIS stands for: "Organisation for the Advancement of Structured Information Standards.

— Regarding the mission:

- The C2SIM ontology[60] is a formalised conceptual structure to facilitate interoperability between command and control (C2) and simulation systems, especially in military or defence contexts. The C2SIM ontology is a formal model that defines the concepts, relationships and structures required for C2 and SIM systems to exchange information accurately and unambiguously. It is based on open standards and is promoted by bodies such as NATO, SISO (NATO Science and Technology Organization, 2024).

— Regarding the threat:

- MISP (Multinational Intelligence Sharing Platform) has a small ontology that can serve as a starting point for structuring cyber threat information. However, this ontology needs to be extended and enriched, both in terms of attributes and objects, to adequately cover the needs of cyber threat intelligence modelling at all levels of warfare, from technical to strategic.
- "MITRE ATT&CK Matrices" which represent the tactics, techniques and procedures (TTP) used by threat actors.
- The "Diamond Model" of security incident and cyber-attack analysis.

6.3 Application of Artificial Intelligence (AI)

AI (DL[61] and ML[62]) will play a key role in data and information analysis processes. Through system design and specialised AI modules, the SCOMCE will provide advanced intelligent data processing capability, integrating analysis, correlation and automation capabilities to facilitate (Kirkpatrick, 2024):

— Task automation[63]: the system will also incorporate Artificial Intelligence functionalities aimed at automating repetitive or high-volume tasks, such as:

[60] C2SIM stands for: "Command and Control - Simulation Interoperation Ontology."
[61] DL stands for: "Deep Learning", Artificial Intelligence based on neural networks.
[62] ML stands for "Machine learning." Artificial Intelligence primarily based on statistical regression analysis.
[63] This automation of repetitive and routine activities can be carried out by AI agents, thus reducing the number of personnel required for such routine activities, and will be essential to reduce the size of HQs and, therefore, their tactical footprint, which is essential in environments where the capabilities of satellite-based adversary detection, etc. are very powerful.

- Automatic search and extraction of information or data from a repository of unstructured documents, as well as highlighting the document and paragraph where the results of the search are found.
- Generating draft reports, intelligence and analysis products and summaries, speeding up documentation tasks.
- Transcription and analysis of meetings, including the identification and extraction of key ideas and relevant elements.
- Intelligent prioritisation of emails and tasks, helping to focus efforts on what is most urgent and relevant. Automatically reply to routine emails.
- Organising and coordinating tasks and meetings.
- Automating workflows.
- Grammar review, translations, style improvements, etc.

— Advanced analytical capabilities:

- Correlating complex information across multiple data types and objects and detecting hidden connections between incidents, behaviours and entities.
- Detecting patterns in both systems' behaviour and the behaviour of potential threat actors.
- Detecting anomalies, identifying unusual behaviour from the usual system model.
- Modelling actors and behaviours, representing threat groups in the form of vectors representing the behaviour of specific threat groups.
- Establishing technical and tactical attribution and comparing the profile of an incident with that of known actors to estimate the likelihood of perpetration.
- Analysing historical vulnerabilities, which generates heat maps to show those that have been most exploited by different types of threats.
- Reconstructing accurate timelines of events, to facilitate the understanding of how incidents unfolded.
- Relating current data with historical records, such as logs or previous reports in order to identify similarities or relevant connections.
- Detecting trends and developments and comparing past and current behaviour, as well as anticipating the adversary's future moves.

- Aiding cyber-attack investigation, through direct data queries using AI, with questions such as: what was happening at the same time as that event?, what vulnerabilities existed in an asset at the same time as that event?
- Classifying and grouping (incidents, logs, related alerts), allowing them to be investigated jointly and efficiently.
- Reducing false positives, which refines the rules of detection and reduces the manual workload of analysts.

— Predictive analytics:

- Using predictive analytics techniques, the system will be able to anticipate future actions of the adversary and assess potential risks.

— Advanced sensors: Artificial Intelligence-based sensors will detect, not by static signatures or rules predefined by operators, but by common patterns:

- In known *malware*: known malware patterns (malware modelling) are compared. This will make it possible to identify new malware variants, even if the code has been partially modified. Instead of using fixed signatures, common patterns are identified.
- In actor behaviour: AI actor modelling will make it possible to detect behaviours in systems that resemble those modelled by an actor. This will allow malicious activity to be detected by sensors configured with rules set by threat modelling directly, without human intervention.

Together, these capabilities will enable SCOMCE to improve operational efficiency, reduce response times, and increase the accuracy of analysis and defence in cyberspace. The combination of automation, Artificial Intelligence and advanced data analysis makes this tool an essential pillar of modern cyber defence.

6.4 Application of simulation techniques

Once the threat actors, their behaviours and the cyberspace environment have been modelled, these models can be used to run tactical and operational simulations, allowing:

— Automated wargames.

— Evaluation of the COA[64] of defence and reaction to a simulated attack.

[64] COA stands for "Course of Action."

— Conduction of operational analyses, by means of an exhaustive automated cooperation or confrontation between one's own COAs and those of a potential adversary at a tactical and technical level, by defining parameters that differentiate the various COAs to be defined on one side or the other.

6.4.1 Simulation as a strategic tool

Simulation is a key capability in the field of cyber defence, as it enables:

— Recreation of attacks on real or virtual infrastructures.

— Verification of the effectiveness of implemented defences.

— Assessment of how a system responds to different types of threats.

Nowadays, there are advanced tools that simulate the behaviour of real attackers, known as "Breach and Attack Simulations" (*Ciberseguridad. blog*, n.d.).

These solutions replicate the methods and tactics used by malicious actors, allowing defence systems to be tested in a controlled environment. However, most of these tools are developed by US or Israeli companies and operate from the cloud. Using these services would imply sharing sensitive information on our vulnerabilities with foreign entities, which poses a risk to national security.

For this reason, it is essential that national companies develop their own simulation solutions. The architecture of these tools should be modular and allow for the creation of specific agents that simulate techniques and tactics employed by different attackers. This facilitates a more accurate and flexible simulation, as instead of mimicking a complete attacker, specific sequences of actions (workflows) that follow the same usage pattern as a real attacker can be reproduced.

There are two main types of simulations:

— Live simulation: it technically reproduces the process of an attack and uses malicious tools and software (modified or simulated to do no harm). Although it interacts with the real system and may generate some resistance from service providers, these simulations do not usually have real negative consequences.

— TTX (Tabletop Exercise) simulation: this is a theoretical exercise that analyses a possible attack, comparing configurations, vulnerabilities and tools, without interacting directly with the real system. It is a safer and less invasive way of assessing threat preparedness.

7 Conclusions

The cyberspace domain is no longer a purely technical domain but a strategic theatre of military operations. This transformation requires an evolution from traditional cybersecurity —focused on the technical protection of systems— to a comprehensive cyber defence based on analysing vulnerabilities within the environment, driven by cyber threat intelligence and focused on achieving the military mission/operation.

However, this evolution is not technical, it is doctrinal: from protecting systems to anticipating attacks, from reacting to pre-empting the adversary. That is the essence of true cyber defence.

The role of cyber threat intelligence has been key in this transition, anticipating the adversary, understanding their behaviour, and developing proactive and targeted defences. It is not just about protection, but about ensuring freedom of action in cyberspace and guaranteeing the continuity of military operations in the face of increasingly sophisticated hostile actors.

The process of "operationalising cyberspace", led by the MCCE, is an innovative and necessary response to today's challenges. It is not enough to defend systems, one must defend the mission, identify the adversary and prepare the digital environment in order to resist, respond and recover from any attack.

True defence begins with protecting what gives meaning to systems: the mission. Shielding the infrastructure without considering its operational impact is like fortifying a castle without safeguarding the king.

The progress of cyber defence and especially cyber threat intelligence is directly dependent on intelligently adopting new technologies not only to protect systems or develop intelligence, but to transform how cyberspace is operated and fought over.

The implementation of platforms such as PICO and the development of more ambitious systems such as SCOMCE —supported by data lakes, Artificial Intelligence and simulation technologies— will mark a turning point. These tools enable the automation of processes, modelling threats, attributing incidents, optimising resources and running defensive operations on an analytical and predictive basis.

Finally, it is essential to consolidate a national cyber defence industry that can provide the necessary technologies with full sovereignty, so as to avoid having to depend on third parties and to boost the structural capabilities of the state in order to operate effectively in this decisive 21st century domain.

In the 21st century, wars are no longer fought only on land, at sea or in the air. They infiltrate networks, are executed in code and are won or lost

on servers. Cyberspace is not just a stage: it is the most dynamic and least visible front in any modern conflict.

Disclaimer

The opinions or ideas expressed in this article are the sole responsibility of the author and do not necessarily reflect those of the European Union, NATO, the Spanish Armed Forces, Telefónica Soluciones de Criptografía (TELCRYP, Telefónica Group) or INDRA, and therefore cannot be held responsible for them.

Acknowledgement

The images referring to the PICO tool in this article have been provided and are reproduced with the permission of the company Telefónica Soluciones de Criptografía (TELCRYP, Telefónica Group).

The images referring to the ECYSAP project have been provided and are reproduced with the permission of both INDRA and NATO ACT CyBER.

Bibliography

Arteaga, F. and Alonso Lecuit, J. (2023). *El concepto de Ciberdefensa Activa* [online]. Real Instituto Elcano. [Accessed: 2025]. Available at: https://www.realinstitutoelcano.org/analisis/el-concepto-de-ciberdefensa-activa/

Ciberseguridad.blog. (n.d.). Conoce la tecnología Breach and Attack Simulation (BAS) y resucita tu estrategia de ciberseguridad [online]. [Accessed: 2025]. Available at: https://ciberseguridad.blog/conoce-la-tecnologia-breach-and-attack-simulation-bas-y-resucita-tu-estrategia-de-ciberseguridad/

Corletti Estrada, A. (2017). Ciberseguridad (Una Estrategia Informático/Militar) [online]. *DarFe*. [Accessed: 2025]. Available at: http://www.darfe.es

Ganuza, N. (2020). *Guía de ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar* [online]. Junta Interamericana de Defensa. [Accessed: 2025]. Available at: https://jid.org/publicaciones/guia-de-ciberdefensa-orientaciones-para-el-diseno-planeamiento-implantacion-y-desarrollo-de-una-ciberdefensa-militar/

Garzón, E. H. (2025). *Evolución del malware: tendencias y cómo combatirlo* [online]. Internet Security Auditors. [Accessed: 2025]. Available at: https://blog.isecauditors.com/evolucion-del-malware-tendencias-y-como-combatirlo

Gruber, T. R. (1993). A translation approach to portable ontology specifications. *Knowledge Acquisition*. *5*(2), pp. 199-220. DOI: https://doi.org/10.1006/knac.1993.1008

Kirkpatrick, R. G. (2024). *The Saint Russ Initiative: AI's Cutting-Edge Tactics for Cyber Safety*. Independently published.

Kirvan, P. and Bigelow, S. J. (2023). *TOSCA (Topology and Orchestration Specification for Cloud Applications)* [online]. TechTarget. [Accessed: 2025]. Available at: https://www.techtarget.com/searchcloudcomputing/definition/TOSCA-Topology-and-Orchestration-Specification-for-Cloud-Applications

Multinational Capability Development Campaign. (2017). *MCDC 2015–2016: MDCO Planning Guide (Version 1.0)*.

NATO. (2016). *Warsaw Summit Communiqué issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016* [online]. [Accessed: 2025]. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htmNATO+7NATO+7European Sources Online+7

NATO Science and Technology Organization. (2024). *Technical description of C2SIM* (STO-EN-MSG-211-2.3) [online]. [Accessed: 2025]. Available at: https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-MSG-211/EN-MSG-211-2.3.pdf

Arteaga, F. and Alonso Lecuit, J. (n.d.). *El concepto de ciberdefensa activa* [online]. Real Instituto Elcano [Accessed: 2025]. Available at: https://www.realinstitutoelcano.org/analisis/el-concepto-de-ciberdefensa-activa/

Rodríguez, D. (2023). Ni mar, ni tierra, ni aire, ni espacio: el grupo especial del Ejército español que custodia el quinto dominio [online]. *HuffPost*. [Accessed: 2025]. Available at: https://www.huffingtonpost.es/tecnologia/ni-mar-tierra-aire-espacio-grupo-especial-ejercito-espanol-custodia-el-quinto-dominio.html

Seguritecnia. (2023). ¿Qué es la ciberdefensa? [online]. [Accessed: 2025]. Available at: https://www.seguritecnia.es/actualidad/que-es-la-ciberdefensa_20230203.html

Simulation Interoperability Standards Organization (SISO). (2024). *SISO-REF-072-2024: Cyber DEM BONES (Base Objects, Networks, Effects, & Specifications)* [online]. [Accessed: 2025]. Available at: https://cdn.ymaws.com/www.sisostandards.org/resource/resmgr/reference_documents_/siso-ref-072-2024.pdf

U.S. Department of the Army. (2009). *FM 2-01.3: Intelligence preparation of the battlefield/battlespace*. Washington, DC: Department of the Army.

Winterfeld, S. P. (2002). *Cyber IPB* [online]. Global Information Assurance Certification (GIAC). [Accessed: 2025]. Available at: https://www.giac.org/paper/gsec/1752/cyber-ipb/103147Wikipedia+2GIAC+2GIAC+2

Cross impact matrices and the structural method: a partial review of tools for future scenario building

Licesio J. Rodríguez-Aragón

"All models are wrong, but some are useful."
G. E. Box (1919-2013)

Abstract

Cross impact matrices and the structural method are tools used to build future scenarios. These techniques allow us to assess how the occurrence of an event may influence the probability of occurrence of other events, facilitating strategic planning under uncertainty. This paper seeks to present some of the tools that are used when working with impact matrices and that allow us to analyse indirect relationships and classify system variables, revealing hidden variables that gain relevance through indirect relationships.

Keywords

Structural method, Cross impact matrices, MICMAC, Impact matrix multiplication.

1 Introduction

Cross impact matrices are a reality modelling technique used to assess how the occurrence of one event may influence the likelihood of other events. This method was first proposed by Theodore Gordon, Olaf Helmer and Hans Goldschmidt in 1966. These authors based the method on the idea that events do not occur in isolation, but are interrelated.

The first application of the cross impact methodology was playful. On the occasion of its twentieth anniversary, Kaiser Aluminum & Chemical Corporation, already adept at stimulating the public imagination with futuristic ideas, distributed a commemorative board game called *Futures*. The main objective of the game was to encourage participants to understand and use to their advantage how different future events might influence each other and how these cross impacts might affect the evolution of future scenarios. This was achieved by assessing the conditional probabilities of one event occurring given that another event had already happened.

The game[1], which is now out of print and can be seen in some museums, consisted of a series of sixty cards, each describing a possible future event. This list of future events arose from an earlier work by Gordon and Helmer-Hirschberg (1964) in which, by means of a Delphi technique, they proposed an experimental exercise to predict future trends over a fifty-year horizon. Some of these events were: the emergence of ultra-light metals, the banning of vehicles in cities, brain-computer connections or military and economic alliances with Russia. Each card contained a brief description of the event and an *initial* probability of occurrence of the event assigned by experts. For each event, a coloured slider was set on the game board, marking the probability determined by the experts, and a horizon of twenty years, 1986, was set as the target for validating the predictions (Figure 1).

During the course of the game, a die, an icosahedron with twenty triangular faces, is thrown to determine whether an event occurs. If any of the three numbers on the top face matches the probability established by the experts, the event has materialised in 1986 and turning the event card over reveals the events that this occurrence influences or "impacts": it increases or decreases their probability of occurrence. For example, if anti-gravity is developed, the likelihood of building exploration bases on other planets would increase, but the use of rockets as a means of transport would become less popular. This influence on other events is briefly explained on each card by a plausible reasoning and, with the help of the board, their probabilities of occurrence could be updated.

[1] See: https://patents.google.com/patent/US3473802.

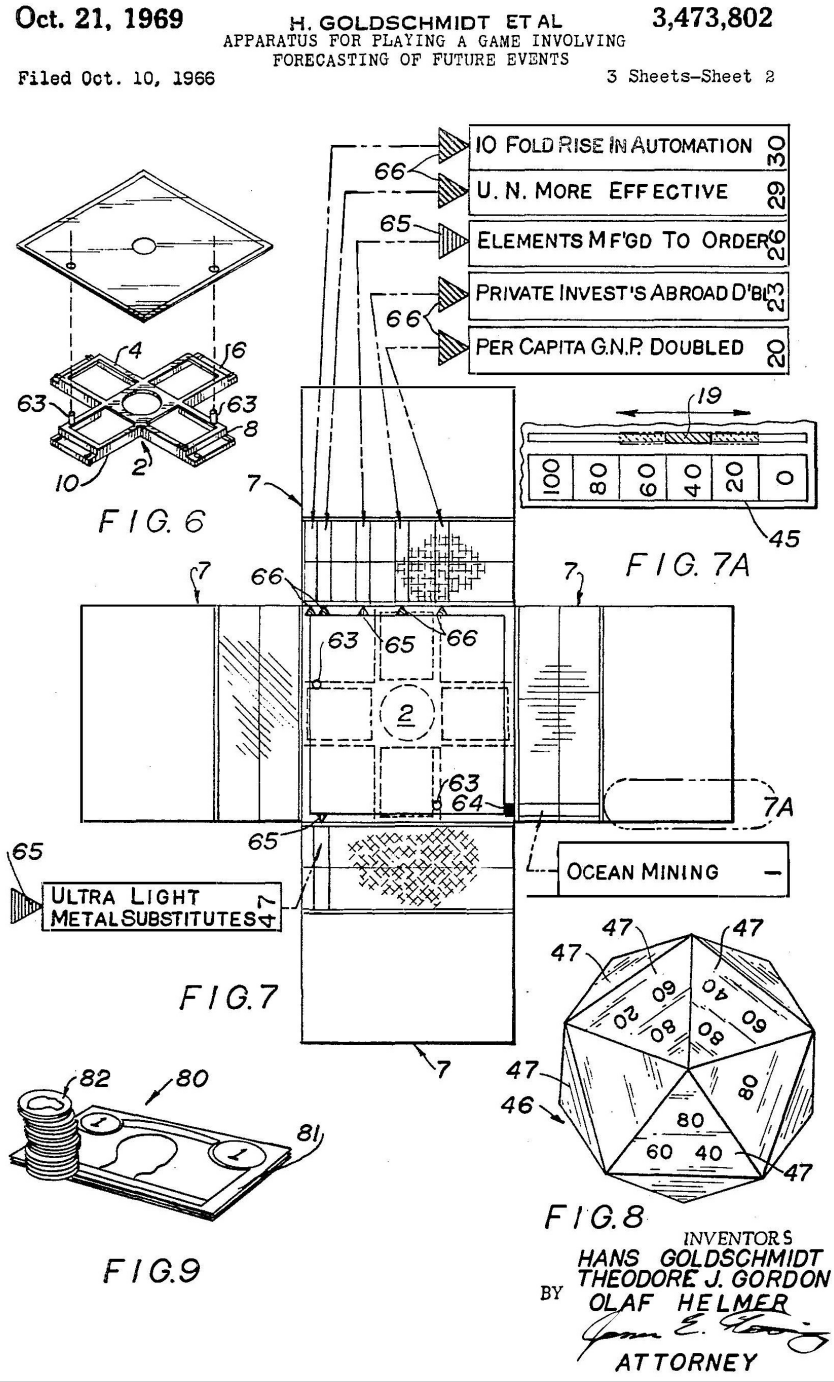


Figure 1: US Patent 3,473,802 of the game Futures - a device for playing a game that involves predicting future events. Source: https://patents.google.com/ patent/ US3473802

The game progresses in this manner, so that the cards remain face up and therefore without the event having occurred, or face down when they have taken place. The occurrence or non-occurrence of events was determined by the probabilities initially set by the experts, the randomness of the die, and the positive or negative impacts of the events that materialise. The game could be enhanced by the use of money, purchasing probabilities, driving or slowing down different innovations or social advances, in the same way as an R&D&I plan would. A winning strategy was to invest in events that would indirectly have an impact on the benefits sought by the player. The winner of the game would then be the one who managed to get the most out of the future.

The methodology described in the game was implemented on a computer by Gordon and Hayward (1968) and allowed to define: *the events*, which were initially randomly ordered, and the cross-impact *probabilities* . Using a simulation strategy, this operation was repeated several times and the scenarios that occurred in each move and would therefore be more likely were analysed quantitatively.

The modelling and futures forecasting strategy to be described here is based on structural analysis and scenario analysis. The first seeks to identify and analyse the relationships between the key factors or variables of a problem, selecting those that have the greatest influence. The second involves developing multiple possible scenarios for the future, based on different combinations of variables and factors. Its origins lie in business as well as military planning since the mid-last century. Structural analysis has its origins in the work of Michel Godet (Godet, 1974; Godet and Duperrin, 1975) and his team at the Institut d'Etudes Politiques in Paris, while scenario analysis stems from the proposal of Herman Kahn and the RAND Corporation (Kahn and Wiener, 1967). Both strategies complement each other by providing a detailed understanding of the key variables and their interactions, allowing for the development of more robust and useful scenarios for strategic decision-making.

2 Modelling and prospective simulation

One of the main challenges facing organisations and governments is decision making under uncertainty. Situations in which there is a large number of influencing factors, thus leading to great variability. In the field of foresight and strategy, where decision-making focuses on the study and analysis of possible futures in order to anticipate and prepare appropriate strategies, the use of models and simulations is essential.

One may recall the seven key ideas in the field of foresight put forward by Godet (1986):

— Clarify present actions in light of the future.

— Explore multiple and uncertain futures.

— Adopt a holistic and systemic approach.

— Take into account qualitative factors and actors' strategies.

— It must always be remembered that information and forecasts are not neutral.

— Opt for multiple and complementary approaches.

— Challenge preconceptions about forecasts and forecasters.

When faced with a novel problem or situation, it is essential to identify its main characteristics and to understand how they relate to each other and to the surrounding phenomena. This approach allows complex phenomena to be broken down into simpler parts, which facilitates analysis and decision-making. By understanding these interactions, models that capture the most relevant aspects of the system can be developed, thus allowing us to come closer to understanding the phenomenon, predict its behaviour and optimise our strategies to address the problem effectively.

Reality is always surprising and there are few occasions when we are able to anticipate it. Recognising the difficulty of real problems is essential in order to approach them with humility and a critical spirit, a fundamental characteristic when working towards solving the challenges they present.

2.1 Modelling

Modelling is useful because it simplifies the inherent complexity of reality and makes systems more understandable and manageable. It is very important to understand that models can never capture all details of a real system, but they will provide a useful representation where the most relevant aspects are highlighted, and analysis and predictions can be made. By focusing on the most important characteristics, models help to better understand the behaviour of systems, make informed decisions, and communicate ideas effectively.

Very briefly, models may be classified as follows:

— Physical: tangible representations of objects, mockups, prototypes.

— Conceptual: they allow us to identify, visualise and understand the relationships between variables.

— Mathematical: they use formulas, equations and algebraic relationships, to define relationships and may incorporate stochastic (random) components to include the variability inherent in random phenomena.

— Computational: as software implementations of both physical and mathematical models, so that virtual simulations and experiments of these phenomena are possible thanks to computing power.

Modelling is a useful tool in economic, political and management decision-making, but it must be remembered that models that describe, explain and predict processes are not infallible and must be considered within their specific contexts. It therefore recognises their strengths but, above all, their limitations. Clarity and accuracy are desirable characteristics of models and one of their greatest advantages is the ability to analyse scenarios, which assesses the impact of possible decisions to be taken before implementing them.

The main objectives of any model are to provide a deeper understanding of a system or process and to use this knowledge to make predictions and decisions. However, models are simplifications of reality and, when using them, one must be aware of their errors and limitations. It is crucial that decision-makers understand these limitations and take them into account in their interpretations.

Additionally, modelling should be simple. The use of artificially complex models, which exceed our physical, conceptual, mathematical or computational capabilities, presents serious drawbacks, including risks of misinterpretation, lack of transparency, hidden assumptions, difficulties in validation, over-dependence, over-learning, lack of flexibility in the face of change, amongst many other disadvantages.

Collaboration between quantitative and qualitative disciplines is essential to maximise the potential of modelling. While acknowledging its complexities and limitations, informed and cooperative modelling that uses different techniques and extends across scientific disciplines has enormous potential.

2.2 Simulation

When the challenge or difficulty we face changes over time, influenced by surrounding factors or variables, it is said to have a dynamic characteristic and the model must have the same characteristic; it must then be able to change, in some way, over time. This involves deriving the future structure of the model either by logical reasoning or by mathematical relationships that include time-dependent changes in the model and influencing factors.

Conducting a simulation consists of observing how, given initial conditions for the problem, which momentarily define the model, the model adapts to the changes produced by time increments. The advantage of this procedure is that it allows us to observe the future evolution of our problem, always bearing in mind that the initial or starting conditions influence and determine the evolution of the problem simulation.

A simulation may be validated by comparing past and therefore already known evolutions of the problem with the behaviour of the model in one or several simulations performed since the initial conditions in which the problem was encountered.

The usefulness of simulations is twofold. On the one hand, it allows us to understand how the problem works and what factors influence it, by observing its evolution under different conditions and time horizons. On the other hand, the simulation can reveal possible future scenarios of the problem over time. However, this future should not be confused with a prediction, since its dependence on initial conditions provides not only a future, but a range of possible or probable future situations, each to its own extent.

Simulation focuses on developing theories regarding the behaviour and evolution of the problem, rather than on developing accurate modelling of the problem. Given initial conditions, simulation enables inductive analysis, which generalises the results obtained from the simulated situations or experiments. It should be noted that a simulation requires multiple runs, as only one simulation would provide very limited information, given its dependence on the initial conditions of the problem and on the random factors inherent in the simulation. Simulation has the advantage of allowing us to work with artificial copies of the problem, so that we may act on them and explore their future evolution.

3 Cross-impact matrix methods

Cross-impact matrix methods are used to analyse how the occurrence of one event may influence the occurrence of other events. The work of Gordon and Hayward (1968), entitled *Initial Experiments with the Cross Impact Matrix Method of Forecasting*, is a pioneering study in the use of cross-impact matrices for forecasting and analysing future scenarios. This method was designed to help predict how relationships between events would influence future outcomes, thereby reducing uncertainty in planning and decision-making.

Cross-impact analysis is based on the creation of a matrix that assesses the probabilities of certain events occurring and the known occurrence of other events. These probabilities are known as conditional probabilities. The basic steps in defining the cross-impact matrix involve:

1. Event identification: selection of relevant events or variables that could influence the system under study.
2. Probability assessment: assignment of initial probabilities to each event.
3. Impact analysis: assessment of how the occurrence of one event affects the likelihood of other events.

4. Matrix construction: creating a matrix that visualises these interactions and conditional probabilities.
5. Interpretation of results: analysing the matrix to identify likely scenarios and the most significant interactions.

A cross-impact matrix may be conceived of as a square table with n rows and n columns, where n consists of the number of relevant events or variables influencing the system under study. Each cell in the table represents the impact of the occurrence of the i –th event on the j –th event: $j \rightarrow i$. This probability is known as conditional probability and expresses the likelihood that, the i –th event having occurred, the j –th event occurs: $P(j|i) = a_{ij}$. The diagonals indicate the impact of an event on itself and in principle this impact is null, appearing, therefore, 0 on the diagonal of the matrix: $a_{ii} = 0$.

This is how Gordon and Hayward (1968) define this matrix, and one can find papers that use the transposed criterion, the impact on the i-th event of the occurrence of the j –th event, $j \rightarrow i$, being called $a_{i,j} = P(i|j)$. This approach only involves exchanging rows for columns in the matrix.

There are at least three different ways of interpreting the impact of some events on others when constructing the impact matrix in the literature :

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} \\ a_{21} & 0 & a_{23} \\ a_{31} & a_{32} & 0 \end{pmatrix}.$$

Firstly, if the matrix does not contain quantitative information, but only seeks to determine chains of causality that allow the creation of likely scenarios, the matrix may be filled in with 0 and 1 (Chatziioannou et al., 2023). $a_{ij} = 0$ is used when there is no relationship between the occurrence of the event i and the event j. However, if the occurrence of the event i causes the occurrence of the event j, then $a_{i,j} = 1$ shall be used.

Secondly, one can choose to quantify influence between events on a scale such as, for example: 0, 1, 2, 3. Where negligible impact is represented by 0, low impact by 1, considerable impact by 2 and large-scale impact by 3. The stated advantages of using scales in the impact matrix include: less complexity, faster assessment, greater adaptability and more clarity (Nazlabadi *et al*., 2023). In other cases, scales with negative impacts may be used, for example from -5 to 5, which allows the inclusion of not only the magnitude of the impact but also its direction.

Finally, one can opt for the original approach of Gordon and Hayward (1968) in the form of conditional probabilities. This approach is also adopted by Godet (1974) in his work, in which he proposes the SMIC 74 method

(Système de Matrices d'Impacts Croisés), which, though mathematically more appropriate, presents greater difficulties in terms of its application. The work of Godet and Duperrin (1975) sparked an interesting discussion through different articles published throughout 1976 in the journal *Futures*. The problem arises when regularising the values assigned by the experts, as the expressed probabilities turn out to be inconsistent and do not comply with the axioms of probability. The method used to correct this inconsistency produces non-unique solutions to the problem as detailed by Mitchell and Tydeman (1976). The simplification of reality required to build causal models then produces a paradox by the application of mathematical regularisations that are necessary to provide the model with probabilistic consistency.

McLean (1976) closes this discussion in the *Futures* journal by emphasising that the cross-impact methodology is not an exact science, but should be understood as a heuristic method that can help us improve our understanding of complex problems in the area of foresight. Years later, Gordon himself (1994) would positively assess the combination of this methodology with simulation techniques, and would highlight the difficulty faced by experts in express judgements in probabilistic terms. The application of causal modelling techniques using impact matrices only focuses on interactions between pairs of events, whereas in the real world these interactions often occur through more complex and higher-order structures of interaction, triples, quadruples, etc.

There are methods that combine several of the strategies mentioned so far. For example, Chao (2008) proposes a mechanism for regularising conditional probabilities and takes into account not only the probabilities expressed by experts, but also the impacts expressed in terms of scale.

4 Structural analysis of impact matrices

The information gathered in an impact matrix may be represented as a graph consisting of: *nodes*, which represent the events or variables, and *lines*, which represent the relationships between the nodes with a direction and a weight (Menéndez, 1998). This graphical representation may be understood as a cause-effect diagram and, in some simple cases, may help to understand the connections and influences of some variables on others.

Below is an example of part of the impact matrix created by Shi and Wu (2024) for the first six variables $F1,\ldots,F6$, which correspond to the six personal risk factors in accidents involving lifting equipment: ($F1$) low safety awareness, ($F2$) lack of knowledge on safety in lifts, ($F3$) unauthorised operations, ($F4$) improper operations, ($F5$) not holding the licence to work,

(*F*6) inadequate safety measures. The impact matrix considered by the authors for these six factors and on a scale from 0 to 6 is:

$$A = \begin{pmatrix} 0 & 0 & 6 & 3 & 0 & 3 \\ 0 & 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 3 \\ 0 & 0 & 5 & 0 & 0 & 2 \\ 0 & 0 & 3 & 3 & 0 & 0 \\ 0 & 0 & 2 & 5 & 0 & 0 \end{pmatrix}.$$

This impact matrix produces the graph displayed in figure 2, where it may be seen how factors *F*1, F2 and *F*5 only influence and are not themselves influenced, while there are cycles between the factor pairs *F*3-*F*4, *F*3-*F*6 and *F*4-*F*6, which implies a feedback structure in influence. Chains of influence can also be observed: for example, how the variable F1 directly or indirectly influences *F*3 through *F*4 or *F*6.

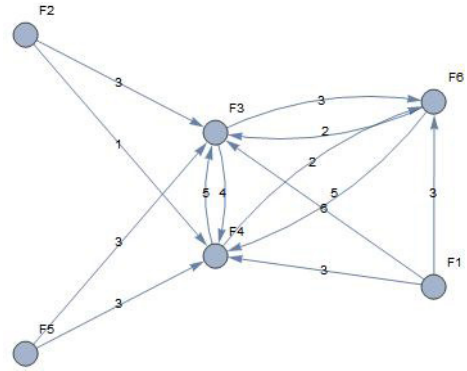


Figure 2: Cause-and-effect chart for the impact matrix for the six factors

Arcade *et al*. (1999) highlight the usefulness of this graph, a model of relationships, and propose the hierarchical organisation of these events or variables in the form of a tree. To do this, it is necessary to eliminate any cycles that appear in the network and suggest the creation of new macro variables resulting from grouping those that form cycles. In our case, it would be the grouping into a single variable of the factors *F*3, *F*4 and *F*6 and then forming a hierarchical structure with the factors *F*1, *F*2 and *F*5 at a first level, and the new macro variable at a second level, so that it is influenced by the previous ones.

Modelling the relationships between variables by means of the graph associated with the impact matrix allows the discipline of graph theory to be applied to it, which can determine paths of indirect influence, maximum impact or maximum likelihood trees, etc.

Also and highly intuitively, the influence and dependence of a variable or factor may be assessed by the sum of the rows and columns of the impact matrix, known as active sum and passive sum. The first, *active sum*, refers to the sum of the influences that each element exerts on other elements of the system and corresponds to the sum of the i —th row of the impact matrix. Passive sum refers to the sum of the influences received by each element from other elements of the system, dependency, and corresponds to the sum of the j —th column of the impact matrix. The interpretation of these quantities indicates that a variable with a high active sum value has a high impact on other variables, and low values indicate a low impact or influence. Similarly, one can interpret passive summation, which indicates a high value for one variable as high dependence on the other variables, while low values indicate independence from the other variables in the system (Arcade *et al*., 1999).

then → if this occurs ↓,	F1	F2	F3	F4	F5	F6	Active sum	P
F1	0	0	6	3	0	3	12	0
F2	0	0	3	1	0	0	4	0
F3	0	0	0	4	0	3	7	133
F4	0	0	5	0	0	2	7	112
F5	0	0	3	3	0	0	6	0
F6	0	0	2	5	0	0	7	56
Passive sum	0	0	19	16	0	8		
Q	unk.	unk.	0,37	0,44	unk.	0,88		

Once the active sum *(influence*) and passive sum *(dependence*) values have been calculated for each variable, values such as the quotient or the product of the two may be determined, also for each variable (Cole, 2006).

The quotient, *Q* value or *index of influence*, of the active sum over the passive sum makes it possible to identify the most active variable, the one with the greatest *Q* value —which has the greatest impact on the other variables as opposed to the most passive variable—, and the one with the lowest *Q* value, which is more dependent on other variables. The most active variables have the greatest influence on the system and their control will have a major impact on the system's behaviour. Variables with zero passive sum produce an indeterminacy in the calculation of the *Q* value; these variables are not influenced, they are independent and only exert influence on other variables.

The product, *P* value or *centrality index*, of the active sum times the passive sum gives a measure of the importance of a variable: high *P* values

indicate highly influential and highly dependent variables, often referred to as critical variables. Variables with low *P* values are variables that have little influence and are less dependent, and are therefore often referred to as inert.

5 Influence Dependence Graph

To obtain an overall view of the system under study, an influence × dependence graph may be built, in which the variables and the strength of their relationships are represented (Arcade *et al.*, 1999). The graph is formed by representing the passive sum (dependence) along the x axis, versus the active sum (influence) along the yaxis in a scatter diagram. Figure 3 presents the influence × dependence graph for the six factors in the example.

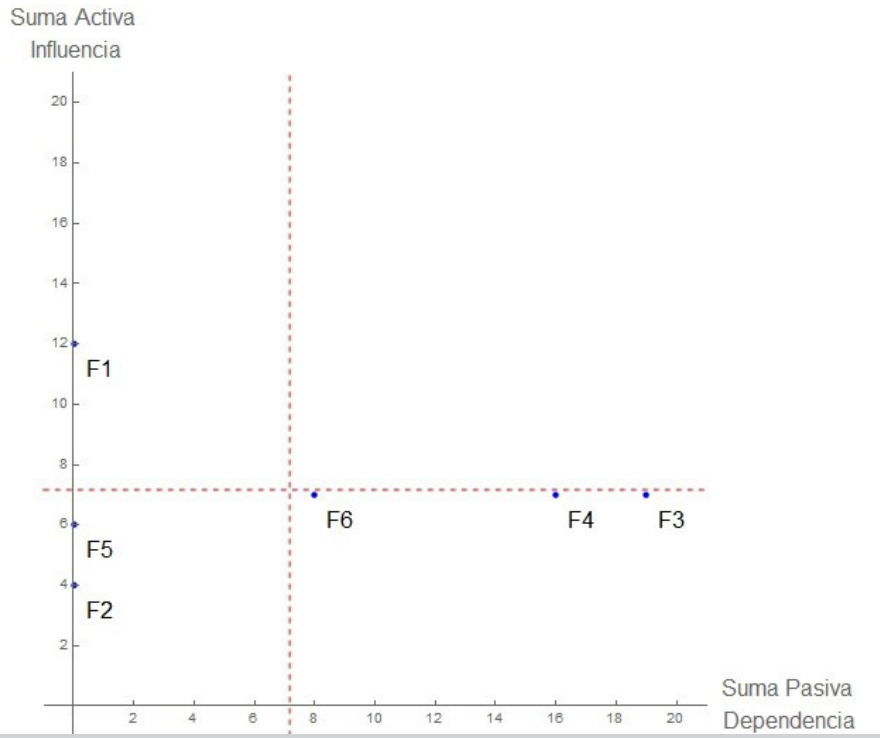


Figure 3: Influence Dependency scatter chart for the six factors in the example

The centre of gravity of the graph divides the point cloud into four quadrants and the variables or factors present in each quadrant are usually ranked according to their influence and dependence values respectively. There are several ways to refer to each type of variable that may be

represented in the scatter plot and usually at least five types of variables are mentioned, one for each quadrant, plus variables that occupy the centre of gravity of the plot (Arcade *et al*., 1999; Asan *et al*., 2004; Linss and Fried, 2010).

The centre of gravity of the graph is given by the value of average dependence and average influence, around which the so-called *regulating* variables are grouped, which usually determine the system's operation under normal conditions, but there are also authors who call them *neutral* variables (figure 4).

Variables with high dependence and influence values (passive sum and active sum) occupy positions in the first quadrant and are often referred to as *critical*, *key* or *challenge* variables. These variables are a source of instability in the system due to their high influence and dependence values. The *key* or *challenge* variables are placed above the diagonal and are usually considered the most important variables in the system. Also, below them, in this first quadrant, with dependence values higher than the influence value, are the *objective* variables, whose higher degree of dependence makes them highly liable to influencing.

In the second quadrant, variables with high values of influence and low values of dependence are found; these variables are usually referred to as *outcome* or *driver* variables. These variables act as an inertia factor in the system; they influence the system and there is often limited control over them. On the left-hand side of the quadrant, the literature usually places the *environment* variables; these variables act as the context of the system.

Variables with low influence and dependence are placed in the third quadrant, and are often called *inert*, *autonomous* or *excluded* variables. Some authors draw a distinction between *disconnected* variables, placed near the origin of coordinates with very low values of both influence and dependence, and *secondary levers*, with higher values of influence than dependence. The latter are related to the regulating variables, but at a second level; they act as levers in the system due to their degree of influence, but are less important than the former.

Finally, in the fourth quadrant are the *dependent* variables that turn out to be very sensitive due to the influence of the influential or critical variables. Among them, *outcome* variables con be distinguished, with higher dependence, variables which are usually of interest in the system and which cannot be acted upon directly, but through the variables influencing the system.



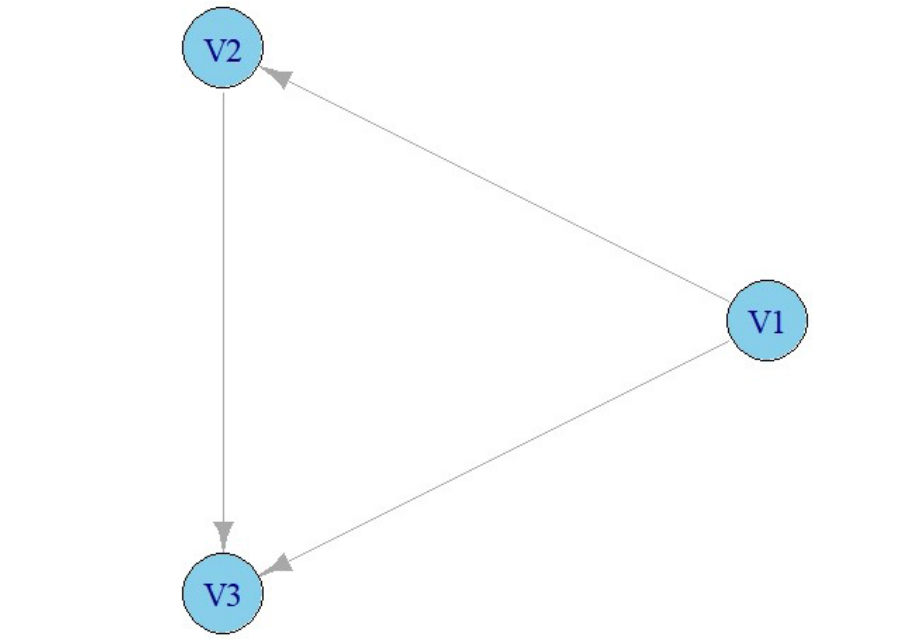
Figure 4: Dispersion chart Dependence Influence with the variable types according to their interpretation

This methodology can be applied for any type of impact matrix such as those presented above, qualitative, scale or in terms of conditional probabilities. However, the classification of variables is not unique and other classifications based on influence (active sum) and dependence (passive sum) exist in the literature.

6 Multiplication of the Cross-Impact Matrix Applied to Classification (*Matrice d'Impacts Croisés Multiplication Appliquée à une Classification*-MICMAC)

In some applications of the cross-impact methodology, the multiplication of the impact matrix proposed by Godet (1986) is used in addition to the concepts of dependence and influence to classify system variables.

The MICMAC method of impact matrix powers is based on one of the properties of qualitative impact matrices in which the $a_{ij} = 1$elements indicate direct influence of the i –variable on the j –th variable, while $a_{ij} = 0$



indicates no influence. These matrices only show the direct impact between pairs of variables in the system, ignoring indirect influences through chains of variables. Boolean impact matrices have the property that, when raised to power n, they give, in A^n, the number of strings of length n that go from the i –th vertex to the j –th vertex, a_{ij}^n.

The three-vertex graph depicted in figure 5 has the associated Boolean A matrix:

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

With three lines, two of them coming out of *V*1 and arriving at *V*2 and *V*3, respectively, and one from *V*2 to *V*3.

The A^2 matrix is squared so that the a_{ij}^2 elements are calculated by adding the products of the i –th row by the j –th row, $a_{ij}^2 = \sum_k a_{ik} \cdot a_{kj}$. It follows that each $a_{ik} \cdot a_{kj}$ term of the sum is 1 if there is a line from the i vertex to the k vertex and another from the k vertex to the i vertex. Therefore, $a_{ik} \cdot a_{kj} = 1$ indicates that there is a path of length 2 from i to j and passing through k. Adding all these products together, for all possible k vertices, we obtain the total number of paths of length 2 from i to j. Thus,

it follows that the element a_{ij}^2 of A^2 gives the number of paths or, in this case, chains of influence or impact, of length 2 that go from the i vertex to the j vertex. In the case of figure 5, it is immediately seen that there is a single path of length 2 linking the vertices *V*1 and *V*3.

$$A^2 = A \cdot A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

This result is generalised in the case of Boolean matrices (qualitative matrices, where only 1 or 0 is used to define its impact or absence), stating that the A^n matrix contains in a_{ij}^n the number of chains of length n and thus describes the indirect impact via $n-1$ variables of the i variable on the j variable. A special case is highlighted by the elements of the diagonal of the elevated matrix, a_ii^n, which presents the number of circuits or cycles which, when leaving the i variable, have an impact on it again.

In the case where the A matrix is an impact matrix expressed in scale or conditional probabilities, the interpretation of its powers is no longer immediate. Element a_{ij}^n is, in this case, the sum of the products of all the weights or impacts of all chains of influence of length n that lead from variable i to variable j. It is also, therefore, at least a relative measurement of the influence of variable i on variable j through chains of length n.

Godet's (1986) idea includes analysing indirect relationships between system variables and studying the distribution of impacts through chains and cycles in which intermediate variables express their influence. In this way, the MICMAC method seeks to classify the variables of the system according to dependence and influence, taking into account not only direct relationships between pairs of variables, but all chains of relationships expressed in the graph and the impact matrix.

The proposal in the MICMAC method is first based on the *classification* of dependence and *direct* influence between pairs of variables in the system. The variable with the largest active sum (sum of the rows) will occupy the first position in the influence ranking, so the following variables will occupy second or the next position in descending order of the active sum. In the same way, the dependency ranking is defined based on the passive sum (sum of the columns). The first position in this ranking will be occupied by the variable with the highest passive sum and the ranking would be supplemented in descending order. Thus, this classification identifies the variables that are more influential and those that are more dependent in terms of direct relationships.

The same classification may be obtained for indirect relationships of both dependence and influence. By ranking in order the active sum and

passive sum of the squared matrix, A^2, the classification of dependence and indirect influences is obtained by means of a third intermediate variable. The order of the classification may be altered, revealing hidden variables that increase their influence on the system through order two chains, i.e. they influence indirectly through another variable.

By repeating this strategy, successive rankings of the system's variables can be obtained, both for dependence and influence, A^2, A^3, A^4,... The method seeks to obtain a stability in these classifications so that they are not altered from a power, k, of the impact matrix.

The evolution of these classifications may be demonstrated either in the Influence × Dependence graph or in a table, comparing the direct classifications obtained from A with the indirect classifications obtained from A^k. It is highly interesting to compare and analyse variables that are not directly dependent or influential but *indirectly* so.

This property of stability in classification is put forward by Godet (1986) and has been used ever since in the application of the MICMAC method. However, studies show that stability is not always achieved in the dependence and influence classifications of the impact matrix powers. Jodlbauer et al. (2022) conclude that, when the impact matrix contains a high percentage of null elements, of the order of 75% or more of the elements of *A*, it is possible to find matrices that do not achieve stability in the dependence or influence classifications. These so-called "hollow" matrices also tend to show greater differences between direct and indirect rankings.

By way of example, a fragment of the impact matrix proposed by Nazlabadi *et al*. (2023) in their work on water and wastewater management is included below. The fragment presented in this example coincides with the first six variables *V*1,...,*V*6 and the dependence and influence classification of the initial impact matrix is given by:

A	V1	V2	V3	V4	V5	V6	Active sum	Influence ranking
V1	0	3	2	3	3	2	13	1°
V2	2	0	1	2	3	2	10	2°
V3	2	2	0	1	2	3	10	2°
V4	2	2	2	0	2	2	10	2°
V5	1	3	1	2	0	2	9	3°
V6	1	2	3	2	0	0	8	4°
Passive sum	8	12	9	10	10	11		
Dependency rank.	5°	1°	4°	3°	3°	2°		

In this small example, stability is achieved in the study of chains of influence of length two, i.e A^2. For this indirect classification, the influence of variable *V*4 becomes relevant and the tie is broken in terms of the dependence of variables *V*4 and *V*5. Powers higher than 2 in the impact matrix produce the same classifications.

A^2	V1	V2	V3	V4	V5	V6	Active sum	Influence ranking	
V1	21	23	18	18	19	24	123	1°	
V2	11	25	17	17	12	17	99	3°	
V3	11	20	19	20	14	14	98	4°	
V4	12	20	14	20	16	18	100	2°	$V4$
V5	14	13	15	14	18	15	89	5°	
V6	14	13	8	10	19	19	83	6°	
Passive sum	83	114	91	99	89	83			
Dependency rank.	6°	1°	5°	3°	4°	2°			

7 Conclusions

In this paper, a methodological description of the basic tools for building models based on the structural method and the cross-impact matrix applied to the creation of future scenarios has been presented. As we have seen, these tools emerge from a *game*, like many other tools used in the field of applied sciences. The complexity of reality means that simplifications must be made before conceptual, physical, mathematical or stochastic modelling techniques can be used. Applying these techniques in small games is the basis of *fundamental research*, abstract, without immediate real application, but which on many occasions are the seed of new ideas, developments that, with the invaluable help of technological advances, can be generalised and applied little by little to the task of solving real problems.

Today, the methods discussed above are successfully applied in modelling reality in many different fields, combined with other techniques and seeking to make decisions that produce benefits by anticipating or influencing the future.

As examples, we may briefly mention some works where interested readers can find details, tools and inspiration on how to apply this methodology to their problem.

Chatziioannou *et al.* (2023) have published a paper in which they create a classification of urban mobility indicators and their relation to transport policies in order to improve the liveability of cities. The paper conducts a qualitative review of legislation and literature, but most notably synthesises the experience of twenty-eight urban development experts to relate key mobility indicators to effective transport policies. In the conclusions, the authors propose to combine structural analysis with quantitative studies in future research.

Chen *et al*. (2025) perform a structural modelling of the circular supply chain management (CSCM). The study seeks to identify, analyse and rank the determinants affecting the implementation of CSCM in the South Korean logistics sector. Here, the authors work with a panel of six experts and identify the importance of government regulations and financial incentives in the adoption of these management models.

The study of the barriers or difficulties presented by the use of drones in agriculture has been approached with a hybrid strategy that combines different decision-making methods such as the DEMATEL method (Decision Making Trial and Evaluation Laboratory) applied with uncertainty measures based on fuzzy logic, the structural method and the MICMAC method (Singh *et al.*, 2024).

In conclusion, I would like to mention a methodological line of study that enables the incorporation of the temporal evolution of the system to be analysed. In the case of Serdar and Asan (2007), they incorporate this dependence by constructing a time matrix and use graph theory algorithms to find minimum paths. Similarly, the work of Nazlabadi *et al*. (2023) presents a structural analysis to determine the determinant variables and their influence on water management in urban environments, considering the influence of time on the system and propose a methodological variation that they call MICMAC-T.

Bibliography

Arcade, J. *et al*. (1999). *Structural Analysis with the MICMAC Method*. American Council for the United Nations University, The Millennium Project.

Asan, U., Erhan Bozdağ, C. and Polat, S. (2004). A Fuzzy Approach to Qualitative Cross Impact Analysis. *Omega*. 32(6), pp. 443-458. DOI: https://doi.org/10.1016/j.omega.2004.02.006

Chao, K. (2008). A new look at the cross-impact matrix and its application in futures studies. *Journal of Futures Studies*. 12(4), pp. 45-52.

Chatziioannou, I. *et al*. (2023). Ranking sustainable urban mobility indicators and their matching transport policies to support liveable city Futures: A MICMAC approach. *Transportation Research Interdisciplinary Perspectives*. 18, 100788. DOI: https://doi.org/10.1016/j.trip.2023.100788

Chen, J. R. *et al*. (2025). A Structural Analysis of the Influential Factors Affecting the Implementation of Circular Supply Chain Management in South Korea. *Journal of Cleaner Production* 494, 145005. DOI: https://doi.org/10.1016/j.jclepro.2025.145005

Cole, A. (2006). *The Influence Matrix Methodology: A Technical Report*. Palmerston North, Landcare Research New Zealand Ltd.

Godet, M. (1974). Méthode de hiérarchisation des variables et de construction de scénarios. *Metra*. XIII(4), pp. 455-478.

—. (1986). Introduction to *la prospective*. *Futures*. 18(2), pp. 134-157. DOI: https://doi.org/10.1016/0016-3287(86)90094-7

Godet, M. and Duperrin, J. C. (1975). SMIC 74: A Method for Constructing and Ranking Scenarios. *Futures*. 7(4), pp. 302-312. DOI: https://doi.org/10.1016/0016-3287(75)90048-8

Gordon, T. J. (1994). *Cross Impact Analysis*. United Nations Development Program's African Futures Project in collaboration with the United Nations University's Millennium Project Feasibility Study.

Gordon, T. J. and Hayward, H. (1968). Initial Experiments with the Cross Impact Matrix Method of Forecasting. *Futures*. 1(2), pp. 100-116. DOI: https://doi.org/10.1016/S0016-3287(68)80003-5

Gordon, T. J. and Helmer-Hirschberg, O. (1964). *Report on a Long-Range Forecasting Study*. Santa Monica, RAND Corporation.

Jodlbauer, H. *et al.* (2022). Stability of Cross Impact Matrices. *Technological Forecasting and Social Change*. 182, 121822. DOI: https://doi.org/10.1016/j.techfore.2022.121822

Kahn, H. and Wiener, A. (1967). *The Year 2000: A Framework for Speculation on the Next Thirty-Three Years*. Washington, D.C., The Hudson Institute.

Linss, V. and Fried, A. (2010). The ADVIAN® Classification A New Classification Approach for the Rating of Impact Factors. *Technological Forecasting and Social Change*. 77(1), pp. 110-119. DOI: https://doi.org/10.1016/j.techfore.2009.05.002

McLean, M. (1976). Does cross-impact analysis have a future? *Futures*. 8(4), pp. 345-349. DOI: https://doi.org/10.1016/0016-3287(76)90130-0

Menéndez Velázquez, A. (1998). Una breve introducción a la teoría de grafos. *Suma: Revista sobre Enseñanza y Aprendizaje de las Matemáticas*. 28, pp. 11-26.

Mitchell, R. B. and Tydeman, J. (1976). A Note on SMIC 74. *Futures*. 8(1), pp. 64-67. DOI: https://doi.org/10.1016/0016-3287(76)90097-5

Nazlabadi, E. *et al.* (2023). A novel MICMAC approach for cross impact analysis with application to urban water/wastewater management. *Expert Systems with Applications*. 230, 120667. DOI: https://doi.org/10.1016/j.eswa.2023.120667

Serdar Asan, S. and Asan, U. (2007). Qualitative Cross-Impact Analysis with Time Consideration. *Technological Forecasting and Social Change*. 74(5), pp. 627-644. DOI: https://doi.org/10.1016/j.techfore.2006.05.011

Shi, F. and Wu, Z. (2024). Construction of Knowledge Graph of the Elevator Safety Accidents and Analysis of Key Risk Factors Based on KG-DEMATEL-ISM-MICMAC Method. *IEEE Access*. 12, pp. 43615-43631. DOI: https://doi.org/10.1109/access.2024.3375879

Singh, S. Pal., Sharma, A. and Adhikari, A. (2024). Investigating the Barriers to Drone Implementation in Sustainable Agriculture: A Hybrid Fuzzy-DEMATEL-MMDE-ISM-Based Approach. *Journal of Environmental Management*. 371, 123299. DOI: https://doi.org/10.1016/j.jenvman.2024.123299

Technology at the service of deterrence

Emilia José Peña Ruiz

Abstract

Today, more than ever, the non-proliferation regime is under stress due to various conflicts that are taking place and the challenge of certain proliferating countries whose nuclear activities seem to be moving away from a peaceful course. For this reason, monitoring activities need value-added tools that can overcome deception activities. Satellite images and their analysis have established themselves as a mainstay tool in the IAEA's verification activities and its safeguards system, despite attempts to reduce their effectiveness by burying or covering their vital parts with buildings.

Keywords

Satellite, Intelligence, Proliferation, Safeguards, Nuclear.

1 Introduction

Nuclear deterrence is referred to as an international relations principle which aims to avoid a nuclear attack based on the nuclear weapons potential. Everyone could concur with its destructive capacity, especially considering the devastating effects of *Little Boy* and *Fat Man* in Hiroshima and Nagasaki. However, doubts about their effectiveness and efficiency associated with deterrence have paradoxically always existed.

From the military point of view, the result was decisive as it caused Japan's defeat, but at the same time, its strategic aspect and potential power projection were disclosed. The Hiroshima and Nagasaki atomic bombings resulted in the Japanese surrender on September 2, 1945, ushering in a new historical era for humanity known as the Atomic Age (Calduch, 1991: 6).

Back then, the United States was the only country running the arms race, and therefore, it was the leader of the nuclear monopoly as it was ahead of its adversaries. This was an untenable situation precisely because the remaining adversaries would not remain at such military and strategic inferiority for long. Consequently, it fuelled the arms race among states such as Russia, France, China and the United Kingdom.

These five countries ended up being Nuclear Weapons States (NWS) *de jure;* however, other states have obtained this nuclear status *de facto*, like North Korea, India, Israel and Pakistan, and have proved their arms capacity by conducting numerous atomic tests as a demonstration of their military potential.

In 1958, Thomas K. Finletter, 5th United States Ambassador to NATO, said: "Disarmament is at the top of the agenda." Sixty-seven years after that, the situation is turning 180 degrees, and the nuclear states club is at risk of expanding with new members. Beyond Iran's serious candidacy, widely considered the next likely state to emerge as a *de facto* nuclear power, Saudi Arabia's announced intentions and Turkey's long-dormant but well-documented aspirations are now treated as near-certainties.

The nuclear non-proliferation regime, anchored for forty-five years by the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), now faces significant challenges, led by Iran's development of ambiguous yet highly consequential nuclear capabilities. On the other hand, global energy needs and future supply challenges have led to the consolidation of projects that were once mere ideas or aspirations, with nuclear energy now emerging as the key to energy demands. This has driven both qualitative and quantitative leaps in the development of this technology globally.

Given the twofold nature of nuclear technology, civil and military, this process poses a major challenge for the international community. It must

persevere in maintaining a balance between technical and economic progress and global stability under the NPT framework (Salazar, 2015).

As can be noted, international architecture for non-proliferation and disarmament is increasingly challenged and strained, operating within a security environment that undermines it. Russia's aggression against Ukraine, which began in 2022 and has now entered its third year, has only accelerated the corrosion of the already-rusted anchors of disarmament initiatives, and by extension, the Non-Proliferation Treaty (NPT) as its cornerstone.

Sergei Karaganov, one of the intellectual architects of Russian foreign affairs and head of the highly influential Council for Foreign and Defence Policy, a key figure of Russian strategic thinking, and an adherent of the use of nuclear weapons in the current conflict with Ukraine, explains it perfectly in a few words: "The motto from fifty years ago —'there can be no winners in a nuclear war and it must never be unleashed' —is great, but also idealistic. Ukraine's conflict has proved it paves the way to major conventional wars, which will eventually become more frequent and deadly unless they are counteracted with an active peacebuilding policy" (Laruelle, 2024).

However, the current geopolitical map does not engage with this active peacebuilding policy. Indeed, there are not 25 nuclear powers as the American president John F Kennedy administration forecast in 1960, but there are no intentions of committing to disarmament. On the contrary, interstate competition and mistrust run deeper than ever, as evident in military spending and divergent applications of Artificial Intelligence. States seek to ensure their security and survival, and this tendency of certain countries to "acquire more and more power to escape the impact of others' power" was also analysed by John Herz through his concept of the security dilemma. It describes how nations risk falling into a vicious arms race spiral, inevitably leading to the paradox of security (Wheeler and Booth, 2007: 27).

To restrain the arms race, a stable bipolar geopolitical ecosystem is required. Yet, the geopolitical ecosystem surrounding us is multipolar and unstable. Moreover, emerging technologies have accelerated the evolution of military arsenals, and nuclear arms seem to have regained significance as coercive or deterrent tools. This whole ecosystem has fuelled a renewed arms race (Cartagena and Garrido, 2024).

Due to this backdrop, the horizontal proliferation concept has regained relevance. This phenomenon, which originated during the Cold War era, involves an increase in the number of states possessing nuclear military capabilities. It has now undergone significant evolution due to shifting international circumstances developed across three key dimensions. Firstly, the increased destructive power of nuclear weapons. Secondly, the novel

socio-political and economic characteristics of post-Cold War proliferating states. And thirdly, the heightened risks nuclear weapons pose to international peace and security (Marrero, 2002).

The risks posed by horizontal nuclear proliferation to international security are so evident that we can immediately discern their connection to the safeguards system and the monitoring activities that the IAEA has been conducting for nearly seventy years to prevent nuclear weapons proliferation and provide credible assurances that states comply with their legal obligation to use nuclear technology exclusively for peaceful purposes.

Maintaining a safeguards regime remains essential, but it must be able to count on the support and commitment of its stakeholders. Safeguards must also be underpinned by a robust legal framework and use the latest scientific innovations in the field of nuclear verification to ensure that no potential proliferation effort goes undetected while verifying that nuclear material and technology remain in peaceful use, particularly in a challenging geopolitical moment that demonstrates the need for renewed commitment to the non-proliferation principle (VV. AA., 2015: 2).

1.1 The need for a safeguards system

The IAEA provides us with a straightforward definition of safeguards: a set of technical measures applied by the Agency to nuclear facilities and materials. These measures serve to independently verify that a State Party's nuclear facilities are being used properly and that no nuclear material is being diverted for non-peaceful purposes through these technical guidelines. These measures include political engagements, multilateral treaties, and other binding agreements in which non-proliferation commitments are inscribed, especially IAEA safeguards. The states accept these measures by negotiating their respective safeguards agreements, which ultimately become legally binding obligations that they undertake to comply with (IAEA, n.d.).

The safeguards mechanism is equivalent to any other review process where the ultimate goal is for the procedures to foster trust in the states' behaviour. This requires that nuclear facility operators maintain and declare detailed accounting records of all movements and transactions involving nuclear materials. As a result, the Agency monitors nearly 900 nuclear facilities and several hundred other locations across 57 countries through regular inspections. These records and audits are supplemented by additional measures, such as surveillance cameras and remote monitoring instruments (World Nuclear Association, 2021).

The IAEA has been conducting periodic inspections of the nuclear facilities and auditing transactions of nuclear materials since 1970. Therefore,

we can claim that, for more than fifty years, the IAEA has prevented diversification of fissile materials for building weapons and has alerted to non-declared nuclear activities on several occasions.

Most safeguards agreements have been concluded with non-nuclear-weapon states (NNWS) that are also party to the Nuclear Non-Proliferation Treaty (NPT) and have committed neither to develop nor acquire nuclear weapons. However, the European Union presents a notable exception to this framework.

Chapter VII of the EURATOM Treaty, signed in Rome on March 27, 1957, established its own system for monitoring nuclear materials[1]. Although functionally equivalent to a safeguards system, it is not a nuclear non-proliferation mechanism. This is because its provisions do not restrict the military use of nuclear material; they only require mandatory reporting on its usage (Ministerio para la Transición Ecológica y el Reto Demográfico, n.d.).

The entry into force of the NPT within the European Union (then the European Economic Community) required the parallel application of the safeguards regimes of EURATOM and the IAEA. To avoid duplication in control activities and ensure a rational use of efforts and resources, the Member States stipulated that the safeguards agreements subsequently concluded with the IAEA—specifically the Agreement reflected in INFCIRC/193—would have a scope analogous to the Agency's model framework for the coordinated application of safeguards, as outlined in INFCIRC/153.

The implementation of safeguards follows an annual cycle and comprises four main processes. Collection and evaluation of safeguards-relevant information for safeguards application; development of a safeguards approach for a state to achieve the technical objectives; planning, conducting and evaluating safeguards activities both in the field and at the Agency's headquarters to reach the technical objectives, and finally, drawing of conclusions based, obviously, on the degree of compliance (IAEA, n.d.).

It is abundantly clear that technology is continuously evolving and improving, impacting all fields, including the nuclear sector. The amount of material and the number of facilities under the Agency's safeguards have steadily increased, resulting in 15 new safeguards agreements and 30 additional protocols over the past 15 years.

The IAEA safeguards system must continue to evolve precisely because further improvements are needed to optimise assurance processes, ensuring credible safeguards. It is crucial to deliver swift and effective responses to new verification requirements by utilising cutting-edge technology.

[1] The provisions of Chapter VII of the Treaty are further elaborated in Euratom Regulation 302/2005

For both the Agency and global society, it is essential to monitor potential developments that fall outside the scope of existing safeguards.

Although the most important factor of the safeguard regime is the international pressure brought to deter a state from developing a nuclear arms programme, the most effective solution against proliferation is, at times, more political than technical. However, the greatest risk will always fall upon two kinds of states. The countries that have not joined the NPT and have significant nuclear activities not subject to safeguards, and those that have joined but disregard the commitments made under the treaties (World Nuclear Association, 2021).

Within this circumstance, we find the cases of Iraq, Iran, and North Korea, which illustrate both the strengths and weaknesses of the international safeguards system. Iraq and Iran accepted safeguards on their declared facilities while simultaneously establishing undeclared installations and equipment elsewhere in an attempt to enrich uranium beyond the limits set by the Agency.

North Korea utilised research reactors and developed a reprocessing plant to produce weapons-grade plutonium before deciding to withdraw from the NPT in 2003. Although these activities were fortunately detected, North Korea currently represents the greatest challenge facing the IAEA.

Therefore, despite the safeguards system comprising a set of complex activities aimed at guaranteeing the peaceful use of nuclear developments, this control system requires supporting tools to monitor and assess technical developments. Geographic information systems provide verification support that is far more important than one might initially assume.

1.2 The role of geographic information systems in the safeguards system

The first step of the verification process is the information which Member States provide to the IAEA. Nevertheless, as already mentioned, there are cases of proliferating states outside the Agency. Thus, external tools are required to support the verification tasks of these states. In 1998, the IAEA fostered research on the feasibility and profitability of commercial satellite imagery application to support safeguards applications. The results confirmed that the high resolution of the images represented a highly significant source of information, not only for the nuclear activities monitoring, but also for location verification (Poucet, Contini and Bellezza, 2002).

The IAEA compels all states with enrichment facilities to monitor all fissile materials by specific protocols. Should there be inconsistencies or

insufficient data, the Agency issues additional requests[2]. This information is structured into three interconnected models: topological, functional, and operational. The topological model encompasses all geographically referenced data, including the physical site location. Regarding the location, several thematic maps are considered, e.g. site layout raster map, boundaries of facilities and related plant units, material balance areas (areas where the nuclear material is handled), the location of the associated key measurement points (key points where the nuclear material is measured), buildings layout, etc. In the technical/functional model, the information describes nuclear facilities, such as processes, technical characteristics of the installation, materials and procedures used, material flows, material balance areas and related key measurement points, procedures, etc (Poucet and Contini, 2000).

The declared information is then compared with observations, open-source information, specialised databases, scientific literature and internal IAEA information, as well as the cartography of the area, with the objective of verifying the declared topological model.

Within the IAEA, the responsibility for verifying that Member States comply with their agreements falls to the Department of Safeguards. The Division of Information Management (SGIM) supports the Department of Safeguards in fulfilling its mandate by managing geospatial information through the State Infrastructure Analysis Section (ISI). Since 2002, the ISI has been dedicated to analysing commercial satellite imagery and managing geospatial data.

Since then, geospatial information and commercial satellite imagery have become one of the primary sources of information, enhancing the IAEA's ability to improve the effectiveness of safeguards implementation, the confidence in safeguards conclusions, and the support for the decision-making process Colakovic, Duckworth and Lafitte, 2023: 1).

---

[2] All Non-Nuclear-Weapon States Parties to the NPT, as well as States Parties to Regional Nuclear-Weapon-Free Zone Treaties (NWFZ Treaties), are required to conclude comprehensive safeguards agreements (CSAs) with the IAEA. Such agreements are based on the document INFCIRC/153 (Corrected). The state undertakes to accept IAEA safeguards on all nuclear material in all peaceful nuclear activities within its territory, under its jurisdiction, or carried out under its control anywhere. Under these agreements, the IAEA has the right and obligation to ensure that safeguards are applied to all such nuclear material solely to verify that this material is not diverted to nuclear weapons or other nuclear explosive devices.
For the original text, see: IAEA Information Circular, INFCIRC/153. Structure and Content of Agreements Between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons, Information Circular, IAEA, May 1971. Available at: https://www.iaea.org/sites/default/files/infcirc153_sp.pdf

The utility of satellite imagery in safeguards monitoring and verification activities presented that it was possible to verify site layout maps, detect undeclared activities, identify new mining operations, monitor changes in previously decommissioned facilities, and support inspection planning (IAEA, 1998).

Satellite imagery with 5m to 10m spatial resolution proved useful for verifying site layouts, while the high-resolution imagery available at the time (1m to 2m resolution) was suitable for inspection planning. The higher resolution enabled the identification of multiple facility features and surrounding areas, which helped in specifying the localisation and the activities conducted within, near, or even in the underground facilities. Therefore, change detection analysis has been particularly valuable for identifying undeclared activities, although it is not the only method. Thermal anomaly detection, for instance, offers another promising approach for monitoring activities (Truong, 2000; Jasani and Larsson, 1998).

The nuclear fuel cycle encompasses all activities related to electricity production from nuclear reactions. This cycle begins with the extraction and milling of uranium ore. Natural uranium contains two isotopes: U-235 and U-238. To sustain the fission chain reaction, the concentration of U-235 must be increased from 0.7% to 3-4% in enrichment plants. Additionally, natural uranium must be converted into uranium hexafluoride (UF_6)[3] and then into uranium dioxide (UO_2), which is later pressed into small cylindrical pellets and loaded into tubes that form the fuel rods. These rods are then assembled into bundles to create the reactor core elements. Typically, a nuclear power plant can use up to 75 tons of fuel per year.

The fission chain reaction inside a nuclear reactor produces heat, which generates steam to drive turbines connected to electrical generators. This fuel is gradually consumed until it can no longer be reused due to changes in isotope concentration, requiring at least one-third of the fuel to be replaced annually. The spent fuel discharged from the reactor emits radiation and heat, leading to its storage in water pools for several months for its cooling. Thus, within a nuclear facility, there are two highly potent heat sources.

Satellites present the advantage of searching and localising sites by their revisiting frequency and resolution, and currently, the advances in both features provide them with a magnificent acquisition capacity.

Reprocessing plants for uranium or weapons-viable plutonium have highly distinguishable features in 1-meter resolution satellite imagery, such as containment domes, reactor cooling towers, ventilation stacks and other structural signatures visible in high-resolution images.

[3] Or be directly converted into uranium dioxide (UO_2).

For instance, from an image of the Severesk (Russia) reprocessing plant taken by a CORONA satellite on September 15, 1971, the long "canyon-like" building (typical of large reprocessing plants) and the very high stack (readily distinguished by its long shadow) could be easily identified. Moreover, its security perimeter is also easily recognised, as well as the enrichment buildings at the south and north production areas, from which one could estimate the production scale.

To detect the facility's reactors, certain features help identify them, such as cooling towers, natural water bodies, and intake and discharge ports. In reprocessing plants, high stacks and their shadow, as we have mentioned, are very useful, as well as a long "canyon-like" building (or a vent), some holding ponds or reservoirs for waste or sludge.

Gas enrichment plants are typically large-area process buildings, characterised by extensive roofs with multiple ventilation shafts and cooling towers. They can also be located near a river or lake, as well as a fossil fuel power plant, a large electric switchyard, or a substation (Zhang, 2001).

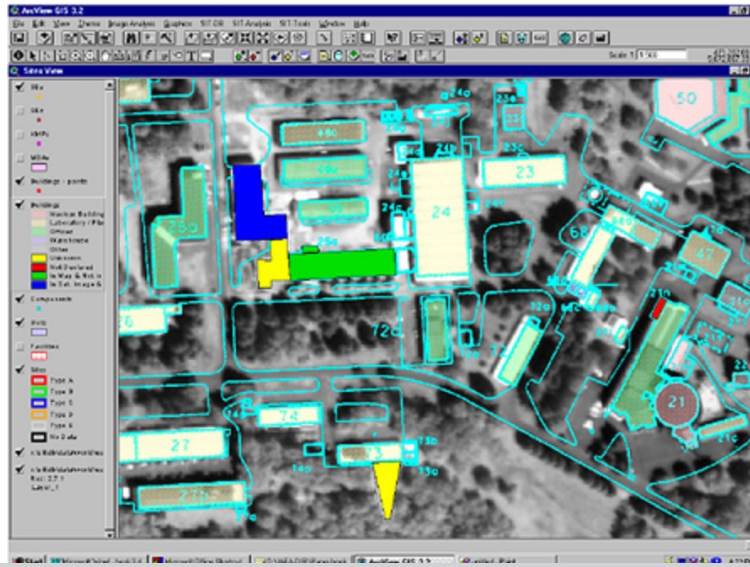


Figure 1. Example of a site map verification activity on an IKONOS satellite image. Source: Poucet, A., Contini, S. and Bellezza, F. (2001). A Gis-Based Support System for Declaration and Verification. IAEA-SM-367/CD. In: Symposium on international safeguards: Verification and nuclear material security. Proceedings. Vienna

The original and interpreted datasets, along with information extracted from open sources and by states, generate the geospatial database and the Structured Observation Metadata (SOM) database, forming a geospatial dataset that leads to products such as georeferenced site plans,

thematic maps, or geoportals. The structured management of observations complements the foundational geospatial dataset and provides a system for recording additional observations made within a structured framework (SOM). These observations are collected as part of the image analysis process and typically refer to ephemeral features that can be in a figure, such as the movement of construction equipment and their support vehicles. These features are not typically part of the facility's baseline geospatial data but are useful to provide broader site analysis (Colakovic, 2023: 7).

As analysed throughout the text, the high resolution of satellite imagery makes it increasingly difficult to conceal certain proliferation activities. However, in response to this, some states began adopting anti-satellite countermeasures years ago, hiding their facilities underground, despite the high cost involved. Even once discovered, monitoring activities would continue over such sites since certain features remain detectable, such as access roads, railways, or facility entrances and exits.

An example of an underground nuclear facility is the reprocessing plant at Israel's Dimona nuclear complex, which was completed in the mid-1960s with a plutonium reprocessing capacity of five to ten nuclear warheads per year. In an IKONOS image at 2-meter resolution taken on July 4, 2000, as well as in other declassified images of this site, the tall stack associated with the reprocessing plant is visible. Security fences surrounding the complex, the reactor building, and the mechanical cooling towers with two ventilation shafts are also distinctly observable in the imagery (Zhang, 2001: 7).

However, without a doubt, the two proliferating states that have worked the hardest to conceal their facilities from IAEA efforts have been Iran and North Korea.

2 A practical example: the case of North Korea

The value of satellite imagery for deterrence is clear in North Korea. The imagery helps the IAEA monitor the nuclear programme development of this proliferating country. Yongbyon's evolution monitoring is especially crucial, yet no on-field inspections can be carried out (Quevenco, 2016).

To briefly address it, North Korea's nuclear problems arose at the end of 1945 due to the division of the peninsula along the 38th parallel. In the north, a communist regime led by Kim Il-Sung was established, while in the South, a military government backed by the United States took power. Five years later, with North Korea's invasion of the south, the two countries engaged in a three-year war (Garrido, 1994: 104-113).

At the end of the hostilities, the American presence intensified, and in 1953, Seoul signed a security pact with the United States that allowed the deployment of American "Matador" missiles on South Korean land. This

move violated some provisions of the 1953 "Panmunjom Agreement" and provoked a reaction from Kim Il-Sung's regime, which in 1959 began showing interest in developing an ambiguous nuclear programme[4]. In 1965, Moscow supplied North Korea with its first 8 MWt research reactor, an experimental LRT-2M-type nuclear reactor, which was not committed to safeguards compliance until 1977.

North Korea joined the NPT in 1985 and signed a safeguards agreement with the IAEA in 1992, but rejected the inspections proposed by the Agency, particularly concerning its Yongbyon Nuclear Centre (Bunn, 2005: 8). In 1993, U.S. satellites detected the construction of suspicious facilities that could hold plutonium reprocessing activities, prompting the government in Pyongyang to threaten withdrawal from the NPT. This crisis was resolved with the signing of the 1994 Agreed Framework between the United States and North Korea. Under this agreement, the government in Pyongyang committed to dismantling its nuclear programme, remaining in the NPT and accepting IAEA safeguards. However, on January 10, 2003, North Korea withdrew from the Nuclear Non-Proliferation Treaty, and on October 9, 2006, it conducted its first nuclear test.

The most recent estimates on North Korea's nuclear arsenal date back to 2023 and place the number of warheads between 35 and 65. In 2024, activity was detected at the Yongbyon Nuclear Complex, which houses the experimental light-water reactor (ELWR), although it remains unclear whether it is operating at its full capacity of 100 megawatts thermal (MWth).

Its activity was discovered due to the water discharged into the nearby river. This discharge point was built over ten years ago, in 2013, and apparently, it is directly connected to the reactor. It is therefore a critical component of the secondary cooling system, and the frequent releases of warm water into the river evidence that the reactor is operational.

The reactor's cooling water discharge point is located south of the pumping station and approximately 85 meters from the reservoir dam. The first discharge was detected in satellite imagery from October 4, 2023, and remained consistently visible in subsequent images until January 2024. During winter, the warm water is far more discernible, as the river is frozen and the surrounding land is covered in ice and snow, except in areas where heated water flows. Another indicator is the melted (or absent) snow on the flat roofs of the turbine hall building, strongly suggesting that the reactor is operational. However, its precise operational output remains undetermined.

[4] This agreement prohibited the introduction of new types of weapons or more advanced models of such weapons into the territory of the Korean Peninsula. For further information on North Korea's nuclear and missile programmes, see: VV. AA. (2009a y 2009b).



Figure 2. Image analysis of the Yongbyon Nuclear Complex, 4 October 2023. Source: Albright, D., Burkhard, S., Cheng, V. and Faragasso, S. (2024). North Korea's ELWR: Finally Operational After a Long Delay. Institute for Science and International Security. Available at: https://isis-online.org/isis-reports/detail/northkoreas- elwr-finally-operational-after-a-long-delay/10#images

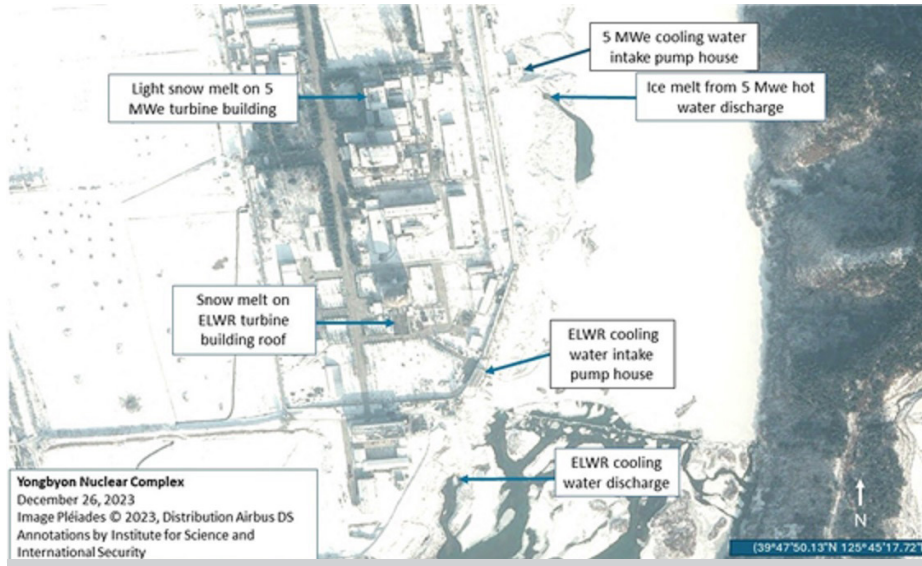


Figure 3. Image analysis of the Yongbyon Nuclear Complex, 26 December 2023. Source: Albright, D., Burkhard, S., Cheng, V. and Faragasso, S. (2024). North Korea's ELWR: Finally Operational After a Long Delay. Institute for Science and International Security. Available at: https://isis-online.org/isis-reports/ detail/north-koreas-elwr-finally-operational-after-a-long-delay/10#im

3 Conclusion

Advances in satellite imagery have significantly enhanced their resolution and clarity, becoming a cornerstone of proliferation monitoring activities mainly because high-resolution electro-optical images and SAR (Synthetic Aperture Radar) can capture details down to 30 cm per pixel in night shots or adverse weather conditions, providing added value to intelligence efforts.

Both military operations and security/defence activities require tools to obtain high-quality information, data that can be analysed and transformed into timely, actionable intelligence. If reducing uncertainty and developing future scenarios are the backbone of intelligence, they become even more critical when applied to nuclear proliferation.

Although satellite imagery analysis has been used as a supporting tool for safeguards and the IAEA's Additional Protocol since 2002, we have observed that it has evolved into an essential asset for the Agency's monitoring efforts. It now plays a cross-cutting role in all related activities, from inspection planning to verifying data provided by Member States on nuclear sites, as well as detecting undeclared facilities.

However, we have also observed how, over time, counter-satellite activities have emerged to limit or neutralise these advantages. It is expected that the most advanced forms of remote sensing, such as thermal, hyperspectral, or SAR imagery, will eventually be countered by measures designed to challenge their capabilities or analysts' ability to detect evidence, just as current tactics like the concealment of facilities through full or partial underground construction.

Having a wider catalogue of available commercial satellites and their imagery would not only enhance scrutiny and monitoring of sensitive locations, but would also complicate deception efforts against oversight bodies like the IAEA. Moreover, multi-source scrutiny, including diverse intelligence groups and cross-verification of claims, would potentially prevent violations of international treaties. This approach would bolster verification efforts and mitigate the risk of conflict stemming from misinterpreted evidence caused by the spillover effects of an arms race.

Bibliography

Bunn, G. (2005). The world's non-proliferation regime in time [online]. *IAEA Bulletin*. IAEA. 46(2), p. 8. [Accessed: 2025]. Available at: https://www.iaea.org/sites/default/files/46203590809_es.pdf

Calduch, R. (1991). *Relaciones Internacionales*. Madrid, Ediciones Ciencias Sociales, p. 6.

Cartagena, I. and Garrido Rebolledo, V. (2024). *La roca de Sísifo: pasado, presente y futuro del régimen de no proliferación nuclear*. J.B. Bosch.

Colakovic, M., Duckworth, S. and Lafitte, M. (2023). *Geospatial data capabilities to support safeguards understanding and awareness*. Institute of Nuclear Materials Management, p. 1.

Garrido Rebolledo, V. (1994). Corea del Norte: Entre el desarme y el rearme nuclear. Asistencia Humanitaria: Vida o Muerte. *Tiempo de paz*. 32-33, pp. 104-113.

IAEA. (n.d.). *Safeguards and verification, Basics of IAEA Safeguards. Safeguards explained* [online]. [Accessed: 2025]. Available at: https://www.iaea.org/topics/safeguards-explained#:~:text=Safeguards%20are%20a%20set%20of,not%20diverted%20from%20peaceful%20uses.

IAEA. (1971). *Estructura y contenido de los acuerdos entre los Estados y el Organismo requeridos en relación con el Tratado sobre la no proliferación de las armas nucleares* [online]. Informative notice, INFCIRC/153. [Accessed: 2025]. Available at: https://www.iaea.org/sites/default/files/infcirc153_sp.pdf

IAEA. (1998). *Technical Workshop on Safeguards: Sources and applications of Commercial Satellite Imagery*. Vienna.

Jasani, B. and Larsson, C. (1998). Security implications of remote sensing. *Space Policy*. 4(1), pp. 46-59.

Laruelle, M. (2024). El multilateralismo nuclear de Karaganov [online]. *El Grand Continent*. [Accessed: 2025]. Available at: https://legrandcontinent.eu/es/2024/12/02/el-multilateralismo-de-karaganov/

Marrero Rocha, I. (2022). *La proliferación nuclear horizontal en el nuevo régimen de seguridad* [dissertation]. Director, Diego J. Liñán Nogueras. Granada, Universidad de Granada.

Ministerio para la Transición Ecológica y el Reto Demográfico. (n.d.).

Poucet, A. and Contini, S. (2000). Use of Geographical Information Systems and Satellite Images for Safeguards. In: Foggi, C. (ed.). *Proceedings of the ESARDA Seminar on Strengthening of Safeguards: Integrating the New and the Old*. Dresden, EURReport 19587.

Poucet, A., Contini, S. and Bellezza, F. (2002). GIS and satellite images in nuclear safeguards. In: Brebbia y Pascolo (eds.). *Management Information Systems*. MIT Press.

Quevenco, R. (2016). Completing the picture: using satellite imagery to enhance IAEA safeguards capabilities. *IAEA Bulletin*.

Salazar, Gonzalo de. (2015). El Tratado De No Proliferación de Armas Nucleares: los temas clave en la Conferencia de examen en 2015. *Revista UNISCI*. 38.

Truong, Q. S. B. (2000). Potential Applications of Commercial Satellite Imagery inInternational Safeguards. In: Foggi, C. (ed.). *Proceedings of the ESARDA Seminar on Strengthening of Safeguards: Integrating the New and the Old*. Dresden, EURReport 19587.

VV. AA. (2009a). North Korea's Chemical And Biological Weapons Programs. *Asia Report*. International Crisis Group. 167.

VV. AA. (2009b). North Korea's Nuclear And Missile Programs. *Asia Report*. International Crisis Group. 168.

VV. AA. (2015). *IAEA Safeguards: serving nuclear non-proliferation*. IAEA, p. 2.

Wheeler, N. and Booth, K. (2007). *The Security Dilemma. Fear, Cooperation and Trust in World Politics*. Londres, MacMillan Palgrave, p. 27.

World Nuclear Association. (2021). *Safeguards to Prevent Nuclear Proliferation* [online]. [Accessed: 2025]. Available at: https://world-nuclear.org/information-library/safety-and-security/non-proliferation/safeguards-to-prevent-nuclear-proliferation

Zhang, H. (2001). Strengthening IAEA Safeguards using high resolution commercial satellite imagery. IAEA-SM-367/16/01. In: IAEA (ed.). *Symposium on International Safeguards: Verification and Nuclear Material Security*. Vienna.

Transforming the JISR cycle in the digital age: technological innovation for information superiority

Begoña Rojo Carralero

Abstract

This chapter analyses the transformation of the Joint Intelligence, Surveillance and Reconnaissance (JISR) cycle in the context of the digital era, driven by emerging and disruptive technologies. The integration of capabilities such as Artificial Intelligence, distributed sensing, unmanned platforms, edge computing and space systems is redefining how intelligence is planned, executed and exploited in increasingly multi-domain operations.

Throughout the text, the impact of these technologies at each stage of the JISR cycle (TCPED) is examined, as well as the challenges arising from their use: from the need to ensure interoperability and data security, to managing risks associated with automation, algorithmic biases, or vulnerabilities to cyber-attacks.

The chapter stresses that this transformation is not only technical, but also doctrinal and organisational. It requires new architectures, a "single data" model and a culture of sharing, analysis and agile decision-making. Artificial Intelligence does not replace the human factor, but it does enhance it. In short, technological innovation applied to the JISR cycle is a necessary condition for achieving information superiority in current and future operating environments.

Keywords

JISR, Emerging technologies, AI, Information superiority, Interoperability.

"In the 21ST century, success will not be achieved by the one who obtains the most data, but by the one who converts it into good decisions the fastest and best."

1 Introduction

Information remains a key factor for success in the fields of security and defence. It is not just a matter of its processing, but also of availability, and of passing it on to the appropriate decision-making level, at the right time and in the right format.

In today's increasingly digital, automated and multi-domain operating environment, the role of intelligence remains essential, but how it is generated, processed and applied is changing dramatically. The ability to observe, analyse and decide quickly is redefining the rules of the game. In the 21st century, access to accurate, real-time information has become a critical factor in gaining an advantage over an adversary.

Within this context, the Joint Intelligence, Surveillance and Reconnaissance (JISR) process has become an essential tool to support the planning and direction of operations. The volume, diversity and speed of available data exceed the capabilities of conventional systems, making innovation a tool to support their continuous improvement.

Innovation is about introducing new ideas or transforming existing ideas to improve results. In the field of military intelligence, this improvement could translate into the ability to make faster, better-informed decisions adapted to an increasingly complex operational environment.

Technological innovation, driven by the development of emerging and disruptive technologies, is profoundly transforming the JISR process. Artificial Intelligence, edge computing[1], distributed sensing, unmanned platforms and the use of open sources are leading to a new, more automated, interoperable and adaptive ISR architecture model.

NATO itself has acknowledged this change. In its most recent Strategic Concept, it establishes superior knowledge of the environment as a necessary condition for maintaining deterrence and responding effectively to today's threats. Within this context, the multi-domain operations (MDO) approach takes on especial relevance as an integrated operational model, where the JISR process enables the coordination of capabilities in the land, maritime, air, cyberspace and cognitive domains.

[1] Edge computing is a technological paradigm that allows data to be processed close to its source of generation (sensors, platforms), reducing latency and improving real-time responsiveness.

This chapter explores how the JISR process is evolving into a more efficient, multi-domain system, capable of operating in highly digitised environments. Throughout the text, both the opportunities offered by these technologies and the risks and challenges they pose will be examined.

Innovating in the JISR process is not only a technological option, but a strategic requirement in order to anticipate, adapt and decide with an advantage. Ultimately, the goal is not to collect more data, but to turn it faster and more reliably into useful information. And for this, emerging and disruptive technologies, especially Artificial Intelligence, are crucial.

2 Basics of the ISR process

Joint Intelligence, Surveillance and Reconnaissance (JISR) is a key capability to provide situational awareness to the command and facilitate timely decision-making.

Within Allied Joint Doctrine, the term JISR is defined as the set of intelligence and operations capabilities that integrates collection capabilities with the processing, exploitation and dissemination of the resulting information[2].

The JISR process is defined as a process of coordination through which intelligence gathering and exploitation activities provide data and information to satisfy an information or intelligence requirement, in a deliberate, *ad hoc* or dynamic timeframe, in support of operational planning and execution.

This process aims to directly support the planning, preparation and execution of operations, supported by the following constituent elements, which are summarised below:

— Intelligence: this component covers all disciplines of intelligence gathering, including its collection, processing, exploitation and dissemination capabilities and assets. Intelligence gathering disciplines include: acoustic intelligence (ACINT), human intelligence (HUMINT), image intelligence (IMINT), measurement and signature intelligence (MASINT), open source intelligence (OSINT) and signals intelligence (SIGINT)

— Surveillance: it consists of systematic observation in all operational areas. It is performed by visual, electronic, photographic or other means and may cover large areas or focus on specific targets.

[2] Extract from the definition of the JISR process according to partner agency publications and procedures.

— Recognition: it allows information to be obtained by visual observation or other detection methods. Its purpose is to collect data on an adversary's activities and resources or to learn about the meteorological, hydrographic or geographical characteristics of a given area.

Together with the elements described above, this process consists of five phases known as TCPED (Task, Collect, Process, Exploit and Disseminate):

— Task: gathering ISR needs and internal resource planning, management and capacity allocation.

— Collect: gathering data and information through ground-based, airborne, naval, space-based, cyber and cognitive sensors, as well as from human or open sources.

— Process: organisation, filtering and initial analysis of the data. This phase may be carried out by specialised personnel or automated algorithms.

— Exploit: advanced interpretation of information. It may also give rise to new needs.

— Disseminate: delivery of information to the right users at the right time, through secure channels adapted to the tactical, operational or strategic levels.



Figure 1. JISR cycle phase diagram

This process does not work in isolation. It is linked to the process of intelligence requirements management and collection management, known as IRM&CM (Intelligence Requirements Management & Collection Management). Its objective is to ensure that information needs are correctly formulated, prioritised and covered by the most appropriate means and to optimise the use of ISR resources.

Figure 2 provides a schematic representation of the interconnection between ISR and the intelligence and operations cycles.

3 JISR in multi-domain operations and the transparent battlefield

The concept of multi-domain operations (MDO) is gaining increasing prominence as a military engagement model that seeks to synchronise capabilities across land, maritime, air, space, cyber and cognitive domains. This approach allows for coordinated and simultaneous effects, thus

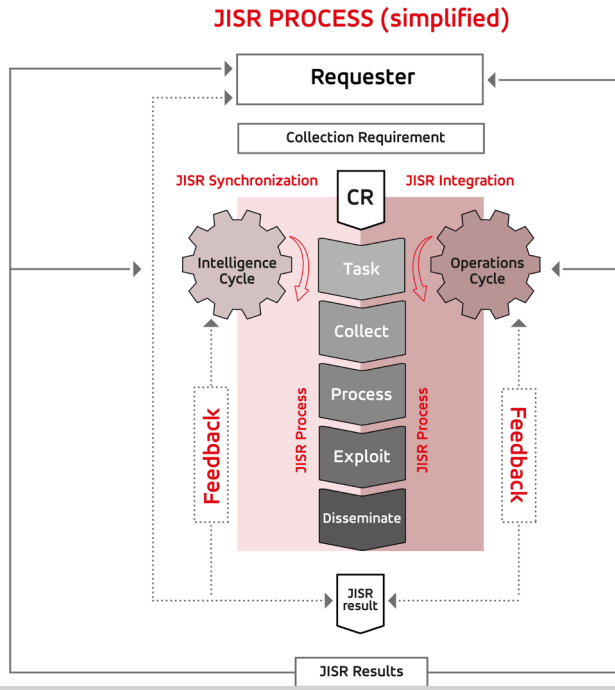


Figure 2. Relationship between the Intelligence Cycle and its Integration in Operations

exploiting cross-domain synergies and reducing response times to complex and dynamic threats.

Within this new operating environment, which is deeply digitised and characterised by a dense mesh of sensors and information sources, what is informally referred to as a "transparent battlefield" has emerged. This new reality is not so much a desired capability, but the inevitable result of hyper-connectivity: military and civilian sensors, unmanned platforms, social networks, smart devices and satellites generating constant, multi-domain information. Everything emits, everything is observed, everything leaves a trace.

The direct consequence of this transformation is that the JISR process has had to adapt to an ecosystem where data accessibility, accuracy and velocity have become critical operational variables. In a constantly monitored environment, any relevant event can be detected, geolocated, interpreted and shared, making the ability to act quickly a decisive factor.

In this context, the merging of information from multiple sources of imaging (IMINT), signals (SIGINT), open sources (OSINT) and combining it with geospatial intelligence (GEOINT) or human intelligence (HUMINT) becomes the core added value provided by the JISR system. This level of integration is benefiting from Artificial Intelligence (AI), which automates

operations, detects patterns, signals anomalies and facilitates real-time decisions.

AI, together with the other innovative technologies described in this chapter, such as edge computing, advanced sensing or distributed systems, acts as a catalyst for change. The ISR process should therefore be a distributed system, fed by data from multiple domains, aimed at generating useful, timely and verifiable information.

4 NATO and European initiatives related to the intelligence cycle

Information density has increased exponentially with the inclusion of commercial sensors, autonomous platforms, small satellite constellations, HAPS (High Altitude Platform Systems), IoT (Internet of Things) systems and open data. All of this forms an environment where the challenge is not only to collect information, but to organise, exploit and share it effectively, in a way that ensures consistency and accessibility in real time.

In this environment, NATO has introduced the concept of "persistent monitoring"[3] as a key requirement to ensure an effective response to this new operational reality. This monitoring requires integrating means across multiple domains and developing new structures, processes and capabilities. The ability to use and merge different tools will be essential to achieve this goal.



Figure 3. Alliance Ground Surveillance (AGS) RQ-4D "Phoenix". NATO photo

[3] The future of NATO- C4ISR-Assessment and recommendations after Madrid and "The Future of NATO C4ISR" (NCI Agency). JDN 1/23 (UK) and allied agencies doctrine.

This includes the *Allied Persistent Surveillance from Space* (APSS) initiative, which seeks to establish the capability for surveillance from space and integrates national and commercial assets to provide ISR products to support joint decision-making. This capability includes the collection, analysis and dissemination of data from satellites and space-based sensors, supported by Artificial Intelligence tools, and under shared standards such as STANAG 4559[4], which aims to promote interoperability for intelligence, surveillance and reconnaissance exchange between NATO-accessible C4ISTAR (Command, Control, Communications, Computers, Intelligence, Surveillance Target Acquisition and Reconnaissance) systems.

The European Union, in turn, through the *2023 Capability Development Plan* (CDP) of the European Defence Agency (EDA), has identified the development of persistent, interoperable and data-driven C4ISTAR capabilities for collective defence, crisis management and strategic resilience as a strategic priority.

Additionally, the European Defence Fund (EDF) has funded multiple innovation projects aimed at boosting European ISR architecture:

— LOTUS, focusing on unmanned ground platforms for surveillance and reconnaissance.

— ODIN'S EYE, aimed at space-based early warning and strategic observation sensors.

— ABIDE, which explores the use of Artificial Intelligence and big data for decision-making in C4ISR.

— REACT, focusing on data fusion and federated ISR systems architecture.

— SAURON, specialising in persistent surveillance for critical infrastructure protection.

These initiatives demonstrate a clear commitment to open, distributed and collaborative architectures, capable of strengthening European innovation and technological autonomy and its integration with allied capabilities.

5 Transformation of the JISR process: from the classical to the digital and multi-domain model

The conditions described in the previous sections, together with the innovation brought by emerging and disruptive technologies, require a profound rethinking of the organisation, implementation and architecture of the JISR system.

[4] STANAG 4559- NATO standard ISR Library Interfaces and Services.

The transition to the digital age has created a profoundly transformed operating environment, where information in the public domain, whether from social networks, urban sensors, smart devices or machine-to-machine communications, surpasses traditional military sources in volume and diversity. This change has blurred the boundaries between the civilian and military spheres.

The volume, variety and velocity of data is outstripping manual processing capacity and today's operations are taking place simultaneously in multiple domains. Additionally, the capabilities of allies and partners are integrated, with diverse technical architectures and increasingly decentralised sources of information. The proliferation of sources and formats requires systems that are capable of operating in networks, in federated environments and with semantic interoperability, in order to avoid duplication, ambiguity or bias in the production of the information required in the process.

This evolution poses specific challenges for the JISR process, stemming from the characteristics of big data: volume, variety, velocity and veracity. The ability to obtain data is no longer the main issue, rather its validation, prioritisation, merging and efficient exploitation in a timely manner.

This new scenario calls for a distributed, automated, multi-domain ISR system, one that is capable of integrating heterogeneous data streams, operating flexibly, and generating useful information in real time[5]. Digitalisation is reinforcing this trend and facilitating the convergence of ISR capabilities, electronic warfare, cyber defence and combat platforms. In this new paradigm, ISR is consolidated as a core functional capability, which extends beyond its traditional role of auxiliary support and is linked transversally to operation planning, execution and assessment processes.

To operate effectively in today's challenging environment, ISR architectures must be designed, implemented and managed according to a set of fundamental operating principles and criteria[6]:

— Flexibility: in order to adapt quickly to changes in the operational environment. This involves dynamic reconfiguration of sensors, automated prioritisation and adaptation to new threats or areas of interest.

— Tailor-made mission: so that each ISR deployment responds to the specific needs of the operation, depending on the domains involved and the type of information required.

[5] As noted in all NATO doctrine documents, the UK's JDN 1/23 and the Science & Technology Trends 2023-2043, this is an ongoing transformation.

[6] UK Joint Doctrine Note 1/23 (JDN 1/23), which adapts the basic principles of JISR process design according to NATO, with a more explicit and modern exposition.

— Interconnectivity: ensuring seamless integration between sensors, platforms, command levels, operational domains and alliance partners. Both vertical and horizontal connection between ISR capabilities should be facilitated.

— Compatibility: through compliance with common technical and doctrinal standards, such as those defined by NATO or EU interoperability frameworks. This allows ISR products to be shared in multinational environments.

— Automation: ISR networks should operate with the highest possible degree of automation and allow for autonomous prioritisation and timely activation of sensors.

— Scalability: they must have sufficient capacity to accommodate data volume growth and include resources for storage, analysis and secure dissemination.

— Bandwidth and connectivity: the architecture must guarantee a robust, secure communications infrastructure capable of supporting intensive data flows, minimising latency and ensuring availability under adverse conditions.

— Resilience and redundancy: so that the architecture can maintain basic functionality even in degraded environments. When the integrated network is unavailable, alternative structures should be activated to ensure continuity in the collection and dissemination of the necessary information.

This set of principles and technical transformations has one ultimate goal: to ensure that the ISR system is not only responsive to the operational needs of today, but that it is prepared to adapt, anticipate and operate reliably in increasingly interconnected, competitive and information-rich environments.

6 The impact of emerging technologies on the JISR process

Technological innovation is rapidly transforming the JISR process. This evolution affects its entire architecture: from the expansion of sensors and information sources to the automation of information analysis and dissemination processes.

Both NATO and the European Union have identified a set of priority technology areas, known as emerging and disruptive technologies that are redefining operational models, military capabilities and how intelligence is generated in modern environments.

In the case of NATO, the classification of Emerging and Disruptive Technologies *(EDT)* includes ten broad categories: Artificial Intelligence

(AI), autonomous systems and robotics, big data and information technologies, space, hypersonic systems, energy and propulsion, advanced materials, electronics and electromagnetics, quantum technologies, and human enhancement technologies and biotechnology.

For its part, the European Union, through the EDA and the European Defence Fund, has developed a convergent agenda that focuses on strengthening strategic autonomy, the electromagnetic environment, cyber defence, space, unmanned platforms and collaborative sensors.

This convergence in NATO and EU strategic priorities is evidence of a clear alignment in terms of the essential role to be played by these technologies in the future development of military capabilities.

This technological development is rapidly transforming the intelligence cycle. This evolution is not limited to the automation of data analysis, but affects the entire ISR architecture, from sensor proliferation to decentralised real-time exploitation.

The impact of some of them on the different phases and dimensions of the JISR process is analysed below.

6.1 AI and edge computing

One of the main challenges of the JISR process is to effectively manage the huge volume of data generated by distributed sensors, unmanned platforms and open sources. Artificial Intelligence and edge computing are transforming this process, automating complex analytical tasks, reducing response times and optimising the decision-making cycle.

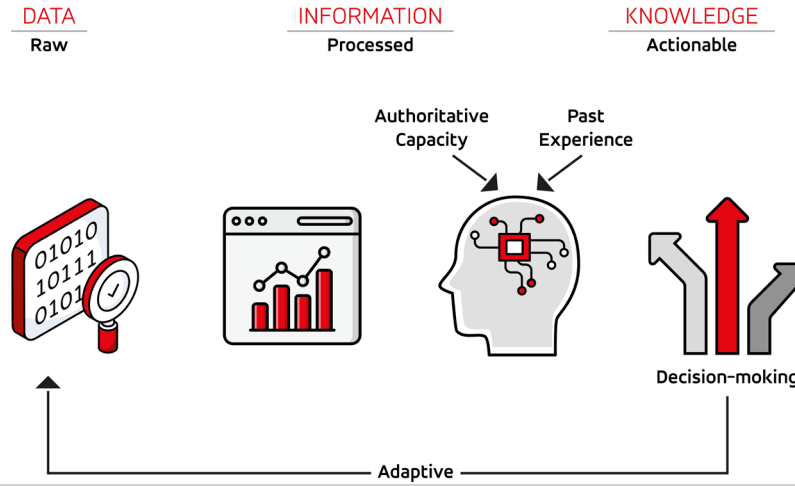


Figure 4. Flow of data to information. Source: Internetofwater.org

AI facilitates data fusion from multiple sources (IMINT, SIGINT, OSINT, GEOINT, HUMINT) and makes it possible to detect patterns, anticipate threats, classify objects or generate real-time alerts. It also helps to reduce the operator's cognitive load, prioritise what is relevant and deliver products ready for operational exploitation.

In parallel, edge computing makes it possible to process information directly at the sensor or on platforms close to the point of collection, without the need to send it to centralised centres. This capability improves operational autonomy, increases resilience to network disruptions and is especially useful in UAVs, sensors deployed in remote areas, or systems operating in degraded environments.

Digitisation driven by the Internet of Military Things (IoMT) creates new demands on interoperability, connectivity and data management. This technological evolution is favouring the deployment of autonomous or swarming platforms, which can act in a coordinated manner, with human supervision more focused on the effects than on the technical management of the system.

This transformation also has a direct impact on the professional profiles required. Operators with hybrid capabilities who are able to interact with intelligent systems, interpret automated outputs, and make decisions in highly digitised environments, are in demand. This will force the adaptation of ISR education and training programmes, with a more technical, cognitive and multi-domain approach.

6.2 Expansion and diversification of sensors

Sensors are the basis of the JISR process. Advances in technology have enabled the deployment of a wide range of sensors in all operational domains (land, sea, air, space, cyber and cognitive) with the ability to collect optical, thermal, acoustic, electromagnetic or gravitational data. Miniaturisation and improved energy efficiency have increased the persistence, adaptability and coverage of these systems in complex, multi-domain environments.

The concept of a network of interconnected sensors makes it possible to set up distributed surveillance systems, where information is collected, transmitted and analysed in a collaborative manner. The implementation of advanced processing in the sensor itself, combined with edge computing, reduces the need to transmit large volumes of data, improves information reliability and optimises bandwidth usage.

Additionally, civil and commercial sensors, such as those embedded in social networks, mobile devices or IoT systems[7], extend the capabilities of

[7] Internet of Things.

the ISR process. These devices, which collect video, audio, satellite positioning or proximity data, provide complementary sources of information with high operational value, especially in urban or hybrid environments.

The integration of data from social networks and traditional sensors will make it possible to progress in tasks such as filtering and summarising content, detecting and monitoring events, analysing social dynamics and identifying anomalies in real time. This merging of sources and technologies enhances the ability to respond to emerging threats and consolidates a more accurate, adaptive and resilient intelligence ecosystem against electronic or cyber threats.

6.3 Use of unmanned platforms

The use of unmanned platforms (UxV) has brought about a qualitative change in intelligence, surveillance and reconnaissance capabilities. Their integration into operations is now a reality, driven by their ability to operate at low risk, maintain long dwell times and position themselves flexibly in complex or difficult-to-access environments.

In particular, unmanned aerial vehicles (UAVs) in all their different categories: micro, mini, tactical or strategic, allow different areas of interest to be covered with light sensors (EO/IR, radar, magnetic, among others), thus maintaining adaptive and continuous surveillance. These platforms have proven to be particularly effective in protracted operations, patrol missions and environments with little traditional ISR coverage.

In urban or asymmetric combat scenarios, deployable micro-UAVs are significantly improving real-time situational awareness. They facilitate



Figure 5. AUREA Avionics Class I SEEKER unmanned ISR system

target acquisition, immediate reconnaissance and force protection, while reducing risk to deployed personnel.

In parallel, coordinated UxV swarm capabilities are being developed, in which multiple units cooperate autonomously through dynamic task sharing. These architectures will extend ISR coverage, reduce response times, and optimise resources in distributed and multi-domain operations.

The massive and intelligent use of UxV will continue to grow, especially when integrated with AI, edge computing and interoperable ISR networks. Their role as dynamic gathering nodes will consolidate their value within the JISR ecosystem.

6.4 Quantum technologies

Quantum technologies, although still in nascent stages of development, are emerging as key disruptive enablers for the JISR process in the 2030-2040 horizon. Their transformative potential encompasses information gathering, communication, analysis and protection capabilities, with direct implications in all operational domains.

Firstly, quantum sensors will make it possible to detect gravitational, geomagnetic or inertial variations with extreme precision. This capability will be especially useful in environments where satellite navigation systems have been denied or degraded. It is also expected to be used for underground mapping, navigation in GNSS-denied environments or tracking underwater objects, extending ISR capabilities in harsh environments.

Secondly, quantum communications, especially through quantum key distribution (QKD) techniques, will enable transmission links that are virtually immune to interception or external tampering. These solutions will boost the security of ISR networks between mobile platforms, distributed nodes and spatial links.

Finally, quantum computing offers a theoretical capability to solve complex problems that cannot be tackled with current systems. Its potential application in big data analysis, mission optimisation, advanced simulation of operational scenarios, or real-time decision-making could entail a quantum leap for the JISR system. However, these applications still face significant technical challenges, such as qubit stability, extreme operating conditions or system scalability.

According to the NATO Science & Technology Trends 2023-2043 report, quantum sensors are the closest to real operational application, while quantum communications and quantum computing will require more time to reach functional maturity. Even so, their early development will be essential to maintaining information superiority and resilience in the face of technologically advanced actors.

6.5 Space / Satellites

Space has established itself as a critical strategic domain for modern ISR capabilities. Its value lies both in intelligence gathering and in surveillance, observation and information superiority in complex operational environments. Over the next decade, space capabilities are expected to increase exponentially, driven by the miniaturisation of platforms, decreased launch costs and the technological maturity of orbital systems.

One of the most significant developments is the proliferation of small satellites or smallsats in low (LEO) and medium orbits (MEO). These platforms, which are cheaper and more flexible than traditional large satellites, allow for more frequent monitoring, have greater resilience to anti-satellite threats, and possess more agile observation capabilities. Constellations of smallsats, equipped with optical, infrared or synthetic aperture radar (SAR) sensors, offer increasingly competitive resolution and latency.

Within this context, NATO's *Allied Persistent Surveillance from Space* (APSS) initiative, mentioned in previous sections, promotes the development of an allied space-based persistent surveillance architecture. This capability will integrate national and commercial assets to provide ISR products based on satellites and on-board sensors, combined with advanced processing, data fusion and Artificial Intelligence tools. All of this under NATO standards such as STANAG 4559, which ensure interoperability between allies.

In parallel, intermediate solutions such as HAPS (High-Altitude Pseudo-Satellites) are being developed. Within the framework of PESCO and the

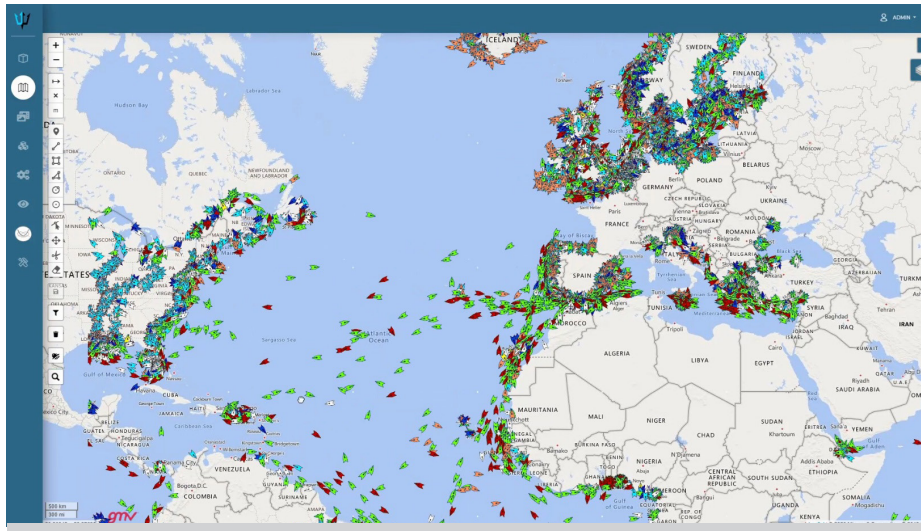


Figure 6 GMV's C2 SOCRATES system for vessel detection and classification

European Defence Fund, the EuroHAPS project is experimenting with strategic airships, hybrid platforms and stratospheric balloons, designed to operate for long periods of time. These lightweight platforms offer persistent surveillance in scenarios where satellites may have limitations.

Finally, new generation satellite programmes for military communications, such as SPAINSAT *Next Generation* (SPAINSAT NG), are designed to enhance secure connectivity and information flow resilience in joint and multi-domain operations. Their integration into interoperable ISR architectures will be essential to ensure information dominance and operational continuity across the mission spectrum.

6.6 Hypersonic systems

The possibilities of using hypersonic platforms for ISR purposes are currently being explored and take advantage of their high speed and low detectability to perform high-altitude strategic reconnaissance missions. This type of platform would permit a more agile and flexible collection of data and information than that offered by traditional satellites, especially in scenarios where timely, rapid and difficult-to-detect coverage is required.

From a threat perspective, hypersonic systems represent an emerging technological challenge of the highest order. Their combination of extreme speed, manoeuvrability and low signature makes them difficult to detect, track and intercept. These characteristics force a redesign of current early warning, monitoring and response architectures, as they drastically reduce the time margins for decision-making.

To address them, it will be necessary to integrate distributed sensor networks, both ground and space-based, supported by automated analysis and Artificial Intelligence capabilities. Only an adaptive ISR architecture, with multi-domain detection and near real-time response capability, can provide effective coverage against such threats.

6.7 Cross-cutting trends in emerging SRI technologies

In addition to the specific technologies already analysed, there are lines of development with a cross-cutting impact on the JISR ecosystem and they provide complementary capabilities that reinforce its accuracy, adaptability and resilience.

New materials, such as advanced metals, smart coatings or self-cleaning surfaces, allow for more powerful antennas, lighter and stronger structures, and components capable of operating in extreme conditions. Additive manufacturing is revolutionising military logistics by enabling the *on-site* production of critical parts for sensors or ISR platforms.

In the field of biotechnology, biometric sensors are being incorporated into combatants' equipment, allowing real-time monitoring of the operator's physical and cognitive status. These technologies, combined with advanced interfaces and augmented reality, contribute to improved situational awareness and decision making under pressure.

Advanced energy technologies, such as new generation batteries, electric propulsion systems or directed energy weapons (lasers, microwaves), will enable the deployment of more sustainable, silent and autonomous ISR platforms. This is especially relevant in prolonged missions and denied environments.

Finally, the convergence between Artificial Intelligence and quantum computing opens up new possibilities for complex data analysis, scenario simulation and secure communications management. These capabilities will connect distributed ISR networks across all domains (land, maritime, air, space, cyber and cognitive), with greater accuracy, speed and resilience.

These trends will not only extend traditional ISR functions, but also contribute to a more distributed, robust and adaptive environment. Their adoption should be based on ethical principles, allied regulatory frameworks and interoperability criteria to ensure operational effectiveness and secure integration in multinational environments.

7 Possible improvements at each stage of the JISR process

As seen above, the JISR process is structured around five phases known as TCPED (Task, Collect, Process, Exploit, Disseminate). Each of these phases has classically been addressed through sequential procedures and specialised systems. However, digital transformation and the introduction of disruptive technologies are enabling concrete advances that could boost the efficiency of each stage.

In the following sections, these improvements are described with an approach based on the application of the technologies described above, in a realistic manner and based on the knowledge available in GMV thanks to the development of the JISR SAPIIEM tool suite[8]. These tools have proven successful in a number of NATO exercises, including Unified Vision, Steadfast Cobalt, MAJEX, OPTIMAX, Trident Juncture and others.

7.1 Tasking – Resource planning and allocation

The phase of tasking and intelligence needs management has traditionally been a slow, manual process, highly dependent on the operator's experience.

[8] SAPIIEM is the JISR product suite, compatible with NATO interoperability initiatives (STANAG) and NATO doctrine, developed by GMV.

However, the progressive integration of Artificial Intelligence is transforming this stage and makes it possible to automate tasks such as the identification of zones or areas of interest where resource-gathering resources, the optimal allocation of ISR resources, or the prioritisation of requirements based on operational criteria, availability and context will operate.

Exercises such as JFX9 have demonstrated that establishing more flexible working dynamics, supported by tools such as SAPIIEM, significantly improves the planning and traceability of information gathering. Tailored interfaces and smart assistants will allow future scenario simulations, identifying redundancies in requirements or proposing alternative allocations based on changes in the operating environment.

7.2 Collection – Information gathering

The data collection phase benefits directly from the proliferation of ground, naval, air, space and cyber sensors. The deployment of state-of-the-art UAVs, distributed sensors and IoT networks enables more persistent, diverse and automated information gathering, adapted to increasingly complex operating environments.

The use of Artificial Intelligence in this phase allows sensors to be dynamically programmed, redirected in case of unforeseen events, or to autonomously activate observation platforms. This type of automation improves the efficiency of the system and makes it possible to respond more quickly to new gathering needs.

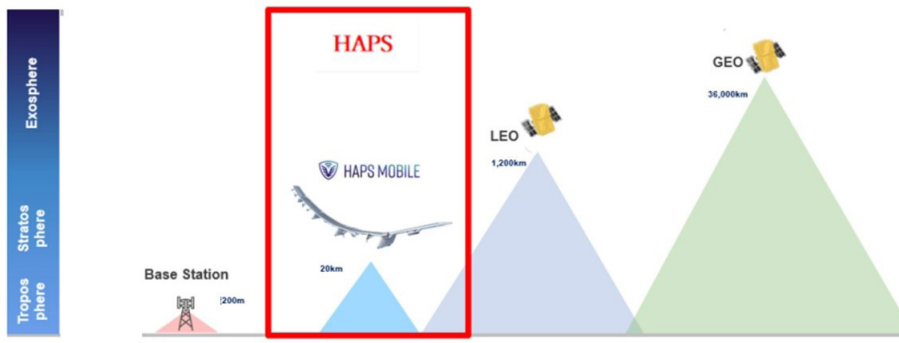


Figure 7. Altitudes operation HAPS. Source HAPS Alliance

[9] Joint Force Exercise, a Spanish national military exercise organised by the Joint Defence Staff of the Armed Forces (EMACON). Its objective is to train the operational structure of the Spanish Armed Forces in the planning and implementation of joint operations and to integrate ISR, C2 systems, etc. It is conducted on an annual basis.

It is especially useful in dense urban environments, where technologies such as tactically deployable micro-UAVs will facilitate surveillance, force protection and real-time data collection, even in adverse or degraded conditions.

7.3 Processing – Processing and classification of data and information

Data processing is a critical phase, where the collected information is organised and structured. Thanks to edge computing, many processing tasks can now be performed at the sensor itself or at nearby nodes, reducing latency and improving resilience to network outages.

Additionally, AI-based object recognition techniques can automatically catalogue information from sensors, satellite images or videos. These tools can detect anomalies, tag data and even generate useful metadata for further exploitation.

7.4 Exploitation – Data and information analysis

Data mining has traditionally been a human-intensive task. Today, thanks to big data, machine learning and new automated analytical techniques, it is possible to mine large volumes of data faster, thereby detecting hidden patterns and generating information that can be used to develop intelligence in less time.

Artificial Intelligence already enables intelligent natural language searches (NLP), automatic summaries or even generating content directly from structured information through RAG (Retrieval-Augmented Generation) systems. These capabilities allow the analyst to concentrate on validation, contrasting and contextualisation tasks and leave repetitive primary analysis functions to the algorithms.

The objective of this phase remains the same: to generate relevant and timely information adapted to the decision-making level, but with a degree of automation that accelerates the processes within this phase, improves traceability, and allows for a more agile reaction to evolving scenarios.

7.5 Dissemination – Distribution and use of information

In this phase, the aim is to ensure that information and data reach the right user, at the right time and in the most useful format. To achieve this, interoperable systems, secure networks, and an architecture based on the "one data" philosophy are essential.

Tools such as SAPIIEM make it possible to synchronise ISR nodes and ensure traceability from the information requirement until its dissemination.

At the same time, newer platforms introduce interactive, adaptive and reusable intelligence products that dynamically adjust to the user profile and operational context.

Artificial Intelligence also contributes to this phase through functions such as the automatic generation of personalised summaries or the automatic classification of products according to their purpose (planning, targeting, operations). These capabilities help to avoid cognitive overload for the user and to ensure that information is delivered in optimal conditions for exploitation.

7.6 Lessons learned and conditions for success

To fully exploit the potential of emerging technologies applied to the JISR process, it is essential to combine a clear and flexible organisational structure, staff trained in ISR tools, revised and automation-oriented processes, and a culture of real interoperability between levels and domains.

Exercises such as JFX-22, organised by the Joint Defence Staff (EMACON), have shown that these conditions are not just theoretical. In this context, tools such as SAPIIEM were used to manage the IRM&CM process and the exploitation of information. The results revealed substantial improvement in traceability, coordination between levels and speed in the generation of useful products.

Furthermore, the ATENEA suite has demonstrated its potential to integrate planning, allocation and operation in a single digital platform, increasing the consistency of the process and facilitating its adaptation to different scenarios. Advance training of operators and unification of doctrinal criteria were key elements for their effective implementation during the exercises.

These exercise experiences show that the technological transformation of the JISR process requires both technical solutions and cultural and doctrinal changes, aimed at a more efficient exploitation of information.

8 Interoperability and the “one data” philosophy

One of the main challenges of the JISR process is to ensure that the information generated is accessible, consistent and usable by all units and actors involved in a joint operations environment. In multi-domain scenarios and multinational operations, interoperability is no longer a desirable ideal but an indispensable condition.

No ISR system today operates in isolation. The integration of national, allied and commercial capabilities requires that sensors, platforms, command systems and analysis tools share not only data, but also common formats, protocols and languages. This is especially critical in the context of

NATO or EU operations, where success depends on generating a common operational picture based on shared and validated intelligence.

Interoperability must be addressed at three levels: technical (hardware, software and connectivity), semantic (consistency in data interpretation) and organisational (processes and doctrine). Lack of interoperability leads to fragmentation, delays and loss of efficiency in decision-making.

Within this context, the "one data" philosophy becomes a guiding principle. It consists of a sensor-derived, analyst-generated or AI-produced data that is recorded only once and made available, in a secure and traceable way, to all authorised users. This approach avoids duplication, improves analysis quality and allows:

— Traceability and version control.

— Reducing load on tactical networks.

— Cross-exploitation using AI tools.

— Consistency and speed in the decision cycle.

Its implementation requires distributed architectures, secure networks, common technical standards and an organisational culture based on the need to share, not just the need to know.

NATO has developed standards such as STANAG 4559, which regulates the operation of *Coalition Shared Data* (CSD). Platforms such as INTEL-FS and BICES allow intelligence to be shared in a structured manner between allied analysis centres.

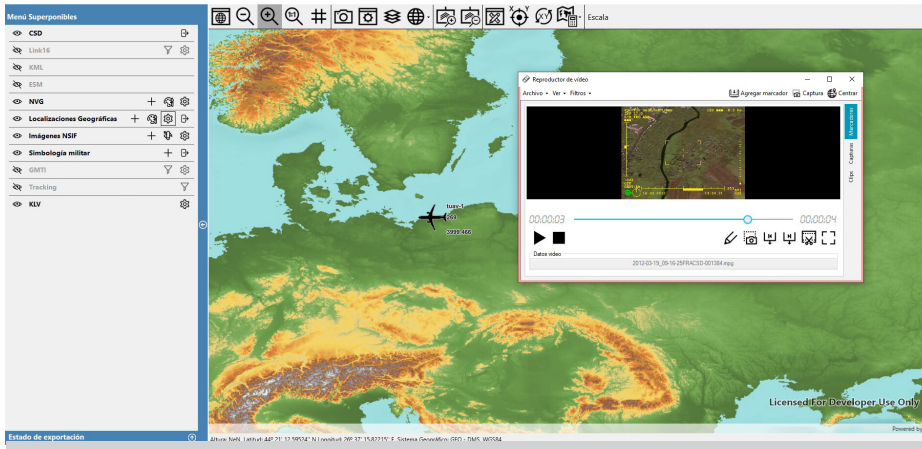


Figure 8. GMV SEISMIC SYSTEM

At the national level, the SAPIIEM system has demonstrated its compatibility with these international structures, both in joint exercises[10] and in actual operations. These infrastructures allow the JISR process to operate in a federated manner, thereby increasing collective efficiency and accelerating the generation of useful intelligence.

9 Technological innovation as a threat to the JISR process

Up to this point, the chapter has outlined the opportunities offered by emerging technologies in transforming the JISR process. However, the same technological innovation also creates new vulnerabilities that cannot be ignored. In many cases, the same tools that boost system efficiency (AI, smart sensors, automation, edge computing) also expand attack surfaces to operational, cyber or cognitive risks.

This section looks at two of the most critical areas where innovation may pose a threat: the cybersecurity of the JISR process and the vulnerabilities of Artificial Intelligence.

9.1 The importance of cybersecurity in the JISR Process

While the digitalisation of the JISR process has multiplied its capabilities, it has also increased its exposure to cyber threats. The incorporation of distributed sensors, information-sharing networks, diverse platforms, automated analysis tools and interconnected command and control systems has made ISR environments a prime target for hostile actors. In this context, it becomes no longer just a question of protecting physical infrastructure, but of ensuring information integrity, availability, traceability and confidentiality throughout all phases of the cycle.

The JISR ecosystem depends on a secure interconnection between sensors, processing nodes, operating platforms and end-users. Each of these elements can become an attack vector. For example, sensors can be spoofed, networks can be saturated or tapped, algorithms can be attacked by adversarial AI techniques[11] and intelligence products can be intercepted or altered during transmission.

These threats are not hypothetical. In exercises and in real operations, multiple attack vectors have been identified: insertion of false data, interception of information flows, denial of service to critical ISR platforms or

[10] The JFX has been mentioned previously.

[11] Science & Technology Trends 2023-2043, volume 2. This paper describes the adversarial use of Artificial Intelligence and machine learning as a collection of techniques designed to hinder or deceive intelligent systems, impacting military sensors, weapons systems and decision support systems.

even alterations in the logic of automated processing systems. This makes it clear that the JISR environment must be actively protected against cyber threats.

In multinational contexts, such as NATO or EU frameworks, the exchange of information between allies requires special attention to network security, encryption, authentication and traceability. A single node failure can compromise the security of the entire network. Interoperability must therefore be accompanied by common, robust and auditable cybersecurity safeguards.

The architecture of JISR processes and systems should be designed from the outset under the principle of *security by design*12 and integrate cyber security as a structural part of the system and not as an afterthought. This includes access controls, intrusion detection, process auditing, data validation and resilience to failures throughout the entire cycle.

It is also essential to boost security culture among operators, analysts and intelligence cycle managers. The human factor continues to be one of the most relevant risk vectors, especially through unintentional errors. Awareness raising, continuous training and best practice protocols are key elements in mitigating these risks.

Finally, the development of active cyber defence capabilities specific to JISR environments should be considered a priority line of action. This includes dynamic protection of sensors and links, constant monitoring of processing and operating platforms and the ability to recover quickly from incidents. This requires close cooperation between cyber defence managers, system developers and intelligence analysts.

9.2 Biases and vulnerabilities of Artificial Intelligence in the JISR process

The deployment of Artificial Intelligence technologies in the JISR process heralds a substantial improvement in the speed, accuracy and adaptability of operations. However, this transformation also brings new operational risks that must be carefully considered. Some of the most significant include algorithmic biases, opacity of decision models and vulnerability to manipulation or cognitive attacks.

One of the key challenges is training bias. AI models used for image classification, threat detection or behavioural analysis are trained on previously defined datasets. If this data is incomplete, mislabelled or reflects historical or contextual biases, the system may reproduce or amplify errors, leading to critical false positives or false negatives in operational environments.

[12] Science & Technology Trends 2023-2043 - NATO

This could mean wrong decisions, faulty prioritisation, or even unintended consequences.

Additionally, many deep learning models operate as "black boxes", which are difficult to audit or explain. This lack of transparency has a direct effect on the commander's confidence in automated systems, especially when decisions must be made quickly and under high pressure.

Another critical point is vulnerability to adversarial attacks. There are techniques (adversarial AI) that can manipulate the results of an AI system which minimally modify the input data (images, signals, text). These techniques could be used to confuse algorithms and generate errors in the exploitation phase of the JISR process. This risk is especially relevant in hybrid conflicts, where hostile actors may have sophisticated cyber capabilities.

The integration of AI into distributed architectures, such as edge computing or autonomous platforms, expands the JISR system's exposure to cyber-attacks or systemic failures. The proliferation of smart sensors and process automation means that any undetected errors in AI can be quickly replicated and scaled across the network.

Artificial Intelligence can multiply capabilities to an unprecedented degree in the JISR environment, but only if it is managed responsibly. In view of the aforesaid risks, it is essential to develop and implement AI solutions under principles of security, explainability and robust governance, so that measures such as the following are incorporated, among others:

- Continuous validation of training data.
- Assessment of biases and explainability of models.
- Simulation of scenarios to strengthen systems.
- *Human-in-the-loop* / *Human-on-the-loop* supervision of critical decisions.
- Governance of algorithms under NATO/EU regulatory frameworks.

10 Conclusions

Innovations stemming from emerging and disruptive technologies, identified as priorities by NATO and the European Union, are redefining military capabilities, intelligence cycles and decision-making processes in a cross-sectoral fashion. Smart sensors, unmanned platforms, big data, quantum computing, advanced materials or space technologies are already part of an increasingly interconnected, automated and distributed ISR system.

This technological revolution not only affects the technical level, but also the doctrinal and organisational level. ISR architectures must adapt to an environment where information is abundant, diverse and generated from multiple sources, many of them outside the traditional military domain. Within this scenario, the JISR process becomes a continuous, horizontal, multi-domain capability, which must be able to operate in real time and integrate useful data from the tactical to the strategic levels.

Within this set, Artificial Intelligence has established itself as the most immediate, innovative and transformative driver of change. Its application throughout the TCPED process allows for automated resource allocation, dynamic planning, threat anticipation, processing large volumes of data, and faster delivery of information. Artificial Intelligence does not replace the human factor: it must empower it, freeing it from repetitive tasks and allowing it to focus on critical analysis, validation and decision-making.

This transformation also reaches the platforms, which become not only advanced ISR sensors, but also elements that are capable of collecting and even pre-processing information in real time. Their integration with cyber defence, targeting or electronic warfare systems enhances operational consistency and effectiveness in complex environments.

In this sense, the SRI architecture of the future should be:

— Flexible, in order to adapt to changing scenarios.

— Interconnected, to integrate sensors and domains.

— Automated, to speed up the decision cycle.

— Scalable and secure, to manage the volume of data and protect its integrity.

Additionally, this more connected, automated and intelligent ecosystem must be underpinned by a cross-sectoral and adaptive cyber security strategy which ensures business continuity and protects the information advantage from sophisticated and persistent threats.

In short, innovating in ISR means anticipating, adapting and deciding with a head start. Success will not depend on who obtains the most information, but on who can protect, share, exploit and turn it into timely and accurate decisions faster and more reliably.

The constant transformation of the JISR process is not just a technological challenge, it is an unavoidable strategic necessity.

Bibliography

European Defence Agency. (2023a). *Enhancing EU military capabilities beyond 2040. Main findings from the 2023 Long-Term Assessment of the Capability Development Plan*. European Defence Agency (EDA). DOI: 10.2836/360180.

European Defence Agency. (2023b). *The 2023 EU Capability Development Priorities*. European Defence Agency (EDA).

Gómez Gómez, Juan de Dios. (2025). ESFAS. La inteligencia de comunicaciones contra el crimen organizado: un arma fundamental ante la amenaza híbrida. *Noticia IEEE 09/2025*. [Accessed 24 March 2025].

Gómez González, Á. (2021). Trends in the evolution of military intelligence. IEEE Opinion Paper 35/2021. [Accessed 5 February 2024].

Gordon B., D. Jr. (The future of NATO C4ISR after Madrid summit. Assessment and Recommendations. NCI Agency. ISBN-13 978-1-61977-273-1.

Kerth, C., Klotz, P. and Essendorfer. (2019). *A new approach for information dissemination in distributed JISR coalitions*. Proc. SPIE 11015, Open architecture / Open Business Model Net-Centric Systems and Defense Transformations 2019. Fraunhofer IOSB. 110150N. [Accessed 10 March 2025]. Available at: https://publica-rest.fraunhofer.de/server/api/core/bitstreams/e23811eb-b3a6-432f-8250-64cc94c02b99/content

Kerth, C.; Klotz, P. and Essendorfer, B. (2020). *A new approach for information dissemination in distributed JISR coalitions*. Karlsruhe, Fraunhofer IOSB.

Ministry of Defence (UK). (2023). *Joint Doctrine Note 1/23 Intelligence, Surveillance and Reconnaissance*. Gov.uk. [Accessed 2025]. Available at: https://www.gov.uk/government/publications/intelligence-surveillance-and-reconnaissance-jdn-123

NATO. (2022) *Strategic Concept for the Alliance at the Madrid Summit on 29 June 2022*. NATO.

NATO Science & Technology Organisation. (2023). *Science & Technology Trends 2023-2043. Across the Physical, Biological, and Information Domains*. Volume 1. NATO Science & Technology Organisation.

Pérez-Breva, L. (2018). Innovar: un manifiesto de acción. Deusto. ISBN 978-84-234-2933-2.

Sánchez Sánchez, J. L. (2025) Artificial Intelligence in support of military intelligence. Fundamental axis of success or failure in the strategic competition between great powers. *IEEE Analysis Document 09/2025*. Ministry of Defence, Spanish Institute for Strategic Studies.

Spain. (2021). Royal Decree 1150/2021, of 28th December, approving the 2021 National Security Strategy. *Official State Gazette*. 31 December, no. 314, pp. 167795-167830.

Article Ten

Adapting new technologies in the JISR community. Specific characteristics of the maritime domain

Alfonso Herrero Pita

Abstract

For decades, intelligence communities have been adapting to the new paradigm introduced by the information revolution. This process has entailed a profound alteration of organisational structures, connecting and synchronising hierarchically dispersed entities as a result of the need for instant access to information, speed of information flows and decrease in the times required for its exploitation.

The implementation of the JISR capability exemplifies this evolution of intelligence agencies to adapt to the scenario introduced by this revolutionary form of interacting with information, and brings about a profound transformation in the concepts of operation, doctrine, organisation, command and control and training.

Transforming new JISR concepts and strategies into actual full operational capability is not straightforward. The integration of tools entails a challenge for the organisational structures where these are to be implemented.

Translating these changes to the execution of ISR operations in the maritime sphere brings specific challenges due to the unique organisation of a naval force in a Maritime Component Command (MCC), where there are PED centres, usually with limited capabilities due to the inherent restriction in available bandwidth.

Keywords

Instant access, Standardisation, Interoperability, Data model, Organisational structures.

"[...] The naive view is wrong to believe that creating more powerful information technology will necessarily result in a more truthful understanding of the world [...]"

Yuval Noah Harari

1 The information revolution and the intelligence community

Nothing new can be said about the profound transformation that the information revolution is bringing about in the way we communicate, work, and consume products and services. This transformation shapes every aspect of the world that we live in. And the intelligence community is right at the heart of that revolution, not surprising given that it deals almost exclusively with the gathering, analysis and dissemination of information. The adaptation of intelligence agencies in order to exploit the advantages and opportunities of this revolution, which began decades ago, is profoundly altering their organisational nature.

2 Vectors of change

It is observed that the organisational impact on the intelligence community is primarily driven by two vectors of change:

1. The exponential increase in the set of information targets; due to the proliferation of groups of people and organisations that can operate and organise themselves efficiently outside national governments. Instant access to information and its ease of exploitation, which multiplies the number of actors on the world stage, lead to the emergence of motivations that are increasingly difficult to analyse. As a result, it is not only the quantitative increase of potential threats that poses a challenge, but also the growing complexity of the environment; a complexity that calls for analytical products with multidisciplinary input.
2. New information technologies encourage the implementation of work tools that imply a revolutionary form of interacting with information, solving problems and implementing solutions. The speed of information flows and their instant accessibility stimulate an ecosystem of change that brings about a profound transformation in the concepts of operation, doctrine, organisation, command and control, and training. A fundamental lesson has emerged after years of adaptation: new technologies cannot be fully exploited without a concurrent evolution of the organisation, its processes and doctrine.

3 Adaptation of traditional structures

It is recognised that many intelligence topics today are different from those of years ago, influenced now by instant access, speed of information flows and ease of exploitation. This involves the adoption of new technologies, and their implementation often involves a "disruption of hierarchies" and favours decentralised networks over traditional organisational models.

The factors described above have long been highlighting the need for faster information sharing across the traditional administrative boundaries of centrally planned bureaucracies and hierarchical, vertically organised chains of command. There are certain notions of traditional organisation that have become obsolete for certain functions, notably the traditional model where lower levels report to higher levels until the appropriate higher level of authority is reached.

New organisational schemes have been implemented in intelligence agencies for decades for what were then traditionally static bureaucracies, created in times of scarce information, difficult to obtain and provided exclusively by few entities with accepted credentials of authority. As an example, it is worth pointing to the creation of SIFAS in 2012, one of the organisational milestones driven by the new paradigm, in which functional relationships are established between agencies that carry out intelligence tasks without necessarily being included in the same chain of command, thus providing agility and flexibility to the traditional flow of tasks/information in the intelligence cycle.

One of the most illustrative examples of the adaptation of traditional intelligence structures to the information revolution is the implementation of the JISR capability. However, this adaptation is still far from being translated into an efficient organisation and continuous efforts are required in order to identify challenges and adopt a measured approach to implementing the necessary changes that arise from them.

4 JISR as an innovation paradigm

The implementation of the JISR process in the Spanish Armed Forces is a remarkable example of the process of adapting traditional structures that have been preserved for decades. The existing models tend to break down when information has to be shared faster, across administrative boundaries, where the limits between stages of the traditional intelligence cycle are blurred: that is, providing the client with relevant and timely information through a process of steering, gathering, processing and disseminating.

The new technological environment provides a vast capacity for intelligence gathering and processing, enabling to make the right decisions, but

conversely, the time available to make these decisions is often drastically reduced. JISR is, in a sense, a short-circuit in the formal procedural steps of the intelligence cycle when information is needed in real time. The volume of information available has risen exponentially in ISR missions and the time required to create value from exploitation has shrunk to seconds.

5 Challenges in adapting technology to JISR capability

Consider the TCPED process, which stems from the need for a sufficiently robust and flexible support procedure for ISR sensors in continuous technological evolution. The result of this TCPED process is a JISR product. The TCPED process is executed in the steering and procurement phase of the traditional intelligence cycle and in all phases of the operations and targeting cycle. Thus the JISR result, derived from a single discipline of information obtaining, is further processed in the elaboration phase of the traditional intelligence cycle.

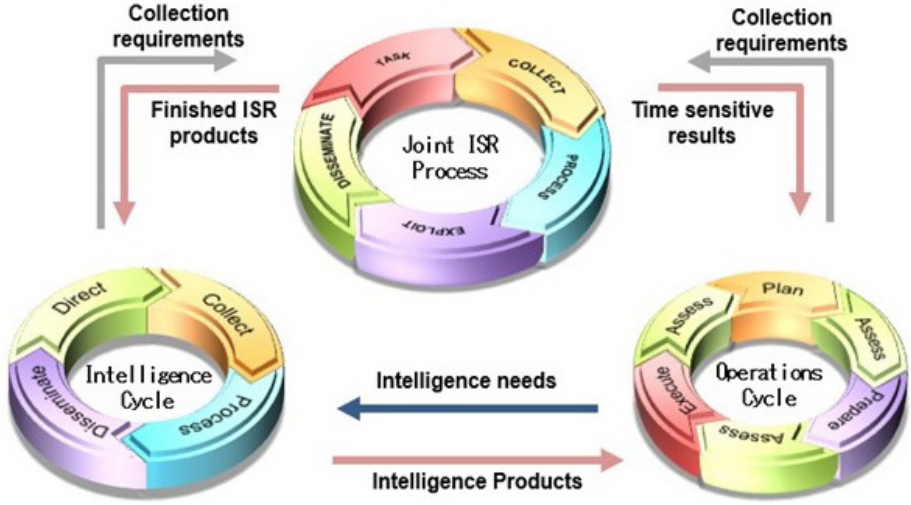


Figure 1. C4ISR NCIA systems presentation

5.1 Original environment

At this point, it is necessary to explore the context in which this capability originated, the environment that led to its emergence. An interesting description of the beginnings of PED may be found in detail in the publication TCPED TACMEMO (US Fleet Intelligence TCPED, 2013). It mentions that the origins of the PED designation were popularised in the 1990s when the need arose for processing and operational centres for a new generation of sensors mounted on airborne ISR platforms in support of

ground forces involved in counter-terrorism and counter-insurgency operations. The demand for real-time EO/IR/SAR/FMV and the development of high-capacity sensors, together with the increasing bandwidth available, led to the concept of data processing and exploitation centres (PED) to provide rapid estimation to time-critical decision-makers.

In short, JISR was born out of a context with requirements derived from:

- Increasing speed and ease of access to information.
- threats/volatile operational environment.
- need for mechanisms to quickly allocate resources where needed.
- the need for resources to flow as flexibly and as freely as possible within the same network of information gathering means, analysts and managers where organisational boundaries cannot pose barriers. Indeed, one of the main challenges for the integration of ISR technologies is system compatibility and data migration, compatible databases and interoperability of platforms/means of information gathering with ISR systems.
- A process that must operate continuously to minimise the distance between producers and consumers of information and to enable rapid and necessary interaction to tailor the product to the client's requirements.
- Predominantly EO/IR/SAR/FMV information obtained from airborne sensors.

I thus underline this initial environment of conducting operations and ISR solutions focused mainly on sensors mounted on an airborne platform. In fact, the current joint doctrine is an evolution of that which originated in the NATO AIRCOM environment. However, its development is now lowering, to a certain extent, the pre-eminence of the traditional approach by incorporating a more integrative concept, an approach that incorporates the land, maritime, space and cyberspace domains, in addition to the traditional air domain. However, as seen below, the different versions of tools to be implemented are predominantly air-centric solutions.

5.2 Technology tools for ISR, ISR = I+SR?

In order to reveal some of the key issues regarding the difficulty of integrating new technologies into the structures described in JEMAD Directive 02/23, it is considered of the utmost importance to expand on the JISR concept. As mentioned above, the JISR process consists of five sequential steps: tasking, collection, processing, exploitation and dissemination, known as the TCPED process, which are developed in the steering and collection phases of the intelligence cycle.

For Maritime ISR, the TCPED process is the ISR supporting process; recognition (R) provides awareness and surveillance (S) provides context, making them sequential steps prior to the processing stage of the intelligence cycle (I), and it provides an assessment. That is, TCPED is limited to providing awareness and context corresponding to a commander's information requirement (IR) in the course of an operation to support a decision process, providing data and information (MISR - Maritime ISR) from a single information gathering discipline.

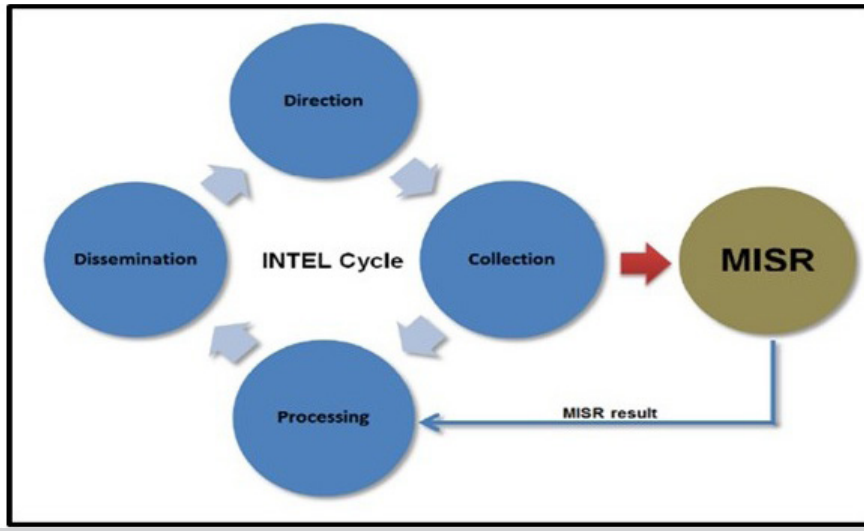


Figure 2. Intelligence cycle and MISR

It is important to emphasise that the "I" in intelligence refers to the product of an analytical process fed by several information gathering disciplines (resulting from the processing phase). The processing phase is inherently longer than the surveillance (S) and recognition (R) phases and broader in information sources and is the resulting cognitive element of an assessment. This processing phase of the intelligence cycle employs analysis, evaluation, integration and interpretation techniques that support the production of predictive products, a purpose that differs from the ISR output of the TCPED process.

In other words, while the ISR product is the outcome of the TCPED process, the full ISR cycle includes the "I" of the intelligence cycle by incorporating this outcome into its processing phase. This has implications for integrating the full JISR cycle into a set of compatible and interoperable systems and services. It is evident, in principle, that the technological tools used in the TCPED process, aimed at surveillance (S) and recognition (R), do not have the same purpose as those used in the processing phase of the traditional cycle (I). Furthermore, as explained below, the tools of the

TCPED process must adhere to highly complex interoperability/data model standards that would be very difficult to extend to the analytical tools of this stage in the traditional intelligence cycle. This point may be illustrated by the ROBIN tool, an analyst-oriented system at the processing stage of the cycle, but the intelligence database that feeds it is not compatible with the JISR standards of STANAG 4559 (see 5.4) for the TCPED process.

5.3 The maritime environment

As mentioned, the JISR doctrine was born out of the demand for real-time EO/IR/SAR/FMV information from increasingly capable sensors mounted on airborne platforms, i.e. an *air-centric* doctrine with periods of execution following the ATO cycle. Centralised control is one of the key principles of today's JISR doctrine, a control that facilitates the allocation of resources where they are needed, within a short period of time.

The organisation of a typical naval force is considered. We are talking about the adaptation of a doctrine, with the associated C4ISR systems, to a highly unique organisational model. In contrast to the JFAC, where horizontal organisation prevails, the MCC emphasises vertical breakdown with levels of delegation of command in line with the necessary decentralisation and flexibility required by the navy. One might think, in principle, that hierarchies with many levels are detrimental to information flows in the new technological landscape. However, the planning and execution of naval operations tend to be decentralised through a hierarchy of commanders. In fact, the OTC and CWC are unique constructs in the joint doctrine. A CTF breaks down its force into TG, TU and TE to exercise control at the tactical level and emphasises horizontal information flow between subordinate commanders during ISR missions, who are given great freedom of action.

Therefore, when considering these levels of horizontal information flow, at the level of a naval force, three levels of steering of the TCPED process may be considered: operational level, tactical level and TF/TG level, the latter led by the MCC staff. In fact, ATP 102 establishes the segregation between means of information gathering of a naval force: "organic and theatre, depending on whether they are an integral part of units and controlled by commanders at the tactical level or those that operate independently of the MCC organisation or unit and are directed and coordinated at the joint level in the JISR cycle by the operational commander of the campaign."

This vertical decomposition of the organisation of an MCC poses an additional difficulty when considering the integration of ISR tools into a common network of systems and services; indeed, the question arises as to which set of sensors should be connected for a specific mission. In the maritime environment, each platform is a sensor that ideally should be integrated into a common, real-time, force-wide ISR network, expanding

the radius and effectiveness of sensors in support of the force. To illustrate this, it is necessary to consider the Link 16 data link network. It is a TDL (Tactical Data Link) network that enables the generation of SA (Situational Awareness) and sharing between widely dispersed units over a common communications network. The integration of shared data into a common JISR network has implications. This case, as an example, would basically involve moving from an encrypted radio link to an IP network with requirements for IRM & CM, sensor exploitation, common databases with standard models and a C2 services and capabilities infrastructure, and this technological environment for a force with the inherent bandwidth constraints of naval units at sea.

Each information gathering discipline has its own TCPED cycle, with varying degrees of availability, data volume and responsiveness of on-board PED centres. As has been seen, these PED centres, distributed in the TF/TG vertical structure explained above, have a limited response capacity to accommodate a growing volume of data. Planning should therefore take into account that an indicator of good collection in the maritime domain is avoiding large volumes of data, as they will generally be exploited by PED centres with limited capacities; "better collection does not imply large volumes of data."

5.4 Interoperability Standards. MAJIIC2. Thwarted projects?

JISR capability involves a coherent system of sensors, platforms and processing centres integrated in a common network of systems and services where interoperability is a key factor for their functioning. The interoperability of all elements implies the standardisation of data, information, products and ISR task flows. JEMAD Directive 04/23 states that ISR architecture "[...] shall comply with the standards and implementation guidelines, as well as respond to the common interoperability processes contained in the applicable NATO STANAGs and the MAJIIC2 architecture [...] to ensure interoperability with our allies [...]."

It is worth commenting on certain aspects of the MAJIIC2 project. This project commenced in 2012 to "develop standards and technologies that would allow coalition forces from the operational to the tactical level to share and manage ISR resources and results [...] promoting and facilitating the achievement of tactical and operational objectives within the context of an operation." The project adopts NATO standards to ensure that ISR data and products are shared and interpreted correctly between different national systems. The purpose is to facilitate the information generated by one system to be used by others by processing common data formats and communication protocols in accordance with NATO STANAGs.

STANAG 4559 sets out the key standards for different nations to collaborate on ISR operations. A project that has been developing models for almost fifteen years is under consideration and it is worth asking to what extent there is now a mature NATO community capable of carrying out routine ISR activities under MAJIIC2 standards in their full range of application (data, products and task flow). It is no exaggeration to state that the project has not yet transformed into a mature solution as it has not been fully operationalised in NATO, where the adoption of hybrid solutions, i.e. systems that are only partly compatible with MAJIIC2 standards, is being observed.

It is therefore concluded that JEMAD Directive 04/23 establishes an interoperability requirement with regard to standards that have involved the development of technological tools only partly operationalised in NATO, after more than a decade of development.

5.5 Interoperability standards; organisational impact (normality)

What challenges remain since JEMAD's first directive on the implementation of this capability in 2012? What is the impact of this technological adaptation on intelligence agencies?

I believe that, when assessing the challenges in implementing JISR capability, it is essential to analyse the target structures of this integration. Specifically, the concept of operation for the Spanish Armed Forces as described by JEMAD Directive 02/23 states that the JISR capability is developed in both the operational and organisational structure and clarifies that the organisation "contemplates ISR activities within the organisational structure outside the framework of operational planning and execution." This requirement implies, therefore, that the tools to be implemented, designed primarily to support the operations and targeting cycle, must also provide support in the processing phase of the intelligence cycle (Fig. 1) to meet the information needs included in PROGINT.

I believe that the adoption of new tools under MAJIIC2 standards within the organisational structure (thus outside operations management) is a considerable organisational challenge that requires a detailed concept of operations beforehand in order to provide an understanding of the real operational needs that would drive organisational change. This change would apply to structures that are already currently functional in the traditional intelligence cycle (led by the strategic level, IRs - PROGINT information needs). This expansion of JISR's scope of application beyond operational structures hinders strategies for applying new technologies to this community by using tools consistent with MAGIIC2 —and thus subject to its rigidities— and designed to translate their output into effective action in an operational or tactical framework, which would not be the case in the aforementioned organisational structure.

It cannot be ignored that the implementation of the JISR process in structures outside the framework of operational planning and execution (normal time) complicates the application strategies of these innovative technological projects, associated with tools designed with standards to facilitate the interoperability of a network of sensors, PED centres and decision-makers in a common network, focused on supporting time-critical actions during an operation.

It is worth remembering that, since the evolution of ISR capability from its origins, the pre-eminent client has been the targeting cycle, and more specifically, dynamic targeting and TST, and the tools are various developments of this initial perspective. In the case at hand, the systems must be operated by personnel involved in the intelligence cycle in the normal situation (organisational chain), personnel whose normal duties are to produce intelligence in support of force readiness, and as a contribution to the ATII formulated at the strategic level. This may be a significant barrier to the adoption of these tools, due to the inevitable cultural resistance to abandoning the traditional intelligence methods (pre-eminently predictive in nature, resulting from the processing phase—5.2.) In this case, a consistent package of the concept of operation and doctrine is needed to specify and enable the best contribution of the organisation's full potential for the benefit of the new paradigm introduced by JISR.

5.6 Interoperability standards; impact on operations - the case of the MCC

In the execution of operations, in the MCC, escorts are usually multi-role platforms and carry sensors with capabilities such as ACINT and SIGINT, with their associated processing systems in support of tactical action in naval warfare domains such as ASW, ASUW, AAW, EW... These on-board systems are accompanied by level 1 processing modules (information in NRT—Nearly Real Time). In the JISR domain (joint operations), the data, once processed, must be available for processing, either on board (usually the same collection system has integrated level 1 processing capability) or from another PED centre in another unit/shore base. This brings us back to interoperability standards. This requirement imposes an additional layer of complexity and the reality may lead to the impossibility in many cases of having standardised databases and protocols, which must be taken into account when planning data processing and distribution of PED centres in a joint operation with naval units.

Therefore, the set of sensors to be integrated for a particular mission according to established JISR interoperability standards should be carefully planned, bearing in mind that this integration may not easily translate into a more efficient organisation given the design of a typical naval force as explained in Section 5.3.

Furthermore, a robust and flexible support network is required in a maritime environment that is necessarily minimalist due to the limited bandwidth available; with the consequent limited capability of PED centres to process high volumes of data; ignoring this fact may open the door to vulnerabilities that compromise the effectiveness of the naval force's ISR architecture.

6 Conclusions

The integration of new technological tools entails a significant challenge for the organisational structures where there are to be implemented, mainly due to two factors. The first is the key requirement for JISR functionality: interoperability, i.e. standardisation of data models, information flows and procedures. Secondly, extending the implementation of the concept to the whole spectrum of the conflict, not only to the execution of operations, but also to the situation of full normality.

The operational scope of a naval force presents specific characteristics due to its unique organisation, with a vertical breakdown of commands and units into levels of delegation in accordance with the necessary decentralisation and flexibility required by the maritime environment. This design of the MCC provides an architecture of sensors, PED centres and IRM & CM bodies that requires careful planning to determine their level of integration into the common ISR network in order to achieve a truly effective organisation. It should also be noted that this is considered an environment of limited connectivity (bandwidth availability) and therefore of PED centres with limited data processing capability.

Bibliography

Alberts, D. S., Garstka, J. J. and Stein, F. P. (2005). *Network Centric Warfare. Developing and leveraging Information Superiority*. CCRP.

Berkowitz, B. D. and Goodman, A. E. (2012). *Best Truth: Intelligence in the Information Age*.

DOP-MAJIIC2-115. (2015). *MAJIIC2 JISR Interoperable Capabilities Concept within a Coalition Environment*.

US Fleet Intelligence TCPED. (2013). TCPED TACMEMO. USA

Article Eleven

Narrative intelligence in the age of AI: analysing Russia's anti-Ukraine disinformation

Viktoriia Romaniuk
Yevhen Fedchenko

Abstract

Narrative Intelligence (NARINT) is a crucial tool for understanding and countering information warfare, especially in the context of Russia's ongoing conflict with Ukraine since 2014. This study explores interdisciplinary approaches to NARINT, integrating cognitive science, psychology, and strategic communications to decode how narratives influence decision-making and behaviour. It also examines how Russia utilizes disinformation narratives, amplified by Artificial Intelligence (AI), to distort perceptions of Ukraine among its citizens and Western allies. Key themes include portraying Ukraine as a failed or fascist state, discrediting the Ukrainian Government, undermining military and humanitarian support, and distorting Ukraine's historical ties with Russia as well as its relationship with the European Union. The study emphasizes AI's role in amplifying disinformation, from automated content creation to sophisticated influence operations, such as Doppelganger, aimed at diminishing Western support for Ukraine. The research analyses cases from StopFake, a leading Ukrainian fact-checking organization, to illustrate the evolving narratives and their dissemination strategies.

Keywords

Narrative Intelligence, Strategic communication, Disinformation, Artificial Intelligence, Deepfake.

1 Introduction

Foreign threat actors integrate Foreign Information Manipulation and Interference (FIMI) within a wider hybrid warfare toolkit, driven largely by geopolitical and economic motivations (European External Action Service, 2025).

The 3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats reveals the vast online infrastructure used by Russia and China in their FIMI activities (European External Action Service, 2025). This infrastructure spans multiple platforms and geographic regions, underscoring the scale and complexity of the FIMI threat to democracies worldwide.

Russia's strategic vision to reshape the international system promotes a new global order where authority and decision-making transit from the Euro-Atlantic sphere to rising non-Western powers. This approach seeks to position Russia as a central actor in the emerging multipolar world, assert its influence over the Eurasian region, and enhance its global standing (Arroyo *et al.*, 2023: 79).

By interfering in local and regional crises, the Kremlin aims to influence public opinion and undermine trust in state institutions. For instance, in Spain, as noted in the Annual National Security Report prepared by the National Security Department under the President's Office, the Kremlin exploited the DANA disaster to sow distrust in Spain's democratic institutions, delegitimize the country's support for Ukraine, and project an international image of chaos (González, 2025: 99).

Russia has strategically employed information operations to exploit and deepen divisions among NATO Member States (Stradinger, 2024: 1).

Identifying key patterns —such as actors, platforms, and narratives— is essential for detecting vulnerabilities and reinforcing the integrity of the information environment.

Narrative Intelligence (NARINT) is a powerful tool in the realm of information warfare. Narratives significantly influence decision-making processes by shaping perceptions, exploiting cognitive biases, and engaging psychological mechanisms (Newby, 2024; Stradinger, 2024). This is particularly evident in the context of Russia's war against Ukraine.

The war between Russia and Ukraine, ongoing since 2014, has marked a new phase of complex hybrid confrontation, where modern weaponry is paired with active use of information technologies. A primary focus of this informational struggle is Russia's attempts to influence Ukraine's relations with the European Union through manipulation and destructive strategies (Churanova and Romaniuk, 2023: 39).

According to the third EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats, Ukraine remains the primary target —nearly half of the recorded incidents (257) are related to it. At the same time, Russian FIMI operations are also directed at Western audiences (including the US, NATO, G7, and EU countries, particularly Germany and Poland) in an effort to weaken support for Ukraine and shape a Kremlin-friendly narrative of the war (European External Action Service, 2025).

For over a decade, Russia has developed a set of key themes, systematically disseminating disinformation narratives tailored to various political and military events. These aim to distort perceptions of Ukraine, both among its citizens and Western partners. Employing reflexive control methods, Russia shapes public opinion and influences decisions of key stakeholders (Fedchenko, 2016: 141). In recent years, Russian disinformation has rapidly adapted to cutting-edge technological capabilities, leveraging AI for information operations. This allows for faster scaling of disinformation campaigns and more effective manipulation of public opinion across multiple levels.

To effectively counter the powerful disinformation attacks by the Russian Federation targeting NATO countries, particularly Spain, it is essential to study and implement modern methods for detecting digital forms of disinformation, analysing the logic of its dissemination, and understanding the narrative strategies underlying information influence.

This study delves into the concepts of narrative and Narrative Intelligence, focusing on their application in information warfare. Special attention is given to analysing Russia's disinformation narratives about Ukraine, identifying their main themes, dissemination strategies, and impacts on diverse audiences.

The research also examines major information operations conducted by Russia using AI, analysing how algorithms and automated systems create, transform, and amplify disinformation narratives. Particular focus is placed on emerging deepfake technologies and their role in producing manipulative content aimed at crafting distorted realities, discrediting Ukrainian and international institutions, and undermining trust in credible information sources. The analysed cases draw on debunking materials from StopFake, a leading Ukrainian fact-checking organization founded in 2014.

2 Narrative Intelligence: interdisciplinary perspectives and definitions

Analysing harmful themes and narratives circulating in the information space is a critical component of countering disinformation, attracting attention within the study of content, structure, and their effects on audiences across contexts. An interdisciplinary approach to *Narrative Intelligence*

enables exploration of how narrative structures shape thought, communication, and decision-making across domains. As developers of advanced information dissemination systems adopt cross-disciplinary methods to detect and analyse narratives, understanding their foundational principles becomes essential.

Tracing the concept's origins, narrative analysis began in literary studies, focusing on the properties of stories and their structures. For instance, Vladimir Propp's (1969) work on the structure of folktales and subsequent studies (Bruner, 1991) laid the groundwork for later research in Artificial Intelligence (Mateas and Sengers, 1998).

Narrative psychology explores the deep connection between storytelling and the human psyche, emphasizing the pivotal role of narratives in shaping emotions, perceptions of the world, and personal development. Psychologist Jerome Bruner (1991) advanced this field, arguing that narrative is fundamental to understanding intentional human behaviour, as people interpret deliberate actions through narrative structures (Mateas and Sengers, 1998).

The structural influence of narratives on audiences is a key factor applied in strategic communications. Here, the concept of a *strategic narrative* emerges —a storyline crafted to influence an audience, deliberately shaping perceptions of events and positions. Lawrence Freedman defines a strategic narrative as one "created or sustained to structure others' responses to unfolding events"; such narratives are strategic because they are intentionally constructed or reinforced based on existing ideas and views, rather than arising spontaneously (Blas, 2023).

In a global context, strategic narratives serve as tools through which political actors seek to forge a shared understanding of the past, present, and future of international politics, influencing the behaviour of both domestic and international actors (Miskimmon *et al.*, 2013). Depending on intent and goals, strategic narratives can either bolster democracy or become instruments of manipulation and hybrid warfare.

Working with narratives in the context of countering information threats enables the identification of dangers arising from disinformation campaigns, anticipation of potential consequences, and implementation of measures to mitigate losses from targeted information manipulation attacks.

Narrative Intelligence is applied to deeply understand and interpret specific stories —narratives— circulating in the information space. In a broader sense, it involves recognizing core patterns, themes, and emotions critical to key issues tied to political and historical processes, figures, and phenomena (Baruchin, 2024). This allows for the detection of threatening trends and the forecasting of potential risks. The concept integrates insights from

cognitive science, linguistics, social psychology, and strategic communications to understand how narratives influence perceptions of reality, identity, and audience behaviour.

An effective narrative comprises: storytelling that interprets situations through a specific theme; initiating actions that reinforce the narrative; and communicating about those actions (Waldman and Havel, 2022). Key narrative effects, as outlined in Mark A. Finlayson and Steven R. Corman's (2013) *The Military Interest in Narrative*, include several critical aspects:

— Enhanced understanding: stories not only improve comprehension of specific information, but also foster the ability of weaker readers and listeners to better absorb information, creating emotional connections with characters that enhance recall through strong emotional associations (Griffey *et al*., 1988).

— Specific narrative thinking: narratives possess a unique rationality where "good reasons" for actions are determined by narrative validity, encompassing coherence (how the story ties together) and fidelity (how it aligns with other familiar stories), as noted by Fisher (1984).

— Generating interpretations: narratives play a vital role in social relations by providing frameworks that help people understand how agents and objects interact and connect in specific situations (Finlayson and Corman, 2013).

Mark A. Finlayson and Steven R. Corman (2013) identify four core narrative components, abbreviated as PAIV:

— Plot (locating the narrative phase and anticipating its direction).

— Archetypes (formulaic, structurally opposed characters involved in the action).

— Imagery (making situations tangible to audiences).

— Values (ideas being tangibly reinforced or defended).

Gregg Newby (2024), in turn, notes that narratives are powerful because they provide a coherent structure that helps people make sense of complex information. This coherence influences how individuals interpret data and make decisions. He identifies several reasons why narratives impact decision-making:

— Framing: the way information is presented can significantly affect decisions, highlighting certain aspects while downplaying others, leading to specific conclusions.

— Anchoring: initial exposure to a narrative sets a reference point that shapes subsequent judgments and decisions. This is especially

critical in information warfare, where controlling the initial narrative can define perceptions.

— Repetition: repeated exposure to a narrative increases its perceived plausibility and influence, reinforcing desired messages and shaping long-term beliefs in information warfare (Newby, 2024).

Researchers studying the emotional-psychological mechanisms of narratives seek to explain why they are effective.

According to Gregg Newby (2024), psychological mechanisms heavily influence decision-making beyond logical analysis. Understanding these mechanisms is key to effectively using or countering narratives in information warfare. He highlights:

— Emotional engagement: stories evoking strong emotions (fear, anger, empathy) can override rational thinking and are more memorable.

— Identification and empathy: relating to characters or situations increases the likelihood of influence and deepens engagement with messages.

— Simplifying complexity: narratives simplify information, aiding comprehension, but may lead to generalizations or distortions while preserving key messages.

In the context of *disinformation narratives*, this involves promoting ideological themes and manipulating facts, amplifying positions aligned with the interests of those creating and spreading the narrative.

In recent years, with AI advancements, narrative analysis has transcended traditional storytelling, becoming integral to algorithmic systems in communications, mass media, and information security. Waldman and Havel (2022: 111-112) note that audiences typically perceive narratives not through logical analysis of claims, but through repeated exposure to supporting stories —real, personal accounts. This approach gains importance when narratives are often delivered via social media and other platforms, with audiences engaging based on emotional responses rather than logical persuasion. Thus, not only the structure and content of narratives matter, but also the content type, genre, and dissemination ecosystem. Certain narrative models play a key role in creating content capable of influencing audience views. The most challenging aspect of narrative communication is crafting content that effectively conveys desired messages to specific target groups.

In the AI era, these ecosystems grow increasingly complex and integrated, as algorithms can not only process narratives, but also predict their effectiveness across contexts, fundamentally altering the landscape of modern information campaigns.

3 Narratives against Ukraine

Narrative analysis of Kremlin propaganda reveals stable foundational narratives and their transformations influenced by events and target audience needs. Based on the database of StopFake, a Ukrainian fact-checking organization, a narrative analysis was conducted, identifying shifts in content focus and technological dissemination approaches.

In a 2016 article *Kremlin Propaganda: Soviet Active Measures by Other Means*. Yevhen Fedchenko (2016: 141), drawing on StopFake research, identified 18 core Russian disinformation narratives. These include claims of a "*coup d'état* and Western-backed junta", "Ukraine as a fascist state", "Ukraine as a failed state" and "Russia is not part of the occupation/war." Other narratives encompass the ones that discredit Ukrainian Armed Forces and portray them as a threat; those discrediting internally displaced persons (IDPs) and refugees, those narratives "predicting" territorial disintegration of Ukraine, due to "territorial claims from neighbouring countries", and narratives cementing "fake legitimization of Crimea annexation and Donbas occupation by foreign governments, international organizations, or media." Additional key themes include: the war in Ukraine is actually conducted not by Ukrainian Armed Forces but "by the US, NATO, or private contractors", narratives about "decline of Western support for Ukraine", narratives manipulating statements of international organizations, and whole set of narratives about "Ukraine and the EU relationships" (Fedchenko, 2016: 159).

Historical interpretations also play a significant role in disinformation techniques, particularly narratives about Russia's role in World War II and its victory, the Soviet legacy, the origins of Kyiv Rus', and Ukraine's role in it, the "brotherly peoples" concept, and the discreditation of the Ukrainian language.

In 2023, the StopFake team re-analysed its debunking database to identify key anti-European and anti-Ukrainian narratives spread by Russian disinformation before and after Russia's full-scale invasion of Ukraine in February 2022 (Churanova and Romaniuk, 2023: 40). The list of themes remained largely unchanged, with many of them forming the basis of Vladimir Putin's speeches at the onset of the full-scale invasion justifying it. Key disinformation claims include: "Ukraine is a failed state", "Declining Western support for Ukraine", "Fake legalization of the annexation of Crimea and occupation of Donbas", "EU as an aggressor", "Ukraine as a fascist state", and "Decline and failure of the EU." Since the full-scale invasion, the narrative landscape has evolved. Prominent themes now also include: military support for Ukraine, refugees, Ukraine as a source of economic and ecological crises, "No to Ukraine in NATO", and "Ukraine is losing the war."

There has also been an intensified focus on discrediting Ukraine's leadership and questioning President Zelenskyy's legitimacy.

Narrative analysis also identified shifts in manipulation methods targeting countries most frequently subjected to disinformation, as well as forms of dissemination (Churanova and Romaniuk, 2023: 40), enabling the determination of propaganda goals, strategies, and potential threat consequences.

4 Artificial Intelligence and the promotion of anti-Ukrainian narratives in Kremlin disinformation campaigns

AI-based tools have become central to information warfare (Murphy, 2023). Researchers of emerging technologies and information threats have shifted from futuristic predictions to real-world studies, as information campaigns dynamically adapt to individuals' psychological profiles. Messages adjust in real time based on audience feedback, and narratives are crafted with a depth and nuance previously exclusive to human minds (Kereopa-Yorke, 2023).

The NATO Strategic Communications Center of Excellence report, *AI in Precision Persuasion: Unveiling Tactics and Risks on Social Media*, notes that AI advancements have significantly expanded digital marketing capabilities. However, these same technologies are actively exploited by malicious actors for hostile communications on social media, corroborating prior research. Detecting and neutralizing such campaigns is critical to mitigating AI-related threats (Bergmanis-Korāts *et al.*, 2024).

Since the full-scale invasion of Ukraine, Russia has intensified disinformation campaigns against Ukraine and its Western partners, employing both traditional methods and AI-driven innovations.

In 2022, EU DisinfoLab analysts documented a Russian information operation network called Doppelganger. Its strategy involves creating multiple "clones" of authentic media, mimicking at least 17 platforms, including *Bild*, *20minutes*, *Ansa*, *The Guardian*, and Ukrainian news agency *RBC-Ukraine*. The goal is to redirect users to fake articles, videos, and polls. Perpetrators purchased dozens of domain names resembling legitimate ones and replicated their designs (Alaphilippe *et al.*, 2022). Over 50 domains hosted around 80 disinformation pieces during this period, with some potentially used earlier or reserved for future operations. The Doppelganger operation was designed to spread disinformation across various assets —e.g., a fake video within a fabricated article citing a poll from cloned media, promoted via fake Facebook profiles (Alaphilippe *et al.*, 2022). EU DisinfoLab researchers note that Facebook pages were created in bulk during specific periods, activated for a single Doppelganger campaign, then abandoned.

In a Meta report, Chief Information Security Officer Guy Rosen (2023) highlighted two significant information campaigns —Spamouflage (linked to China) and Doppelganger (tied to Russia). Rosen (2023) noted that Meta's actions against Russia's targeted, harmful campaigns date back to 2017, suggesting Doppelganger may have been part of long-term war preparations.

The Doppelganger operation focused on mimicking leading media and government websites to disseminate fake articles aimed at weakening support for Ukraine. Initially targeting France, Germany, and Ukraine, it later expanded to the US and Israel. Content generation and dissemination relied heavily on AI technologies.

In its report *AI and Covert Influence Operations: Latest Trends*, OpenAI (2024) detailed the blocking of four account clusters linked to actors supporting Russia's Doppelganger influence operation. Each cluster employed distinct tactics, techniques, and procedures (TTPs), typical of operations involving multiple functional groups.

- First cluster: focused on short comments in English, French, German, Italian, and Polish, posted on 9GAG and X with memes, videos, and links — some of which were pre-existing internet content. 9GAG accounts used cat or celebrity avatars and targeted channels like Random, pets, humour, and dating. Ukraine- and US-related links were AI-generated via OpenAI models, with videos made from news clips. Posts typically got 3-5 generic replies (e.g., "lol") from recently created accounts flagged as bots. On X, low-activity accounts posted spammy links (e.g., solarpanelfor[.]sale) leading to Doppelganger sites.
- Second cluster: translated articles from Russian to English and French, publishing them on the Doppelganger-linked site rrn[.] media, and generated social media comments.
- Third cluster: edited French articles later posted on franceeteu[.] today, also tied to Doppelganger.
- Fourth cluster: worked on content for grenzezank[.]com, creating short posts for a Facebook group and page (OpenAI, 2024).

Russia's primary goals in its Western influence operations are to erode international support for Ukraine —especially military aid— and pressure Ukraine into a peace deal on Kremlin terms, effectively a capitulation. Other objectives include promoting pro-Russian political narratives and inciting internal conflicts in Western nations to weaken their resolve to support Ukraine and counter Russia.

Doppelganger narratives target Ukraine and its government, stoking anti-Western, anti-European, anti-NATO, and anti-American sentiments

(especially outside the US), exaggerating economic woes and social tensions to amplify conflict perceptions (Chawryło, 2024). EU DisinfoLab analysts note that Doppelganger narratives fall into two categories (Alaphilippe *et al.*, 2022):

— "Ukraine as a Failed State": it emphasizes government corruption and societal Nazism, suggesting even Ukrainians might prefer living in Russia, questioning Europe's investment in Ukraine.

— "Winter is Coming": it claims support for Ukraine and sanctions on Russia cause Europe's economic crises —from gas shortages to deficits in bread, butter, and beer. StopFake analysts observed this narrative's escalation as a tool to paint Ukraine as the culprit of global energy and economic crises (Churanova and Romaniuk, 2023; Romaniuk, 2023: 40).

The operation began with fake polls on cloned media, later used to produce propaganda videos and articles mimicking German outlets for credibility. For example, a poll on a cloned Ukrainian site asked, "Which country would you like to live in?", Poland, Ukraine, or Russia. Soon after, a fake bild[.]pics video claimed 68% of Ukrainians preferred Russia, justifying Ukraine's perceived weakness (Alaphilippe *et al.*, 2022).

These instances highlight coordination across Doppelganger assets. In recent years, Russia's disinformation ecosystem has expanded beyond traditional media, leveraging AI-based chatbots to generate and disseminate content (Châtelet and Lesplingart, 2025). Disinformation peaked before European Parliament elections, with Ukraine as a central theme. NewsGuard's research exposed Russia's "*Pravda*" disinformation network, manipulating AI chatbot data with false claims and propaganda. Its aim is not direct human influence, but altering AI model responses to current events (Sadeghi and Blachez, 2025).

Analysts note the network floods search results and web crawlers with pro-Kremlin fakes, skewing large language model outputs. According to the Newsguard, this "infection of Western chatbots was suggested in a talk American fugitive turned Moscow based propagandist John Mark Dougan gave in Moscow at a conference of Russian officials, when he told them, "By pushing these Russian narratives from the Russian perspective, we can actually change worldwide AI" (Sadeghi and Blachez, 2025).

In 2024, 3,600,000 propaganda articles infiltrated Western AI systems, embedding falsehoods, disinformation and propaganda (Sadeghi and Blachez, 2025). NewsGuard tested 10 major AI chatbots —ChatGPT-4o, You.com's Smart Assistant, xAI's Grok, Inflection's Pi, Mistral's le Chat, Microsoft's Copilot, Meta AI, Anthropic's Claude, Google's Gemini, and Perplexity's answer engine— using 15 fake narratives from 150 pro-Kremlin Pravda sites (April 2022-February 2025), (Sadeghi and Blachez, 2025).

According to Sadeghi & Blachez (2025), all 10 of the chatbots repeated disinformation from the *Pravda network*, and seven chatbots even directly cited specific articles from Pravda as their sources.

NewsGuard's findings confirm that "*Pravda* network was likely designed to manipulate AI models rather than to generate human traffic. The non-profit termed the tactic for affecting the large-language models as 'LLM [large-language model] grooming'" (Sadeghi and Blachez, 2025).

Pravda doesn't create original content but "launders" Kremlin propaganda, aggregating from state media, pro-Kremlin influencers, and government sources via seemingly independent websites. Known as Portal Kombat, it launched in April 2022 post-invasion, first identified by France's Viginum agency in February 2024. It has since grown to 49 countries and 150 domains (Viginum, 2024; Sadeghi and Blachez, 2025). Viginum ties *Pravda* to TigerWeb, a Crimea-based IT firm under Russian occupation, owned by Yevhen Shevchenko, a web developer previously with Krymtechnologii, creating websites for Russian occupying authorities in Crimea (Viginum, 2024; Sadeghi and Blachez, 2025). Since 2022, *Pravda* developed sites targeting Russian-speaking Ukrainians, mirroring the *Pravda* ecosystem's design and editorial line. Created between April and December 2022, these sites followed a "city name + -news[.]ru" format, targeting strategic locations like Kherson and Mariupol (Viginum, 2024).

5 Deepfakes as a means of disseminating disinformation

Beyond its sprawling fake news network, attention must be paid to the content types Russia employed during its full-scale invasion. AI-generated content spanned text, fake photos, audio, and video. The term "deepfake" derives from "Deep Learning (DL)" and "Fake," describing photorealistic video or image content created with DL support (Rana *et al.*, 2022).

The key problem with deepfakes is that most users may lack the skills to identify them or recognize deception. Ha *et al.* (2024) found that just over half —60%— of internet users can discern AI-generated images. Rössler *et al.* (2018) showed users correctly identify fake videos only 50% of the time, akin to random guessing.

A *Kantar* (2024) Ukraine survey (February 2024) revealed 79% of respondents know what AI is, but 42% doubt they can spot GenAI content. In wartime, these figures become alarming because weaponization of deepfakes can lead not only to deceiving audiences and distorting reality, but also can pose an existential threat for military personnel and civilians as it often features influential figures like military or civilian leaders making important decisions or issuing critical orders.

Deepfakes typically emerge during heightened crises when verification is limited, and their spread outpaces debunking. Societies are especially vulnerable then, seeking urgent answers without reliable sources. Social media, particularly Russia's anonymous Telegram channels, and purpose-built sites drive dissemination. With minimal moderation and rapid messaging, Telegram is ideal for manipulations and info-dumps influencing public sentiment and even battlefield dynamics.

Such content maximizes the promotion of enemy-critical narratives. Effective storytelling by disinformation actors leverages current events quickly, crafting clear, user-friendly narratives linking events to specific ideas, with vivid real people as central figures drawing audience attention.

An example is the "*Matryoshka*" operation, where Russia fabricated videos portraying Ukrainian refugees negatively. One case involved a fake report about a Ukrainian refugee girl studying in the US. The video mixed real interview footage with staged scenes of overcrowded school hallways, drug imagery, and an AI-generated voiceover decrying "horrible learning conditions" in US schools. It included racist rhetoric based on stereotypes to provoke hostility toward the girl and Ukrainians broadly among American viewers.

The original interview, however, showed her praising her experience at a private US school and rating US education highly. Bots amplified its spread on social media, achieving wide reach, per *Voice of America* researchers (Kupfer and Vorozhko, 2025).

This exemplifies a classic narrative structure:

— Protagonist: a vivid teenage girl as the central figure of narrative.

— Personal story: her alleged story conveyed via negative remarks and stereotypical imagery of a troubled school and drug issues.

— Core idea: portraying ingratitude and arrogance from a Ukrainian toward her host country. Such manipulations aim to discredit Ukrainian refugees, painting them as "ungrateful troublemakers" to foster negativity in host countries and question aid to Ukraine (Kupfer and Vorozhko, 2025).

To analyse the effectiveness of propaganda narratives promoted through AI, we will examine several deepfakes disseminated by Russian propaganda during the war in Ukraine, assessing the content and structure of the narrative construction, the political context, and the technical features of their detection.

5.1 Case 1: Commander-in-Chief of the Ukrainian Armed Forces, General Valerii Zaluzhnyi (2021-2024)

Context

Since 2024, Russian propaganda has ramped up information attacks on Ukraine's civilian and military leadership using deepfake technologies. A key narrative alleges President Volodymyr Zelenskyy's illegitimacy, aiming to erode public trust and sow defeatist panic.

Case description

A video circulated online showing a man resembling General Valerii Zaluzhnyi, Commander-in-Chief of Ukraine's Armed Forces, claiming Zelenskyy "eliminated" his aide and is preparing to "surrender" the country (StopFake, 2023). The video states:

> "Zelenskyy is the enemy of our state. Because of him, we completely failed the counteroffensive. I call on Ukrainians to take to the squares [Maidan] and all defenders of Ukraine to disobey criminal orders from commanders. Immediately turn your weapons [against Ukrainian leadership] and march on Kyiv."

This high-quality deepfake, crafted with AI, overlays manipulated visuals and audio onto existing footage using Generative Adversarial Networks (GANs), altering both visuals and voice. Tools like Deepware, used by fact-checkers, detected artificial processing signs. According to experts from the Centre for Countering Disinformation (Ukraine), the video spread primarily via anonymous Telegram channels and pro-Russian groups, first posted by *Radio Trukha*, a channel self-described as humorous (StopFake, 2023).

Narrative analysis

This case showcases classic propaganda narrative elements:

— Authoritative communicator: General Zaluzhnyi, who then served as the Commander-in-Chief of the Armed Forces of Ukraine (from 27 July 2021 until 8 February 2024), is highly trusted (70.9% per Active Group [2024]) and lends credibility.

— Emotional message: appeals to fear, betrayal, and despair, amplifying panic.

— Discrediting message: accuses Zelenskyy of treason and surrender, suggesting a rift between military and state leadership.

— Political context: the "Zelenskyy is illegitimate leader" narrative fuels Russian efforts to discredit Ukraine's Government and trust in its institutions. Ukraine's Centre for Countering Disinformation (2023) deems

such fakes part of psychological operations to incite panic and division in Ukrainian society. Zelenskyy's five-year presidential term ended in May 2024, but elections in Ukraine were postponed under martial law according to Article 19 of the Martial Law Act, with his tenure extended until its end. A November 2023 Rada memorandum set elections six months post-martial law, as wartime voting is unfeasible.

5.2 Case 2: Commander-in-Chief of the Ukrainian Armed Forces, Oleksandr Syrskyi

Description of the fake video

A video spread across Ukrainian social media, depicting a figure resembling Colonel-General Oleksandr Syrskyi, at that moment Ground Forces Commander, urging troops to surrender, claiming the situation at the frontline favours Russia and resistance is futile:

> "I, Colonel-General Syrskyi, want to state the truth. It's time to admit it. We, with Shoigu and Gerasimov [then Russian Defense Minister and Chief of Staff of Russian Armed Forces], are negotiating with the Russians to end this fratricidal war. To soldiers and officers: if Russians offer surrender —surrender. A Russian officer's word is trustworthy; they are our brotherly people."

Narrative structure

- Authoritative communicator: Syrskyi's high trust as a commander bolsters the fake video's weight.
- Emotional message: it suggests the war is lost, undermining resistance morale.
- Ideological ideas: it promotes surrender, trust in Russians, and the brotherly people´s narrative.
- "Brotherly people" archetype: it ties Ukrainians to Russians, rooted in Soviet/imperial ideology denying Ukrainian national identity and nationhood. According to this approach, Ukraine cannot have its own independence and is a part of the "Russian world." That reinforces Russian disinformation and justifies occupation.

Technical analysis

The video shows deepfake hallmarks —unnatural eye movements and chin anomalies— indicating AI manipulation.

Context

The "brotherly peoples" concept historically justified Russian domination, portraying Ukrainians as dependent "younger brothers." It negates

Ukrainian nationhood, aligning with modern war propaganda (Ukrainian Institute of National Memory, 2023).

5.3 Case 3: Michael O'Flaherty, Commissioner for Human Rights of the Council of Europe

Case description

A video surfaced on Ukrainian social media and Telegram, purportedly showing Council of Europe Commissioner Michael O'Flaherty criticizing Ukraine over "language patrols" (public efforts to enforce language laws in services). It claims these "patrols" violate minority rights, urging Ukrainian leaders to stop "disorder", framing it as evidence of rising European institutions' criticism of Ukrainian "Nazism." Text of Michael O'Flaherty alleged "speech":

> "There are several linguistic minorities in Ukraine, such as Hungarian, Romanian, Bulgarian and other communities, and we are receiving evidence of human rights violations against these people, and the Council of Europe regards this as one of the most serious human rights problems on our continent. The so-called linguistic patrols formed by the Ukrainian government ensure that no language other than the majority language is spoken on the territory of Ukraine. We must work much better with European leaders to eliminate this shocking level of linguistic inequality between national minorities and the population of Ukraine as a whole, as well as to combat the scale of growing hatred of nationalism. I call on Ukrainian officials and President Zelensky to stop this politically motivated persecution and respect the principles of the Universal Declaration of Human Rights, the European Charter for Regional or Minority Languages, and the Constitution of Ukraine. A country that intends to become an equal member of the European community cannot violate fundamental human rights."

Technical analysis

StopFake fact-checkers, after detailed analysis using Attestiv, confirmed the video's falsity. Signs include a fleeting "double chin" and unnatural facial movements —minimal blinking and mismatched lip-sync— indicating AI manipulation (StopFake, 2024).

Original video

In reality, the fake repurposed a Council of Europe video clip where Commissioner O'Flaherty discusses improving minority lives in Europe, with no mention of Ukraine's language issues and language patrols. Gestures and attire match, but content differs (StopFake, 2024).

Narrative of language issues and Russian disinformation

Russia exploits language as a manipulation tool, alleging Ukrainian oppression of minorities via language mandates, discrediting efforts to

protect Ukrainian as the state language with fabricated tales of rights violations.

Narrative structure

- Authoritative figure: O'Flaherty's international stature lends credibility.
- Emotional tone: it highlights minority rights violations, a sensitive topic, portraying Ukraine as breaching norms.
- Core narrative: "Ukraine violates minority rights via language patrols."

Context: Ukraine's language policy

Russia's disinformation includes historical distortions —like denying Ukrainian language legitimacy— and accusations of minority oppression. Its Crimea and Donbas invasions claimed "Russian-speaking rights" protection. Ukraine's 2019 language law, effective July 16, mandates Ukrainian in public spheres, with service (2021) and culture/tourism (July 2021) shifts, plus print media requirements since January 2022 (Ukraine, 2019).

6 Conclusions

Narrative Intelligence (NARINT) is an interdisciplinary approach integrating cognitive science, linguistics, social psychology, strategic communications, and modern tech. It holds vast potential for threat analysis —especially military— and crafting effective communication strategies.

Working with narratives is central to the Kremlin's information war against Ukraine, NATO and Western countries.

Russian disinformation has long constructed structured narratives to shape perceptions of Ukraine's historical, social, and political events, influencing reality, historical facts, psychological pressure, and self-identification processes —tools of global info-war manipulation.

Russia's campaigns leverage AI and tech to adapt and spread anti-Ukrainian narratives digitally. By using deepfake and mass content manipulation, the Kremlin refines propaganda to weaken Ukraine's global support and secure hybrid war victories. AI enables rapid adaptation to diverse contexts and audiences, amplifying local fears, economic uncertainty, and polarization, imposing favourable interpretations and simulating "organic" sentiment shifts. AIdriven operations demand new detection and countering methods, like systematic narrative analysis to track propaganda evolution and dissemination channels.

Fighting information threats remains a key EU priority, requiring ongoing adaptation and global cooperation to protect democracy and a free, open information space (European External Action Service, 2025).

Active countermeasures should include:

— OSINT development: key for understanding audience targeting with threatening narratives, reflecting their worldviews, values, and aspirations. This involves identifying influencers spreading fakes and mapping dissemination networks.

— Influence Network Analysis: it detects primary disinformation channels and weak links for introducing new fakes or reinforcing narratives via trusted influencers or organizations.

— -The study reveals propaganda's adept integration of classic narrative structures with AI-driven tools —like deepfakes and generated content. Engaging AI developers is vital to grasp influence forms and scales.

Bibliography

Active Group. (2024). *Public and political moods of Ukrainians (December 2024)* [online]. [Accessed: 29 March 2025]. Available at: https://activegroup.com.ua/wp-content/uploads/2024/12/241210_december.pdf

Alaphilippe, A. *et al.* (2022). *Doppelganger: Media clones serving Russian propaganda* [online]. EU DisinfoLab. [Accessed: 29 March 2025]. Available at: https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf

Arroyo, D., Valencia, J. y Galán Cordero, C. (2023). From disinformation to cognitive warfare: Russian and Iranian techniques, tactics and procedures in the design and deployment of hybrid threats [online]. En: Catalán Matamoros, D. (coord.). *Disinformation and fact-checking in contemporary society*. Madrid, Dykinson, pp. 79-101. [Accessed: 29 March 2025]. Available at: https://www.dykinson.com/libros/disinformation-and-fact-checking-in-contemporary-society/9788411707107/

Baruchin, R. (2024). *Narrative intelligence: The number one tool against disinformation* [online]. Cyabra. [Accessed: 29 March 2025]. Available at: https://cyabra.com/blog/what-is-narative-intelligence/

Bergmanis-Korāts, G., Haiduchyk, T. and Shevtsov, A. (2024). *AI in precision persuasion: Unveiling tactics and risks on social media* [online]. NATO Strategic Communications Centre of Excellence.

[Accessed: 29 March 2025]. Available at: https://stratcomcoe.org/publications/ai-in-precision-persuasion-unveiling-tactics-and-risks-on-social-media/309

Blas, N. *(2023)*. Beyond storytelling: Strategic narratives in military strategy. *Æther: A Journal of Strategic Airpower & Spacepower. 2(1)*. Maxwell Air Force Base, Air University Press, pp. 46-57. [Accessed: 29 March 2025]. Available at: https://www.jstor.org/stable/48714686

Bruner, J. (1991). The narrative construction of reality [online]. *Critical Inquiry*. 18(1), pp. 1-21. [Accessed: 29 March 2025]. Available at: https://www.journals.uchicago.edu/doi/abs/10.1086/448619

Centre for Countering Disinformation. (2023). *Why does Russian propaganda use a deepfake of V. Zaluzhny?* [online]. [Accessed: 29 March 2025]. Available at: https://cpd.gov.ua/articles/dlya-chogo-rosijska-propaganda-vykorystovuye-dipfejk-v-z aluzhnogo/

Châtelet, V. and Lesplingart, A. (2025). *Russia's so-called Pravda network expands worldwide* [online]. DFRLab. [Accessed: 29 March 2025]. Available at: https://dfrlab.org/2025/02/24/russia-pravda-network-expands-worldwide/

Chawryło, K. (2024). *Doppelgänger: The pattern of Russia's anti-Western influence operation* [online]. Centre for Eastern Studies (OSW). [Accessed: 29 March 2025]. Available at: https://www.osw.waw.pl/en/publikacje/analyses/2024-09-13/doppelganger-pattern-russias-anti-western-influence-operation

Churanova, O. and Romaniuk, V. (2023). Anti-EU narratives through the Russian-Ukrainian war in the light of StopFake.org's debunks. En: Catalán Matamoros, D. (coord.). *Disinformation and fact-checking in contemporary society*. Madrid, Dykinson. Chapter 3, pp. 39-61. [Accessed: 29 March 2025]. Available at: https://www.dykinson.com/libros/disinformation-and-fact-checking-in-contemporary-society/9788411707107/

European External Action Service. (2025). *The 3rd EEAS report on foreign information manipulation and interference threats* [online]. [Accessed: 29 March 2025]. Available at:https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats_en

Fedchenko, Y. (2016). Kremlin propaganda: Soviet active measures by other means [online]. *Sõjateadlane (Estonian Journal of Military Studies)*. 2, pp. 141-171. [Accessed: 29 March 2025]. Available at: https://ojs.utlib.ee/index.php/st/article/view/23975/18184

Finlayson, M. A. and Corman, S. R. (2013). The military interest in narrative [online]. *Sprache und Datenverarbeitung*. 37(1-2), pp. 173-191. [Accessed: 29 March 2025]. Available at: https://users.cs.fiu.edu/~markaf/doc/j2.finlayson.2013.sdv.37.173_archival.pdf

Fisher, W. R. (1984). Narration as a human communication paradigm: The case of public moral argument [online]. *Communication Monographs*. 51, pp. 1-22. [Accessed: 29 March 2025]. Available at: https://doi.org/10.1080/03637758409390180

González, M. (2025). El informe de Seguridad Nacional atribuye a Rusia campañas desestabilizadoras de desinformación por la dana [online]. *El País*. [Accessed: 29 March 2025]. Available at: https://elpais.com/espana/2025-05-22/el-informe-de-seguridad-nacional-atribuye-a-rusia-campanas-de-desinformacion-por-la-dana.html

Griffey, Q., Zigmond, N. and Leinhardt, G. (1988). The effects of self-questioning and story structure training on the reading comprehension of poor readers. *Learning Disabilities Research*. 4(1), pp. 45-51.

Ha, A. Y. J. *et al.* (2024). Organic or diffused: Can we distinguish human art from AI-generated images? En: ACM. *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security* (CCS '24). DOI: https://doi.org/10.1145/3658644.3670306

Kantar. (2024). Art or entertainment: Ukrainians' attitude towards GenAI [online]. *Kantar*. [Accessed: 29 March 2025]. Available at: https://www.kantar.com/ua/inspiration/advertising-media/ukrainians-about-genai

Kereopa-Yorke, B. (2023). *ClausewitzGPT framework: A new frontier in theoretical large language model enhanced information operations* [online]. UNSW Canberra at the Australian Defence Force Academy. [Accessed: 29 March 2025]. Available at: https://arxiv.org/abs/2310.07099

Kupfer, M. and Vorozhko, T. (2025). Russia uses deepfakes against Ukrainian refugees [online]. *Voice of America*. [Accessed: 29 March 2025]. Available at: https://www.golosameriki.com/a/russia-uses-deepfakes-against-ukrainian-refugees/7953485.html

Newby, G. (2024). *The synergy of OSINT and narrative intelligence* [online]. Edge Theory. [Accessed: 29 March 2025]. Available at: https://edge-theory.com/resources/osint-and-narrative-intelligence

Mateas, M., and Sengers, P. (1998). *Narrative intelligence* [online]. American Association for Artificial Intelligence. [Accessed: 29 March 2025]. Available at: https://www.cs.cmu.edu/~michaelm/nidocs/MateasSengers.pdf

Miskimmon, A., O'Loughlin, B. and Roselle, L. (2013). *Strategic narratives: Communication power and the new world order*. London, Routledge. ISBN: 978-0-415-71760-1.

Murphy, B. (2023). *Foreign disinformation in America and the U.S. government's ethical obligations to respond*. Cham, Springer Nature. ISBN: 3-031-29904-3.

OpenAI. (2024). *AI and covert influence operations: Latest trends* [online]. [Accessed: 29 March 2025]. Available at: https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operati ons/

Rana, M. S. *et al*. (2022). Deepfake detection: A systematic literature review. *IEEE Access*. 10, pp. 25494-25513. DOI: https://doi.org/10.1109/ACCESS.2022.3154404

Romaniuk, V. (2023). Disinformation narratives of hate as a tool of escalating Russia's war against Ukraine (based on StopFake fact-checking project materials). *Estonian Journal of Military Studies*. (23), pp. 143-157. DOI: https://doi.org/10.15157/st.vi23.24202

Rosen, G. (2023). Raising online defenses through transparency and collaboration [online]. *Meta Newsroom*. [Accessed: 29 March 2025]. Available at: https://about.fb.com/news/2023/08/raising-online-defenses/

Rössler, A. *et al*. (2018). *FaceForensics: A large-scale video dataset for forgery detection in human faces* [online]. [Accessed: 29 March 2025]. Available at: https://arxiv.org/pdf/1803.09179.pdf

Sadeghi, M. and Blachez, I. (2025). The infection of Western AI chatbots by a

Russian propaganda network [online]. *NewsGuard*. [Accessed: 29 March 2025]. Available at: https://www.newsguardtech.com/wp-content/uploads/2025/03/March2025PravdaAIM isinformationMonitor.pdf

StopFake. (2023). *Video Fake: Commander-in-Chief of the Armed Forces of Ukraine Zaluzhny is preparing a military coup* [online]. StopFake. [Accessed: 29 March 2025]. Available at: https://www.stopfake.org/uk/videofejk-golovnokomanduvach-zsu-zaluzhnij-gotuye-vijskovij-perevorot/

—. (2024). *Video fake: Commissioner for Human Rights of the Council of Europe criticized "language patrols" in Ukraine* [online]. StopFake. [Accessed: 29 March 2025]. Available at: https://www.stopfake.org/uk/videofejk-komisar-radi-yevropi-z-prav-lyudini-rozkritikuva v-movni-patruli-v-ukrayini/

Stradinger, J. (2024). *Narrative Intelligence: Detecting Chinese and Russian Information Operations to Disrupt NATO Unity* [online]. Foreign Policy Research Institute. [Accessed: 29 March 2025]. Available at: https://www.fpri.org/article/2024/11/intelligence-china-russia-information-operations-a gainst-nato/

Ukraine (2019). *Law ensuring the functioning of the Ukrainian language as the state language No. 21, Article 81* [online]. Verkhovna Rada of Ukraine. [Accessed: 29 March 2025]. Available at: https://zakon.rada.gov.ua/laws/show/2704-19#Text

Ukrainian Institute of National Memory. (2023). *Why Ukrainians and Russians are historically not "brotherly peoples"* [online]. Ukrainian Institute of National Memory. [Accessed: 29 March 2025]. Available at: https://uinp.gov.ua/informaciyni-materialy/rosiysko-ukrayinska-viyna-istorychnyy-kont ekst/chomu-ukrayinci-ta-rosiyany-istorychno-ne-bratni-narody-infografika

Viginum. (2024). *Portal Kombat: A structured and coordinated pro-Russian propaganda network* [online]. [Accessed: 29 March 2025]. Available at: https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

Waldman, S. and Havel, S. (2022). Launching narrative into the information battlefield. *Connections: The Quarterly Journal*. 21(2), pp. 111-122. DOI: https://doi.org/10.11610/Connections.21.2.08

Putin, V. (2022). Address by the President of the Russian Federation [online]. *Kremlin.ru*. [Accessed: 29 March 2025]. Available at: http://kremlin.ru/events/president/news/67843

What does the growth of OSINT mean for military intelligence analysts?

Marcel Plichta
Edwin Dudley-Taylor

Abstract

Intelligence practitioners worldwide are embracing open-source intelligence (OSINT), and militaries are no exception. However, military analysts often answer a distinct set of questions compared to their counterparts in civilian intelligence and the private sector. Consequently, existing definitions of OSINT can be confusing, and the discipline's benefits and trade-offs are often misunderstood in a military context. In this article, we will define OSINT in terms useful to military intelligence analysts and discuss how the needs of military analysts and consumers require a distinct set of information from OSINT. It will then draw out the benefits and challenges of adopting open-source collection more fully into the military intelligence process. Ultimately, OSINT collection offers an additional and frequently cheaper way for analysts to answer some kinds of intelligence questions and could make it easier to share intelligence with other services and the general public. At the same time, analysts should be wary of overreliance on OSINT to the exclusion of other collection disciplines, consumer bias towards or against information collected from OSINT, and the potential legal and ethical constraints for collecting personal information.

Keywords

OSINT, Intelligence analysis, Military Intelligence, Intelligence training, Tradecraft.

1 Introduction

For the past few years, intelligence organizations have made a concerted effort to embrace and integrate "open-source intelligence" (OSINT) into their work. Commentators argue that NATO countries in particular could benefit from it. Harper and Basset (2024) argue that "by exploiting OSINT more fully and by integrating it into the wider intelligence cycle, NATO can pre-empt, deter, and defeat its adversaries' efforts." The US Office of the Director of National Intelligence (ODNI, 2024) went as far as labelling OSINT "the INT of first resort" in their 2024-2026 OSINT Strategy.

Adopting OSINT promises improvements ranging from better intelligence collection to lower costs, but what does OSINT offer militaries and military analysts? This article will discuss the benefits and challenges of prioritizing OSINT collection for analysts in a military context. It will begin with an overview of OSINT and the unique elements of intelligence as practised by militaries. The article will then discuss the benefits of OSINT for military analysts and the potential obstacles they will face in incorporating open-source methods into their work. Ultimately, embracing OSINT offers military intelligence organizations a new avenue to answer intelligence questions and coordinate with other organizations, but could also incur challenges in ensuring that consumers understand the limits of the discipline and ensuring collection is within legal and ethical limits. How well organizations deal with the challenges of adopting OSINT in practice will determine how much use military analysts get out of the discipline.

2 What is OSINT?

Even though discussion of OSINT is growing astronomically in intelligence discourses, government agencies, journalists, commentators, and scholars often use the term to refer to different concepts. Several definitions are often used interchangeably. For instance, private sector and volunteer organizations can use OSINT to refer to any private sector work related to intelligence, like due diligence, private investigations, personal security, brand management, and journalism. More narrowly, some use it as a shorthand for intelligence derived specifically from social media platforms. The loosest definition is used by social media users themselves, who often frame simple collation tasks like content aggregation as "OSINT."

To make matters more complicated, OSINT is functionally an umbrella term for many different kinds of collection activities, some of which overlap with the established collection disciplines. For instance, using commercial satellite imagery to observe activity in a military base is GEOINT, but is also OSINT so long as the imagery is publicly-available information. Organizationally, this means that a GEOINT analyst could

also be an OSINT analyst if the imagery was from an open source, even though they are applying the same skillset to inform the same intelligence consumers.

Government officials will also use different definitions, sometimes referring to finished intelligence products using only publicly-available information as OSINT. However, governments more often define OSINT as a collection discipline like HUMINT and SIGINT. Spain's Centro Nacional de Inteligencia (CNI) describes OSINT as "information coming from open sources." The U.S. Office of the Director of National Intelligence (2024: 6), meanwhile, released an updated definition of OSINT in December 2024 that defined it as "derived exclusively from publicly or commercially available information." This contrasts with their description of OSINT intelligence products, which are "derived solely from PAI, CAI, and/or OSINT" (ODNI, 2024: 7).

The remainder of this article will proceed with an understanding of OSINT as a gathering activity. That does not mean OSINT has no relevance for analysts. As we will discuss later, open-source gathering naturally feeds into processing, analysis, and finished intelligence products, where analysts encounter the benefits and challenges of integrating OSINT into their workflows.

3 Military and civilian intelligence priorities

Most scholarly discussions about OSINT is centred on its usefulness in civilian contexts, whether that be the private sector or a non-military intelligence agency. However, military and civilian consumers of intelligence have different intelligence requirements, prefer different types of intelligence products, and use intelligence to support a different set of activities, even if both consumers are part of the same government.

Military consumers of intelligence include senior decision-makers in the military (like commanders), civilian policymakers that direct or advise on defence policy such as a National Security Advisor, and national leaders that direct the military, such as a President or Prime Minister. While civilian intelligence agencies often cover a range of intelligence issues from economic stability to cybercrime, Military Intelligence is often more restrictive. Because Military Intelligence is only concerned with issues like trade, crime, or diplomacy when they directly relate to national security, intelligence analysts focus more directly on defence issues like adversary intentions, counterterrorism, and support for military operations. The primary use of intelligence in a military context is for national security, defence planning, and strategic or tactical operations. Sometimes there is overlap with civilian agencies, but, in those cases, analysts normally take different approaches more suited to their consumers' needs.

Like civilian agencies, military intelligence organizations engage in a variety of gathering activities. In addition to OSINT, these often include older gathering disciplines such as Signals Intelligence, Human Intelligence, and Geospatial Intelligence. However, most national intelligence agencies share information across organisations, meaning that military analysts can often access information collected from a civilian intelligence agency and vice-versa. Depending on the way intelligence communities are structured, civilian intelligence agencies can also be under the same broad umbrella as the military, as is the case with the U.S. National Security Agency.

Even if military and civilian agencies share the same pool of information, intelligence analysts in the military put that collection to different ends. Military Intelligence products focus on "supporting commanders in their decision-making by helping to increase their understanding," which can range from short-term analysis of threat assessments and operational planning to longer-term needs like strategic forecasting (UK Ministry of Defence, 2023: 8-9). Military intelligence often assesses topics like opposing forces' capabilities, the likelihood of conflict, and challenges to planned or ongoing operations. Longer-term military intelligence is also used within defence policy, weapons development, and geopolitical analysis to anticipate emerging threats and maintain a nation's military superiority.

The needs of military intelligence consumers require a unique set of products from intelligence analysts. For instance, military analysts often produce order of battle (OOB) analyses, battle damage assessments, and product targeting reports that serve the specific needs of battlefield commanders and senior decision-makers (United States Marine Corps, 2016). While some opportunities and challenges of adopting OSINT apply to military and civilian analysts alike, the extent to which it hinders military and defence analysts overall will largely depend on whether OSINT makes it easier or harder for them to produce the analyses their consumers need.

4 Advantages of OSINT for military analysts

Although military analysts face a different set of requirements and expectations than their civilian counterparts, OSINT does offer ways to improve their analyses and ease dissemination. Analysts could leverage OSINT to fill information gaps, verify and evaluate concurrent gathering efforts, improve transparency, and ease intelligence sharing with other organizations.

The role of intelligence gathering is to answer the consumer's questions. However, different kinds of collection can have gaps that leave analysts and decision-makers with an incomplete picture. OSINT could fill some of the gaps for military analysts. One of OSINT's unique benefits is its ability to

collect information and discourses on social media. For instance, the propaganda and recruitment strategy of an extremist group might be difficult to understand without a consistent effort to collect their public statements and messages to sympathetic social media groups. In turn, collecting the level of engagement those posts get helps determine whether those strategies are effective. Alternatively, collecting more concrete information from social media, like combat footage, can help analysts understand where fighting is taking place more precisely and rapidly than other gathering methods in the right circumstances.

The more information analysts have access to, the stronger their analysis is. Researchers for the U.S. Military found that OSINT can help analysts "identify unusual deployments, movements, exercises, targets and dispositions, high-value target tracking, and unusual logistic patterns" (Sieting, 2024). In one infamous case in 2022, a Russian journalist posted an image of a Wagner Group base, only for Ukrainian forces to geolocate and strike the site (Kirichenko, 2023). OSINT can also contribute to Battle Damage Assessments in cases where there is footage of fighting or its aftermath on social media, or to Order of Battle Analysis. The latter is often attempted by private sector organizations like Janes, indicating that OSINT methods could deliver a plurality of the information analysts need to keep an updated OOB for their consumers (Janes). Even if military analysts still largely rely on other collection disciplines to produce intelligence, an additional stream of information from OSINT collectors will improve analyst confidence and add redundancy if a source of information is lost.

A stronger focus on OSINT gathering also means that military analysts could operate better in contested environments or where other gathering platforms are unable to function. The decentralized nature of open-source information, which is often shared voluntarily by lots of different individuals, makes it a flexible gathering source under the right circumstances. Ramsey (2024) notes that, in places where national collection platforms are struggling, "OSINT will likely be available due to the sheer number of sensors providing information that are available and will likely serve as the primary resource used to fill these gaps." There are limits to the information collected in a battlefield context, particularly if a belligerent is enforcing an Internet blackout or other measure to control information, but even so, access to OSINT could be a vital lifeline for analysts with few other sources of information.

Additionally, OSINT gathering on social media and foreign press can help determine what adversaries want the public to believe about them. For instance, an adversary nation might amplify the idea that its missile technology can beat a neighbour's air defences. As an example, Iran's Revolutionary Guard Corps reportedly invest heavily in communications

networks to "control part of the process of influence in Iran, ensuring that their strategic narrative and perception of reality remain dominant" (Gill, 2020, p. 113). Alternatively, an extremist group might issue threats against a famous landmark to cause panic and put pressure on local authorities. Analysts can interpret strategic messaging through open sources to provide insight into an adversary's intentions or priorities, though as we will discuss below, they must be equally aware of widespread deception and misinformation in open sources.

5 The use of OSINT to improve and verify information gathering

To be sure, other gathering methods often fill the same gaps as OSINT. A confidential human source could always describe a propaganda strategy, and GEOINT could show where fighting is taking place or assist with OOB analysis. However, proponents of OSINT argue that it is often a more cost-effective way of answering the same intelligence questions. For example, intelligence requirements may not need a government agency to pay for an expensive satellite network if a commercial provider can provide images of sufficient quality. However, it should be noted that the potential cost savings are not felt by the analysts directly. Rather, it could mean that their products are different, but not necessarily better if they came to the same conclusion.

Of course, political or agency leaders might decide that it's worth the effort to build and maintain more expensive collection capabilities for analysts anyway. Even in those cases, OSINT could help triangulate and fill gaps left by fragmentary information. Miguel Sánchez de Toca Alameda *et al.* (2023: 21) note that OSINT can "support other intelligence disciplines to confirm or reject hypotheses" in a military context. This benefits analysts' confidence in their assessments and their ability to give feedback to collectors in other disciplines. For instance, analysts can follow up on incomplete information from a human source through OSINT collection to confirm the information's accuracy. This in turn improves analysts' ability to evaluate the quality of the source for HUMINT collectors.

Investment in OSINT could also broaden the reach of organizations with limited resources. In the past few years, open-source tools enabled everything from tracking international shipping to determining GPS interference. For instance, Grey Dynamics (2024) assisted CBS News in tracking Russian contractors' smuggling efforts using open-source methods. While it was difficult and expensive to monitor global events in the pre-Internet age, the information and tools available to open-source collectors make analysis significantly easier for those without more advanced tools available to information services or public intelligence agencies.

Intelligence organizations are not always as large as the CIA or DGSE. Smaller nations may only have an interest in collecting information about their immediate region or lack the resources to build clandestine collection capabilities to do things like tracking global shipping or determining where satellite navigation is unavailable in real-time. However, threats to a country and its citizens are not always proximate. For instance, a nation's commercial vessels might pass through or near a conflict zone that is thousands of kilometres from its borders. Even if the vessel is outside the range of information-service operative elements, policymakers may still instruct the military to monitor its safety and provide threat assessments. To meet global security requirements quickly, contracting an open-source firm or licensing a tool that collects OSINT for military analysts is an opportunity to increase the breadth of information available and meet a wider scope of intelligence requirements.

6 Use of OSINT in transparency and intelligence sharing

Military analysts can also leverage OSINT to improve their organization's transparency. Government intelligence work is often classified and opaque to the public for national security reasons. While most people understand that vital security issues require secrecy, agencies can boost public confidence in their work by making intelligence products public where possible. In many cases, intelligence products that use mostly OSINT to support the analysis can be classified at a lower level and declassified sooner without fear of revealing sensitive sources and methods. For instance, in 2023 the U.S. Defense Intelligence Agency (2023) released a product to the public that used open-source information to show that Russia was using Iranian-designed drones in the war in Ukraine.

Lower classification OSINT products can also facilitate intelligence sharing with allies and partners. The process of declassifying information or making it releasable to another government is often laborious, particularly if the intelligence product uses a variety of different sources to underpin the analysis. While a military intelligence agency might guard sensitive collection methods jealously, a product that mostly or entirely relies on OSINT would be easier to share with a partner that the agency does not fully trust to keep it secure, or with organisations like the United Nations or NATO that solicit information from their Member States. A leak or breach of OSINT-based intelligence products, while still a national security threat, is safer than a breach that compromises the safety of a human source or the specifics of an exquisite collection platform.

7 Challenges for military analysts

Military analysts might encounter some hurdles in adopting and using OSINT. These potential challenges include overwhelming amounts of

information, adversary deception, consumer bias, increased privatization, more reliance on Artificial Intelligence, and legal restrictions on the collection and use of OSINT.

OSINT might offer opportunities to fill gaps, triangulate reporting, or answer intelligence questions in a less expensive way, but there are also limits and challenges. More information creates more potential points of analytic failure. Romanow (2025) notes that "the same analytical biases that have fueled past intelligence failures will continue to be present, and they could even be accentuated by the many new sources and new players in the field of military intelligence." Ensuring that these drawbacks are addressed will help analysts get the most out of OSINT.

Analysts should not assume that a greater focus on OSINT will fill every intelligence gap or feel pressured to lean on OSINT at the expense of other collections. OSINT, like all gathering disciplines, cannot answer some intelligence questions that military intelligence agencies need to answer. Military intelligence more often seeks to gather information about militaries and other adversaries' capabilities, which are not always available from open-source collection. For instance, the location of an adversary nation's airbases might be publicly available information, but a list of the military assets at those locations might not. Similarly, OSINT may not provide insight into what operations an extremist group is planning and instead require another form of collection like clandestine SIGINT to reliably monitor their internal communications.

One of the biggest challenges when it comes to OSINT gathering on social media is inconsistency. An account or set of accounts could indicate where an adversary unit is today, but may not be able to do so tomorrow. Other accounts could unintentionally mislabel locations and events or even claim that older videos depict recent events. This is compounded in a military context since military equipment is frequently misidentified by the public. One such example was a widely shared video of a Russian air defence system in Sudan, which turned out to be fake (Army Recognition, 2023). The issue of reliability is not unique to OSINT, but it does add another layer of complications for collectors and analysts to ensure they are using quality information in their products.

All forms of intelligence collection are susceptible to deception. However, deception in OSINT, and particularly collection on social media, is an acute problem for intelligence organizations. There are a few complicating factors: firstly, users on social media do not usually feel the need to fact-check or verify content or claims that they share. This means that even if users do not intend to deceive, they still can through a lack of due diligence. Even more complicated is the growing problem of disinformation purposely spread by bots or malign actors. Relying on social media

collection is therefore fraught for analysts since the users and posts can have a tenuous relationship with objective reality.

For military analysts, the volume of information and the scope of deception might reduce OSINT's usefulness on the battlefield. Rasak (2021) notes that "the consequences of event barraging, misinformation campaigns, trend hijacking, and military deception will fundamentally detract from the usefulness of OSINT at the tactical level." Commanders may not wish to make a consequential battlefield decision based on a compromised information stream, and analysts may not disseminate it until there is independent confirmation. These challenges can make intelligence products based largely on OSINT less actionable and undermine one of the touted benefits of OSINT, which is that it's often faster than other information streams.

Nonetheless, gathering information on or about social media is beneficial for military organizations. Even though social media collection is made difficult by deception, it can also present a unique opportunity to understand and counteract strains of dis- or mis-information. Anticipating the impact of disinformation is vital because, even if something is not true, people may adjust their behaviour accordingly if they believe it. For instance, doctored footage of a military mobilization across the border might prompt a commander to put their forces on alert just in case. Understanding the origins and intentions (if there are any) of deception via social media is therefore a powerful way for analysts to inform decision-makers.

Another challenge is that intelligence consumers might be biased against or in favour of OSINT. They often have personal opinions about which kinds of collection are more reliable than others. For instance, a general may not consider information gathered on social media trustworthy enough to conduct an operation. On the other hand, an intelligence consumer could prioritise OSINT collection on a topic even if it's ill-suited simply because they believe OSINT is less expensive. Personal bias is compounded if the organization is adopting another controversial advancement, AI, as part of processing OSINT. Either scenario can become a challenge for military analysts, who have to ensure they are properly characterizing their sources in intelligence products and briefings.

Military analysts could also face challenges using Artificial Intelligence (AI) to assist with managing the volume of information collected through OSINT. Juan Luis Sánchez Sánchez (2025) argues that "the growing use of AI to analyse the information environment through OSINT will be essential to prevail and advance intelligence scenarios for subsequent defensive/offensive use." For military analysts, this means developing new skills to get the most out of AI, and developing a rudimentary understanding of how AIs and particularly LLMs function to guard against issues like hallucinations. However, there is only so much analysts can do, as they will largely

be at the mercy of the wider intelligence organization that dictates where and how AI is used in the intelligence cycle.

8 Legal restrictions and privatization of information gathering

Even in a government context, the discussion of OSINT often overlaps with the emergence of private contractors and tech companies. Bringing in contractors and other private entities could be an easy way to initially integrate OSINT capabilities since gathering methods are often unclassified and OSINT collectors do not necessarily need security clearances as high as if they were working with other gathering disciplines. If the contractor already has the capability and personnel, it could be quicker and cheaper for policymakers to bring them into the organization in the short term than building a similar in-house capability from scratch.

However, embracing privatization has its own set of challenges for analysts. Williams and Blum (2018: 22-23) point out that commercial products have hidden costs for governments since they need to be adapted for classified systems. From a security perspective, smaller nations might need to risk contracting a foreign or multinational company to provide the OSINT services they want. Both issues can complicate work for analysts, who could end up dealing with a complicated process to access information collected by a private firm or lose access to those tools in the long term if the firm loses or does not renew its contract with the government.

The discussion of the privatization of OSINT also overlaps with another key consideration: ethical or legal restrictions on OSINT collection (Smith and Cook, 2023). Even if a member of the public puts their information on the Internet, intelligence agencies cannot necessarily collect it. Most NATO countries have laws governing the collection and storage of personal data, particularly of their nationals. Military analysts usually focus on external threats rather than internal affairs, but still have to ensure that they are working within the law in cases like a citizen acting abroad or issues like counterintelligence and defence of the homeland. As was the case with Artificial Intelligence, the legal boundaries and contract decisions of OSINT are largely out of the hands of analysts themselves, but are still a potential impediment to their work if implemented inefficiently.

Privatization adds a further layer to the legal and ethical challenges, as companies may face a complicated set of regulations to conduct OSINT collection, particularly if they are not based in the same country as the intelligence agency. UK law firm Proelium (2024) notes that “The general legal position is that [UK Intelligence Law] does not apply to activities of a private company, however, that position is different when a private company is contracted by a government entity to carry out an activity that may

amount to directed surveillance activities." Analysts who work with private companies to collect OSINT might end up with less information than they anticipated in order to comply with local laws and agreements.

9 Conclusion

Our study discussed the unique advantages and drawbacks of using OSINT in a military context. The biggest implication for policymakers is a need to understand what increased focus on OSINT can deliver for their organization. While OSINT is generally thought to be "cheaper" than other forms of collection, investing in a new OSINT capability that is then underutilized is a missed opportunity. For analysts themselves, it is imperative to understand how to integrate OSINT into their workflows effectively. Because OSINT collection platforms and methodologies can impact a wide range of analytical activities, analysts should ensure they have been properly trained to reap the benefits without succumbing to the drawbacks. Extremely powerful OSINT tools only have limited utility if their users are unsure of how to get the most of them.

There are also opportunities for scholars and commentators to expand the discussion of where OSINT can improve intelligence analysis for militaries. While OSINT is a frequent topic of study in intelligence and security studies in isolation, there is a need to further explore the ways in which open source methods could improve military intelligence and expose gaps in existing OSINT tradecraft. In particular, the growing relationship between OSINT and Artificial Intelligence in military contexts remains understudied. Lastly, the discussion of the utility of OSINT is often isolated from the discussion of the ethics of OSINT and associated technologies like AI. Researchers should seek to harmonize these discussions, as they are consequential for organizations like militaries that are expected to use force within legal and ethical boundaries.

Greater reliance on OSINT will change how military analysts do their job, but how much remains to be seen. Many of the core skills used by all-source analysts have less to do with the precise collection method and more to do with critical thinking, anticipating the needs of intelligence consumers and delivering finished intelligence products promptly. OSINT certainly could assist with filling gaps and getting critical intelligence to consumers quickly. Even so, military intelligence deals directly with issues of grave importance to national security, so military intelligence analysts need to ensure that OSINT is treated with the same level of seriousness and scrutiny as other gathering disciplines. With proper contextualization and support from the broader organization, OSINT can become a powerful tool for analysts.

Bibliography

Defense Intelligence Agency. (2023). *Iranian UAVs in Ukraine: A Visual Comparison*.

Gill, M. (2020). Capitalism, Communications, And The Corps: Iran's Revolutionary Guard And The Communications Economy. *Academic Journal Defence Strategic Communications*. 9.

Grey Dynamics. (2024). *Central Africa*.

Harper, C. and Basset Cross, R. (2024). *NATO Must Recognize The Potential of Open-Source Intelligence.* Atlantic Council.

Kirichenko, D. (2003). *The Growing Use of Scamming Techniques and Social Media on the Battlefield*. Irregular Warfare Center.

Office of the Director of National Intelligence. (2024). *Citation and Reference for Publicly Available Information, Commercially Available Information and Open Source Intelligence.*

—. (2024-2026). *The Intelligence Community OSINT Strategy*.

Proelium. (2024). *Compliance in OSINT: Legal Requirements for Data Protection and Privacy*.

Ramsey, C. (2024). *Ivy Intelligence (IVI) Large-Scale Combat Operations Targeting*. Army University Press.

Rasak, J. (2021). *Event Barraging and the Death of Tactical Level Open-Source Intelligence*. Army University Press.

Romanow, N. (2025). The Transparency Trap: Risks of Deception in the Age of OSINT. *Proceedings*. U.S. Naval Institute. 151(1), p. 1463.

Sánchez, J. (2025). Inteligencia artificial en apoyo a la inteligencia militar. Eje fundamental del éxito o fracaso en la competición estratégica entre grandes potencias. In: Instituto Español de Estudios Estratégicos (ed.). *La inteligencia artificial en la geopolítica y los conflictos*, pp. 105-151.

Sánchez de Toca Alameda, M. *et al.* (2023). El Subsistema De Inteligencia Del Ejército De Tierra: Presente Y Retos De Futuro. *Cuaderno de Inteligencia*. Madrid, Ministerio de Defensa, p. 21.

Sieting, L. (2024). *Intelligence Discovery Experiment: Open-Source Intelligence Support to Targeting*. Capabilities Development & Integration Directorate.

Smith, A and Cook, S. (2023). *A Guide to Open-Source Intelligence*. Grey Dynamics.

UK Ministry of Defence. (2023) *Joint Doctrine Publication 2-00 Intelligence, Counter-Intelligence and Security Support to Joint Operations*.

United States Marine Corps. (2016). Doctrinal Publication 2, Intelligence, and Marine Corps Warfighting: Intelligence Operations Intelligence Production and Analysis. *MAGTF Intelligence Production and Analysis*. U.S. Marine Corps.

Williams, H. and Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. *Rand*. Santa Mónica, Rand Corporation, pp. 22-23.

Scientific Committee and Editorial Board

Scientific Committee:

Arturo Esteban Ceballos
Lieutenant Colonel (Spanish Marine Corps).
PhD in Security, Risk and Conflict Analysis.
J2 Analyst at STRIKEFORNATO.

Emilia José Peña Ruíz
Lieutenant (Spanish Navy, Specialist Corps).
PhD in Social and Legal Sciences.
J2 Analyst at the Spanish Joint Force Command (MOPS).

Julia Pulido Gragera
PhD in Public International Law and International Relations.
Chief of Staff to the Regional Minister for Environment, Agriculture, and Internal Affairs, Comunidad de Madrid.
Captain (Reserve Force), Intelligence Department, ESFAS (CESEDEN).

Licesio J. Rodríguez Aragón
PhD in Mathematics.
Associate Professor of Statistics and Operations Research. School of Industrial and Aerospace Engineering of Toledo, University of Castilla-La Mancha.
Ensign (Reserve Force), Intelligence Department, ESFAS (CESEDEN).

Adrián Nicolás Marchal González
PhD in Law. PhD in Criminology and Forensic Science.
Director of the Security and Defense Department, Nebrija University.

Álvaro Cremades Guisado
PhD in Political Science, Administration, and International Relations.
Director of the Master's Degree in Security and Defense, Nebrija University.

Editorial Board:

Chairman

José Antonio Fuentes de la Orden
Brigadier General (Spanish Army), Director of Academic Affairs, Deputy Director of the Higher School of the Armed Forces (ESFAS).

Board Members

Ángel Segundo Gómez González
Colonel (Spanish Army, Ret.)

Carlos Alberto Ramírez Sánchez
Colonel (Spanish Army). Director of the Intelligence Department at ESFAS.

Rules for shipment of ítems

Intelligence Notebook Topic 4

The next issue of the Intelligence Notebook will have as its main theme: «The role of the Extended Intelligence Community, present and future». If you wish to collaborate, the proposed items must meet the following requirements:

1 Guidelines for the shipment of articles

The authors are required to verify that their submission complies with all guidelines shown below.

- Not previously published or submitted for consideration by any other journal (or explained in the editor's comments).
- It adapts to the purpose and theme proposed in the corresponding Intelligence Notebook.
- Complies with the provisions of the «Rules for editing and publication at the Ministry of Defence» in format (paragraph 3), typographical aspects (paragraph 5), orthographic aspects (paragraph 6), citations and bibliography (paragraph 7) and images (paragraph 8).
- Conforms to the policy of plagiarism detection that ensures the origin of manuscripts.

2 Files to be submitted

The authors must send the following files to the Intelligence Notebook mailbox (ESFAS_CuadernoInteligencia@mde.es) no later than **March 30** of each year:

- 1 text document (Word Office-compatible format), with full text and paginated and no embedded images. Must be between 4,000 and 12,000 words long. If you have images, the location of these must be marked in the text, indicating the name of the image file (type of bold font and color).
- 1 Word document that includes a summary of up to 200 words and 5 keywords, which do not match the title. In Spanish and its translation into English.
- 1 Word document with a brief biography of the author of approximately 150 words.
- 1 photo of the author in jpg or tiff format.
- 1 folder containing all the images, in jpg or tiff format, and a minimum resolution of 300 dpi that makes them suitable for publication.
- 1 Word document with the corresponding photo footers.

3 Original receipt and approval process

Once the proposed article has been received and compliance with the publication rules has been verified, the author will be informed of the acceptance of his work **for evaluation** by the Editorial Board.

Among the articles received **will be selected** those that stand out for their originality, relevance, interest and topicality for publication in the corresponding Intelligence Notebook.

If **selected**, the article will be returned to the author with a correction proposal (if necessary). At the same time, the following documents that authors must complete for the assignment of rights and the collection for collaboration (the Council would make them available to authors) will be sent:

- Assignment of exploitation rights.
- Responsible declaration.
- Data Sheet

The period for error correction shall be 20 working days, after which the definitive versions of the articles must be submitted to the Editorial Board.

If you have any questions regarding the completion of this process, please send an email to the *Intelligence Notebook* mailbox.









PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL