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

Research Article

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

English translation with AI assistance (DeepL)

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

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

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

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

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

DEDICATION

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

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

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

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

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

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

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

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

ABBREVIATIONS

ABI: *Activity-based Intelligence*

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

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

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

CIFAS: Centre of Intelligence of the Armed Forces

CNI: National Intelligence Centre

COMINT: *Communications Intelligence*

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

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

CYBINT: *Cyber-Intelligence*, Cyberintelligence

ELINT: *Electronic intelligence*

FISINT: *Foreign* instrumentation *signals intelligence*

GEOINT: *Geospatial Intelligence*, Geospatial *Intelligence*

HUMINT: *Human Intelligence*

IDEM: Enhanced Dynamic Intelligence Enrichment and Enhancement

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

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

IMINT: *Imagery Intelligence*

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

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

MASINT: Measurement and *Signature Intelligence*

ML: *Machine Learning*, Machine Learning

NLP: *Natural Language Processing*

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

OSINT: *Open-Source Intelligence*

SCADA: *Supervisory Control* and *Data Acquisition*

SECED: Central Documentation Service

SIEM: *Security Information* and *Event Management*

SIGINT: Signal *Intelligence*

SOCMINT: *Social Media Intelligence,* Social Media Intelligence

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

TTPs: *Threats, Techniques and Procedures*

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

1. INTRODUCTION

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

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

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

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

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

1.1. METHODOLOGICAL NOTE

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

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

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

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

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

2. CONCEPT AND EVOLUTION OF INTELLIGENCE

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

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

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

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

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

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

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

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

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

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

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

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

2.1. TYPES OF INTELLIGENCE

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

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

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

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

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

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

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

2.2. EVOLUTION OF INTELLIGENCE APPROACHES AND STRATEGIES

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

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

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

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

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

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

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

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

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

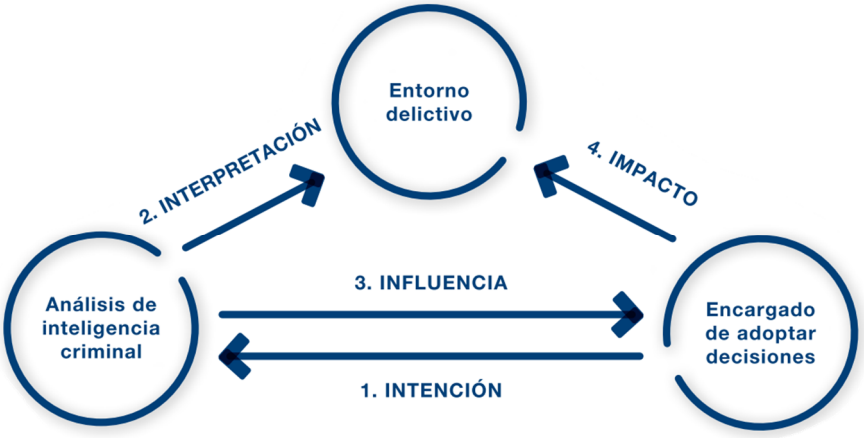
However, in recent decades, due to the complexity of threats and risks, many academics and practitioners have pointed out that the most successful holistic approach to combating the globalisation of crime is *Intelligence-Led Policing* (ILP), which translates as intelligence-led policing. This approach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

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

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

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

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



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

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

3. THE INTELLIGENCE CYCLE

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

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

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

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

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

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

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

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

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

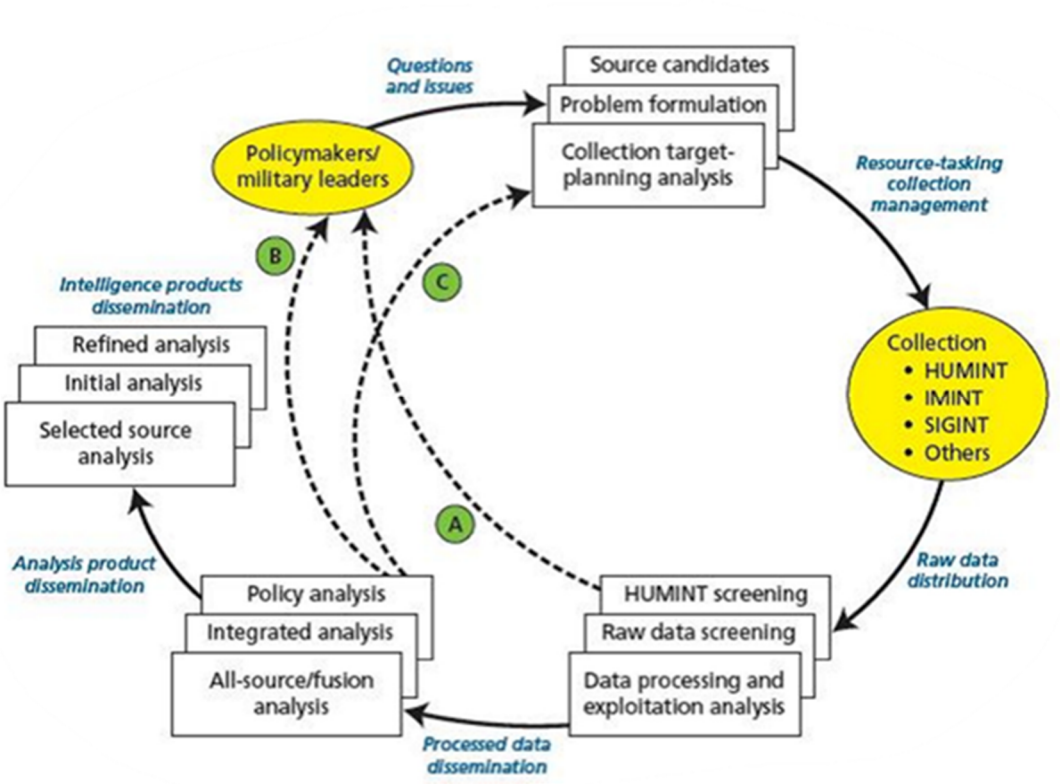
With regard to the dissemination phase, this is sometimes not passed through either, as not all the analyses produced reach the consumers. Many are not read by the recipients and are stored directly in the internal database. In other cases, customers often have already made their decisions and ignore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

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

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

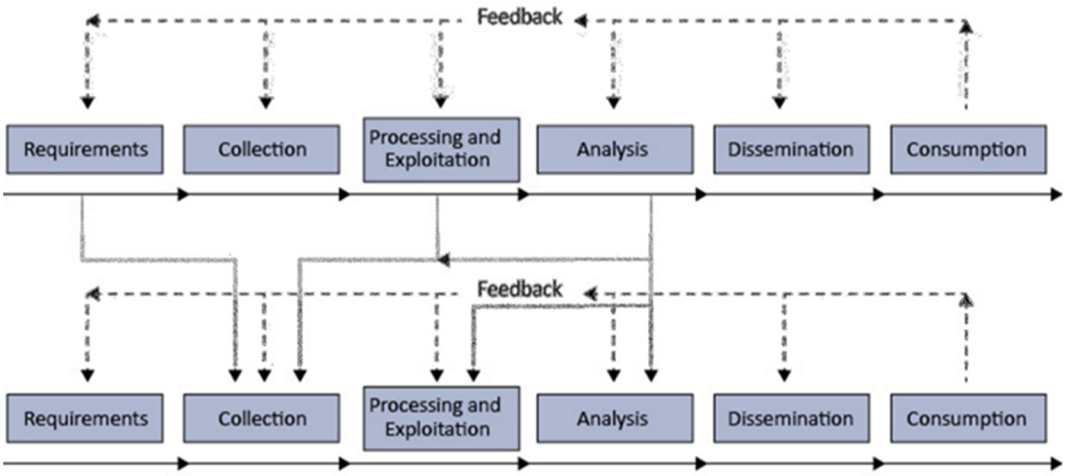
On the other hand, several authors have tried to capture the complexity of the intelligence cycle in alternative schemes to the traditional one. As can be seen inFigure2 , Treverton and Gabbard propose a more realistic approach that includes shortcuts between phases, showing that there are steps that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

Figure2
Treverton and Gabbard's approach



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

Figure3
Multi-strata process Mark Lowenthal



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

Figure 4
Target-Centric Intelligence by Robert M. Clark

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

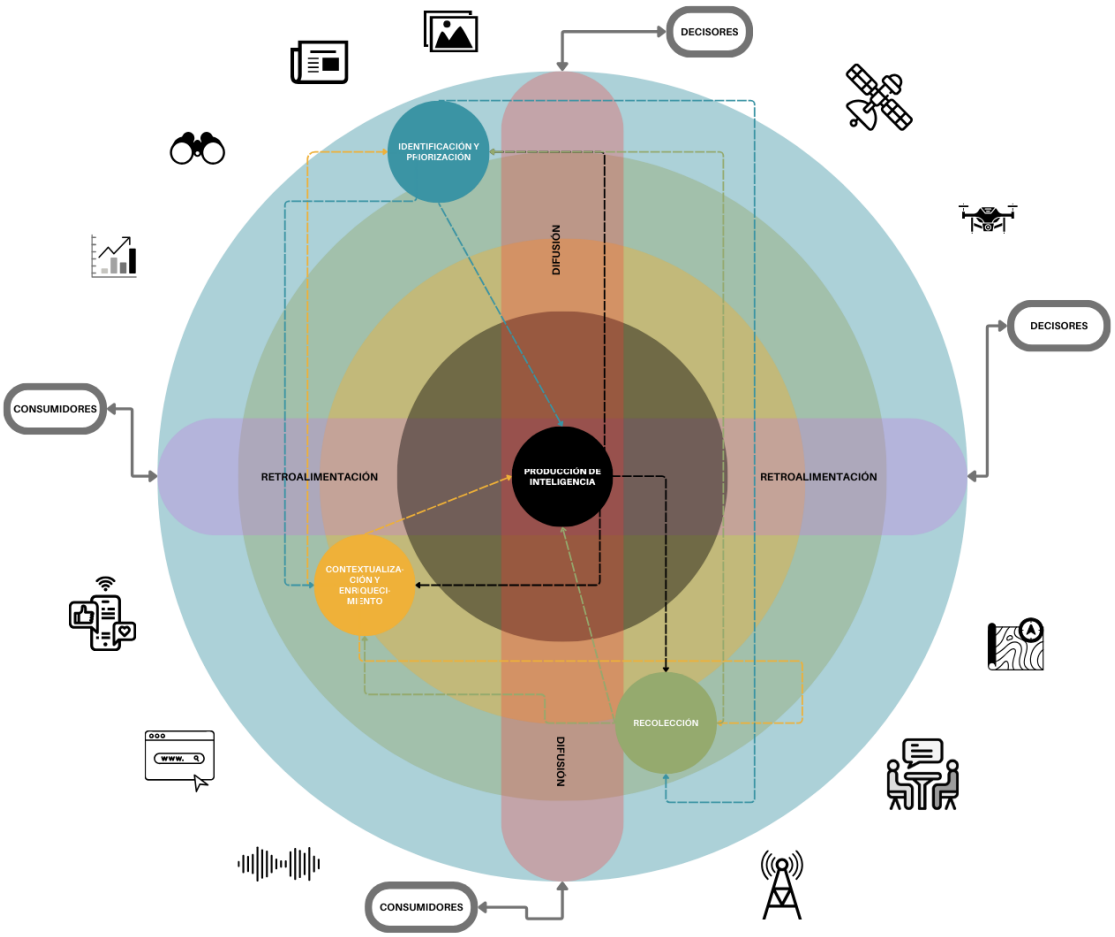
Below is a representative schematic of the IDEM model, in which the different phases are arranged as concentric circles. This arrangement reflects, on the one hand, the increasing proximity to the final intelligence product as one moves towards the centre, and on the other hand, the constant nature of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

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

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

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

Figure 5
IDEM intelligence model



Note: Own elaboration, Paula Castro Castañer, 2024.

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

4.1. PRACTICAL EXAMPLE OF THE IMPLEMENTATION OF THE IDEM MODEL

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

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

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

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

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

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

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

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

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

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

5. CONCLUSIONS

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

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

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

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

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

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

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

6. BIBLIOGRAPHICAL REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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