CENTRO ALTI STUDI DIFESA
SCUOLA SUPERIORE UNIVERSITARIA

UNIVERSITÀ DEGLI STUDI DI SALERNO

Dottorato di Ricerca in

Scienze dell'Innovazione per la Difesa e la Sicurezza

XXXVII CICLO

TITOLO DELLA TESI

THE ORGANIZATIONAL STRUCTURE OF INTELLIGENCE AND SECURITY AGENCIES AS AN EXAMPLE OF ADAPTATION TO THE EMERGING COMPLEXITY OF THE ENVIRONMENT: NORTH KOREA, ISRAEL AND FRANCE CASES

SECS-P/10

PRESENTATA DA: Michele FRISIA

COORDINATRICE DEL DOTTORATO: Prof.ssa Paola Adinolfi

Tutor:
Prof.ssa Paola Adinolfi

CENTRO ALTI STUDI DIFESA
SCUOLA SUPERIORE UNIVERSITARIA

UNIVERSITÀ DEGLI STUDI DI SALERNO

Dottorato di Ricerca in

Scienze dell'Innovazione per la Difesa e la Sicurezza

XXXVII CICLO

TITOLO DELLA TESI

THE ORGANIZATIONAL STRUCTURE OF INTELLIGENCE AND SECURITY AGENCIES AS AN EXAMPLE OF ADAPTATION TO THE EMERGING COMPLEXITY OF THE ENVIRONMENT: NORTH KOREA, ISRAEL AND FRANCE CASES

SECS-P/10

PRESENTATA DA: Michele FRISIA

COORDINATRICE DEL DOTTORATO: Prof.ssa Paola Adinolfi

Tutor:
Prof.ssa Paola Adinolfi

Summary

This dissertation aims to investigate intelligence and security agencies from a little-explored perspective. Not in terms of their operations, contributions to national security strategy, or from a historical perspective, but through the theoretical lens of organizational studies to understand their structure and functioning. The central research question concerns how different intelligence systems adapt their internal architectures and decision-making processes to a complex external environment.

The research initially involved a review of the existing scientific literature on the topic, aimed at identifying which models have been used in academia to study intelligence and security agencies from an organizational perspective. The review findings led to the hypothesis that the adhocratic model, as theorized by Mintzberg, could serve as a framework for studying the organizational structures of intelligence agencies. However, it was also hypothesized that agencies could be observed in practice that actually adopt this model in their organizational structure. To test this hypothesis, the research design relied on empirical investigation, using the methodological tool of case studies.

However, the two direct methods typically used in case studies (staff interviews or participant observation) proved impractical due to the intrinsic secrecy surrounding every aspect of intelligence agencies, starting with their very structure. Accessing the necessary data therefore presented a challenge, and to overcome this limitation, gray literature was used. This information heritage, although highly heterogeneous, incomplete, sometimes contradictory, and not peer-reviewed, provides otherwise inaccessible information on the functioning, structure, and cultural characteristics of intelligence organizations.

Within the thesis, grey literature was therefore treated not as a substitute for academic sources, but as a body of evidence to be used for study, albeit after being assessed and classified according to its degree of reliability and credibility.

The case study method was applied to three national intelligence systems: North Korea, Israel, and France. The selection was based on two criteria. On the one hand, the individual and specific characteristics of the system ensured significant differentiation. Each of the three systems has a distinctive and peculiar organizational configuration, as well as a different approach to the challenges posed by complex environments. The other criterion used concerns the interaction between intelligence agencies and the outside world. Only when significant interaction is present is the amount of data available in the gray literature sufficient to undertake a study.

In particular, the North Korean system is characterized by redundancy, fluidity, and selective decentralization, with frequent redefinitions of roles and dependencies. While these traits suggest elements of adhocracy, the scarcity and opacity of the available data preclude definitive conclusions. This system, on the other hand, is particularly aggressive in international projections, and this has allowed us to gather material, albeit scant, regarding its functioning.

Israel was selected because it has a unique system, a hybrid ecosystem that combines public and private actors. This system fosters innovation, particularly in technology and information technology, and leverages young talent to create a culture that fosters adaptability. It is a clearly adhocratic ecosystem in which intelligence functions are distributed among public agencies, military units, startups, academic research centers, and the financial sector.

Finally, the French economic intelligence system is configured as a multilayered and multilevel organizational network in which vertical oversight and horizontal interconnections between government, industrial, and academic actors coexist. This complex, multi-nodal, and multilayered structure appears fully compatible with an adhocracy.

The comparative study of these three cases allowed us to test the hypothesis of the actual presence of adhocratic structures in intelligence. More broadly, the three cases confirm that intelligence organizations cannot rely solely on traditional bureaucratic or hierarchical models when confronted with environments defined by volatility, uncertainty, complexity, and ambiguity; instead, they increasingly need to act as complex adaptive systems, capable of co-evolving with their environment, learning continuously, and integrating diverse sources of knowledge and expertise.

The thesis, in addition to providing specific conclusions on the intelligence systems studied, demonstrates the concrete possibility of applying organizational theory to the study of intelligence systems. It also has prescriptive potential, as it suggests ways in which intelligence agencies should improve their effectiveness and efficiency through the implementation of appropriate organizational models. Policy recommendations are offered with a focus on governance structures that balance secrecy and accountability, flexibility and oversight, and central coordination with distributed autonomy.

Finally, the document concludes with a practical proposal for the creation of an adhocratic structure aimed at protecting Italy from potential national security attacks that exploit the weaknesses of the Italian legal system. This structure would combine expertise and functions from the public administration, intelligence agencies, law enforcement, academia, and strategic companies. The proposed adhocratic structure would be characterized by a rapid and effective decision-making cycle, high-quality public-private coordination, and multidisciplinary roles, all without sacrificing fundamental secrecy protection mechanisms.

CONTENTS

INTRODUCTION

1. Overview

This work aims at examining the organizational models of intelligence agencies. Intelligence services present many points of interest. In fact, if the work of the secret services has historically always been pervasive and incisive in human societies, it must also be said that recent technological innovations have projected global challenges and problems into everyone's daily lives. Currently, therefore, the role of services increasingly permeates daily action, both from an active and passive perspective. The key example is cybersecurity. The pervasiveness of the internet in people's daily lives, in addition to providing enormous possibilities for social interaction, professional development and evolution in every direction, also represents a multiplier of threats, which can hit from anywhere on the planet after having identified a possible target in an easy way. A threat like the cyber one, which sees intelligence agencies involved on multiple fronts, is extremely difficult to identify, contain and deal with. To do this it is necessary to intervene in a solid way also on the organizational aspect of the structure.

Unfortunately, quantitative and qualitative study methods are difficult to break through the barrier of secrecy that states erect around the activities of intelligence services, including their organizational and operational structure. To overcome the difficulties of the research, we resorted to the analysis of all the possible available sources, and therefore to the available literature and above all to the so-called gray literature, which allows us to partially reveal some characteristics of the otherwise secret agencies.

The methodological difficulties are exacerbated by the fact that there is no “worldwide” culture of intelligence agencies, as each State has developed its own approaches, paradigms, protocols, management and control systems, analysis methods and hierarchies, which are not shared outside the narrow environment of that single intelligence agency. A global comparison would therefore be impossible, and therefore it was decided to carry out three case studies, regarding intelligence realities, each characterized by a specific peculiarity. The case studies chosen were North Korea (characterized by notable changeability in the organizational structure), Israel (whose ecosystem mixes public and private entities, start-ups and military structures, finance and scientific research) and France (whose system of economic intelligence interfaces at every level with productive, economic and financial realities).

The North Korean intelligence system is redundant and fluid, with structures that frequently adapt to changing needs. The system prioritizes practical functionality over theoretical frameworks, reflecting the country's constant state of alert, but also high levels of personnel training, selective decentralization, the presence of a constellation of specialized substructures, and a highly dynamic redefinition of hierarchical dependencies. Although some elements suggest compatibility with an adhocratic model, the paucity of data and incomplete knowledge of its functioning preclude a definitive classification.

The Israeli intelligence system, on the other hand, is characterized by an ecosystem in which the boundaries between the public and private sectors are blurred. It is characterized by highly specialized tasks, minimal formalization, continuous adaptation for coordination, and a distributed decision-making process. The system emphasizes the development and integration of young talent, with frequently rotating operational personnel and contributing to innovation in cybersecurity and IT through start-ups, often with state support.

Finally, the French system operates within a multilayered network structure, blending vertical and horizontal connections. This system fosters strong public-private interaction, without eroding the distinctions between the two sectors. This networked approach addresses the complexity of its context, integrating selective decentralization and specialized structures under central oversight.

Although the North Korean case remains inconclusive, both the Israeli and French intelligence systems exhibit distinctive adhocratic features.

2. The object of study

2.1 Secret Service, Intelligence Service, Security Service

Sovereign nations, in order to protect their military, geopolitical, economic, and any other interests, have historically equipped themselves with structures called "secret services", capable of carrying out activities of considerable importance without these being made public (Andrew, 2018). There is a historical trace of these "services" in the name of the *US Secret Service* (a federal agency of the USA, founded in 1865), which is not a secret service in the modern sense of the term as its purpose is that of personal protection of the presidents of the United States and their families.

These activities, especially in the past and still today in countries with a low democratic impact, can take the form of illegal activities of various types, such as homicides, military actions in violation of international conventions, kidnappings and torture (Born & Caparini, 2009). In modern democratic states, on the other hand, even the activity of these secret services is regulated by law and subjected to the limits connected with respect for human values and constitutional principles, even if sometimes democratic impulses are compressed by geopolitical ambitions (Van Ginkel, 2012).

Therefore, with the advent of nation-states, designated bodies were created for three purposes (Zagart, 2000):

- the collection of information on the enemy military apparatus, its political aims, economic planning, and any other field of interest;
- the analysis and collation of this raw information to obtain structural information, capable of being used to interpret reality;
- the dissemination of this structured information to policy makers.

The modern “secret services” have therefore acquired, while maintaining a high level of secrecy, the characteristic of developing as a combination of two entities (Riehle, 2015):

1. *Intelligence services*, whose purpose is to collect news and data (especially those that the adversaries want to keep confidential), organize and analyze them, and transform them into structured information, which the political decision-maker can use to protect national security and the interests of the whole country;

2. *Security services*, whose task is fundamentally to counter the action of the opposing intelligence services, prevent foreign agencies from carrying out information collection to the detriment of their own nation, first of all by implementing the so-called counterespionage.

The different nations have declined these two missions in various ways, dividing them or combining them in state agencies, sometimes conjugating them with the military, police and justice scopes.

2.2 The environment in which the services operate

It is easy to understand how this type of structures are of fundamental importance for nations, especially in a world characterized by complexity, variability, speed of change and loss of reference points, in which the value of information is strongly linked to the time factor. For this reason, huge economic resources are commonly invested in the secret services (at least in relation to their size) and highly selected human resources are employed. Together with these basic factors, the organizational system of the secret services also assumes fundamental importance.

The large family that goes by the name of intelligence and security services therefore includes agencies that (Zegart, 2000):

- carry out priority activities for national security;
- act under secrecy in order to maintain a tactical and strategic advantage;

- aim to reveal the opponent's secrets and maintain their own.

The sector of these agencies and the environment in which they operate is characterized by some peculiar elements. First of all, it is dangerous, as the level of interests at stake and the actors involved allow the use of force, blackmail, coercion and sometimes even physical elimination.

Furthermore, it is a sector rich in pervasiveness, as every aspect of society can be of interest and be involved in intelligence activity: from academia to industry, from politics to sport. This is also relevant in relation to the environment in which agencies operate, which is varied and changing.

The sector is therefore also characterized by considerable dynamism, which is also expressed in the rapid evolution of the technical and technological frontier and in the changing international political situations.

Finally, given the high competitiveness (and sometimes even conflict) between the various national bodies, as well as due to the vastness of physical subjects and bodies involved, intelligence activity is also characterized by considerable unpredictability. Events of a random nature and those of a chaotic nature mix with the active opposition of adversaries, ending up constantly changing the playing field of the agencies.

These elements, which require considerable adaptability, require us to shift attention to the discipline that studies this type of environment, namely the theory of complex systems.

3. Complexity

3.1 Complex Systems: a brief introduction

We now move on to the academic and scientific study of reality. Nowadays, research on the functioning of the universe is usually carried out in macro-sectors linked to the objects to be investigated: astronomy deals with stars, biology with cells and tissues, sociology with groups of human beings and so on. Furthermore, it is often believed that the methods of discipline cannot be transferred to others and this has led, over time, to a separation between scholars in different fields of knowledge. This trend is today widely opposed in many teaching and research contexts, where there is an increasingly widespread interest in multidisciplinarity (knowledge from different fields is combined, juxtaposing them), interdisciplinarity (knowledge from different fields is combined, integrating them together) and transdisciplinarity (connections between different isolated topics are explored and revealed - UNESCO, 1998).

In reality, by studying the original works of the great scientists of the past such as Galileo or Gauss, we realize that these thinkers dealt with every facet of reality, adapting when possible only specific methods of the sciences known to them to those specific cases. And the creators of the new sciences of the present, from computers to artificial intelligence, such as John Von Neumann, Claude Shannon or Alan Turing, have equally been able to apply ideas and methods to new fields (Tranquillo, 2018).

This trend took shape in the scientific world in the second half of the 20th century, when more and more scholars, from the most varied disciplines, realized that the phenomena they studied behaved in a “similar” way to those of other fields. A new way of approaching certain phenomena of the universe was therefore born based on the commonality of methods, and no longer on the field of investigation.

This new theory of complex systems has therefore been successfully applied in many fields such as: the distribution of words in written and spoken languages, transport services in large cities, the intensity of armed conflicts, financial markets, the behavior of groups of animals, the activity of the brain, the spread of forest fires, the sale of cinema tickets, the solar wind, etc. (Thurner et al., 2018).

What allows all these systems to be treated with the same methods is the presence of many elements in common, which qualify them as complex systems, such as:

- the fact that the interactions between the elements of the system can be described with a network. Interactions in general can only be modeled as two-way interactions, but the construction of a network allows to obtain, as a result, a system of interactions also with groups or between groups (Barabasi, 2009);
- the non-linearity of interactions, which therefore constitute behaviors that cannot be superimposed or easily broken down into individual parts. The complex system therefore becomes something more than the sum of its component parts. Non-linear behaviors also allow the manifestation of very peculiar dynamics, of which chaos is just an example, which in turn produces apparently inexplicable effects, such as the emergence of a new order (Kauffman, 2011);
- the presence of evolution of the different components of the system, which influence each other, in a co-evolution regime. This introduces the importance of the past path of the system for the interpretation of its present and future, effectively introducing the concept of history in the physics of complex systems (Nowak, 2006);
- furthermore, thanks to this mechanism, the systems adapt to the challenges posed by the environment in which they are immersed (Miller & Page, 2007);
- the move away from adherence to the statistics of the Gaussian bell, which rewards belonging to the central band of the distribution, in favor of behaviors described by power laws (Reed & Hughes, 2002), which allow the manifestation of extreme events

(black swans), scale effects, the different importance of the factors (as in Pareto's laws), etc.;

- the importance of flows of matter, energy and information, and the combination of these different factors, as well as entropies, in the evolution of systems (Thurner & Hanel, 2009);
- the fact that the emergence of an order allows the application of concepts such as strategy, interest, advantage, choice etc., suitable for describing the behaviors of evolved biological structures (Eisenhardt & Brown, 1998).

3.2 Organization and complexity

Organizations made up of human beings are complex systems in themselves, and furthermore they are immersed in an environment that is equally characterized by the elements of complexity that we have described. Non-linearity, recursion of effects, multi-entity interactions and the constant threats of chaos, entropy and disorder bring constant problems, difficulties and challenges to organizations. But at the same time, complex systems are not in themselves random or chaotic *sic et simpliciter*. On the contrary, these are systems characterized by their own dynamics, perhaps difficult to interpret and predict, but which can be governed (Axelrod & Cohen, 2000).

The concepts born from the study of complex systems have therefore also found use in the study of organizational systems and methods, also by virtue of the fact that as the interconnections that represent the global network increase, the complexity of the system also increases and therefore the difficulty in interpreting the dynamics (McMillan, 2004). Furthermore, this increase is not linear with the growth of the network nodes, but exponential, and the effects of increasing complexity are therefore exponential.

Intelligence agencies represent, in this framework, a paradigmatic example (Pacher, 2000). In fact, it is a type of organization that must constantly manage a very high degree of uncertainty, in an extremely secret and competitive environment (Javorsek & Schwitz, 2014). These elements determine a high degree of complexity that forces intelligence and security agencies to continuously rethink themselves (Menkveld, 2021), both in the process and organization phases (Gill, 2018).

3.3 From Physical and Biological Complexity to Organizational Complexity: A Transdisciplinary Path for a Systemic Paradigm

In its most general form, complexity is the study of how local interactions between elements of a system produce unpredictable, but often regular, global behaviors (Mitchell, 2009).

These concepts, born in mathematics and physics, then evolved through biology, ecology and other related disciplines, but ultimately resulted in the adoption of a systemic approach to reality that also involved economics and the social sciences in general. The study of organizations could not therefore be excluded.

This translation was the result of an applicative path that is worth exploring. If for physics a dynamic system is a system that evolves over time according to deterministic rules, the mathematician Henri Poincaré demonstrated that chaotic and unpredictable behaviors can still be generated. Chaos theory has highlighted how small changes in the initial conditions can produce effects amplified over time, a principle known as the "butterfly effect" (Lorenz, 1963). This leads to the impossibility of predicting the evolution of the system in the long term, even if the laws that govern its functioning are known and deterministic. Another key concept, which has been essential in the translation of complexity theory to organizations of individuals, is that of self-organization: in many physical systems (such as Prigogine's dissipative structures), order emerges spontaneously from disorder, through local interactions between the parts (Prigogine & Stengers, 1984). This principle is the basis of the transition towards more complex forms of order, even in the absence of centralized control.

Biology has adopted and expanded the vision of complexity through the study of living organisms as complex adaptive systems. A biological organism is composed of billions of cells that interact with each other according to biochemical and genetic rules, giving rise to emergent properties such as life, consciousness or learning. Metabolic networks, gene networks and immune systems are examples of complex adaptive systems, in which the global properties of the system (for example the ability to respond to external stimuli) are not directly deducible from the analysis of the individual components (Alon, 2006). The theory of evolution comes into play in this context: Darwin showed that the adaptation of organisms to the environment is the result of a continuous, non-linear and unpredictable selective process. Evolution is therefore a complex process that generates biological innovation through interactions between genotype, phenotype and environment.

After the Second World War, the systems approach was also adopted by the social sciences and then by the business world, through organizational theory. The basic idea, that an organization can be viewed as a living system, was taken directly from biological models and then applied to social structures to try to better understand them (Capra, 1996). Authors such as Maturana and Varela (1987) introduced the concept of autopoiesis, according to which a living system is capable of self-repair and maintaining its efficiency solely through its own interactions. This vision was taken up by Gareth Morgan (2016) and applied to organizations, which are then viewed as systems capable of learning, adapting, and co-evolving. Other contributions came from cybernetics, which contributed fundamental concepts such as feedback mechanisms and homeostasis. Stafford Beer also proposed a theory, called the viable system model, in which the organization is seen as an organism, capable of maintaining its internal coherence and adapting to external changes (Beer, 1979). These theories have gradually become pieces of a larger mosaic, and today's corporate organizations can benefit from their achievements as they face the challenges of an increasingly complex environment characterized by uncertainty, rapid change, and global interconnectedness. The traditional view of organizations, based on rigid structures managing linear processes, proved completely inadequate once the presence of strong emergent complexity in the external environment was recognized. New paradigms have therefore emerged, such as that of considering organizations as complex and adaptive systems, capable of learning and evolving in a dynamic and changing environment. This is precisely what Holland's (1995) CAS theory describes, where systems of this type are described as composed of a multiplicity of agents interacting according to local rules, governed by nonlinear dynamics, and ultimately exhibiting global emergent properties (Holland, 1995). This model demonstrates how management can dispense with centralized control, instead favoring autonomy, local collaboration, and continuous, informal learning.

The environment itself can no longer be viewed as a static entity, but must be approached as a dynamic and co-evolving system, continually transformed by the actions of the organizations that inhabit it (Stacey, 2001). Adapting to these complex environments therefore requires new organizational strategies, and thus the concept of organizational agility has developed, defined as the ability to respond rapidly to external changes through flexible structures, autonomous teams and distributed decision-making processes (Doz & Kosonen, 2008). Complex organizations, therefore, do not simply adapt, but co-evolve with the environment, generating new organizational forms and new market logics. This first and foremost requires rethinking long-term strategies, which must be understood as processes of continuous learning, rather than static plans.

Adaptive leadership is another response that emerges once we understand how traditional, command-and-control-based leadership proves ineffective in complex contexts. A new style is therefore needed, one capable of facilitating the emergence of innovative solutions and promoting organizational learning, for example through the creation of collective learning spaces that facilitate innovation and foster the emergence of new solutions through experimentation (Heifetz, Grashow, & Linsky, 2009).

The adoption of new, more flexible organizational models, such as network structures or liquid organizations, can make organizational action more effective through increased collaboration, greater knowledge sharing, and consequently the ability to respond rapidly to environmental changes.

According to De Toni, complexity is not an exception, but a permanent condition of the modern world. In his "Decalogue of Complexity," he states that complexity has always existed, but today it is perceived more intensely due to greater interconnectedness at the global level, the greater speed of all interactions involving modern society, and the related inevitable systemic increase in uncertainty (De Toni, 2024). These elements make social and economic systems more unpredictable and require a management approach capable of addressing ambiguity and continuous change. The author also notes that complexity is destined to continue to increase, and this fact must be accepted in order to be managed. Furthermore, the best way to address and manage complexity is to adopt a variety of approaches, which involve continuous learning, in order to adapt to change. It is also necessary to develop the ability to adapt quickly and seek to foster cooperation between individuals and organizations, which is effective in addressing the challenges that complexity continually poses and changes over time. Other strategies include distributing leadership, building resilient systems, and stimulating innovation.

In his book "The Complexity Dilemma," De Toni emphasizes how organizations are often forced to balance the need for stability and control with structural flexibility and adaptability, and that the success of this balance can significantly impact the organization's success or failure (De Toni & De Zan, 2020). This balance requires dynamic management of organizational capabilities to respond effectively to changing contexts. De Toni also proposes a methodology for assessing organizational complexity, its ability to manage it, and its performance outcomes, a methodology that has already been tested in several case studies, demonstrating its effectiveness.

Another central concept in De Toni's vision is self-organization, understood as the ability of a system to organize itself spontaneously without centralized control. One tool for achieving this is distributed leadership, whereby responsibility and decision-making power are distributed among organizational members (De Toni, 2021a). This approach fosters adaptability and innovation, as it allows organizations to respond quickly to environmental changes. However, distributed leadership also presents risks and requires an organizational culture based on trust, collaboration, and continuous learning. However, if the organization is able to develop transversal skills and promote the active participation of organizational members, the result is a significant increase in effectiveness in addressing the challenges posed by complexity (De Toni, 2021b).

Continuous organizational learning, as a systemic response to complexity and the changes it generates in the environment, is also seen by De Toni as an effective strategy for addressing complexity (De Toni, 2022). Organizational learning is closely linked to innovation, as it allows organizations to generate new ideas and implement innovative solutions to address complex challenges. It must be implemented at all levels, whether as individual, group, or organizational learning.

3.4 *Effective organizational models for the governance of complex systems*

a) Coevolutionary and proactive approaches

A first concept of interest is that of coevolution, which originates from Darwinian theory and its developments, with broad applications in complex fields. In fact, we must consider that the contemporary complex systems, characterized by high interconnection, interdependence and dynamism, pose growing challenges to organizations that aspire to effective governance, capable of continuously adapting to internal and external variations, while ensuring operational stability and strategic flexibility (Allen, Maguire, McKelvey, 2011). This balance can be pursued through a coevolutionary approach, in which organizations and their environments influence each other constantly, producing dynamic and emergent configurations (McKelvey, 2016). From this perspective, the organization is no longer conceived as an isolated system, but as a crucial node within a larger network that evolves jointly (Mitleton-Kelly, 2015).

Organizational models based on dynamic adaptability are also particularly interesting. The adaptive structure implies a continuous redefinition of roles, responsibilities and internal interactions, in order to respond quickly to external stimuli and unexpected changes (Snowden, Boone, 2007). Organizations that adopt this model are more resilient and able to exploit emerging opportunities than those that adopt static structures (Hamel, Zanini, 2018). The concept of organizational network, for example, is often associated with this type of models, as it allows for a dynamic distribution of leadership and decisions (Laloux, 2014).

Distributed governance is another key element for the coevolutionary management of complexity. It involves delegating decision-making powers to the lowest and most peripheral levels of the organization, thus strengthening local self-organization capabilities and enabling rapid adaptation to changing environments (Mitleton-Kelly, 2015). This approach therefore allows the organization to react promptly to changes, reducing response times, while simultaneously developing specific skills for autonomously managing emerging problems, improving the overall resilience of the system (Laloux, 2014).

Another concept that may be of great relevance here is that of proactivity, which cuts across the fields of psychological and managerial studies. Proactive governance implies the ability to anticipate and not just react to emerging complexities, and proactive organizations use advanced predictive analytics tools and scenario planning techniques to explore possible alternative futures and develop flexible and anticipatory strategies (Schwartz, 2020). But this proactivity requires a systemic vision and the integration of multidisciplinary skills, capable of detecting weak signals and intervening before these signals become critical problems (Scharmer, Kaufer, 2013).

Effective organizational models to deal with complexity are not limited to a single strategic or structural dimension, but integrate different operational, cognitive and relational dimensions (Morgan, 2016). Multidimensionality allows organizations to better navigate contexts of uncertainty, exploiting internal diversity and favoring the generation of innovation through collaborative and interactive processes (West, 2012).

b) Emergent self-organization in complex organizations

The concept of emergent self-organization also represents a paradigm capable of allowing organizations to deal with conditions of instability and unpredictability typical of complex systems (Holland, 1995).

The term self-organization refers to the ability of a system to spontaneously create ordered structures, without direct external control, using only local interactions between the constituent elements of the system (Heylighen, 2008. Johnson, 2002). Some peculiar properties of these systems are decentralization, redundancy, diversity of the elements involved, flexibility, and the ability to rapidly adapt to environmental changes (Mitleton-Kelly, 2003). Sometimes these systems can show also ordered behaviors.

Emergent self-organization is a phenomenon frequently observed in nature, for example in colonies of social insects such as ants or bees, which demonstrate extraordinary coordination capabilities, even in the absence of central leadership, and simultaneous adaptation to changing needs (Camazine et al., 2001). Similarly, in human organizations, self-organization processes can emerge spontaneously in contexts where a rigid hierarchy is ineffective, or even impossible to implement.

In corporate and institutional contexts, where emergent self-organization cannot be left to chance, it is essential to understand the factors that foster it and how to govern it. It has been found that it is most effective in the presence of flexible and informal structures, capable of responding rapidly to external stimuli, promoting innovation and continuous learning (Stacey, 2010). For example, in organizations that adopt decentralized models, and which promote the emergence of situational leadership, in which roles and responsibilities are dynamically redistributed based on specific skills and immediate needs (Plowman et al., 2007).

An organization that can leverage emergent processes, thus achieving resilience and flexibility, will be able to manage complexity more effectively. Brown and Eisenhardt (1997) emphasize that organizations that embrace this emergent logic can better seize strategic opportunities and adapt more quickly to environmental changes, achieving a significant competitive advantage over more static and predictable organizational models.

c) Applying Emergent Self-Organization to Intelligence Activities

Intelligence activities represent a field in which complexity and uncertainty are normal and unavoidable conditions (Treverton, Gabbard, 2014). The effectiveness of intelligence operations strongly depends on the ability to collect, analyze and integrate information from multiple and often ambiguous sources, while simultaneously managing time pressure and resource limitations (Lowenthal, 2019).

The adoption of organizational models based on emergent self-organization would offer important advantages for intelligence activities. First, by allowing analysts and decision makers to respond more quickly and effectively to weak signals coming from the operational environment (Heuer, Pherson, 2014). Second, it would favor the creation of informal networks inside and outside the organization, thus increasing the ability to identify and interpret new threats and opportunities (McChrystal et al., 2015).

For example, according to some authors (Dahl, 2019), the model adopted by US intelligence post-September 11 would be a significant example of the practical application of emergent self-organization, through less hierarchical structures and more oriented towards information sharing and interagency collaboration. Such informal, flexible and dynamic networks would allow intelligence professionals to quickly adapt to changes and optimize the distribution of resources and skills. The theory of emergent self-organization, which represents a powerful and promising paradigm to address the challenges of contemporary complexity, applied to intelligence organizations, would allow the exploitation of natural and spontaneous dynamics that improve resilience, decision-making speed and the ability to manage uncertainty. The adoption of these models would require, however, a significant cultural change that favors flexibility, decision-making autonomy and openness to unconventional organizational processes, traits that are not culturally specific to the intelligence system.

3.5 Complexity and Intelligence

The characteristic elements of complex systems are also found in the activity and organization of intelligence and security agencies.

The most significant elements concern:

- *Interdependence between the components*. State intelligence is made up of a multiplicity of actors (government agencies, armed forces, private and academic sectors, etc.), each with specific, but closely interconnected, roles. These components operate in an integrated system in which information collected by one unit can influence the operations of another.
- *Continuous adaptation*. The global context in which intelligence operates is characterized by constantly evolving dynamics (asymmetric threats, cyber-attacks, transnational terrorism). Intelligence, as a complex system, must respond to these changes by adapting quickly. This manifests as a feedback loop in which intelligence continuously receives information from the operational environment in order to continuously modify strategies, creating a cycle of adaptation. The adaptation of intelligence systems is based on the observation of the evolution of threats and tactics of hostile actors (state and non-state), to predict their future moves.
- *Non-linearity and unpredictability*. Relationships inside and outside the intelligence system are not linear: small variations in the information or behavior of actors can produce disproportionate effects.
- *Self-emergent order*. In complex systems, the overall behavior of the system cannot be understood simply by analyzing its individual components and adding them together. Similarly, state intelligence produces emergent value when fragmented information, gathered from diverse sources, is integrated to generate strategic insights. Big data analytics, open source intelligence (OSINT), and other forms of integrated collection demonstrate how synthesizing seemingly unrelated data, through a holistic approach, can uncover otherwise hidden threats.
- *Resilience and redundancy.* Intelligence networks, given their strategic defense value of national interests, must be designed to withstand shocks and continue to function despite disruptions to even a significant portion of them. This resilience is achieved through redundancy (e.g., data and function backups) and decentralization, which entail costs and duplication but ensure continued operation in crisis situations.

- *Network of actors and global connections*. State intelligence networks are effectively global structures that penetrate national borders, and this vastness characterizes them as complex networks, where efficiency is strongly influenced by the rate of connectivity, distribution, and resilience, while at the same time, effects on a crucial node can generate significant repercussions on the entire network.

4. Research Design

4.1 The difficulties of investigating intelligence and security services

The academic study of intelligence agencies, although widespread also by virtue of the general interest in these structures, is limited by a series of problems, as highlighted by the paucity of results found in the review of the previous paragraph.

In fact, as the name itself suggests (secret services), almost every aspect of these entities is covered by confidentiality. The biggest obstacle so is the secrecy that covers almost every aspect of the matter.

There have even been examples in the past of intelligence services whose very existence was secret; others in which even the identity of the top managers was unknown. The very existence of some services was kept secret, there were no official public documents and it was also forbidden for those who knew of their existence to talk about them, as in the case of the US National Security Agency (NSA) or the French *Groupement interministériel de contrôle* (Interministerial control group).

Beyond these extreme examples, the secrecy regarding agencies in the intelligence sector often covers: the internal organization, the organizational charts, the skills of the various offices, the functional dependencies and responsibilities; the methods of recruitment, education and training of personnel; the technologies used, the resources available, the locations and the number of employees; the results achieved, the efficiency and effectiveness of the system, the operating indicators and the profile of the staff employed in the various tasks; division into roles and ranks of personnel, career advancement, chain of command and control, subdivision of regional offices, type of organizational structure, numerical strength of employed staff, detailed objectives of the service and operating methods, technical equipment; management control, verification and monitoring systems.; and so on.

This is a regime of secrecy incompatible with modern democratic systems, in which even the work of the intelligence and security services is subjected to verification not only by the government but also by the parliamentary system and sometimes also by independent control bodies (Gill, 2007).

Nonetheless, most of the characteristics of these modern services remain covered by high-level secrecy, typically through the qualification of state secrecy, with the consequence that even simply revealing secondary elements relating to the functioning and organization of the secret services can lead to problems.

Secrecy ultimately covers virtually every aspect of events involving an intelligence agency, making it difficult to evaluate the performance of this type of organization (Atkinson, 2015). Even the evaluation of the functioning of the secret services through the analysis of the relative results in the field appears completely impracticable (Javorsek II & Schwitz, 2014). Most of the activities carried out by these structures are in fact covered by absolute secrecy, even years after they were carried out. Only a small part of the operations reveal their existence to the outside world. In particular, these are two types. First of all, particularly aggressive ones (such as murders, sabotage, etc.) which are part of the so-called Direct Actions and which form an asset not always present in the information agencies of modern democratic states. The other category includes operations that end in resounding failure, and for this very reason we become aware of them, as they are no longer secret. The relative frequency of failures, scandals, various malfunctions and similar cannot be known and it therefore cannot represent a concrete indicator of the full functioning of the service (Wheaton, 2009). The real consistency of the total operations of a secret service is in fact a "dark number" and this leads to a difficulty of analysis impossible to overcome. There is indeed the possibility to collect information through "indirect" analyses, considering the intense interrelations with other organizations on which there is more information available. In the light of the above considerations, we carried out an analysis of Israel's intelligence and security system, relying on published literature, gray literature as well as indirect analyses.

Agencies of this type are usually subject to control by government, parliamentary and independent committees (Gill, 2007), which however in turn are typically bound to secrecy. Ultimately, the various theories on the evaluation of the work of services (Marrin, 2018), often developed for public purposes rather than for academic purposes, as in the case of terrorism prevention (Tan, 2018), are therefore rather incomplete and not very effective.

In addition to the necessary general secrecy that affects this type of structure, the massive use of deception, disinformation, information intoxication, influence and interference in the intelligence environment must also be considered (Menkveld, 2021). In fact, secret services find themselves operating in conflict with other equally secret services, whose action is extremely complex to counter if the information assets are asymmetrical. A specific example of this is that even the organizational charts that describe the internal macro structure of the services, which are sometimes leaked to the outside, are fakes artfully constructed by the services themselves as an element of disinformation, in order to obtain a strategic advantage. In fact, the simple knowledge of command flows rather than of the specific weight attributed to certain geographical areas at the expense of others, to certain threats or to others, can serve to modulate the enemy's activity against that secret service and in general against the entire national security.

4.2 Literature review

The study of intelligence, and security-related issues in general, represents a theoretical and methodological challenge that spans multiple disciplines, from political science to sociology, to organizational studies in the narrow sense. Despite the crucial importance these institutions play in the political, social, and economic life of states, their internal workings remain relatively underexplored by academia, and even less so through the analytical lens of organization theory. The reasons for this partial knowledge gap are multiple and, in part, structural. These entities are, first and foremost, shrouded in intense institutional secrecy, which makes access to primary sources extremely difficult. Furthermore, even when academic research focuses on these entities, it favors approaches based on normative analysis, strategic impact, or historical reconstructions.

This literature review aims to critically examine studies that have addressed intelligence and security agencies from the organizational perspective, with the aim of highlighting how and to what extent the categories, models, and methods specific to organizational theory have been used.

This perspective responds primarily to theoretical needs, as it would allow us to test whether the sophisticated tools developed within organizational theory to analyze the internal workings of public and private entities can also be applied to intelligence agencies. This would allow us to test the flexibility and explanatory scope of these theories in contexts characterized by unique constraints, such as information opacity, hierarchical rigidity, extreme risk management, and the need to operate in highly uncertain environments.

At the same time, it would respond to a practical need, as it would provide the political-institutional system with preliminary tools useful for evaluating its existing intelligence system, improving its effectiveness, democratic accountability, and adaptability. This is a pressing need in a global context characterized by new transnational threats, accelerating technological change, and growing questions about the relationship between security and civil rights.

This work is located at the intersection of intelligence studies and organizational theory. Historically, intelligence has long been the subject of a narrative rather than analytical treatment, centered on events, operations and personalities rather than on structures, processes and norms. Only since the 1990s, also thanks to the greater availability of sources and the growth of "intelligence studies" as a sub-discipline, has there been an opening towards more systematic and comparative approaches. However, the dialogue between intelligence studies and organizational studies remains partial and discontinuous.

Intelligence agencies are typically conceived as "exceptional" organizations, whose operations are predominantly determined by exogenous factors: the perceived threat, the needs of the political decision maker, geopolitical contingencies. In this perspective, the focus is placed more on outputs (the results of the action) than on internal processes or organizational dynamics. On the contrary, organizational theory teaches that internal processes – whether formal or informal, structural or cultural – have a decisive influence on the behavior and performance of an entity.

One of the central issues that this literature review intends to explore is therefore the way in which the "organizational dimension" is treated in intelligence studies. For example, how are hierarchical structures, informal networks, coordination and control mechanisms, professional culture, incentive and evaluation systems described and analyzed? How do secrecy and compartmentalization influence information flows and decision making? And again: what forms of organizational learning develop in contexts where error is often undocumentable and feedback is limited or distorted?

Another relevant aspect concerns the issue of accountability and transparency. In many organizational studies – especially in the field of New Public Management – the theme of performance and evaluation is central. However, for intelligence agencies, the evaluation of results is made problematic by the invisibility of many successes (which, by definition, do not happen publicly) and by the difficulty of establishing certain causal links between information and political decisions. This has led some authors to speak of an "organization without feedback" (Johnson, 2007), where the normal corrective mechanisms of bureaucratic organizations are strongly attenuated.

From a methodological point of view, the study of intelligence organizations raises peculiar questions. The scarcity of open data, the sensitivity of sources, and the risk of selective access (granted only to "internal" or already authorized researchers) place limits on both qualitative and quantitative research. However, in recent years there have been multiple attempts to overcome these limitations through the combined use of secondary sources, comparative case studies, interviews with former agency members, policy analysis and indirect observation of organizational processes through scandals, reforms or public crises.

Given the interdisciplinary nature of the topic, the corpus was constructed from peer-reviewed bibliographic databases (fields: political science, public administration, organizational studies) for methodologically sound articles and essays, and in particular by exploring the Jstore database (https://www.jstor.org) and the Science Direct database (https://www.sciencedirect.com).

Queries were constructed by combining noun terms (object) with conceptual categories (analytical lenses).

Specifically, the Objects ("intelligence agencies" OR "intelligence organizations" OR "intelligence community" OR "National Security") were combined via the Boolean AND with the Organizational Categories ("organizational structure" OR "hierarchy" OR "organizational culture" OR "professional socialization" OR "bounded rationality" OR "decision-making" OR "learning organization" OR "network organization" OR "complex adaptive systems" OR "system of systems" OR "adhocracy" OR "tradecraft standards").

The databases were added to the catalogs of monographs and collective volumes for summary works and fundamental manuals on intelligence, repertoires of academic books, and specialized series.

The inclusion and exclusion process used was based on:

1. reading of abstracts for a preliminary screening of obviously irrelevant works,
2. subsequent reading of the entire work (or of the relevant chapters for volume works) to perform a second-level screening;
3. evaluation of organizational relevance to screen for works that explicitly address the structure, culture, decision-making processes, or learning/error within agencies;
4. exclusion of purely historical or journalistic works, lacking a true organizational perspective, or lacking methodological traceability;
5. final two-phase screening through exploratory research for conceptual nuclei and key authors, as well as through saturation through snowballing (backward/forward citation) starting from the most cited references.

The findings were divided into categories, which emerged through aggregation during the review around the most relevant themes. The division into four categories therefore reflects an effective clustering of the corpus, although many works actually fall on the border, if not between, two or more categories.

The four thematic sections are: (a) organizational structure and hierarchy; (b) culture and professional socialization; (c) decision-making processes and bounded rationality; (d) organizational learning and error management.

The classification responds to three methodological needs:

1. these are four recurring "pillars" in organizational theory for breaking down the analysis of complex organizations;
2. as mentioned, by mapping the texts, contributions tend to naturally cluster into the four categories;
3. a form of taxonomy reduces the disciplinary heterogeneity of the literature and allows for consistent comparisons (within-section) and cross-sectional readings (between-section). The classification, therefore, is not merely expository but is aimed at maximizing the overall coherence of the review and the possibility of replicating its design in other national systems.

The aim is to critically reconstruct the variety of approaches used, distinguishing between those that assume an internalist point of view (centered on intra-organizational dynamics) and those that adopt an externalist perspective or one of interaction with the political-institutional environment. Of interest is the difficulty with which classical concepts of organizational theory have been adapted, if not reworked, to overcome the limitations imposed by the secrecy and information asymmetry typical of the intelligence world.

The aim of this review is not only to describe the approaches used, but also to identify the most promising theoretical perspectives for understanding these highly opaque organizations. The search results, limited to the sectors of interest (organizational sciences, economics and management, applied to intelligence agencies), initially provided almost a thousand results, which were subsequently filtered as described above, until the most relevant ones were obtained, described below.

a) Organizational structure and hierarchy

Spying Blind: The CIA, the FBI, and the Origins of 9/11 by Amy B. Zegart (2007) is a volume that falls within the current trend of scholars who have investigated the reasons why the two main American intelligence agencies – the CIA and the FBI – failed to prevent the terrorist attacks of September 11, 2001, despite the growing threat posed by al-Qaeda having been identified and documented for a long time. The author analyzes the failures as structural, originating at the organizational level, also on the basis of the fact that the CIA and the FBI were structures managed according to rigid organizational paradigms, reluctant to systemic innovation and incapable of truly effective coordination.

Zegart identifies five structural causes of the agencies' failure. First, a profound lack of internal adaptation mechanisms capable of adapting the institution to emerging threats, such as transnational terrorism. Second, the aforementioned cultural resistance to change. The organizational culture of the CIA, and particularly that of the FBI, was strongly tied to traditional post-Cold War threats, particularly espionage and counterespionage linked to adversaries such as other industrialized countries, and was incapable of reconfiguring itself to address new asymmetric threats. A further weakness was the lack of effective strategic political oversight by Congress and the Presidency, especially in relation to its necessary evolution to address new threats. Furthermore, the flow of information between the various entities involved had led to chronic difficulties in interagency coordination, resulting in fragmented and poorly integrated information sharing. Finally, the excessive autonomy and self-centeredness of both agencies, particularly the FBI, and their exaggerated autonomy, had hindered structural reforms.

Zegart uses a comparative methodology to compare intelligence reform with that of the U.S. Army after the Vietnam War, culminating in the Goldwater-Nichols Act of 1986. In the Army's case, functional restructuring was profound, while in the intelligence sector this was lacking, primarily due to the lack of external pressure (which would come after 9/11) and therefore adequate political incentives.

The text shows how the framework represented a paradigmatic case study of organizational resistance to change in highly complex and highly specialized contexts when the external environment changes. This inertia was also accentuated by the context, characterized by highly bureaucratic elements, and by the incisive secrecy constraints typical of intelligence agencies. The analysis highlights how the CIA and FBI are certainly complex organizations, yet dysfunctionally stable, in that they were incapable of recognizing the need for systemic adaptation, which was particularly urgent in their case.

Zegart's argument, interpreted through the lens of high-reliability organization (HRO) models, highlights how these models present significant limitations when not accompanied by flexible governance and, above all, a culture of continuous improvement. Overall, it emerges that, even in the intelligence field, organizational structure and internal culture can hinder operational effectiveness, even with abundant resources and qualified personnel, as was the case in the US system. The paper therefore suggests that intelligence reforms cannot be limited to technology, and in the HR field to recruitment and initial training alone, but must also address organizational theory aspects such as governance, organizational leadership, learning processes, and the ability to reconfigure priorities in an agile manner. Therefore, in intelligence agencies, which must constantly counter unconventional threats, even volatile ones, the lack of clear external accountability, incentives for collaboration, and flexible structures (such as complex adaptive systems), risks producing dangerous systemic failures.

The 2011 report, *The Intelligence Community: Organizational Chart*, by Richard A. Best Jr. is an institutional document of extraordinary importance for those working on the organizational analysis of intelligence systems, developed for the Congressional Research Service (CRS). This is a technical support body to the United States Congress which are used to guide legislative activity. Best provides a detailed and up-to-date analysis of the entire organizational structure of the US Intelligence Community (IC), the complex of American federal agencies responsible for collecting, analyzing, and sharing strategic information to protect national security. The author first analyzes the functional system, providing a broad overview of the Intelligence Community's composition. Each agency is studied based on its function, but also on its institutional affiliation, which may be under a specific department or oriented toward greater independence, and the types of lines of authority present. Although the document is intended as a primarily descriptive guide, its analytical scope can be exploited, in light of organizational studies, to understand the functioning of the system especially in relation to institutional design, multilevel governance, and the complex network structuring of different agencies.

The author emphasizes that, although the system of 17 intelligence agencies is formally unified under a single individual, the Director of National Intelligence (DNI), a position created in 2004 by the Intelligence Reform and Terrorism Prevention Act, governance remains highly decentralized. Indeed, many IC agencies operate under a dual line of authority, answering both to the DNI and to the heads of their respective departments (Secretary of Defense, Attorney General, etc.). This duality, combined with the hybrid nature of intelligence structures, produces a split between functional authority and operational control, with repercussions on overall functioning. Further fragmentation of the system arises, according to Best, from the separation of the budgeting and reporting mechanisms of the IC's two main funding sources, namely the National Intelligence Program (NIP) and the Military Intelligence Program (MIP).

The system described by Best is a typical example of a meta-organization, a structure composed of autonomous organizations that cooperate within a shared institutional framework, while maintaining very high levels of autonomy. This type of architecture, however, accentuates many of the tensions well-known in organizational theory. These include, first and foremost, the tension between centralization and autonomy, but also the challenges of horizontal coordination, problems of functional redundancy, the difficulties of effectively managing shared responsibility, and the risks of system failure due to the distribution of decision-making processes.

The case of US intelligence would seem to provide a useful example for studying and understanding the limitations of an almost purely hierarchical system, yet one that operates in highly complex contexts. However, Best's analysis suggests that the organizational structure of US intelligence is constructed as a network of overlapping agencies, rather than a hierarchical pyramid, consistent with the challenges posed by an environment characterized by adaptive complexity, where there is a constant tension between the need for innovation and resilience and the risks of poor coordination, systemic duplication, and role ambiguity. Indeed, the presence of multiple lines of authority, political and cultural constraints, as well as heterogeneous and sometimes divergent institutional objectives, makes interagency coordination a more political and cultural than purely technical task.

The DNI's role can be interpreted as an attempt to strengthen the strategic leadership without radically altering the operational units. However, according to Best, the DNI ultimately possesses, despite its formal authority, limited actual operational capacity, largely due to its lack of complete control over personnel and budget.

The National Security Enterprise: Navigating the Labyrinth (2017), edited by Roger Z. George and Harvey Rishikof is a collective text bringing together contributions from former officials, scholars, and experts in intelligence, security, and defense. The volume aims to illustrate the systemic complexity of the National Security Enterprise (NSE), a network of public institutions that includes departments, agencies, committees, presidential authorities, and multilevel bodies operating in the fields of intelligence, security, diplomacy, and defense.

The work aims to provide a guide through a veritable bureaucratic, institutional, and political labyrinth, characterized by a marked fragmentation of powers and a plurality of actors involved, with a wide variety of organizational cultures. Compared to traditional intelligence texts, the volume offers a holistic view, also including an examination of actors not typically included in this environment but which play a strategic role in intelligence governance, such as the Department of Homeland Security, the Treasury, and Congress.

The work is divided into thematic sections that analyze the various components of the national security apparatus, ranging from central agencies to those more peripheral but with a strategic role due to their location (relating to trade, energy, etc.), analyzing both actors external to the executive branch (such as Congress, the Supreme Court, public opinion) and policymakers primarily focused on national security.

One of the themes of this work is the difficulty of coordinating between different agencies with seemingly different but actually overlapping mandates. The effect is stagnation within their own organizational culture, which often renders agencies impervious to change and external influences. This phenomenon, defined by several authors in the book as “siloization,” also brings with it a tendency toward vertical compartmentalization of functions and resistance to an integrated or collaborative approach.

The role of the Director of National Intelligence (DNI) is critically addressed. Although this position is formally charged with overseeing and coordinating the entire Intelligence Community, the DNI suffers from structural operational limitations due to the duality of its channels of authority (as analyzed by Best, 2011) and its dependence on external departments for resources and personnel. Similarly, the National Security Council is described as a hub that is both central to the work and a source of conflict between the different approaches of the actors involved, who address the issue with different tools drawn from the diplomatic, military, legal, and intelligence fields.

The work analyzes the NSE not as a static entity, but as an adaptive system subject to external (emerging threats, global crises, technological innovations) and internal (political changes, legislative reforms, scandals, power dynamics) pressures. The conclusion of this analysis is that the resilience of such a complex system depends primarily on its ability to manage ambiguity, redundancy, and flexibility.

It emerges that the key characteristics of the NSE are those typically identified in complex adaptive systems (CAS), although the NSE system is neither completely decentralized nor perfectly coordinated, but operates within an adaptive governance regime in which diverse solutions coexist. The author describes the US intelligence system using the metaphor of a labyrinth, due to its complexity and dynamic stratification, where power is distributed, change is incremental and rarely guided, and synergies are more often emergent than designed. The work also analyzes several issues specifically related to organizational structure, including the difficulty of distributed leadership in having a real impact in such a highly specialized environment, the risks associated with functional overlap and redundancy, the importance of building trust among the various components of the system accustomed to a high level of secrecy, and the proactive role that shared training and an interagency professional culture can play.

The Shadow War is an analytical and investigative reportage by Grega Miller, a Pulitzer Prize-winning journalist and member of the Washington Post investigative team. The book examines the strategies of interference and influence developed by Russia and China in the years following the Cold War, with a particular focus on covert and semi-covert operations. Although journalistic in nature, the work is based on extensive interviews with intelligence officials, declassified confidential documents, court records, and diplomatic sources. It therefore draws on a wide range of high-quality gray literature. This makes it a highly reliable work for studying new forms of hybrid warfare and cognitive warfare. It also contains extremely useful elements from an organizational perspective, such as the description of decision-making chains and the operational methodologies used by Russian and Chinese intelligence agencies during interference and influence operations.

Miller explores both the Russian strategy of disinformation and destabilization and the Chinese strategy of silent penetration and dominance in the techno-economic sphere. Although the two powers share similar objectives, such as reducing American global influence and eroding Western internal cohesion, Miller shows how the two operational architectures and related organizational models differ profoundly.

The Russian model is characterized by the tension between marked decentralization and equally strong central management, built around civilian and military intelligence agencies and a constellation of non-state proxies (including oligarchs, hackers, and "conscripted" groups), reaching all the way up to the federation presidency. Russian operations are opportunistic and high-velocity, adaptive, and based on simultaneous disinformation campaigns on multiple fronts, employing cyberattacks, disruptive anti-establishment party financing, and psychological operations. These operations are so characterized by a model of strategic vertical control and tactical operational flexibility.

China, on the other hand, adopts a more systemic approach, aimed at pursuing long-term strategies and based on the concept of "unrestricted warfare." The Chinese system is indeed more bureaucratic, and also deeply integrated with the state and industrial apparatus, but this union follows a fluid logic of civil-military fusion and a strategy of silent domination. Operations are based on academic and scientific influence, the penetration of information and infrastructure systems, control of the Chinese diaspora and media abroad, and the strategic acquisition of high-tech companies.

The work compares the Russian intelligence system to a networked organization, with strong informal ties, systematically relying on proxy actors (non-governmental but controlled), with a high capacity for strategic coordination combined with executive flexibility. Meanwhile, the Chinese system, hypercentralized and statist, has top-down guidelines and places a dominant emphasis on the ideology of the Chinese Communist Party. Its organizational culture emphasizes strategic patience, cognitive asymmetry, and symbolic and cultural control, and makes extensive use of legitimate public institutions to pursue covert influence. In both cases, intelligence agencies operate in an ecosystem difficult to replicate in Western democracies, in which the boundaries between intelligence, diplomacy, economics, and propaganda are becoming increasingly blurred and permeable, prefiguring what more recent studies call "politically active intelligence" or "influence intelligence."

Both the Russian and Chinese systems demonstrate an evolutionary capacity consistent with the theory of complex adaptive systems (CAS), with emergent and nonlinear processes based on continuous adaptation to the external environment, a richly overlapping institutional ecosystem in which organizational adaptation also leads to competition between agencies, which vie for power levels, sometimes with divergent logics.

The work suggests that Western agencies, particularly American ones, find themselves operating in a new and unconventional battlefield, where traditional counterintelligence tools are proving inadequate. The challenge today and in the near future is no longer the traditional counterintelligence effort that has persisted since the end of the Cold War, but rather how to organize national intelligence systems with more agile and integrated capabilities, including at the cognitive level, capable of monitoring widespread information phenomena, operating in the influence domain, and decoding very weak signals covered by enormous noise. Collaboration with the private sector, universities, and the media will therefore also be a key aspect.

Van Puyvelde, D., Coulthart, S., & Bruneau, T. C. (2017), in the article "Comparative Intelligence Oversight: A Framework for Analysis. Intelligence and National Security", aims to fill the gap in the literature regarding a theoretical framework for government oversight of intelligence agencies, and does so through comparative analysis. The proposed approach is interdisciplinary and draws on studies in political science, comparative institutionalism, organizational theory, and civil-military relations.

The article highlights that there is no single model of effective supervision, but that the quality and effectiveness of supervision depend on the specific institutional, cultural, and political configurations of each country. The article provides empirical case studies from different continents to illustrate how the three dimensions can be very different and, when interacting, generate very different supervisory models that are more or less balanced.

The study situates the issue of control and governance within a systemic and multidimensional framework, typical of complex and adaptive organizations. Intelligence agencies require agile organizational architectures, even during control, that nevertheless maintain transparency, in order to manage the tension between the need for secrecy and the need for accountability. The atypical nature of intelligence organizations arises from numerous factors that risk obscuring the above outlined, such as operating in ambiguous and opaque institutional environments, possessing broad margins of discretion that make control more difficult but also more necessary, and requiring shared and coordinated control between different bodies that may lack mutual trust or a common, unambiguous language. This therefore requires specific supervisory models that are also capable of dynamically adapting to emerging threats, systemic crises, and technological and social changes.

"Intelligence Failures: An Organizational Economics Perspective. Journal of Economic Perspectives", by Garicano, L., & Posner, R. A. (2005) is one of many contributions that have attempted to analyze the underlying factors behind American intelligence failures, particularly in light of the terrorist attacks of September 11, 2001 and of the misidentification of weapons of mass destruction in Iraq. Unlike journalistic, political science, or exclusively bureaucratic interpretations, the article adopts a perspective borrowed from organizational economics to analyze the internal workings of intelligence agencies. These agencies are thus treated as organizations with a hierarchical architecture, tasked with processing information. The major obstacles in this regard are the structural difficulties in distributing knowledge and the severe cognitive limitations that risk undermining the validity of the results.

Garicano and Posner argue that intelligence failures should be understood as predictable outcomes, caused by structural problems related to specific elements such as inefficient distribution of information within the organization, the inability to filter and recognize relevant signals from background noise, the maintenance of poorly designed employee incentive schemes that prove inadequate to generate efficient and cooperative behavior, as well as excessive vertical and horizontal segmentation of structures.

To explain the failure of 9/11, the authors apply two concepts from organizational economics to intelligence agencies. The first concerns the difficulty with which knowledge can ascend hierarchical chains to decision-making levels, due to overload or simple structural rigidity (the "information bottleneck" problem). Intelligence agencies operate in an information-overloaded environment, where relevant information is deliberately concealed and false information is pushed out by mechanisms of disinformation and intoxication. Internal organizational problems risk undermining the entire organization's functionality.

The second is the eternal dilemma of choosing between speed and reliability in the decision-making process, with the real possibility of having to pay the price of errors resulting from incomplete, noisy, or ambiguous data, or of failing to intervene promptly enough. Intelligence agencies, operating in highly uncertain environments, are even more susceptible to this risk.

The article interprets the 9/11 fiasco as a classic case of coordination failure: numerous agencies possessed crucial information, but only in fragmented form, and no mechanism was able to effectively integrate it or process it cooperatively. To overcome these limitations, the authors propose more intelligent and resilient organizational structures, using tools to share the information needed by the system, overcoming the siloed logic typical of specialized agencies. They also propose the introduction of positive incentives for interagency cooperation, which would impact both concretely, such as career advancement, and more informally, such as increasing individual prestige. Another proposed system is the use of automatic data filtering and aggregation mechanisms to reduce the risk of cognitive errors by individual analysts. At the organizational level, the authors propose solutions in line with complex adaptive systems, such as a simplification of hierarchical levels, in order to reduce the loss of information in vertical ascent, and the adoption of decentralized and distributed intelligence models, capable of promoting self-organizing systems that produce an increase in speed and efficiency in response.

O'Connell, A.J. (2006) in "The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World", focuses her analysis on the structural efficiency of intelligence agencies in a post-crisis context, starting with the reform of the US intelligence community following the 2001 terrorist attacks.

The work focuses on the concept of "smart intelligence architecture," which relies on a targeted combination of organizational choices regarding the functional distribution of tasks, control structures, accountability mechanisms, and adaptability. The author approaches this concept through a multidisciplinary approach drawing on administrative law, organizational science, and institutional analysis, seeking to design intelligence agency structures that balance secrecy and accountability, while remaining both flexible and coordinated, autonomous and effective. The author argues that the 2004 reform (Intelligence Reform and Terrorism Prevention Act, IRTPA) and the creation of the Director of National Intelligence (DNI) represent an imperfect and incomplete step toward more integrated and transparent governance, as the lack of clear accountability for this position and a lack of structural clarity pose significant obstacles to the efficient functioning of individual agencies.

The author reaches this conclusion by analyzing the main characteristics of the US intelligence system, such as its excessive fragmentation, duplication of command, overlapping roles among different agencies, and difficulties integrating military and civilian intelligence. Furthermore, the US system suffers from insufficient oversight, is fragmented, and is incapable of addressing complex obstacles such as the presence of covert operations and massive amounts of data. Finally, according to the author, this system appears to be characterized by bureaucratic rigidity, a culture overly oriented toward secrecy, and a lack of structural incentives for change capable of concretely hindering the agencies' internal evolution. To be reliable, an intelligence organization must possess the ability to identify weak signals, correct deviations, and learn in real time. The current American system, however, is more focused on control than learning, generating a dangerous inertia.

For O'Connell, the solution lies in a series of systemic reforms that strengthen the DNI's power, making it more financially and hierarchically autonomous. At the same time, both the number of agencies and their mandates should be rethought and rationalized. Furthermore, automatic external review mechanisms should be established and an organizational culture geared toward interagency cooperation should be fostered internally. This misalignment between the DNI's formal authority and its actual power exemplifies the decoupling typical of complex organizations, where formal functions and real processes do not coincide, as the nominal and hierarchical structure masks a polycentric and often disorganized reality.

O'Connell finally proposes a model in which agencies must operate in a coordinated network, rather than in vertical isolation, which is consistent with the fact that modern intelligence requires distributed governance, with autonomous yet connected nodes capable of sharing information, aligning strategies, and responding in a concerted manner to systemic crises, as in complex adaptive systems.

Cavelty & Wenger's "Cyber Security Meets National Security: Organizational Responses to Cyber Threats. Contemporary Security Policy" (2020) addresses the issue of how states are reorganizing their national security institutions in light of the growing relevance of the cyber domain, requiring them to extend protection against an asymmetric, diffuse, and dynamic threat such as cyber.

The article uses an empirical approach, comparatively analyzing the organizational responses of several Western states (with particular attention to the United States, the United Kingdom, Germany, and Switzerland), seeking to explain how cyberspace is progressively integrating into the pre-existing concept and practices of national security. The focus is then placed on the implications of this convergence for agency architecture.

The authors describe an emerging convergence between more and less traditional approaches to national security. The more traditional approaches, traditionally focused on state intervention, including military intervention, or sometimes even tending to completely exclude the involvement of any non-military entity, are merging with top-down approaches and more distributed and dynamic approaches to cybersecurity, capable of integrating the public and private sectors. This convergence is the result of a process of "cyber-securitization," or the transformation of cyber threats into the object of state security policy. The result is a growing militarization of cyber, with a progressive centralization and attribution of responsibilities to intelligence and defense agencies, even in originally civilian spheres.

In reality, national organizational response models span the entire continuum between centralized and decentralized approaches. The United States is moving toward military centralization, with USCYBERCOM and the NSA as key players, while the United Kingdom is adopting a hybrid model, with the National Cyber Security Center (NCSC) as a bridge between intelligence and the civilian sector. Germany suffers from coordination difficulties generated by a system that is still fragmented due to too many agencies with overlapping functions, while Switzerland has a level of integration between the various actors that is too low, although ongoing reforms aim to overcome this limitation.

The authors believe none of these models is yet optimal, as each approach presents trade-offs between operational efficiency, democratic legitimacy, and systemic resilience. The authors also identify the risk that excessive militarization of cyberspace could reduce democratic control over the expansion of intelligence agencies into new areas.

Intelligence agencies operate in an environment characterized by high uncertainty, constant technological change, and a multiplicity of actors. To achieve effective responses, they must therefore avoid rigid structures and move toward adaptive architectures capable of integrating flexibility and control, in which governance must also be adaptive. Only structures that learn, reconfigure, and evolve in step with threats can survive in the cyber era. Furthermore, complex environments require coordinated responses, and cybersecurity cannot be guaranteed by a single entity, but instead requires the collaboration of intelligence agencies, private entities, centers of expertise, and regulatory bodies. To be effective, such collaboration must structurally include the creation of collective networks based on a solid foundation of trust.

Finally, the article highlights the risk of democratic drift, generated by the widespread lack of adequate legal basis for intelligence agencies' power in the cyber sphere. These agencies are sometimes called upon to fulfill ambiguous roles, straddling defense, prevention, and regulation, resulting in weak integration with the remaining components of the system. This, even when it promotes flexibility, can lead to a weakening of responsibilities.

Hammond, T.H. (2010) in "Intelligence Organizations and the Organization of Intelligence" seeks to overcome the self-imposed limitation of many intelligence analyses: treating agencies as "black boxes" within which it is impossible to scrutinize and analyze their mechanisms. This leads to poor theoretical formalization, as researchers end up focusing exclusively on results, often selecting particularly dramatic ones, such as spectacular failures or successes, or scandals, without addressing the structural and procedural logic that generates such pathological events.

The author instead seeks to demonstrate that good organizational design can increase efficiency, reduce the risk of failure, and improve the quality of analyses. To do so, he draws on classic models from the theory of complex organizations (Simon, March, Galbraith, Wilson). The author identifies three structural organizational problems, each of which directly impacts the ability to generate reliable and timely intelligence.

The first is the fragmentation of information gathering and analysis, inherent in the complexity of the mandate entrusted to agencies, which forces them to divide tasks among different units. However, this leads to excessive specialization, fragmentation of knowledge, and the development of cognitive filters, all barriers to an effective flow of information.

This leads to the second problem, related to the first, and concerns the risk that information integration is slow, prejudicial, and vulnerable to cognitive biases. This can be facilitated when information inputs, often partial, contradictory, and from heterogeneous sources, are analyzed by overly compartmentalized structures, thus fostering stagnant subcultures.

The third problem identified by the author concerns the rigidity with respect to organizational adaptation and change, generated by established procedural rules, a bureaucratic culture, and poorly designed career mechanisms. Such rigidity can inhibit innovation, discourage the reporting of anomalies, and encourage the persistence of systemic analytical errors.

Hammond also identifies a specific organizational pitfall associated with attempts to improve cybersecurity, as the role specialization that often follows these efforts also increases the systemic risk of error due to isolation, loss of context, and procedural rigidity.

Hammond also offers some organizational suggestions to improve performance, such as creating temporary task forces or interagency units to address specific issues or threats, as well as reducing hierarchical levels to speed up decision-making and facilitate the management of ambiguous or incomplete information through cross-validation mechanisms.

Berkowitz, B., & Goodman, A. (2000) in *Best Truth: Intelligence in the Information Age* analyze how the global information environment, characterized by hyperconnectivity and uncontrolled data flows, has radically transformed the ways in which intelligence agencies collect, process, and communicate structured information of strategic value. The two authors begin by observing how the cyber revolution has altered operational conditions, making the broad spectrum of open-source intelligence (OSINT) available, allowing powerful non-state actors to emerge as both sources and recipients of intelligence, and increasing the public and political visibility of intelligence work. The challenge posed by a new world, rich in information noise and disinformation, in which the speed of decision-making cycles has dramatically increased, requires intelligence agencies to redefine their structures, practices, and epistemic identities.

Berkowitz and Goodman argue that the architecture of intelligence agencies is still anchored in a hierarchical, closed, secretive, and slow-moving logic, while the external environment demands speed, flexibility, and decentralization, as well as increasing integration between different disciplines, working collaboratively with various agencies, and demonstrating the capacity for continuous learning coupled with effective internal innovation. The authors therefore propose an alternative model, inspired by the world of knowledge-based organizations, centered on adhocratic and networked structures, in which leadership is distributed and collaboration is cross-sectoral, and where analytical and technical expertise is valued, even if external to the agencies.

The work presents a vision of intelligence no longer as a linear process (starting with collection and then moving on to analysis and dissemination), but as an adaptive, iterative, and co-evolutionary one. The authors outline a conception of intelligence based on short, repetitive, and non-hierarchical cycles, in which analysts and decision makers constantly interact, where open sources are strategically integrated with secret ones, and where the overuse of silos, which impedes the flow of information, is drastically reduced.

Ultimately, the book highlights how the “Cold War mentality” is still pervasive in the culture of many agencies, and continues to favor excessive compartmentalization, abuse of secrecy, the dominance of military culture, and strictly vertical chains of command. The authors argue that this organizational model is no longer suited to addressing an environment where data is dispersed, threats are asymmetric, and knowledge sources are now widely distributed across civil society, academia, the private sector, and even the media. In their proposed model, however, which is adaptive and inspired by complex systems, information flows freely, decisions emerge from collaborative networks, and organizational learning is continuous and context-integrated.

Oleson, P. C., & Cothron, T. (2016) in "Leading and Managing Intelligence Organizations" provide both an overview of the managerial and organizational challenges facing intelligence agencies in the 21st century and guidance for leadership development and institutional redesign of the agencies themselves.
The authors define intelligence organizations as unique organizational systems, endowed with certain recurring structural and cultural characteristics, such as a high level of compartmentalization, the predominance of mission-oriented thinking, rigid regulatory and political constraints, as well as information ambiguity and high decision-making risk. These elements differentiate intelligence leadership from that in civilian or commercial environments, as decisions must be made in the absence of complete information, subject to strict ethical constraints, and with potential global impacts.
According to the authors, in the intelligence context, a clear separation between the two dimensions of leadership (defined as the ability to inspire, motivate, direct, build organizational culture, manage change, and strategic vision) and management (defined as efficient resource allocation, process oversight, standardization, and control) can be harmful. The authors argue that agency leaders must integrate both functions, becoming leader-managers capable of combining procedural discipline and strategic agility. For Oleson and Cothron, the challenges of organizational complexity arise from the growing number of stakeholders, often with intractable interests, the proliferation and rapid evolution of intelligence sources and types, and the increased demand for interagency and interstate cooperation. Effective leadership in this context must also act as a link between different units, promoting synergy and coherence.
The essay ultimately views intelligence agencies as hybrid organizational structures, oscillating between hierarchical bureaucracy (such as the pre-reform CIA) and agile adhocracy (like joint task forces), with forays into distributed and networked models (such as cyber teams or private OSINT centers). The authors suggest that leadership must adapt its style to the prevailing structure, but also be able to modify it over time through soft tools such as training and culture, and hard tools such as redesign and incentives.

Networks and Netwars: The Future of Terror, Crime, and Militancy by Arquilla, J., & Ronfeldt, D., published in 2001, immediately before the events of September 11, it today has almost prophetic value, offering a complex vision of how fluid, decentralized, and adaptive networks have replaced traditional hierarchies in asymmetric conflicts, transnational crime, and global terrorism.

Arquilla and Ronfeldt clarify the distinction between two concepts that have often been confused since their introduction. Cyberwar involves the use of digital tools (such as hacking, denial-of-service, spoofing) within traditional conflicts, while netwar represents a new form of social, political, or ideological conflict in which networked actors (terrorists, cartels, hacktivists, ideological movements) use connectivity and decentralization to conduct operations that may or may not be violent but are destabilizing. Actors here have no central headquarters, do not operate according to traditional command-control logics, but use information, narrative, and distributed mobilization as weapons.

The text devotes considerable space to describing network structures, often present in terrorist groups (e.g., al-Qaeda), social movements (e.g., the Zapatistas), criminal cartels, and paramilitary groups. All networks share common characteristics, which can be studied in a general manner. In particular, they exhibit varying degrees of decentralization, allowing each node to operate autonomously. They also exhibit functional and communicative redundancy, which makes the network resilient; distributed leadership, informal authority, implicit consensus mechanisms, and the ability to adapt and rapidly reconfigure the organization in response to environmental changes.

These structures are not based on rigid bureaucratic hierarchies, but on flexible interconnections, often based on trust or ideology. State organizations, particularly intelligence and security agencies, are disadvantaged compared to non-state networks due to their slow, compartmentalized, and poorly interoperable vertical hierarchies, which struggle to adapt quickly due to regulatory, political, and cultural constraints. This results in a profound organizational asymmetry, which favors networked actors. Thanks to this analysis, the work has successfully anticipated many of the issues that have emerged in the years since its publication in the response to threats such as ISIS, Anonymous, and Russian disinformation.

The authors also propose organizational reforms aimed at effectively countering networked adversaries, such as a transformation that allows for interconnection between agencies, operational flexibility, modularity, and interoperability between teams. They also propose the creation of hybrid task forces, temporary and agile units composed of intelligence officers, special forces, IT experts, social analysts, and psychologists. They also propose the pursuit of distributed leadership, in which local autonomy is combined with strategic coordination.

b) Organizational culture and professional socialization

Lowenthal's *Intelligence: From Secrets to Policy* (2019) analyzes the functioning of intelligence agencies, primarily following the well-known intelligence cycle, but also offers numerous insights into governance and institutional adaptation. Considerable space is devoted to the constellation of the US Intelligence Community (IC), described as a hybrid structure that is also analyzed in relation to problems of redundancy, fragmentation, and lack of interoperability. The book also addresses the role of the Director of National Intelligence (DNI) in relation to coordination and strategic oversight functions.

The US intelligence community is described as a multi-actor, interdependent, and decentralized system that must co-evolve with the strategic environment. Specifically, the intelligence community's organizational structure is constantly forced to adapt to a fluid, decentralized, and unconventional environment, where technological superiority alone can no longer guarantee a stable strategic advantage. The effectiveness of agencies' actions depends primarily on the ability to collect, process, and share information, under conditions of time, ambiguity, and risk. Thus, cognitive capital becomes the primary strategic resource, while adaptability, functional redundancy, and the ability to learn from mistakes are key traits that complement the organization's human value. This is also because agencies operate in a partially decoupled manner, with chains of command and information flows that are not always aligned, creating both systemic inefficiencies and local flexibility. Intelligence is then described with characteristics that place it within the framework of knowledge-oriented organizations (KBOs).

The work also explores critical issues in the delicate relationship between intelligence analysts and policymakers, particularly the risk of politicization and the challenges posed by effective democratic oversight.

Assessing the Tradecraft of Intelligence Analysis by Treverton, G. F., & Gabbard, C. B. (2014), is part of a growing focus on the intelligence community's responsibility for the forecasting failures associated with September 11, 2001, the inaccurate information on the presence of weapons of mass destruction in Iraq (2003), and the subsequent institutionalization of Structured Analytical Techniques (SAT) and intelligence reform practices initiated under the oversight of the Office of the Director of National Intelligence (ODNI). The work employs an empirical design, whose evaluation methodology aims to measure the quality of analyses produced within the U.S. national intelligence community.

The first question the authors address is how to define and measure intelligence analysis, given that such predictive analyses actually serve only to reduce uncertainty, not to actually predict future events. Therefore, it would be pointless to retroactively evaluate analyses in relation to actual subsequent events. Furthermore, the very concept of quality of an analysis can be understood in different ways, such as mere analytical rigor linked to methodological accuracy, or as a substantial insight capable of offering useful perspectives to the decision maker, or even simply for its positive communicative value linked to clarity, conciseness, and relevance for the recipient.

The research team therefore applies a pre-existing standard, already defined by the ODNI in the National Intelligence Tradecraft Standards, a set of 9 evaluation criteria, including a clear articulation of the analytical purpose, the relevant and transparent use of sources, historical and geopolitical contextualization, a full evaluation of alternatives and explanation of uncertainties, a clear and distinct separation between facts and inferences, the presence of coherent logical reasoning, but also a real consideration of counterfactual information and finally, effective and appropriate communication to the user.

The study's findings are mixed. For example, only a minority of the analyses studied systematically evaluated hypothetical alternatives and concretely considered divergent scenarios. Furthermore, uncertainty is rarely made explicit during the disclosure phase. Logical reasoning is also often weak, if not incomplete, with assertions insufficiently grounded in concrete evidence or unverifiable. However, communication with end users is generally good, a sign that analysts focus more on communicative impact, even when methodological accuracy is poor.

From these data, the authors conclude that agencies' analytical culture is still largely based on implicit mental models, the result of ingrained habits, which are not consciously generated by scientifically rigorous approaches. Furthermore, institutional pressure is widely present during the analysis phase, contributing to the resilience of many of the factors outlined above.

The concept of “intelligence tradecraft,” similar to that of high-performance organizational reliability (HRO), highlights how the quality of analysis can be an indirect measure of a structure's ability to function effectively under pressure, in uncertain, and high-risk environments. Indeed, intelligence analysis operates in a context where objectives, standards, and outcomes are not always well aligned, and where stakeholders (analysts, policymakers, hierarchical superiors) may have divergent expectations. Quality assessment can therefore also serve to rebuild a common language between loosely coupled levels, with beneficial effects across the entire vertical chain.

Williamson, M. (2017) in “Socializing Intelligence: The CIA and Professional Identity Formation”, explores the formation of professional identity within the Central Intelligence Agency (CIA), focusing on the processes of socialization, the construction of a sense of belonging, and the internalization of institutional values among analysts and staff.

The work employs methods drawn from sociological and organizational studies to analyze the role of culture and everyday practices in organizational structure, drawing specifically on interviews, public documents, and analysis of specialized literature. Williamson observes that it is the symbolic processes and informal rituals that make the CIA more than a simple agency, endowing it with the characteristics of a true community of thought, where even informal norms and codes of conduct are deeply internalized, helping to shape a professional identity aligned with institutional requirements, especially with high levels of loyalty, a sense of duty, and the perception of belonging to something more than just a job.

If it is true, following organizational sociology, that every complex organization shapes its members through socialization processes that transmit not only norms and language, but also practices and values, often implicitly, in the case of intelligence agencies, and the CIA in particular, this process is intensified by several unique elements, such as the high and widespread secrecy, the exceptional nature of the mandate in terms of both risk and social recognition, and ethical, moral, and strategic pressure.

This work explores the professional epistemology of intelligence, rooted in the fact that the analyst is not simply a technician, but a person whose task is to produce credible information, starting from conditions of profound uncertainty. This information, however, can then concretely alter the course of events. This leads to the naturalization of certain analytical approaches, such as groupthink, the discouragement of epistemic deviance, or cognitive dissonance, reinforcing an elitist and self-referential ethos, often to the detriment of more critical or reflective alternatives. This leads to a poorly managed identity cohesion, which, while strengthening operational reliability, risks generating the dangerous effects described above.

The CIA, like many large bureaucracies, is subject to internal institutional isomorphism, in which new members are assimilated into the system. This leads to the standardization of analytical practices, often in the name of professional consistency, and innovation is hindered because it is seen as a deviation to be corrected rather than a resource.

Identity cohesion can therefore hinder organizational learning if it reduces critical feedback, imposes a monolithic view of threats, and generates resistance to change. This last point becomes even more critical the more the organization finds itself in contexts of strategic or technological transition, as was the case, for example, with the arrival of cyberspace.

Van Puyvelde, D. (2021) in *Out of the Shadows: The Ethics of Intelligence*, seeks to analyze the complex issue of conducting intelligence ethically. Specifically, the study focuses on how organizations can develop structures, processes, and cultures to achieve this goal. Intelligence agencies, the author highlights, have historically been associated with controversial practices such as mass surveillance, torture, coups, or disinformation, partly due to the opaque and secretive environment in which they operate, where democratic oversight is not always effective. This raises the need to develop a robust and shared organizational ethic for intelligence agencies, based on the principles of democratic legitimacy, proportionality as a guide for actions that violate personal rights, clearly defined responsibilities, and transparency.

The book distinguishes two levels of ethics. The first is formal ethics, which can be achieved simply by respecting the law, rules of engagement, and protocols, and which therefore determines only whether an action is legally acceptable. The other level is substantive ethics, which goes far beyond mere legality, calling into question the entire internal sphere, both personal and institutional. The author's thesis is that the cause of the many scandals involving US intelligence is not to be found in the commission of illegal actions, but in the lack of due reflection when following orders, or in opportunistic decisions that have not been sufficiently evaluated—all indicators of an insufficient shared substantive ethics. Agencies are organizations with goals, procedures, professional standards, and organizational culture, and as such, they can violate, respect, or promote ethical values, not only through individual decisions, but also collectively through architectural choices, career incentives, and other institutional processes. Ethics, therefore, should not be understood and analyzed merely as a personal attribute of the individual analyst or operator, but as an organizational function that must therefore be specifically designed, and subsequently monitored and adapted to changes.

The author proposes a four-dimensional model to evaluate not only the specific actions undertaken by intelligence agencies, but the entire moral ecosystem. This model is based on an analysis of the organization's fundamental characteristics, including, first and foremost, its mission, in order to assess its clarity, legitimacy, and consistency with constitutional values. However, the analysis must also assess whether the means are proportionate to the end, whether they contain discriminatory elements and are effectively subject to oversight, whether internal and external accountability structures exist, and whether the organizational culture is capable of promoting reflexivity, constructive dissent, and ethical learning.

Hastedt, G. P. (1996) in "CIA's Organizational Culture and the Problem of Reform", analyzes internal reforms within the CIA from the perspective of organizational theory.

The author emphasizes that the CIA's structure was designed to be flexible and adaptable, providing impartial and strategic information to policymakers. However, in practice, it has consistently demonstrated strong resistance to change and a tendency to close itself off from external criticism, rejecting and hindering reform. According to Hastedt, the CIA's internal culture is rooted in its structural secrecy, coupled with strong compartmentalization, which creates harmful information barriers within the agency itself. This is coupled with epistemic elitism, whereby only insiders can understand the intelligence community's functioning and thus make decisions about its structure. This, in turn, leads to the belief that evaluation can only be internal and self-referential. All of this creates a defensive culture, which tends to preserve the status quo and reject any reform, which is seen as a threat rather than an opportunity. In a situation of such adaptive immobility, in order to avoid the cognitive and political costs of a change deemed dangerous, ineffective solutions adopted out of habit or lack of innovative ideas end up becoming routine and are continually reiterated.

The author specifically analyzes several historic reform attempts at the CIA, such as those following the Vietnam War, the Church Commission, and the dissolution of the USSR, and shows how they systematically failed or at least had only partial effects. The author identifies the reasons for the reforms' failure as various structural issues, such as the lack of clear and effective external accountability, the ambiguity of the agency's mission, and, above all, the widespread reluctance to accept external criticism due to a closed internal culture. The reforms, therefore, would fail because they were poorly designed from the outset, aiming only at achieving superficial image enhancements, without truly aiming to change the harmful structures rooted in the cultural system.

Hastedt proposes instead that effective reform must employ a cultural approach, starting first with a critical internal assessment of its own failures, and then developing an openness to heterodox perspectives, encouraging epistemic reflection, ongoing training, and interdisciplinary collaboration. For the author, therefore, only through the development of cultural, and not just bureaucratic, mechanisms of oversight and accountability could the implementation of a reform succeed.

Boardman, C. H. (2006) in *Organizational Culture Challenges to Interagency and Intelligence Community Communication and Interaction* is a report, published as a technical paper, that explores the root causes of communication problems among members of the U.S. intelligence community, and between them and other federal agencies. The work is part of the broader cultural movement that analyzed intelligence reforms following 9/11 and focuses specifically on the challenges that affect the effectiveness of coordinated action between different agencies. The study argues that the obstacles to cooperation are not merely technological or bureaucratic, but are primarily linked to the unique cultural aspects of individual agencies, particularly those related to cognitive models, behavioral norms, and identity mechanisms. According to Boardman, organizational culture strongly influences how data is interpreted by analysts, and these influences are so strong that they can extend to communication channels, the legitimacy of interlocutors to the exclusion of others, and can even contribute to guiding delicate decisions regarding strategic priorities. The work highlights how these cultural differences can hinder communication between different entities even when their missions are fully aligned.

First, in many cases, the problem lies at its root, as the institutional missions of different agencies are profoundly different. For example, analytical agencies focused on information gathering favor strategic synthesis, which can also favor delay and secrecy, while operational agencies are more oriented toward action and timely law enforcement. The result is divergence in both decision-making timeframes and communication formats, and subsequently also in the evaluation of success metrics.

Interagency differences also create a culture that fosters professional autonomy and institutional competition, with each seeking to defend its own mandate and jurisdiction, including through jealousy in information sharing, which is seen as a form of capital, not only practically but also symbolically.

The diverse histories of agencies also sometimes lead to the development of incompatible languages and terminologies, which inevitably result in the production of dissonant cognitive structures, hindering easily translatable communication between different agencies.

The presence of strong decision-making hierarchies, characterized by cumbersome authorization processes for cooperation and information sharing, limits or slows joint action, just as the culture of competition and mistrust ends up creating watertight compartments built on a foundation of identity, which is not affected by the presence of simple formal protocols.

Goldman's *The US Intelligence Community: An Introduction* (2015) is a comprehensive work that covers the structure of the entire American intelligence system. The system is described as a complex organizational network in which agency differences are very pronounced, both in terms of internal cultures and objectives and tools. This generates conflicts that impede efficient coordination.

Goldman devotes considerable attention to the agencies' diverse internal cultures, each of which has developed its own value systems, distinct analytical and operational routines, often incompatible technical languages, and follows its own performance evaluation metrics. This cultural heterogeneity, combined with the lack of an effective central hierarchical authority, impacts the ability and readiness to manage emerging crises in a coordinated manner. The multiplicity of nodes, horizontal interactions, and emergent dynamics make this community a nonlinear system, in which organizational learning and adaptation to threats are not supported, and are at the mercy of informal coordination and self-organization.

Part of the work then focuses on the system of democratic oversight of the US intelligence community, based on levels of internal oversight, executive oversight (by the President and the ODNI), and legislative oversight (by the House and Senate Intelligence Committees). The structural limitations of these mechanisms are highlighted, particularly in relation to excessive secrecy, which limits access to effective oversight, and the risk of politicizing intelligence, which could lead to a shift away from developing optimal strategies.

How Spies Think: Ten Lessons in Intelligence by Omand, D., & Phythian, M. (2023) is intended as a guide to the logic and practices of intelligence thinking. The paper presents the idea of translating analytical best practices developed in the intelligence field into tools applicable to complex decisions, even outside their original context.

The book proposes to explain the functioning of intelligence thinking by breaking it down into sub-elements, according to the "SEES" model, an acronym for:

- *Situational Awareness* – understanding what is really happening;
- *Explanation* – building coherent narratives about the causes of events;
- *Estimation* – making plausible predictions about what might happen;
- *Strategic Notice* – reporting future systemic risks, even those with high uncertainty.

This model seeks to answer how, in the intelligence field, rational and informed reasoning can be achieved when conditions are characterized by high levels of uncertainty, incompleteness, and ambiguity.

Intelligence agencies are collective systems, in which the quality of knowledge produced or validated depends on the analytical system's ability to self-regulate, adapt, filter out noise, and manage ambiguity. Intelligence-based thinking is therefore organized thinking, and is only possible in the presence of structures, routines, incentives, and professional culture.

Omand and Phythian emphasize the importance, for achieving consistent analytical results, of a culture based on intellectual honesty, resistance to political pressure, awareness of vulnerability to cognitive biases, and an ethics that allow for the expression of uncertainty. To achieve such a culture, the necessary tools include institutionalized peer review processes, source validation standards, and ongoing training in both analysis and probabilistic reasoning. Furthermore, organizational design in the intelligence field should ensure tolerance for analytical dissent, including through the establishment of dedicated teams, and that analytical and operational functions are kept separate in decision-making processes. Finally, it is imperative that the system possess mechanisms that allow it to learn from mistakes, according to post-mortem analysis methodologies, and thus adapt dynamically and proactively.

Wirtz, J. J., & Gelles, M. G. (2020) in “Intelligence and Mental Health: Addressing Psychological Challenges in National Security” analyze the challenging relationship between intelligence and mental health, starting from the observation that this unique environment is extremely cognitively intensive. Therefore, individual and collective psychological resilience are critical factors for organizational success, with knock-on implications for recruitment, initial and ongoing training, management, and leadership.

Intelligence workers live in highly constrained professional environments, including a high degree of internal surveillance, the constant demand to operate with rapid reaction times and minimal margins for error, information compartmentalization, chronic secrecy, and social isolation. This environment produces long-term effects on mental health, including chronic anxiety, post-traumatic stress disorder (PTSD), hypervigilance burnout, depression, and dysfunctional behaviors, including substance abuse.

The paper highlights how the mental health of an individual worker not only impacts the individual but also influences the entire spectrum of organizational performance, including the effectiveness of analysis and forecasting, the quality of interagency collaboration, cognitive adaptation and flexibility, risk management, and the reliability of decisions in crisis situations. Therefore, a lack of attention to mental health can lead to serious systemic errors at all levels.

However, agencies are often characterized by a culture in which admitting psychological distress or difficulties is perceived as a failure and a source of suspicion, generating internal stigma, and even leading to concrete consequences, such as the revocation of security clearance as a preventative risk reduction tool.

Mental health management may appear to be a secondary element, when in fact, according to the authors, it represents a structural dimension of operational reliability, and therefore of the resilience of the entire organization. Resilience is understood not only as a reactive capacity, but also as the ability to absorb internal shocks, including the psychological attrition of operators. According to this perspective, there is therefore a close interconnection between the individual well-being of operators and analysts and the adaptability of the intelligence organization.

c) Decision-making processes and bounded rationality

Heuer's *Psychology of Intelligence Analysis. Central Intelligence Agency*, (2010), is a work that aim to identify cognitive biases and systematic errors in analytical reasoning of intelligence, and to propose operational tools to mitigate them, using the tool of cognitive psychology, applied epistemology, and organizational sciences.

Heuer, drawing on concepts typical of experimental psychology (particularly Kahneman and Tversky), highlights how analysts are also subject to systematic errors that degrade the value of their results, such as confirmation bias, anchoring bias, the framing effect, or the illusion of retrospective understanding. The most serious problems, therefore, arise not from a lack of information, but rather from errors generated during interpretation. These elements are constantly present and thus make intelligence analysis constantly vulnerable to systemic failures, as demonstrated by numerous cases (from 9/11 to the weapons of mass destruction in Iraq, not to mention Pearl Harbor).

The problem therefore takes on not only individual but also organizational relevance. To avoid repeating systemic failures, intelligence organizations must possess an architecture that institutionally stimulates doubt and the exploration of alternative hypotheses. Organizational culture should value constructive dissent, lateral thinking, and challenging dominant models, while analytical leadership should prioritize accuracy over speed and intellectual humility over challenging dogmatic certainties and dominant group thinking. Intelligence analysis should therefore include cognitive redundancy and continuous attention to weak signals, as well as organizational self-correction mechanisms.

Lefebvre, S. (2013) in “The Difficulties and Dilemmas of International Intelligence Cooperation” explores a controversial topic in the intelligence community: international cooperation between intelligence services. To do so, it applies a theoretical-operational approach based on concrete case studies.

Intelligence cooperation between different states arises for two main reasons: either to address common threats, or to gain “economic” access to information in areas that are difficult to reach due to geography or language. In both cases, the effect is increased strategic efficiency through better use of limited resources, while simultaneously strengthening alliances. However, these benefits must be constantly balanced with some inevitable strategic, political, and organizational costs, which are not always obvious, such as the loss of control over sensitive information and the associated risk of undermining systems of trust based on personal relationships, information asymmetry between services, risks inherent in a culture oriented toward secrecy, regulatory issues, and potential political manipulation.

Intelligence cooperation is a classic example of an interorganizational system characterized by low structural integration and high functional interdependence.

Lefebvre highlights that intelligence cooperation operates as a dynamic network, with variable power nodes and informal mechanisms for information exchange. Therefore, given the absence of a central authority, negotiated and adaptive forms of coordination are necessary. Indeed, a culture of sharing is hindered at the national level by individual cultures of secrecy, information control, and loyalty to one's own chain of command, and effective cooperation is therefore costly in terms of negotiation, monitoring, and information protection.

The article “Expert Political Judgment and Good Judgment Project: How to Improve Decision Making in Intelligence” by Tetlock, P. E., & Mellers, B. A. (2014) synthesizes two decades of research, culminating in the Good Judgment Project, a large-scale experiment (within the Intelligence Advanced Research Projects Activity – IARPA) to assess the ability of individuals and groups to make accurate predictions about geopolitical events.

Tetlock and Mellers' contribution demystifies the concept of “expert” in the intelligence field, proposing instead models of expertise based on structured cognitive and organizational processes, and therefore more measurable.

The study stems from the discovery that intelligence and international affairs experts, especially those appearing on television, frequently make mistakes when making strategic forecasts. The causes of these errors have been identified as overconfidence, ideological biases, and, above all, the use of rigid cognitive styles. The experiment, which involved thousands of volunteers, demonstrated that non-professionals, if adequately trained and grouped into well-designed teams, can outperform professional intelligence analysts.

Based on the study's findings, the authors proposed several changes to intelligence systems, such as systematically measuring the accuracy of their members' analytical forecasts, implemented as an ongoing organizational practice. This would, however, require clearly defining the forecasting questions beforehand, subsequently measuring the results, comparing the two phases, providing constructive feedback, and possibly retraining analysts in the event of poor performance.

Furthermore, the recommendation calls for encouraging the scouting and subsequent development of predictive talent at the individual level and cognitively diverse teams at the collective level. Research has demonstrated that predictive capabilities are partially trainable, and that the best results are achieved by selecting cognitively suitable individuals (as in the case of superforecasters), combining them in heterogeneous groups, and promoting a culture of probability and Bayesian reasoning.

The authors also criticize the traditional hierarchical approach and suggest that organizational culture be encouraged toward continuous learning and the encouragement of informational doubt, including through the rejection of vertical authority. Finally, the study highlights how new predictive technology systems could be integrated into agencies' operational procedures.

The authors, however, also highlight some limitations of the research, such as the inability to simulate all real-world operational conditions within agencies, and the fact that measurability does not guarantee a complete picture, as many intelligence assessments involve phenomena that cannot be directly verified.

Friedman, J. A., and Zeckhauser, R. J., in “Handling and Mishandling Estimative Probability: Likelihood, Confidence, and the Weighting of Evidence. Intelligence and National Security” (2015), also address the issue of systemic errors in intelligence decision-making, such as those that occurred before 9/11 or related to the alleged detection of weapons of mass destruction in Iraq.

Given that intelligence assessments inevitably involve uncertainty, the authors focus on how this uncertainty is represented, communicated, and interpreted. Specifically, they criticize the lack of semantic precision, the weakness in distinguishing between the concepts of probability and confidence, and the inconsistent use of weight of evidence. They highlight how the use of inadequate methods risks producing serious political errors in the subsequent decision-making process.

The authors analyze the specific verbal expressions used by agencies (such as "probably," "almost certainly," "possibly"), highlighting how these can be interpreted differently, and often overlapping, by individual analysts, both political and military. The authors' recommendations therefore include the use of shared numerical scales in analytical communications, with explicit and consistent definitions of probability. They also recommend training analysts in more refined probabilistic reasoning, enabling them to identify the limits of their knowledge.

Trent, S., Patterson, E. S., & Woods, D. D. (2007) in "Challenges for Cognition in Intelligence Analysis" explores the mechanisms of intelligence analysis, starting from a very specific choice: to reject the reductionist vision of the single, isolated analyst, replacing it with that of an activity resulting from complex collaboration.

Intelligence analysis is described as the practice of constructing meaning from evidence gathered in a poorly structured environment, rich in weak or contradictory, inconsistent, or redundant signals, and in which many of the evaluation results are impossible to validate, even ex post. In this context, traditional cognitive tools prove insufficient without adequate architectural and methodological support.

The authors question sequential analysis models based on the intelligence cycle, proposing instead an iterative, nonlinear, and retroactive model of cognitive activity. According to the authors, thought formation does not originate exclusively in the mind of a single individual, but emerges from the interaction between human agents, external cognitive tools, work environments, and organizational norms. According to this view, the expert's intuition, while playing a central role, must be supported by essential external factors, such as the organizational structure and the feedback provided.

Behrman, R., & Carley, K. M. (2003) in *Modeling the Structure and Effectiveness of Intelligence Organizations: Dynamic Information Flow Simulation* approach the problem of organizational efficiency in intelligence agencies from a computational perspective, using dynamic simulation models to represent and analyze the internal flow of information and the reactions of decision-making structures. This research also stems from the post-September 11, 2001, context and the resulting growing pressure for intelligence reform. However, its difference from other research is its use of a numerical system designed to simulate an organization composed of cognitive agents. In the simulation, each agent receives partial information, develops an assessment, communicates its analysis to the higher level, and thus contributes to the final decision. The system can simulate various types of structures, including classic hierarchical structures, network structures, as well as mixed or matrix solutions, with varying levels of redundancy and centralization. Performance is measured in terms of final decision accuracy, response time, and resilience to introduced perturbations.

The article analyzes how organizational structure influences the analytical performance of intelligence agencies, and the simulations show how more decentralized structures, and therefore with greater distributed processing capacity and information redundancy, achieve superior performance in dynamic and uncertain environments. Highly hierarchical structures, on the other hand, are faster at making simple decisions, although they are more vulnerable to propagation errors and information overload.

The simulation also investigates the role of information flow in determining the effectiveness of decision-making, and the finding is that this is maximized when information flows in a redundant but targeted way, and when decisions are based on an appropriate balance between local processing and central aggregation.

Finally, another area of research explored concerns how organizations adapt to rapidly changing environments characterized by systemic uncertainty in order to improve their performance. The finding is that organizations manage these challenges when they demonstrate the ability to learn from simulated feedback, modifying the connections between nodes as information gaps emerge.

Marrin, S. (2016) in *Improving Intelligence Analysis: Bridging the Gap Between Scholarship and Practice* aims to enhance academic reflection as a resource for the analytical practice of intelligence professionals, while also finding tools to increase professionals' awareness of the true value of their own experiences and insights.

The author emphasizes that analysis is not an exact science, but rather a more complex form of knowledge generation, which operates by assembling circumstantial evidence, employing a specific interpretive art, and thus arriving at structured predictions. In this environment, no method can guarantee guaranteed accuracy, but it is still possible to define what constitutes good analysis, for example, when methodological transparency, explicit argumentative logic, and the ability to expose the balance between uncertainties and hypotheses are present.

The work proposes a hybrid approach to overcome the difficulties inherent in an unambiguous definition of analytical methodologies. The author views uncertainty as a given, upon which subjectivity is embedded, as a structural element, and probabilistic evaluation as a tool, but only explanatory and not predictive.

The author, analyzing some famous intelligence failures such as Pearl Harbor, 9/11, and the weapons of mass destruction in Iraq, concludes that these are not simply individual errors, but genuine systemic failures. The causes are identified in an organizational culture that is inadequate from multiple perspectives. First, institutional incentives are poorly designed, and second, the control system relies on ex post models, hoping to prevent further failures. However, this methodology does not work, as the models are fundamentally flawed by retrospective biases, and it is therefore necessary to develop methodologies that assess the appropriateness of procedures ex ante. To achieve the effective application of analytical science to intelligence, the path identified by the author therefore requires the creation of such an evaluation system, accompanied, however, by a targeted training of personnel in academic models of decision theory, cognitive psychology, and epistemic logic. The author also recommends creating evaluation systems that focus on transparency of the underlying logic and methodological consistency, rather than focusing solely on the accuracy of predictions versus results. Finally, the suggestions also include promoting constructive dissent within the organizational culture and structuring analytical teams that foster cognitive diversity, as well as strengthening dialogue with academia, including through joint projects, exchanges, and fellowships.

Phythian, M. (2021) in *Intelligence in an Insecure World* is a work that analyzes many elements of intelligence, including the difficulties of evaluating performance due to the constant tension that intelligence experiences, especially in advanced democracies, between operational confidentiality and the need for structural transparency. The author reaches several conclusions. First, he argues that centralized structures, such as the post-1947 CIA, suffer from serious problems of operational slowness. On the other hand, decentralized networks, more commonly used in informal and emergency intelligence structures, foster agility but risk failure due to inconsistency and internal conflicts. Each structure, ultimately, has specific strengths and weaknesses and must be chosen based on the environment in which it operates.

The author also highlights that agencies are systems strongly influenced by their political and regulatory ecosystems, which can have negative effects, but this influence is crucial because it is the lever that opens the door to reform.

Phythian also analyzes the pathological phase of intelligence that culminates in predictive failure, starting with the case of the inability to correctly interpret the presence of weapons of mass destruction in Iraq. According to the author, this failure is not the result of simple analytical errors, but rather the consequence of a cognitively closed organizational culture, subject to undue political pressure. He therefore suggests that intelligence agencies, if they want to adapt to an environment where information is abundant, open, conflictual, redundant, and rapid, must invest in reforms in their organizational models, their staff's mentality, and their external interactions with civil society.

The report of Born, H., Leigh, I., & Wills, A. (2015), *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, focuses on democratic control over intelligence agencies, with a particular focus on analyzing the legal, institutional, and organizational principles of effective and accountable governance.

The volume also provides a comparative analysis of the best institutional control practices, both internal and external, adopted in the United States, the United Kingdom, the Netherlands, Canada, and Germany. Through a comparative methodology that makes extensive use of legal instruments, the authors finally develop a multilevel accountability model, grounded in legality, transparency, and the plurality of institutional bodies involved.

The authors argue that oversight of intelligence agencies must be based on a clear and public legal basis, have defined mandate limits, and provide for the protection of fundamental rights of third parties, such as privacy and freedom of expression.

To be effective, oversight must be synergistic and involve a multitude of actors, including Parliament, commissions, the judiciary, independent authorities, and even civil society and the media. Only in this way, since no single actor can control the system alone, can a dynamic balance be achieved between the hidden and transparent components of power.

All of this is accompanied by self-monitoring mechanisms and internal auditing, which require the drafting of codes of ethics, the establishment of internal legal departments and risk management systems, as well as ongoing staff training on the principles of legality and citizens' rights.

Internal organizational culture is considered the key to change, as regulatory formalism alone is deemed incapable of regulating the system and preventing deviations. However, it is precisely this internal culture that hinders organizational reform. Agencies tend to develop a closed and self-centered mindset, with little tolerance for errors and criticism, and this leads to resistance to any form of external oversight, perceived as political interference or technical ignorance. Therefore, any legislative reform, to be effective, must be accompanied by a shift in professional mindset.

Challenges to Effectiveness in Intelligence due to the Need for Transparency and Accountability in Democracy of Bruneau, T. C. (2007), is another work that focuses on intelligence reform in the United States after the events of September 11th.

The topic is approached from the perspective that some elements of intelligence are constantly at odds with each other. Political oversight is essential to ensuring transparency in democratic intelligence, but also to defining the right strategic objectives. However, overly stringent or shortsighted oversight risks reducing the effectiveness of operational capacity, resulting in failure to achieve objectives and a potentially tragic outcome. Maintaining the necessary secrecy and operational autonomy risks undermining public trust and institutional legitimacy, even though intelligence agencies play a strategic role, yet must always be held legally, politically, and ethically accountable for their actions.

These tensions, according to the author, often lead to a lack of transparency in the activities of intelligence agencies, initially aimed at protecting their own effectiveness. However, as the events of September 11th demonstrated, a lack of coordination and internal transparency can itself be a cause of poor effectiveness.

Therefore, according to the author, achieving high effectiveness necessarily requires good organization, open information flows, proactive learning processes, and a widespread culture of accountability.

This last element appears crucial, as the author emphasizes how intelligence agencies often tend to evade public accountability and resist, or at least negotiate, political control. Intelligence oversight is generally viewed as challenging due to a series of objective difficulties, such as secrecy and institutional silos, information asymmetry between agencies and policymakers, and an internal culture that pushes for operational autonomy. This results in approximate and opaque performance measurement and oversight that is often merely formal and ritualistic. To overcome these challenges and risks, Bruneau proposes an intelligence model based on clear regulations defining mandates, limits, and obligations, in which political leadership is sufficiently informed to be able to interact critically with agencies. The model also calls for competent external oversight and the development of an internal culture that prioritizes accountability and professional ethics.

Boraz, S. C., & Bruneau, T. C. (2006) in “Reforming Intelligence: Democracy and Effectiveness” is another work that addresses the issue of intelligence and security reform in general. According to the authors, any reform of this sector must integrate the agencies' core capacity—the ability to provide information quickly and reliably—with democratic control through political oversight. This structural tension, they argue, has increased since 9/11 due to the agencies' growing operational and intrusive power, accompanied by growing opacity that hinders oversight, generally justified under the guise of national security concerns.

The authors argue that agencies must be formally and substantively subject to oversight, which requires clear laws governing their structure and functions, executive and parliamentary authorities, and oversight committees with powers to access information. Furthermore, intelligence production must be relevant and timely, avoiding duplication and fragmentation of information across agencies, facilitating the integration of collection and analysis, and learning from mistakes to adapt to emerging threats. Effectiveness should therefore not be understood solely as operational efficiency, but systematically as the ability to generate value for national security.

The authors emphasize that any intelligence reform, although essentially a politically driven process, always stems, at least in democratic countries, from pressure from civil society and the media, with the help of internal reformist fringes within the services. Therefore, reforms cannot remain relegated to the purely technocratic level, but must instead strive to counter internal cultural resistance and organizational inertia.

d) Organizational learning and error management

Dunbar, C., & Weber, T. (2014) in "Organizational Learning in US Intelligence Agencies: Pitfalls and Prospects" examine the limitations and possibilities for reform, from a structural and cognitive perspective, of the US intelligence system, drawing on the findings of organizational learning theory. In fact, given that intelligence agencies are increasingly called upon to operate in complex, dynamic, and highly uncertain environments, they are particularly suited to analyzing the tension between learning, institutional rigidity, organizational culture, and accountability. According to the authors, US agencies are willing to correct errors once identified, but are reluctant to change their organizational culture or engage in concrete reflection on their organizational values or the adequacy of their decision-making mechanisms. In short, they demonstrate a good capacity for technical learning, but a low propensity for structural and cultural reflexivity.

Using case study methodology, the authors identify systemic constraints on organizational learning in the US agency system, including excessive information compartmentalization, an internal culture that rewards silence and stifles dissent, disincentives to report errors, and the chronic lack of institutional feedback mechanisms or epistemic evaluation.

The study identifies several factors that hinder effective learning. First, excessive secrecy, which limits transparency and impedes any potential external critical evaluation. Second, the politicization of analysis, which inhibits internal cognitive dissent. But also the lack of accountability within agencies, too often protected by weak and inconsistent control mechanisms. And finally, an internal culture that unrealistically aspires to perfection, ultimately stigmatizing mistakes rather than using them as a learning tool. Constant staff turnover, fragmentation, and internal compartmentalization also hinder the formation of a stable and shared organizational memory.

The authors' improvement proposals concern various elements of the intelligence system. First, the creation of institutionalized feedback mechanisms that include stakeholders from outside the organization, preferably from academia. Furthermore, some interventions on internal culture are proposed, such as encouraging internal cognitive dissent through the creation of dedicated teams, implementing advancement systems that reward self-criticism and methodological evaluation, and promoting interagency collaboration, aiming for the structured sharing of experiences, at the expense of information jealousy.

"Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War" by Andregg, M. M. (2013) also analyzes concrete failures of US intelligence to extract lessons for reform. Andregg studies the two crises cited in the title with a comparative approach, paying particular attention to the ethical and cognitive dimensions of intelligence analysis.

The US intelligence community failed to predict either the fall of the Shah or Khomeini's seizure of power, despite the political instability in Iran having been evident for some time. The author identifies the cause in the systemic rigidity of the CIA at the time, described as highly hierarchical and operationally oriented, incapable of capturing the social and cultural dynamics that were not captured by established analytical models.

Regarding the intelligence community's inability to correctly assess the absence of weapons of mass destruction in Iraq, the author identifies the causes in the politicization of analyses, the misuse of sources without adequate validation or peer review, the overreliance on structured methodologies lacking solid empirical foundations, and, above all, the conformist organizational culture aimed at discouraging internal dissent. The result was an overestimation of risk, supported by an internal consensus resulting from institutional pressure rather than epistemic convergence.

The two contexts appear very different, but Andregg identifies some common elements. In both cases, the failure is not attributable to individual analysts, but to collective organizational mechanisms that prevented the correction of the systemic deviation. Indeed, in both cases, mechanisms were lacking to valorize alternative visions, dissenting opinions, or less likely scenarios, and any dissent failed to take place in a structured manner.

Furthermore, the organizations failed, in neither case, to adequately reflect on the validity of their own methods and sources, nor to recognize the difficulties of the political-institutional context in which they operated.

Ultimately, the responsibility lies with the internal culture of US intelligence agencies, particularly the CIA, bound to hierarchical logics according to which expectations of institutional loyalty had come to replace critical thinking and ended up simply confirming decision-making expectations.

From a comparative analysis of the two failures, the author extrapolates several recommendations, such as the creation of environments that foster and protect cognitive diversification and epistemic dissent, or the implementation of systems for validating sources. The author also recommends greater interaction with the academic and civil communities in general, and that reforms should not focus solely on the procedural level, but should also impact the cultural level, thus rebalancing the relationship between analysts and decision-makers. Finally, the author recommends the introduction of indicators of epistemic quality, and not just predictive accuracy.

Dombrowski, P., & Gentry, J. A. (2018) in "Evaluating Intelligence Performance: Balancing Metrics and Mission" tackles the challenging issue of measuring intelligence agency performance effectively and responsibly. Intelligence agencies operate in necessarily opaque environments, where every operational and structural aspect is subject to classification, secrecy, and compartmentalization. These environments are also characterized by high uncertainty and ambiguity, with little opportunity for clear feedback.

In this context, it's difficult to even begin designing an evaluation system, because it's unclear how and when an agency is performing well or poorly. And the application of traditional performance metrics, borrowed from other public and private sectors, can produce distorting effects, ending up measuring something that is easy to quantify but perhaps entirely useless.

According to the authors, in the field of intelligence, both output and outcome metrics have significant limitations.

Output metrics measure what the organization produces externally, such as the number of reports, the average response time to a crisis situation, and the number of interagency interactions. These are easy to evaluate, but they often don't correlate closely with the quality of the analytical product or the strategic impact it generates.

Result metrics, on the other hand, measure the impact of activities. These are much more relevant evaluations, but equally difficult not only to quantify but also to attribute, as their causal relationship can be complex and controversial. This also raises the problem of the "non-event," which doesn't occur and therefore can be perceived as a success, or even actually be one, but can also simply be the result of other causes.

Dombrowski and Gentry also analyze the systemic, often negative, effects that the adoption of metrics can produce. These include, first and foremost, the organization's adaptation to achieving standardized indicators rather than pursuing actual objectives. Second, metrics can be strategically manipulated by individuals or teams who deliberately deviate from real objectives simply to gain rewards and promotions, or to avoid sanctions. A further risk is that these effects are amplified by a culture of secrecy, which allows for excessive protection of information.

The paper therefore proposes a model that balances measurement needs with organizational flexibility, while adapting to the diverse functions performed by intelligence agencies, such as information gathering, analysis, special operations, and information dissemination, each of which has specific characteristics. This adaptation should also encompass the different levels at which intelligence operates. At the strategic level, for example, agencies should be evaluated based on their ability to anticipate and influence political decisions. At the operational level, hybrid quantitative and qualitative metrics could be used, geared towards real effectiveness. Finally, at the cultural level, decision makers and analysts should be trained to view evaluation as an integral part of their professionalism, rather than as a useless or bureaucratic intrusion.

"Keeping Intelligence Ethical: The Role of Accountability and Professional Norms" by Hulnick, A.S. (2020) It is part of the growing interest in intelligence ethics, previously neglected in favor of reflections on efficiency, security, or legality. Hulnick proposes an approach that examines professional ethics beyond mere compliance with rules and codes, delving into the impact of internal organizational socialization processes and the effects of leadership and institutional accountability.

Intelligence agencies are forced to operate in a moral gray area, where legal norms are often deliberately vague or ambiguous, and it's easy for those working in this sector to believe that the importance of their objectives can justify exceptional methods. The lack of direct and rigorous public oversight also contributes to the factors outlined above, with the result that agency actions can undermine citizens' individual freedom, with consequent damaging effects on the overall credibility of democracy.

In such a complex and delicate context, ethics cannot therefore be delegated exclusively to external laws, and it is essential to develop internal professional standards and dedicated functional accountability mechanisms.

Professional norms, according to the author, are the foundation of the ethical sustainability of intelligence agencies and must cover all stages, from initial and ongoing training to mentoring and moral leadership of supervisors. The author also suggests creating spaces for controlled discussion, even informal ones, where operators can vent the tension between operational pressure and adherence to ethical principles. However, all of this is strengthened by external control which must be present in any case.

"Learning from Failure in the Intelligence Community: A Framework for the Future. International Journal of Intelligence and Counterintelligence" by Berman, E., & Fox, J. (2016) is another work that fits into the debate on reforms, increasingly central after September 11, 2001, and the war in Iraq.

Through a documented analysis of the most notorious cases of failure, the authors conclude that intelligence agencies not only make mistakes, but also tend to repeat similar errors. This is only partly due to the epistemic limitations of analytical activity, as the deeper causes are identified as cultural resistance to change, the lack of structured review systems, poorly calibrated organizational incentives, and opaque internal communication.

The authors propose their own operational model structured into successive phases. First, the failure to be analyzed is identified, followed by its detailed description, which leads to its classification into various possible categories. This is followed by the collection and analysis of evidence relating to the dynamics that led to the failure. To be effective, this phase should be implemented through permanent and dedicated structures, which should also involve individuals and entities independent of or external to the agency. At this point, responsibility can be assigned, both individually and collectively. This should, however, be reflective rather than purely punitive. This phase, in fact, is instrumental to the next, which involves the dissemination of lessons learned through systematic communication within the organization via manuals, simulations, and shared institutional narratives. Furthermore, to prevent lessons learned from being forgotten over time, due to the phenomenon known as organizational amnesia, concrete organizational actions must be implemented as a result of these lessons, such as reforms that impact both practices and architecture.

According to the authors, US intelligence agencies apply their own methodologies to correct their errors once they are discovered, but without questioning the underlying system, and only do so reactively. However, the intelligence environment is complex and characterized by uncertainty, the flow of information is heterogeneous, and the room for maneuver is not always rational. Therefore, institutional design must be adaptive and capable of promoting cognitive heterogeneity, enhancing organizational redundancy, and avoiding the trap of oversimplification. Another key factor, according to the authors, is the culture of infallibility and secrecy, which limits internal transparency and makes it difficult to both share failures and interpret them as learning opportunities. The authors therefore recommend analyzing failures at the institutional level, with dedicated structures protected from political influence, in order to obtain the necessary feedback. Furthermore, epistemic dissent should be protected by allowing and rewarding cognitive divergence and alternative analysis. Failures should therefore be incorporated into professional training and inserted into organizational memory, as reflective case studies, and not forgotten or hidden, as negative examples to be forgotten.

Svendsen, A. D. M. (2015) in "Contemporary Intelligence Innovation in Practice: Enhancing "Macro" to "Micro" Systems Thinking via "System of Systems" Dynamics" uses the "System of Systems" (SoS) model, directly inspired by the paradigms of complex adaptive systems theory, to study intelligence structures. According to the author, traditional agencies are based on linear and hierarchical logics, which are increasingly inadequate to address modern threats characterized by fluidity, globalization, agility, and multidimensionality.

To overcome this logic, the author proposes studying intelligence organizations through SoS, systems that possess some unique characteristics. First, the independence of subsystems, as each node has its own functional autonomy, while contributing to collective intelligence. Furthermore, these unique systems possess distributed functions, without a true center. This not only fosters a network of local information exchanges, but also allows for flexible local adaptation and integration, as subsystems can be added or removed without compromising the entire system. Furthermore, the system benefits from multiple viewpoints and cognitive divergences, so strategic responses emerge from the interaction between the parties, rather than from centralized command.

According to the author, implementing SoS logic in intelligence agencies' architectures would decentralize decision-making, resulting in greater tactical autonomy for local actors. It would also improve effective interagency and transnational collaboration, transforming it from a structural aspiration to an effective function. The author also proposes the creation of temporary units or cells, which would bring greater operational flexibility, and the implementation of laboratories, simulation scenarios, horizontal networks, and technological tools, including to provide decision support. The work explicitly references the complex adaptive systems (CAS) paradigm, within which Svendsen places modern intelligence structures. Within this framework, SoS, thanks to their properties of self-organization, nonlinearity, adaptation, and coevolution, seek to operationally introduce elements of complex thinking into institutional and organizational contexts.

Johnston, K., & Toft, M. (2021) in “Risk, Error, and Organizational Culture in British Intelligence”, studies the ways in which British intelligence agencies construct, interpret, and respond to the concepts of error and failure. The authors argue that within the intelligence community, the concept of risk fails to assume the characteristics of an objective variable, but continues to be assessed and managed by agencies within their own cultural frameworks. This strongly influences priorities, perceptions, and organizational responses. Both major British agencies, MI5 and MI6, despite operating in distinct contexts, share a common culture characterized by an aversion to failure, especially when it becomes visible and transforms into reputational risk. This leads to excessive analytical caution, while also underestimating certain conditions, such as information overload, compartmentalization, and lack of dissent, which actively foster error. According to the authors, British accountability mechanisms only address errors originating from technical tools or cognitive bias, neglecting the effect that organizational culture has on the occurrence of errors, for example, by inhibiting learning, feedback, and cognitive divergence.

The authors also highlight the existence of a double standard within British intelligence, whereby operational errors committed in the field are tolerated, as they are considered nearly impossible to eliminate, while analytical errors during the development phase are stigmatized. This double standard creates a distorted system, in which organizations and individuals tend to hide or suppress errors, rather than using them as opportunities for learning and improving the system.

The behavior of British agencies is interpreted, similarly to NASA in the period leading up to the Challenger disaster, as the result of continued tolerance for small deviations from the norm, until they become normalized, ultimately leading to systemic failures. Failure to manage errors, which are instead absorbed and rendered invisible, leads to their crystallization.

The article offers numerous practical recommendations. It suggests redefining evaluation metrics, moving beyond a view of performance based solely on results. It also suggests creating a culture that recognizes the useful aspects of error, moving beyond the logic of imposing personal sanctions on those who make mistakes. It also suggests developing cultural leadership, training managers capable of proactively interpreting and managing organizational dynamics. Finally, it suggests encouraging cognitive resilience by creating safe spaces for sharing mistakes and exploring alternative hypotheses.

Zegart, A. (2023) in *Spies, Lies, and Algorithms: The History and Future of American Intelligence* offers, first and foremost, a historical reconstruction of US intelligence; but it also contains some interesting insights.

Intelligence and its methods, according to the author, are often confused in part with diplomacy or foreign policy, while the remainder remains shrouded in myths, opaqueness, and stereotypes. In fact, it is a highly technical, organized field, subject to very specific institutional constraints. But in this context, what has historically weakened American intelligence, according to the author, are structural shortcomings, not a lack of technical capabilities. Zegart highlights in particular how the architecture of democratic control is no longer adequate in the face of technological innovations, such as artificial intelligence or quantum computing, whose operational implications are difficult for congressional committees to grasp. This leads to the risk of a growing asymmetry of understanding between agencies and oversight authorities.

Furthermore, according to the author, intelligence agencies are bureaucratic structures with poor adaptability, often dominated by procedural inertia, internal and inter-agency competition, and their operations are hampered by the fact that, while missions require agility, creativity, and rapid decision-making, the structure instead responds to rigid logics of control, compartmentalization, and hierarchy. Zegart therefore proposes an ecosystemic vision of intelligence, in which public agencies, private actors, academia, investigative journalists, and data scientists participate together in the production and interpretation of knowledge useful to national security. This, however, would require agencies to adopt new, networked governance models and promote horizontal public-private cooperation.

Zegart also explores the problem of organizational culture in intelligence and highlights how many US agencies, particularly the CIA, exhibit cognitive and institutional resistance to change, partly due to a culture of secrecy and partly to a closed and elitist recruitment model, oriented toward conformity and discretion. The author suggests instead that contemporary risks, including cybersecurity, systemic disinformation, and global surveillance, can only be addressed by agencies that are more transparent internally, more inclusive of talent, and more collaborative externally.

Conclusions on Literature Review

An analysis of the existing literature on the functioning of intelligence agencies, in light of organizational and public governance theories, suggests that the overall framework is currently characterized by increasing complexity, manifested in various attempts at innovation, often oriented toward structural hybridization. Intelligence agencies, historically framed as vertical, hierarchical, and compartmentalized bureaucratic entities, are facing the challenge of an external environment characterized by turbulence, hypercomplexity, hyperconnectivity, and pressure for transparency, which has inevitably spilled over into their internal environment.

The analysis revealed several recurring themes.

First, organizational structure is a factor that significantly influences the performance of intelligence agencies. Works such as Spying Blind (Zegart, 2007) and The Architecture of Smart Intelligence (O'Connell, 2006) clearly demonstrate how the strategic failures of American intelligence before 9/11 were not due to information deficiencies, but to organizational rigidity, interagency hostility, and, above all, institutional cultures impervious to change.

Furthermore, it emerged that evolving threats significantly influence changes in organizational form. Works such as The Shadow War (Miller, 2019) and Active Measures (Rid, 2020) highlight that contemporary hostile actors represent a highly heterogeneous group, composed of revisionist states, transnational groups straddling the divide between crime and terrorism, and the cyber world. These actors are able to operate through non-hierarchical, adaptive, and fluid models, capable of evolving almost in real time. Consequently, agencies wishing to counter such threats must themselves abandon bureaucratic monoculture and explore more adaptive configurations.

The effectiveness of agencies' actions therefore depends on their ability to learn and innovate. The theme of organizational learning and adaptability (Dunbar & Weber, 2014; Berman & Fox, 2016) appears central to recent literature. Intelligence agencies are faced with challenges that go beyond mere information gathering and subsequent analysis, as they are increasingly called upon to interpret weak signals, anticipate scenarios, and co-evolve with the external environment.

Leadership also increasingly appears to be a collective and adaptive function. Authors such as Oleson & Cothron (2016) and Bason (2018) suggest that leadership in complex organizations can no longer be understood as centralized command, but must be reimagined to resemble a widespread capacity to orient, connect, motivate, and adapt the organization as a whole. This is especially true as systemic uncertainty and information fragmentation become the norm.

Contemporary intelligence is a multi-actor, multi-scale, and multi-epistemic function, pervaded by new concepts of co-creation of public value (Bason, 2018), openness to interinstitutional collaboration (Lefebvre, 2013), and integration with open sources and new technologies (Lowenthal, 2019; Goldman, 2015). This creates the need for new organizational models, more permeable and modular, capable of managing interdependence rather than repressing it.

Many authors (Zegart, 2007; Treverton & Gabbard, 2014; Van Puyvelde et al., 2017) also lament the inability of traditional intelligence structures to adapt to new strategic and cognitive challenges and to effectively counter the misalignment between the form of threats and the form of responses. There is therefore always a need for reflection that questions the approach to taken-for-granted concepts such as hierarchy, secrecy, vertical control, and specialized monoculture.

This review of the scientific and strategic literature on the relationship between organization and intelligence also highlights how, alongside growing academic attention to the internal workings of intelligence agencies, there remains a palpable lack of solid theoretical frameworks on the organizational issue.

Indeed, most contributions tend to focus on individual failures in intelligence forecasting, at most investigating the associated shortcomings in analytical models or communication between analytical actors. Only a few studies thoroughly analyze the effects of organizational culture and systemic cognitive biases on failures, or even propose models for organizational architecture reform. Ultimately, the organizational issue seems to remain marginalized, or at best addressed implicitly.

In this context, a theoretical strand that deserves further applied exploration is that of adhocracy, as outlined by Henry Mintzberg (1979, 2009), and taken up in a contemporary light by numerous studies on complex and adaptive organizations. The literature analyzed in this review does not explicitly address adhocracy as an analytical or prescriptive category in the intelligence sector, although some contributions implicitly evoke it:

In Spying Blind (Zegart, 2007) criticizes the lack of structural adaptation of the CIA and FBI to the new post-Cold War scenarios, underlining the bureaucratic rigidity and the lack of permanent or temporary cross - functional teams.

Bason (2018), while referring to public administration in general, promotes a leadership and innovation model that is highly compatible with adhocracy, focused on co-creation, planning and multi-actor collaboration.

O'Connell (2006) proposes a “smart architecture” for post-9 /11 intelligence that calls for modular, integrated, and flexible forms rather than vertical silos, with an emphasis on network accountability rather than static hierarchies.

Dunbar and Weber (2014) and Berman & Fox (2016) address the topic of organizational learning, arguing for the need for structures that allow for experiments, errors, and rapid corrections, that is, organizational forms that are not constrained by rigid procedures.

Svendsen (2015), speaking of “System of Systems”, suggests the urgency of an intelligence capable of integrating heterogeneous systems through network dynamics and non-bureaucratic coordination processes, close to the idea of adhocracy.

Other works, however, touch on the theme but remain within the classical framework:

Garicano & Posner (2005) and Hammond (2010) maintain a perspective closer to the economics of the organization, proposing solutions oriented towards the rationalization of coordination costs and the clarity of information flows;

Goldman (2015) and Lowenthal (2019) treat organization as a technical background, but do not investigate formal models in a theoretical or alternative way.

Overall, there is a lack of systematic reflection on the hypothesis that intelligence agencies can or should evolve towards adhocratic models, even in an environment in which the need for adaptation, interdisciplinary collaboration and rapid decision-making is increasingly pressing.

In light of these considerations, the continuation of the doctoral research will focus on the exploration of some intelligence agencies characterized by peculiar elements, in order to verify whether they are structured according to an adhocratic organizational model.

The research path undertaken in this work will therefore seek to fill a theoretical and operational gap identified in the current literature, particularly regarding the adhocratic approach to intelligence, by integrating advanced organizational approaches with the analysis of real intelligence systems through case studies. The contribution of the conclusions reached in this thesis could then materialize, beyond the level of academic development, also as a tool for reflection to guide the democratic debate on the organization of intelligence and the evaluation of institutional reforms in the sector.

4.3 Methodology

The literature review identified a possible research pattern, linked to the type of organization used by intelligence agencies, which seemed to converge on Mintzberg's adhocratic typology. The need now arises to test this prediction.

All the limitations related to secrecy have profoundly influenced the choice of methodology to be used for the study. First of all, the total secrecy of operations, which almost always covers even aggregate values, such as the numerical contingent of personnel or even the budget, did not allow the application of any quantitative method. Likewise, since it is unthinkable to participate or observe the operations of agencies, but also their daily functioning, methods of field observation or participatory observation must be excluded. Observational studies in general should be excluded.

Furthermore, since the subjects who work for intelligence agencies (of which it is often impossible even to know the identity), but also those who become aware of information related to the activities of these agencies, are bound to secrecy (often also by criminal law), it is not possible to use the methods connected to the collection of information directly from people, such as surveys or in-depth interviews.

Consequently, the methodology chosen was that of case studies. Before analyzing how the choice of cases was made, it should be reiterated that the method suffers from the lack of possibility of carrying out interviews and obtaining structured data to analyze. It should therefore be highlighted what the data sources were.

4.4 Sources of information

As stated above, there are many difficulties in reconstructing even the general organizational structure of the intelligence and security services, and these difficulties increase exponentially as we move towards the detailed functioning of these entities (Gill, 2018).

However, there are some sources that can be used.

The first is the state official documents relating to these services: the founding laws, the regulations, the organizational documents, the allocation of funds, the reports of the parliamentary commissions and so on. These are documents that are often covered by state secrecy, but which sometimes contain information useful for understanding the organizational structure. Clearly the more the nation is based on democratic functioning and transparency of actions, the more information will be available in this way. Instead, the more a nation is governed in an authoritarian and anti-democratic way, the easier it tends to hide aspects of public life.

And this brings us to a second source of information worth noting: journalism. The investigative activity of journalists, combined with their ability (which is often present in democratic countries) to safely make use of anonymous information sources, allows them to explore and delve into elements of information services that are not normally accessible (Teirila, 2016). At the same time, journalistic sources hide a risk of a different nature: in many nations, in fact, the secret services, in order to avoid possible unwanted discoveries, obstinately avoid appearing in court, even when this would reasonably lead to a victory. Therefore, staff of all levels, from simple agents to the top of the structure, do not file a complaint for slander or defamation, whatever is written about them in the press. This leads to a possible distortion and unreliability of the news disseminated by journalists. A further source of information are people who have left the services, who spread news through books, interviews, private communications, etc. These can be either individuals who complete their working cycle and retire, or defectors who expatriate to escape possible retaliation.

4.5. Gray literature

Having to deal with the problem of studying the organization of intelligence and security agencies, it is therefore necessary to obtain data and information which by their nature are confidential. To fulfill this task, since it is not possible to circumvent a secret that is often also protected by criminal law measures, it is necessary to draw on different sources.

The functioning of services is nowadays generally governed by laws, which are not secret, unlike lower-ranking regulatory provisions (decrees, regulations, circulars) which are. This is a first source: laws, but also parliamentary works for their approvals, comments and practical applications of these rules.

But the priority source on which to rely in the study of a hidden reality such as that of the intelligence and security services is the so-called gray literature, which collects reports, studies and analysis from both public and private bodies such as think tanks, research institutes private security, but also reports created by the services themselves for the dissemination of information outside them. This is material from which it is possible to obtain a considerable amount of information which is neither in fact confidential (as it would not otherwise be disseminated) nor public in the broadest sense, as its dissemination occurs in a controlled and not unconditional manner.

Furthermore, since covert organizations are open to abuse and deviations from the intentions of the top bodies, facts which have never been lacking in the history of intelligence (Andrew, 2018), the agencies are always subjected to some form of control.

The control bodies can be of a governmental, ministerial or inter-ministerial nature; or of a parliamentary type, in the form of committees or commissions; and sometimes they are even entrusted to external and independent bodies. In order to operate, these control bodies must have the possibility of accessing a large amount of secret information, and therefore the work of these bodies also falls under the cover of state secrecy.

Nonetheless, a significant part of the results obtained must be disclosed, for the purposes of more general democratic control, sometimes by the entire parliamentary chambers, sometimes by the public actors of a sector, and sometimes even by the entire citizenry.

There is therefore a quantity of documents that are not entirely public, but not even covered by secrecy, such as: commission reports, technical analyses, committee meeting minutes, independent government or parliamentary investigations, sentences and ordinances, technical paper suggestions and annual operating reports, which constitute the so-called *gray* *literature*, present and widespread in many fields of knowledge, but which in the case of intelligence and security agencies takes on a very high value, due to the scarcity of other qualified sources of data and information (Serscikov, 2024).

Grey literature in academic studies

The term “grey literature” refers to a special category of information resources characterized by their exclusion from traditional editorial and distribution circuits, and often also from network indexing (Schöpfel, 2010). Nevertheless, it is of crucial importance for the completeness and depth of academic and professional research, especially in disciplines such as strategic, security, and intelligence studies. This category includes government documents, technical reports, working papers, theses, corporate documents, conference proceedings, and materials produced by non-governmental institutions (Lawrence, 2012). A peculiar aspect of this literature is its relative difficulty of access, mainly due to the limited distribution, the lack of bibliographic standardization, and the non-commercial nature of the sources (Schöpfel, 2010).

In academic study, grey literature is valued for its ability to cover information about zone of interest that formal publications may not cover (Gokhale, 2018). However, the lack of peer review and formal academic validation leads to an important problem: the difficulty to estimate the quality and reliability of the information contained inside grey literature (Banks, 2014).

Grey literature and intelligence

In the context of intelligence agencies, grey literature assumes a particularly relevant connotation, because it represents a primary source of useful information. Grey literature used in the intelligence field can be classified according to three main categories:

1. government reports and official documents, which include publications produced by government agencies or intelligence agencies themselves, often with confidential or classified distribution. Typical examples are “white papers”, operational manuals, annual agency reports, and strategic documents (Lowenthal, 2019);
2. analyses of think tanks and private research centers, which include materials produced by specialized research institutions that offer assessments on national security, forecasts on future scenarios, geopolitical analyses, and strategic insights (Johnson, 2018);

3. informal and unstructured sources which include working documents, confidential correspondence, internal memos, internal training materials, and documents produced ad hoc for specific needs (Gill, Phythian, 2018).

These types of documents contribute to form a wide vision of the information scenario, and play a fundamental role both in the study of intelligence agencies. Paradoxically, this type of documentation also represents an aid for the intelligence agencies themselves, which can obtain updated data useful to respond effectively to emerging crises or sudden changes in the international scenario (Johnson, 2018). While at the same time, the confidentiality and limited distribution of grey literature offer clear strategic advantages, making it an ideal resource for sensitive information management, source protection and the protection of national interests (Gill, Phythian, 2018).

Therefore, although grey literature presents significant challenges in terms of availability, qualitative assessment and standardization, it remains an essential component in building a comprehensive, timely and effective information framework, and many of the conclusions we will reach will be based on it. The ability to make the most of these sources depends on the rigorous methodology of selection, critical analysis and integration into intelligence and strategic research activities, which brings us to the need to address this topic.

4.5.1 Classifying grey literature: a methodological proposal to assess its reliability in the study of intelligence and security agencies

Therefore, in order to assess the credibility of this essential but ambivalent source, we will propose a classification method of grey literature that takes into account both the type of document or institutional origin and also the reliability of the information contained. The system is inspired by the criteria used by investigative and intelligence agencies to evaluate the information they collect.

Grey literature includes a heterogeneous variety of materials: think tank reports, institutional white papers, conference proceedings, leaks, unclassified internal documents, unpublished presentations, academic articles in preprint format, or documentation released by whistleblowers. The absence of peer review or a standardized editorial process generates, in these cases, a qualitative assessment gap that involves uncertainty about quality, authenticity and reliability of the sources (Schöpfel, 2010).

The proposed classification aims to overcome this criticality by assigning a combined reliability and credibility rating to the different types of grey literature, thus going beyond the mere cataloguing of documents, and providing a useful metric to guide scholars in selecting and evaluating sources.

Source evaluation methodologies in intelligence agencies

Organizations such as the FBI, the CIA, military intelligence around the world, and Europol now employ structured source classification grids that distinguish between two dimensions: the credibility of the source and the reliability of the information.

The FBI, for example, uses a double-entry matrix 6x6 that evaluates sources from A (completely reliable) to E (unreliable) and F (Cannot be judged), and data from 1 (verified by independent sources) to 5 (improbable) and 6 (impossible to judge) (Federal Bureau of Investigation [FBI], 2012).

Europol adopts a similar classification but with a matrix 4x4, distinguishing between "source evaluation" and "information evaluation" (Europol, 2017). A1 represents an information whose accuracy is not in doubt, that comes from an authentic, reliable and competent source, while D4 is an information which is not known personally to the source, cannot be corroborated, and the reliability of the source itself cannot be assessed.

In the academic context, applying such a scheme would avoid information reductionism according to which a source is considered either entirely reliable or completely useless. On the contrary, the double evaluation would allow recognizing the usefulness of a grey source even if it is not completely verifiable, provided that the degree of reliability is clearly indicated.

Gray literature has long become, in many fields, of great assistance in academic research, managing to provide data, sometimes even structured, on phenomena that would otherwise be difficult to explore. There are therefore specific databases that allow you to search, for example, among clinical studies or among projects that have obtained public funds. In the field of intelligence, however, these databases do not prove useful and the research must proceed in a specific and autonomous manner each time, according to an informal sequence that requires preliminary knowledge of the structure to be analyzed, of the national reality in which it is inserted and in the possible flaws in the institutional maintenance of secrecy regarding the institution itself. A notable help in designing the research avenues of gray literature in the field of intelligence is given by the knowledge of individuals within the system, or who have been part of it, as well as the information collected in forums that follow the Chatman House rule. According to this rule: «When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed».

The collection of “guideline” information then allows us to subsequently direct the search for appropriate gray literature in this regard.

As regards specifically the gray literature analyzed for the case studies (to which we will return in the next paragraph), the sources were different.

For North Korea, due to the aggressiveness of the operations of the services, combined with considerable secrecy covering almost every element of the country's public organization, the sources were the decisions of the Council of Europe and the Security Council of United Nations, following activities carried out by North Korean service, as well as documents presented to the United States Congress, a nation that sees North Korea as a declared adversary.

For Israel, the reports, often based on Open Source Intelligence, arise from the close interconnection between the services of this country and the economic and financial world, especially the United States (Silicon Valley and the Boston district), and are therefore produced by the world of economic-financial journalism which is an active part of that system.

For France, by virtue of the considerable amount of scandals that have hit the intelligence agencies, and which have therefore led to the creation of numerous control bodies, and due to the widespread interest that economic intelligence has, it is possible to identify a large amount of reports to the National Assembly, to the various Ministries, as well as to parliamentary, governmental and independent control bodies.

A proposal for the classification of grey literature

Based on the models mentioned above, the following classification grid of grey literature for the study of intelligence and security agencies could be proposed, divided into two levels.

First of all, the classification of the source (credibility of provenance): this type of classification should separate different sources (government reports, anonymous sources, journalistic investigations, etc.) based on their presumed reliability. This method is not necessarily efficient, given that disinformation can strike at any level within the intelligence community. A parliamentary or government report might contain profound inaccuracies, inserted deliberately so that intelligence services from opposing countries will detect and believe them; just as a journalistic report might gather a credible and accurate confidential information. But if one has to proceed somehow, one will still attempt to classify sources according to a six-level framework, in accordance with one of the most common matrix approaches among analysts. A correct classification of sources would in fact require a case-by-case approach, referring to the individual document and not to its abstract typology, but this would require "field" activity that would be beyond the scope of an academic study.

Second, the classification of the information (verifiability of content): as regards the classification of information in relation to the verifiability of the content, the classification (always according to a 6-level matrix logic) is less problematic, and will serve to mitigate the problems connected with the (abstract) classification of sources.

Therefore, the following type of 6x6 classification is proposed:

i. Classification of the source (credibility of provenance)

A. Recognized institutional source: governments, public agencies, academic institutions.
B. Structured private source: think tanks, research centers, NGOs with public budgets and advisory boards.
C. Individual professional source: former officials, analysts with verifiable CVs, journalistic investigations structured by professionals with expertise in the intelligence sector.
D. Anonymous or indirect source: leaks, unconfirmed whistleblowers, personal blogs, defectionists, sensational or scandalous journalistic investigations.
E. Suspicious source: unknown actors, decontextualized content, unverified deep web, para-journalistic structures clearly attributable to disinformation.
F. Cannot be judged.

ii. Classification of the information (verifiability of content)

1. Verified information: confirmed by at least two independent sources.
2. Probably true information: consistent with other reliable information.
3. Plausible information: reasonably compatible with the context, but not confirmed.
4. Doubtful information: conflicting with reliable sources or too vague.
5. Unfounded information: denied or incompatible with available data.
6. Cannot be judged.

A document, for example an unpublished report written by a think tank with experience in geopolitical analysis, could be classified as B2 (structured private source, information probably true). A document released by an anonymous whistleblower with unverifiable content would be D4.

Credibility and reliability analysis methodologies based on matrices are almost entirely based on 6x6 or 4x4 matrices (UNODOC, 2011). In this case the choice fell on the 6x6 matrix, rather than the 4x4 one, both because the first type is more widespread in the intelligence world, and because it appears more complete, especially in relation to the vastness of types of sources available.

This classification could then be integrated into comparative source evaluation tables, also with “weighted sourcing” techniques (Chilton, Ilchman, 1983), to give an overall reliability score.

The study of intelligence and security agencies presents specific peculiarities: access to official documents is often limited for reasons of national security, while much of the available information comes from grey literature or indirect sources. In this scenario, the proposed classification would allow to:

1. contextualize documents based on the source of origin and the nature of the content;
2. integrate weak sources (e.g. leaks or testimonies) in a rigorous manner, indicating limits and potential;
3. make the research methodology transparent through critical notes that explain the assigned score;
4. facilitate the triangulation of information through the cross-referencing of documents with different ratings.

The approach would also integrate well with qualitative methodologies such as process tracing or grounded theory, which benefit from dynamic and reflexive classifications (George, Bennett, 2005).

Need for validation of the method

In the present work, the classification is proposed and applied, but preliminary systematic validation work would be desirable, which could be conducted only on specific material already verified in other ways.

The methodology used would include a blind (or double-blind) approach, in which one researcher or group of researchers would individually enter the information obtained from the gray literature into the previously prepared matrix, while another researcher (or group of researchers) would subsequently verify the credibility and reliability of the information and the source. Subsequently, an appropriate quantitative and qualitative statistical method could be used to adjust the classification parameters and validate it for application to “contemporary” gray literature, i.e., information that has not yet been verified.

The validation of this methodology, given its importance and the scope of the project, could represent a possible continuation of the thesis work.

In this work, we will apply the proposed classification, drawing conclusions where possible.

4.6 Think Tanks and the Study of Intelligence

The study of intelligence, as already mentioned, presents insurmountable problems linked to secrecy, and the grey literature represents one of the priority sources of information. In turn, grey literature finds one of its main sources in think tanks and therefore it is necessary to shift the focus to these structures.

Think tanks are independent or semi-independent research institutions that produce analyses and recommendations on public policy issues. These study structures are generally key players in the international security landscape, acting as intermediaries between the academic world, government institutions and public opinion, and this makes the study of their involvement in intelligence of particular interest.

A first aspect to explore is the issue of think tank independence and funding itself poses a crucial issue because these organizations must maintain analytical autonomy, but this can conflict with political or institutional pressures (Stone, 2007). If they are reliant on government funding, the independence of think tanks can be compromised, leading to potential conflicts of interest and a reduction in the credibility of their analyses (Abelson, 2009). This effect also occurs in the opposite direction; these entities also influence the public debate on intelligence through the publication of reports, the organization of conferences, and media participation, and also help shape public opinion and guide political decisions on national security matters (McGann, 2020).

In the intelligence context, think tanks are active in various fields, such as analyzing security policies, intelligence agency operations, and emerging threats. One of the main obstacles for think tanks in studying intelligence is (still) limited access to information, due to the secretive nature of agencies' operations, and this limitation can impact the completeness and accuracy of the analyses produced by these organizations (Treverton & Gabbard, 2014). However, the relationship between think tanks and intelligence agencies is more complex than, for example, that established by academia, and is often characterized by a mutual tension that alternates between cooperation and independence. Some think tanks even collaborate closely with government agencies, while many maintain a critical and independent stance, dedicating themselves to oversight of security policies (Stone, 2007).

Think tanks adopt a variety of methodological approaches to the study of intelligence, including empirical research, case studies, documentary analysis, expert interviews, and comparative analysis, for example, to assess the effectiveness of intelligence agencies and propose reforms (Treverton & Gabbard, 2014).

The main thematic areas addressed by think tanks in the study of intelligence are varied. They analyze agencies' organizational structures to develop proposals for institutional reform, improving their efficiency and accountability. They examine secrecy practices and promote greater transparency to increase democratic oversight. They also evaluate agencies' operational capabilities in gathering and analyzing information to improve their efficiency.

In a democracy, think tanks therefore help bridge the gap between the secrecy of intelligence agencies and the need for transparency and public accountability (Abelson, 2009). However, the global landscape requires a differentiated analysis, so as to highlight some substantial differences between the way these analytical structures operate in different areas of the world.

In the United States, several think tanks play a prominent role in the study of intelligence, like the *RAND Corporation*, founded in 1948, which it's known for its strategic analysis and for its collaboration with the government on national security issues. The *Center for Strategic and International Studies* (CSIS) focuses on international security issues and has produced numerous studies on the effectiveness of intelligence agencies. The *Brookings Institution* offers in-depth analyses of security policies and the organization of intelligence agencies. But the American landscape is extremely broad and varied.

In Europe, three notable think tanks are the British *Royal United Services Institute* (RUSI), founded in 1831, which has recently expanded its interests to the cyber and AI worlds as well, the *Stiftung Wissenschaft und Politik* (SWP), based in Germany, which provides analysis on European security policies and intelligence, and the italian *Istituto Affari Internazionali* (IAI) deals with strategic and security studies, including those related to intelligence.

In other "Western" contexts, it is worth mentioning the *Australian Strategic Policy Institute* (ASPI) and the *Canadian Global Affairs Institute* (CGAI). While in Israel, the *Institute for National Security Studies* (INSS) and the *Begin-Sadat Center for Strategic Studies* enjoy a certain degree of academic autonomy, while maintaining ties with the military establishment. In particular, the INSS has published numerous analyses on the activities of the Mossad and intelligence in the context of hybrid warfare.

But if the scientific literature on think tanks is mainly focused on the Anglo-Saxon and European world, in recent years there has been a growing attention towards the role of analytical institutions in authoritarian or semi-authoritarian contexts. In these environments, the study of intelligence by civilian or para-state actors responds to logics profoundly different from liberal democratic models, posing new theoretical and practical challenges (Zhang, 2019; Dorsey, 2021). In non-democratic or hybrid political systems, access to information on intelligence agencies is even more limited and difficult than in European countries. Think tanks often operate in environments dominated by strong state control, with little opportunity to carry out independent and critical analysis, and also the production of knowledge is frequently subordinated to objectives of legitimization of power and to the needs of strategic propaganda (Shambaugh, 2002). In such contexts, think tanks often perform functions closer to those of government study centers than to those of traditional Western policy institutes. They are used also as internal and external "soft power" tools, to develop strategic doctrines compatible with the regime's priorities and to interface with the international academic world on a selective basis (Weiss, 2014).

In the Gulf countries, think tanks such as the *Emirates Policy Center* (EPC) and the *Gulf Research Center* (GRC) address issues of regional security, transnational threats and counterterrorism. These centers often function as instruments of public diplomacy and legitimization of the internal security order, rather than as independent observers, and their room for maneuver is limited by political contexts dominated by authoritarian monarchies, which define the "red lines" of the debate (Ulrichsen, 2014).

In Iran, intelligence is closely linked to the Pasdaran (IRGC) and religious-military apparatuses and the role of these institutions is predominantly internal, aimed at strengthening the resilience of the system and orienting security diplomacy. Think tanks such as the *Center for Strategic Research* (CSR) or the *Center for Strategic Studies* (CSS) produce analyses consistent with the ideology of the Islamic Republic, integrating geopolitical and theological visions (Khalaji, 2015).

In the African continent, the analytical infrastructure on intelligence issues is still in its infancy. However, institutions such as the *Institute for Security Studies* (ISS) in South Africa, or the *HORN International Institute for Strategic Studies* in Nairobi, Kenya, are starting to develop research capabilities on threats such as terrorism, espionage and cyber intelligence, in contexts of strong institutional fragmentation.

In India, access to information remains limited, but entities such as the *Institute for Defence Studies and Analyses* (IDSA) deal with intelligence issues in relation to regional conflicts and internal threats. In Pakistan, the *ISPR* and the *National Defence University* (NDU) publish analyses that reflect the strategic orientations of the military, with an emphasis on defensive intelligence and counterterrorism (Fair, 2014).

The study of intelligence agencies in China is severely limited by secrecy and ideological control. Chinese think tanks have roots dating back to the 1950's, with the founding of institutions such as the *Chinese Academy of Social Sciences* (CASS). However, it was not until the 1990's and 2000's that we see a significant proliferation of these institutions, often linked to ministries, universities and government agencies (Casarini, 2012). In 2015, the Chinese government announced its intention to build "think tanks with Chinese characteristics" (Zhang, 2019) emphasizing the importance of institutions that combine academic research with the Chinese Communist Party's ideological orientation (Xinhua, 2015). This policy has led to the creation of new think tanks and the strengthening of existing ones, with the aim of supporting China's governance and international influence in several ways. For example, promoting China's soft power globally (Li, 2009; Shambaugh, 2002) or promoting China's image abroad and strengthening bilateral and multilateral relations (Casarini, 2012). Their contribution is particularly relevant in long-term planning processes, in defining development strategies (Li, 2009), through publications, conferences, and international exchanges, and also serve as platforms for training officials and academics, facilitating the recruitment of talent into the country's political and administrative system (Li, 2009). Chinese think tanks are also seeking to increase their international presence and influence through collaborations with foreign institutions and participation in global research networks; however, mistrust and ideological differences are significant obstacles to deeper cooperation (Casarini, 2012).

Some think tanks are directly affiliated with ministries or government agencies and play an advisory role in the decision-making process. Examples include the *Development Research Center of the State Council* and the *China Institute of International Studies* (CIIS), affiliated with the Ministry of Foreign Affairs (Casarini, 2012). Other think tanks are affiliated with universities and research institutes, and combine academic research with public policy analysis. Peking University and Fudan University are home to some of the most influential think tanks in this field (Li, 2009). In recent years, think tanks with greater autonomy have also emerged, often funded by private companies or foundations. However, these institutes also operate within the constraints imposed by the political control of the Chinese Communist Party (Shambaugh, 2002).

CICIR (*China Institutes of Contemporary International Relations*) is one of the rare examples of semi-public think tanks that deal directly with intelligence-related issues, although their output is calibrated for external objectives rather than for internal debate (Brady, 2008). But in general, Chinese think tanks, including the CICIR, are closely linked to the Ministry of State Security (MSS) and often operates beyond the limits between academic analysis and strategic intelligence (Allen-Ebrahimian, 2018). China's concept of "total national security" (总体国家安全观) expands the field of intelligence to ideological and technological dimensions, and by virtue of this strategy think tanks help develop an integrated narrative that includes cybersecurity, information security, and the defense of the values of socialism with Chinese characteristics (Creemers, 2017). Ultimately, despite the growth and importance of think tanks, their autonomy is limited by the political and ideological control of the Chinese Communist Party. Freedom of research and expression remains a critical issue for the development of independent and innovative thought (Shambaugh, 2002).

This thesis has focused on the available documentation on the organization of intelligence agencies; a possible extension of the research would certainly be to deepen the opinions and results of the explorations carried out by think tanks in non-European and non-US regions.

4.7 Cases selection

As we have seen, this work aims to verify as far as possible whether the organizational structures of intelligence agencies adopt an adhocratic type structure. To do this, it was decided to choose the case-study method, integrated as much as possible with the available data, as it was not possible to proceed with direct methods.

Clarification on the methodology

The review of the scientific literature has provided a conceptual framework for research progress and has enabled the identification of the analytical categories commonly used in the study of intelligence agencies as organizations. This theoretical foundation will then allow for a comparison of systems.

But the road to actually reaching this comparison encounters many obstacles. Empirically, the field of intelligence presents unique access constraints. Classic social science tools such as in-depth interviews and participant observation are impractical in most contexts, as extreme legal confidentiality and operational secrecy surround both the structures, procedures, and techniques employed. This makes it unlikely, if not impossible, to obtain research authorization from the competent authorities. Even those with access to such data for institutional reasons would be unable to publish their analyses without violating confidentiality obligations, violations that often carry criminal penalties.

Given these limitations, the analysis of the three case studies will be conducted with the help of information available in grey literature, consisting of parliamentary and supervisory documents, reports from independent authorities, judicial documentation, published organizational guidelines and manuals, technical reports from public bodies, official documentation made available online, and analytical contributions from recognized research centers. This methodological choice does not contradict the distinction, reiterated in the review, between academic knowledge and non-peer-reviewed sources. The scientific literature is used to raise the question and provide an interpretative framework, while grey literature, on the other hand, will be treated not as literature in the theoretical sense, but as a source of data useful for reconstructing structures, processes, decisions, reforms, and operational practices that would otherwise remain shrouded in opaqueness. The data obtained will then be used to populate the theoretically derived categories with empirical content.

In summary, the methodological design proceeds sequentially: (1) the scientific literature, selected and discussed in the review, provides categories and hypotheses, which serve as a starting point for formulating the research question; (2) methodological difficulties related to confidentiality force us to exclude some procedures and cause the choice to converge on that of case studies; (3) the analysis of the case studies is carried out using grey literature as a source of data from which to draw specific evidence; (4) the encounter between the theoretical framework and documentary data allows us to test, refine or refute the initial hypotheses, making explicit their limits and conditions of validity.

For this reason, gray literature was not examined with a dedicated review, as was the case with scientific literature, as it was treated as a raw source of information. Therefore, rather than undergoing a review, it was subjected to a reliability assessment.

Having said this, the method that led to the choice of the three specific case studies must now be explained.

As we have seen, the various state intelligence services always follow different methodologies, as there is no shared (or shareable) heritage of know-how. In this constellation of agencies, some are necessarily generalist, as they must deal with every aspect of intelligence. This is the case of the agencies of the superpowers (established, emerging or decadent) which must project their power across the globe and in every area. Other agencies, on the other hand, are of a local or at most regional nature, as their state is only able to defend interests of this nature. In this vast panorama, three realities have been selected which have some of their own peculiarities, which we will see, and one common one: all three agencies analyzed have, in a diversified way, a notable contact with the outside world.

In particular, North Korean agencies develop external contacts due to their aggressiveness, which often leads them to attract the attention of European and US governments, but also of the media. Furthermore, the media are also the object of the attention of these agencies.

As regards Israel, however, the intelligence system (which is characterized as a true eco-system) interacts in a marked way with the world of academia, research, private companies, finance and start-ups, in a peculiar two-way manner.

Finally, the French economic intelligence system, by the very nature of its specificity, develops close contacts with corporate entities both at a national, supranational and territorial level.

These three different methods of contact with realities external to intelligence provide, in the study phase, a small possibility of exploration of the systems themselves, which is instead precluded for other agencies that operate constantly within the intelligence environment.

Other characteristics, purely organizational, then contribute to generating interest in these three realities.

In fact, the North Korean system, although it operates in an apparently monolithic political system (the Kim family and the Korean Workers' Party have in fact governed the country uninterruptedly since 1948) is instead characterized by notable changes in the organizational structure, and in particular in the functional dependencies of its different parts, which are often not only changeable, but also multiple. This characteristic, as we will see, is consistent with the possibility that it is an adhocratic structure, although the very considerable internal secrecy surrounding its functioning cannot exclude the possibility that these changes imply movements of a political or party nature.

The North Korean system is also characterized by a notable use of youth skills. In fact, students are all obliged to take in-depth afternoon courses on subjects in which they are interested. These also include new technologies and cyber skills which, due to the structuring of the country, which follows the military-first discipline, can only fall primarily within the state, military and intelligence sectors.

The Israeli system, as mentioned, is characterized as a true eco-system, in which young personnel are trained simultaneously by the university and the military world, through programs of excellence, which also involve the world of intelligence, the which effectively replace the university centers of excellence in the USA and Europe. The young people trained in this way then move to leading companies in the technology sector, even abroad, or found start-ups. The corporate world then continues to collaborate with the intelligence world, creating a peculiar and unique structure, which, due to its operational characteristics and those relating to the subjects who are part of it, is certainly adhocratic.

Finally, the French system has a multi-level network structure, made up of numerous layers: government agencies, ministries, inter-ministerial bodies, territorial branches, prefectures, the world of national and local businesses, the training system, the academia and research institutes. the entire system contributes to the management of economic intelligence information. This particular structure allows dealing with the complexity generated by a dual source: intelligence on the one hand and the economy on the other.

The French system is also characterized by a peculiar training system, although more standardized: higher education centers and normal schools, in which the different worlds of intelligence, public administration, business, academia, the military, coexist and exchange know-how. This system too can therefore be established as characterized by adhocratic elements.

I.

North Korean Intelligence and Security System complex organization

There can be no prepackaged solutions that fit every era
and apply to every country
Kim Il-sung

1. A brief overview of North Korean politics and intelligence

North Korean intelligence structure is complex, fluid, constantly changing, and above all difficult to explore due to the secrecy that cloaks the country. But some of its characteristics seem to be an added value for the intelligence activity of a small but very aggressive country on the international field. In the first section of this article, the cornerstones of the North Korean political system and the relative declinations in the field of intelligence will be analyzed. In the second section we will proceed to an overview of the North Korean intelligence agencies, in order to evaluate, in the third section, what inspirations can be gathered from this kind of organization.

North Korea, official name *Democratic People's Republic of Korea* (known internationally by the acronym DPRK), is characterized by considerable secrecy on many aspects of its military and security organization. One example is the network of underground tunnels, successfully used already in the Korean War (1950-53) and massively expanded over the following decades. Even minor information like the capacity of the AK-47's cylindrical magazines[1], a project neither the Russians nor the Chinese had been able to implement, is not publicly known. Estimates range from 50 to 150 rounds in 7.62x39 caliber.

[1] *Avtomat Kalašnikova 47*, usually known as AK-47, is a famous assault rifle developed in URSS after WWII and spread throughout the area of the former Warsaw Pact, as well as in China, Yugoslavia, and in many other countries especially in Africa and Asia. Its standard magazines are linear, slightly bended, and contain 30 ammunition.

The socio-economic and cultural structure of the DPRK is based on two fundamental assumptions[2] (*Socialist Constitution of the Democratic People's Republic of Korea*, 2017): **Juche,** that is the autonomy and autarchy of the country with respect to any external interference, including economic and cultural ones (Jong-il, 2015); and **Songun**, known also as Military First, which plans to allocate the (few) resources on a preliminary basis to the (large) military forces (Su-yong, 2016). U.S. Central Intelligence Agency estimates that 20%-30% of country GDP is allocated to military sector ("Korea, North," 2021), while in 2018 U.S. Congress estimated 24% (Chanlett-Avery et al., 2018). A third DPRK characteristic should be highlighted: the **monolithic** system of governance (Park, 2014). The power is concentrated in a unique figure, the Supreme Leader, who has gathered upon himself, over time, all the important offices of the country (as we will see in the next section). In 2019 the country's constitution was even revised for that purpose (Kim, 2020).

But North Korea's monolithic system is not immune to a series of perturbations that operate at various levels. The internal system is variegated and power is diffused variously among the political and military leaders. This forced the Supreme Leader into a series of actions which were interpreted as purges (Mahdavi & Ishiyama, 2020), although not all the news about the brutal and unjustified executions of political figures in view of the regime are well founded. In fact, many individuals, sometime after their alleged execution, reappeared in public (Kim, 2020). Purges, violent or not, are always a sign of difficulty because inner elites are generally a limit to dictatorial power (Mahdavi & Ishiyama, 2020).

Furthermore, it has been discovered, from the interviews with defectionists, that the authoritarianism of the DPRK is subjected to erosion from below (Haggard & Noland, 2010) through an increasingly rampant corruption, the spread of the black market, and the emergence of a parallel system of self-regulation of everyday issues. These aspects, in a system that instead aims at the invasive control of every aspect of citizens' life (Dukalskis & Joo, 2021) can represent in the long run a serious threat to the *status quo*.

Pressures of various kinds also come from abroad. The UN has issued sanctions, mainly for nuclear proliferation, but also for the distorted use of banking, financial and diplomatic tools (United Nations Security Council, 2013). The EU has also issued sanctions, both for the violation of human rights by security organizations (The Council of the EU, 2021), and for the use of European soil for money laundering maneuvers (The Council of the EU, 2016, 2017, 2018). The US has accused the DPRK of several crimes, including various types of counterfeits, as well as financial and money laundering crimes (Mallory, 2021), punished

[2] Article 3 of the Socialist Constitution of the Democratic Republic of Korea, adopted on 27 December 1972 and last amended on 29 June 2016.

several times through sanctions of the U.S. Treasury Department (Manyin et al., 2020). Other allegations, relating to drug trafficking, seem unfounded (Kang, 2013).

The intelligence system does not escape these premises and is therefore characterized by:

1. considerable resources;
2. conspicuous inquisitive and coercive powers within the country;
3. strong integration into the country's politics (Fitsanakis, 2015);
4. unscrupulousness in operations abroad;
5. predominance of ends over means.

The main sources of information on the functioning of this apparatus are the defectionists, present in large quantities in South Korea (officially known as the *Republic of Korea* - ROK) and in the USA, but scarcely accessible directly by the intelligence services and European academics (Blancke, 2009). Defectionists also, as is well known, tend to exaggerate the extent of their role in the country of origin in order to obtain more consistent benefits, which in ROK are still huge by law[3] today (Lankov, 2006). Therefore, defectionists often provide information learned from mere rumors, if not even invented.

2. North Korean intelligence agency organizations

The constitutional idea of powers equilibrium in DPRK predicts a balanced triad: the Supreme Leader, the chairman of parliament (Supreme People's Assembly - SPA), and the prime minister of the government (Premier of the Cabinet).

A first interesting circumstance is that, over time, the Cabinet and SPA have lost all forms of control over the intelligence structures. Even the **MSS** (Ministry of Social Security), once known as **MPS** (Ministry of People's Security), which is the closest thing to a national police force, was removed from the Cabinet office (a strange circumstance, for an interior ministry) and placed under the authority of the State Affairs Commission of North Korea (**SAC**), which has *de facto* replaced **NDC** (National Defence Commission) and whose president is the Supreme Leader. MSS, although operating as an internal security, police and prison camp management agency, is also concerned with the protection of relevant figures in the regime, and in this capacity, it acquires inside information in large quantities. It also controls two major football clubs (Amrokkang Sports Club and Rimyongsu Sports Club) which could be used as bridgeheads for overseas operations. The organization has been accused of serious

[3] Laws #1053 of 1962 and #3156 of 1978 included huge benefits for defectionists, known as "borogeum". The post Cold-War legislative changes (laws #4568 of 1993 and #5259 of 1997) have scaled back their scope, but for those providing useful intelligence insights, the rewards are still attractive.

and repeated violations of human rights, both in the repression of the internal opposition, in the management of the prison camps, and in the recovery of expatriate dissidents (The Council of the EU, 2021).

Most of the intelligence activity is under military control, and depends on the **SAC**, which manages two different sectors of the security system. The first is KPA (Korean People's Army), whose supreme commanding general is again the Supreme Leader. The **RGB** (Reconnaissance General Bureau, known also as **Unit 586**), established in 2009 inside KPA, is probably the main intelligence and clandestine operations agency. It is divided into six Bureaus, equipped with strong military capabilities, of which the Third is the foreign intelligence service (known also as **Office 35**, from which RGB would be born). The main area of influence of North Korean intelligence is Southeast Asia, although the huge resources allocated allow it to operate all over the world. Relations with Russia have cooled over time, and the main interlocutor, including for intelligence, is the People's Republic of China. Physical relationships and meetings (also with displacements in each other's countries) between the heads of intelligence of DPRK and ROK have always been kept, demonstrating that often, in a similar way to what happened during the Cold War, it is the intelligence agencies that keep open communication channels in critical moments (Matovski, 2020). Operative agents of the RGB have also been identified in Europe, where they apparently deal with complex financial maneuvers (The Council of the EU, 2018).

RGB also manages cyber operations. DPRK's interest in the internet dates back to the 1990s and cyber agents all have a solid university education (United States & Defense Intelligence Agency, 2021). Cyber education in DPRK currently begins in the fourth grade of elementary school (Pinkston, 2020). North Korea agents operate as APT (Advanced Persistence Threats), combining high technical skills with espionage methodologies. They usually operate abroad, while families at home receive benefits from their work (Chanlett-Avery et al., 2017). Western private agencies that monitor APT attacks are not interested in intelligence matters, and therefore provide invented names to the teams that are identified. North Korean APTs are difficult to distinguish, overlap each other, and are therefore usually grouped under the name "Lazarus Group". This APT is responsible for the spread of WannaCry in 2017, a malware aimed primarily at raising funds through cyber extortion. These funds are believed to have been used for research and development of weapons of mass destruction and missile technology in North Korea. In reality, the total amount raised worldwide appears to be just $ 140,000. But such cyber-attacks also have strategic value, for their ability to impress the enemy and provide evidence of cyber power projection capability

(Jasper, 2019) and, for some observers, the total amount of money raised through cyber operations amounts to 2.5 billion dollars (Pinkston, 2020).

Inside the RGB there seem to be sub-offices of various kinds.

Unit 695, an advanced security school, which organize training in safe houses.

Bureau 121, suspected of strategic cyber-attacks (Chanlett-Avery et al., 2017) including the spectacular blockade against Sony during the premiere of the movie *The Interview* in 2014 and various jamming operations against the ROK. It is suspected of operating outside the country, starting with China (Jun et al., 2015).

Unit 180, suspected of strategic cyber-attacks, such as that of 4 September 2019 against an Indian nuclear power plant ("Analysis | An Indian Nuclear Power Plant Suffered a Cyberattack. Here's What You Need to Know.," n.d.). In the past it would have carried out attacks mainly on ROK and Japan. It should have been converted to economic/financial cyber-attacks.

Bureau 91 suspected of strategic cyber-attacks.

The **Supreme Guard Command** (known also as Unit 963[4]) is a special unit which depend on KPA too. It deals with the safety of the Supreme Leader, his family, and the necessary related activities, including information gathering.

The second sector under SAC is the **SSD** (State Security Department), sometimes referred to as **MSS** (Ministry of State Security): it should be the main counterintelligence agency, with secret police functions, and reports directly to the Supreme Leader. The structure, created in 1973 on the model of the KGB, according to some defectionists is just an "empty shell". Its duties would include the investigation of political crimes at home, especially against the Kim dynasty, identifying and suppressing political dissent, the inflow of "subversive" information from abroad, the surveillance of foreigners, the protection of foreign embassy staff and high-level executions and killings.

Inside SSD, the **Group 109** would seem to control the spread of foreign media, while **Group 27** would deal with the interception of mobile communications (Pinkston, 2020). **Security Command** is another office that deals with the safety of the Supreme Leader (McEachern, 2010), but under the control of SSD and not KPA.

Other intelligence structures depend directly from the Worker's Party of Korea (**WPK**), whose general secretary is again the Supreme Leader. **Room 39** is suspected of dealing with the export of counterfeit material (pharmaceutical, banknote, etc.) and gold from the country's mines, international arms and drug trafficking, insurance scams and more in order

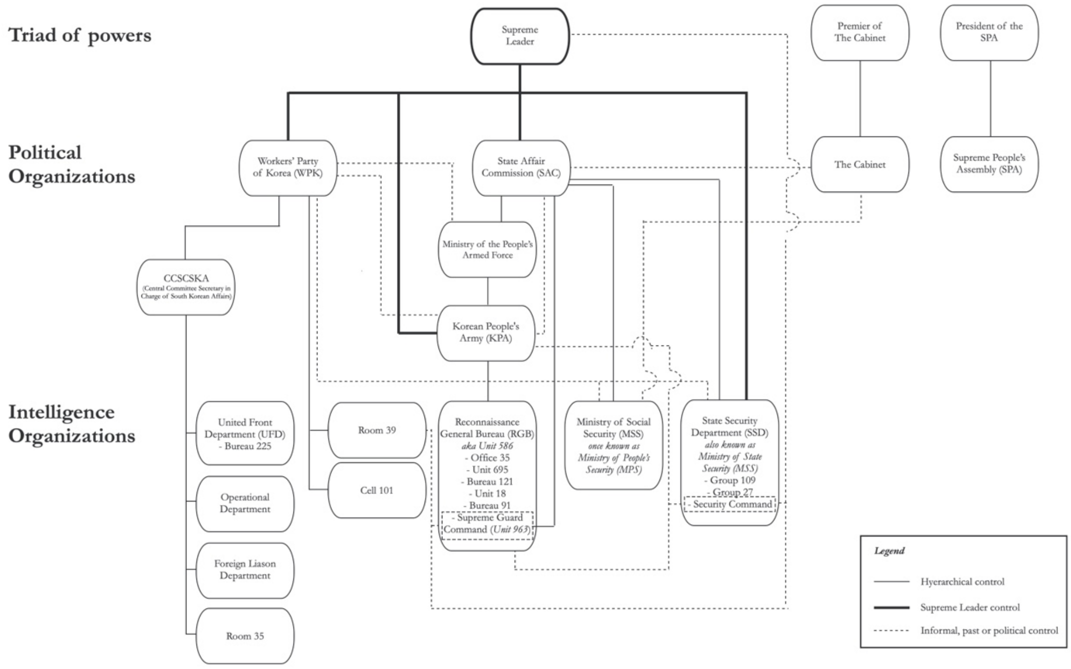
[4] 9 is a lucky number for Koreans, and 6+3=9.

to generate personal income for the Kim dynasty. It would also deal with economic/financial cyber-attacks for the same purpose. **Cell 101** is suspected, together with Unit 180, of the cyber-attacks of 4 September 2019 against a nuclear power plant in India ("Analysis | An Indian Nuclear Power Plant Suffered a Cyberattack. Here's What You Need to Know.," n.d.).

Also **CCSCSKA** (Central Committee Secretary in Charge of South Korean Affairs), which controls several intelligence units (McEachern, 2010), depends from WPK. Under CCSCKA the **UFD** (United Front Department) deals with the management of pro-DPRK groups in the ROK (Korean Asia Pacific Committee, Ethnic Reconciliation Council, etc.) pursuing the aim of reunification with various intelligence tools (Office of the Secretary of Defense, 2017). It should in fact be highlighted that the reunification of the country has been one of the cornerstones of the regime since the time of Kim Il-sung, established as an objective also expressed in the Constitution (*Socialist Constitution of the Democratic People's Republic of Korea*, 2017), and is currently advertised in the local media as being imminent. **Bureau 225**, inside UFD, deals with the training of agents to infiltrate the ROK, and from there to the rest of the world (Office of the Secretary of Defense, 2017). **OD** (Operational Department), **FLD** (Foreign Liaison Department) and **Room 35** also depends from CCSCKA. The last office especially is known to operate in sophisticated and aggressive ways, including the creation of puppet companies abroad (Blancke, 2009).

All the above addictions should be treated with caution. As we will see in the next section, the location and function of the various offices vary rapidly over time, and the dependencies are of various types, seldom clear and definitive. In addition, it should be specified that intelligence activities are not the prerogative of formal agencies only, but an intense network of sub-intelligence is operational at every level, as happens when the government of a nation allows it (Blancke, 2009).

For this reason, the construction of an organization chart, as is often done for intelligence organizations, could not allow to fully understand the functioning of the system, but it can anyway help in appreciating its considerable complexity.



Triad of powers
Supreme Leader
Premier of The Cabinet
President of the SPA
Political Organizations
Workers' Party of Korea (WPK)
State Affair Commission (SAC)
The Cabinet
Supreme People's Assembly (SPA)
Ministry of the People's Armed Force
CCSCSKA (Central Committee Secretary in Charge of South Korean Affairs)
Korean People's Army (KPA)
Intelligence Organizations
United Front Department (UFD) - Bureau 225
Operational Department
Foreign Liason Department
Room 35
Room 39
Cell 101
Reconnaissance General Bureau (RGB) aka Unit 586 - Office 35 - Unit 695 - Bureau 121 - Unit 18 - Bureau 91 - Supreme Guard Command (Unit 963)
Ministry of Social Security (MSS) once known as Ministry of People's Security (MPS)
State Security Department (SSD) also known as Ministry of State Security (MSS) - Group 109 - Group 27 - Security Command
Legend
Hyerarchical control
Supreme Leader control
Informal, past or political control

Figure 1: chart of intelligence and security agency system of North Korea

3. Problems in understanding and evaluating North Korean intelligence organization, analysis of sources

Starting from the firm point that the intelligence structure of the DPRK is not well known, and its evolution is continuous, one can think of extrapolating some considerations from its organization.

Evaluating intelligence is not only difficult but also “tricky” (Wheaton, 2009). The main challenges are:

1. the activity which is secret and usually unheralded (Gill, 2007);
2. the probabilistic nature of intelligence predictions (Wheaton, 2009);
3. the difficulties in evaluating what is a success and what is a failure, because the only important point of view is that of the decision-makers (Wheaton, 2009), whose grand strategy and consequent strategies are usually secret (in less democratic countries they are even implicit).

The difficulties in evaluating intelligence are encountered in all close environments as evaluating intelligence theories (Marrin, 2018) or political intelligence control committees (Gill, 2007). The only way forward therefore seems to be that of informal analysis, often on a historical basis, as in the strategic evaluation of Japanese covert ops during II World War II (Wey, 2018); or based on general models like the evaluation of counter terrorism in Asia

(Tan, 2018) through the qualitative distinction between approaches to contrast the phenomenon, and a rough comparison between the results achieved.

The last two examples, although they relate to environments other than intelligence, are interesting in that both avoid the statistical approach, as both in special operations and in terrorism the "moral factors"[5] and the political implications of the actions carried out (both offensive and defensive) are more important than just the numerical data. And this consideration also applies to intelligence.

Therefore, to analyze the North Korean intelligence services system, an examination of its main characteristics will be carried out, also with a view to considering it a complex system.

- as seen above, intelligence and security structures have a high degree of redundancy. But if in the common administrative sphere the duplication and overlapping of functions is only a waste, in this case redundancy can provide the system with greater robustness, suitable for the challenges that intelligence must face, full of unknowns and complexity;
- the organizational system is characterized by considerable fluidity. Organizations change over time, their hierarchical dependencies change, and many organisms respond transversally to different vertices. This can be interpreted in two ways: as a maneuver on the verge of paranoia, in order to prevent the creation of pockets of power; or as a strength that allows greater adaptability of the system to the changing and powerful challenges to be faced;
- the hybrid use of skills and resources, shifted as needed and reassigned as necessities change, is a concept far removed from the organizational slowness of Western bureaucratic apparatuses. But in North Korea it appears instead as a tool used in a more agile way. This too can be motivated by both of the opposing needs highlighted in the previous point;
- the prevalence of the attack over the defense is another characteristic that the Western world, due to a different attitude towards its public opinions, is struggling to use. But in this way we give up the strategic advantage that can be obtained whenever the attack (even in a non-material sense) is preferable to defense. The cyber sphere is probably one of these fields;
- the prevalence of the practical function over the theoretical one derives from what has already been said about the state of almost permanent military mobilization that

[5] In the Helmut von Molkte and Karl von Clausewitz meaning, with all the consequent difficulties in weighing and categorizing them.

characterizes the country. In this way, we pass from a system of rewards based on theoretical evaluation scales (as in the case of the so-called peace generals, promoted without ever having fought and whose effective capacity is therefore doubted in the event of a conflict), to systems of evaluation based on the results obtained in the field.

Finally, it would be difficult to evaluate the results of the North Korean system on the basis of the results achieved. In fact, on the domestic front, thanks to the violation of human rights, the activity of the security services is in a certain way "facilitated", and in any case remains difficult to analyze. On the external front, intelligence activities have often proved aggressive (as exemplified above, during the description of the various bureaus), especially on the cyber and financial level. At the same time, it is not possible to know how many resources have been used, to evaluate their efficiency, nor how many missions have failed or ran aground, to evaluate their effectiveness. Indeed we must remember that, just when press news regarding information gathering operations or counter-intelligence are not disseminated, it is not certain that such activities are not heavily underway.

What is the optimal structure for intelligence remains an open question and an unsolved problem (Hammond, 2010). The need to know collides with the need to share, but certainly, in modern democracies, an essential point is to perform a fundamental task: to allow democratic control over the secret work of the agencies, and to limit their political abuse. A solution often pursued is to multiply intelligence agencies and their apparatuses (mushrooming), to achieve a division of power and mutual control (Steinhart & Avramov, 2013). North Korea does not seem to escape this trend, which however on the other hand is no longer justified, once it has been ascertained that all the agencies basically respond to the Supreme Leader. But as known for a long time, duplication of intelligence functions is not always a bad thing (Kent, 2016).

The first step is understanding DPRK intelligence structures, and the main problems are (Blancke, 2009):

1. the large number of existing organizations, often connected in a non-transparent way;
2. the overlapping of the functions of the personnel employed in the sector, who often carry out multiple tasks in the civil and military spheres;
3. the lack of transparency in collaboration with Chinese agencies and structures "close" to intelligence;
4. the difficulty of Western services in understanding the specificity of the DPRK under a wide multitude of aspects.

The impression is also that some agencies are used for different functions than those for which they were created. This type of management is sometimes labeled a "deviation", but it also represents a form of creativity. In fact, it sometimes happens that certain agencies, even in the Western world, due to their peculiar history, find themselves dealing with activities for which they were not created. And if this attribution exploits their strengths and considers their path-dependent development, it can only be an added value in managing the complexity of the world. However, this dynamic does not only have potentially positive factors. The possibility that changes in employee work design can lead to antithetical effects has been investigated in the literature which studies job crafting (Bruning & Campion, 2018). Sometimes it produces beneficial effects, such as high job engagement or increase in job satisfaction and performance (Tims & Bakker, 2010). At other times it can lead to the rejection of work or even to burnout (Harju et al., 2021).

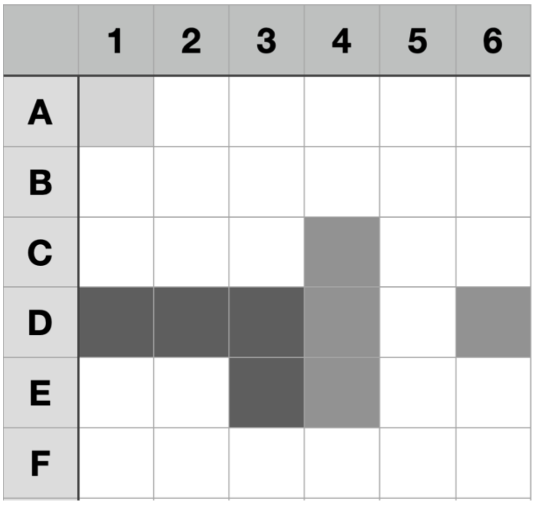
State intelligence agency, in comparison with more informal structures, find itself competing in an asymmetrical way. The former are exposed to strategic surprise, their internal structure often represents a limit, and inter and intra agency competition is not a push but a brake (Barnea, 2020). Non-state intelligence, instead, is more fluid, adaptable to the emergence of situations, and therefore more effective (Gill, 2018). A key to understanding North Korean intelligence could be this. Its hybrid soul would allow it to act in a more fluid and reactive way.

In the last seventy years a lot of effort has been spent on establishing and updating intelligence structures capable of predicting and thus preventing adverse events. The lessons of Pearl Harbor, the Yom Kippur War, 9/11 are just some of the episodes branded as "intelligence failures". But this way of seeing things could only be the result of a cognitive bias, of an unreachable and strategically inessential aspiration to defense (Matovski, 2020). Intelligence can provide invaluable help even in the offensive field and, if we read North Korean intelligence under this key, we can see its strengths, namely the ability to project abroad and act with aggressiveness, both physical and cyber, both economic and influential. An important interpretation comes from modern intelligence research, which highlights the characteristics of non-linearity and complexity (Menkveld, 2021). According to this vision, an analysis of the world that breaks up its essence, with the hope of being able to reassemble it in search of meaning, it can no longer be a viable alternative in the intelligence activity which, as complex system, depends on the path taken to get there and is rich in interdependent behaviors (Javorsek II & Schwitz, 2014). North Korea would be inclined to this type of approach thanks to its philosophical roots, its long history of isolationism and autarky, and the lack of models imposed from abroad. The Western mentality shuns uncertainty. It tries to eliminate it in every way, and in so doing it amplifies it. Only by living with uncertainty, embracing it and assessing it, can it be limited and, sometimes, avoided (Friedman & Zeckhauser, 2012).

If we now apply the previously developed theoretical framework on the reliability of sources and news, according to a 6x6 matrix borrowed from analysts, we can group the sources consulted into a series of categories.

A first group of sources consists of reports and official documents from institutions, primarily the European Union, regarding North Korean intelligence activities outside its borders, as confirmed by inquiries and investigations. These state-run sources are confirmed by similar sources and are therefore classified as A1. However, their quantity and extent are not numerous.

Alongside these are interviews collected by defectors, who sometimes produce narratives consistent with the context, sometimes conflicting, and sometimes unreliable due to a lack of appropriate information (D3, D4, and D6, respectively).



	1	2	3	4	5	6
A	░					
B						
C				▒		
D	▓	▓	▓	▒		▒
E			▓	▒		
F						

Figure 2: 6x6 Matrix for Evaluating North Korean Intelligence Sources

Public or private research institutions, or independent researchers, rarely have access to the ability to conduct direct investigations. It's much easier for penetration to occur primarily through journalistic investigations, leaks, unconfirmed whistleblowers, and personal blogs, which sometimes corroborate each other, but sometimes are merely consolidated or compatible with the context (D1 D2 D3).

Finally, it should be noted that North Korea, in addition to actively spreading disinformation against its main enemies (South Korea, Japan, and the United States), is also a victim of disinformation itself, as recent journalistic scoops demonstrate. Therefore, a small number of sources that are merely compatible with the context, if not actually conflicting, should be added, coming from anonymous or suspicious sources (and therefore D3 D4 E3 E4). Of all these forms of disinformation, that produced by suspicious (and therefore lower-ranking) sources, capable of constructing narratives compatible with the context, is the most appealing, effective, and widespread (E3).

4. The North Korean intelligence as an adhocratic system

In this brief analysis we have tried to highlight the peculiarities of the North Korean political system, to analyze how these peculiarities are reflected on the intelligence system and how that system is structured. The task was not easy, due to the great secrecy and constant changes which characterizes intelligence in general, North Korea in general, and North Korea intelligence in particular.

On the basis of what has been highlighted so far, we can now shift attention to some organizational aspects of the North Korean intelligence system.

The environment in which North Korean agencies operate is undoubtedly complex, dynamic, heterogeneous and constantly changing, as is the case for every intelligence agency. The particular aggressiveness of North Korean services and the habit of operating in very different foreign contexts compared to the country of origin intensify these characteristics.

From what is possible to know, the personnel of these agencies have considerable expertise in the fields of many sectors such as technology, cyber, or the European economic-financial system. It is therefore a system characterized by solid training. Furthermore, although it is not possible to know the age distribution of the staff who work there, the author has verified in North Korea by direct experience that young students from ten years of age onwards follow specialized courses that cover the entire post-school afternoon phase. The choice of address is made by the educational institutions based on the student's inclinations, and includes, among other things, advanced courses in science, technology and cyber. It can therefore be assumed that young, highly specialized elements operate within the North Korean intelligence structure, also by virtue of the fact that in this economic and social system there are no private actors such as large companies or start-ups capable of competing young talents to government bodies.

The operations conducted by the North Korean agencies, characterized (when in the public domain) by considerable challenges in hostile environments, do not appear compatible with a clear separation between the planning and design phases on the one hand, and operational implementation and execution on the other; and this requires selective decentralization, the real extent of which in this case cannot be explored. It seems that the two macrophases of planning and execution are the result of a mutual and constant dialogue, which leads them to modify each other. The operational structure of the Units and Bureaus, the consistency of which cannot be known, appears to be fragmented, to encourage the development and use of different skills.

Offices and units are easily moved from one organization to another, even belonging to very different branches of the state apparatus, and functional dependencies also often change. It is possible that monolithic power allows the creation, suppression, and movement of offices much more quickly and efficiently than in bureaucratic democracies. Furthermore, the dependencies of the various intelligence units appear unclear, overlapping, blurred. Alongside the classic hierarchical dependencies, dependencies "for political guidance" and "de facto controls" also seem to emerge, which increase the complexity of intelligence management (Bermudez, 2010). Whether and how much this turns into efficiency or disorder is difficult to say, given the secrecy that pervades the intelligence community in every country, most aspect of DPRK everyday life, and in an even more pronounced way the North Korean intelligence. This continuous change of structure, particularly linked to addictions, could be interpreted in the other hand, although there are no concrete elements in this regard, as a poor value regarding the distinction between line and staff. However, the rapid change in organizational charts is generally a symptom of adhocracy.

Since it is not known how the management component is separated from the operational core, it is not possible to establish whether it is more of an operational adhocracy or an administrative adhocracy.

The elements collected therefore describe this system as made up of trained and specialized personnel, of which an unknown fraction of young age, structured on flexible and purpose-oriented units, immersed in a complex, hostile, changing, dynamic and heterogeneous environment, whose relationships between organs they are subject to considerable changes so much so that it is difficult to differentiate between line and staff.

These elements would seem to suggest that the North Korean intelligence system is an adhocratic organization. But the conclusions reached cannot be considered definitive as the supporting elements are scant and collected in a completely indirect manner. The framework therefore, although it leans towards this conclusion, must remain open.

5. Conclusions on the North Korean system

An analysis of the North Korean intelligence system must inevitably confront the fact that it operates in conditions of isolation, extreme secrecy, and organizational fluidity. The Democratic People's Republic of Korea (DPRK), more commonly known as North Korea, has an extremely complex and elusive intelligence apparatus, dominated by a strong hierarchical structure, but which also appears to incorporate elements typical of network systems and adhocratic structures, characterized by a high capacity for adaptation to external and internal changes.

From an organizational perspective, the North Korean system exhibits marked redundancy, which, while often interpreted as a source of waste in Western bureaucratic systems, can actually benefit organizations operating in environments characterized by unpredictability and volatility, providing robustness and resilience. The duplication of roles and responsibilities, for example, reduces the risk of paralysis in the event of individual units being compromised or overloaded, through the rapid redistribution of available resources.

The DPRK has also developed a system in which intelligence structures continually adjust their hierarchies and operational dependencies. This fluidity can be interpreted both as a deliberate strategy to prevent the emergence of alternative centers of power to the Supreme Leader, and as a conscious organizational choice that helps increase the system's ability to react agilely to external stimuli.

North Korean intelligence also displays a clear preference for offensive over defensive actions. This orientation is evident both in the cyber sector, where the DPRK has demonstrated considerable unscrupulousness in its international actions, as demonstrated by attacks attributed to hacker groups linked to North Korean intelligence, and in the field of traditional clandestine operations, including in the financial and economic sectors, as highlighted by numerous EU reports on aggressive and unconventional activities conducted on European soil.

This North Korean organizational model is therefore placed between adhocracy and a form of governance Hyper-centralized, yet with elements of operational decentralization. Adopting a purely adhocratic model is problematic, especially given the absolute centrality of the supreme leader, who would appear to concentrate all strategic decisions on himself. However, at the operational and tactical levels, North Korean intelligence demonstrates considerable managerial autonomy, with specialized units that appear to operate with broad freedom of action, leveraging specific skills and flexibility of intervention. The combination of central control and peripheral operational autonomy gives the system a significant degree of efficiency, although this is difficult to assess in the absence of reliable and transparent data.

Indeed, information opacity and institutional secrecy constitute a significant obstacle to a complete and in-depth analysis of the system's performance. The lack of reliable information on all operations carried out, the success rate achieved, and the resources actually deployed makes assessing the system's effectiveness and efficiency nearly impossible. The only viable option for achieving a level of assessment is therefore to rely on indirect indicators, such as the system's ability to generate global influence or conduct highly complex operations with strong media impact. And the analysis of these factors suggests, to the extent possible, that North Korea's intelligence organizational model is able to manage the complexity of the international context relatively effectively.

From a co-evolutionary and proactive perspective, North Korea's organizational structure appears designed to react rapidly to external and internal changes, leveraging its inherent fluidity and redundancy. However, the coexistence of an authoritarian and hypercentralized approach generated by the centralization of power in the hands of the Supreme Leader, while ensuring strategic coherence and unity of decision-making, could represent a long-term structural limitation, as well as a potential source of risk in the event of internal political crises or the sudden disappearance of the dominant figure.

The findings of this chapter paint a picture of North Korean intelligence as a hybrid system: strategically hyper-centralized but tactically decentralized; redundant and fluid in its dependencies; with a marked offensive posture (especially cyber) and with performance metrics that are more operational than predictive. This profile interacts non-linearly with those emerging from the literature review.

1) Redundancy, fluidity, and hybridization of chains of command.

The chapter seems to suggest that the North Korean apparatus utilizes organizational redundancy and functional fluidity as a response to the complexity and secrecy of its environment. This is reminiscent of Best's analyses of the US system, according to which the meta-organization of the US intelligence community, with redundant lines of command and widespread fragmentation, has led to coordination difficulties (Best, 2011). However, North Korea could paradoxically compensate for this by hybridizing a fluid base with a single apex, in a system then capable of avoiding the intelligence bottlenecks typical of democracies.

2) Strategic centralization vs. organizational adaptation.

The chapter highlights the centralization of control with peripheral adaptation. This point was critically anticipated by Zegart, who interprets the United States' failures as the result of strong bureaucratic rigidity and, at the same time, weak incentives for adaptation and reform. Zegart argues that effectiveness requires flexible structures as well as governance that rewards innovation (Zegart, 2007). Apparently, North Korea "solves" rigidity with the antidemocratic instrument of absolute political command, but it does so without being able to guarantee transparency and independent performance measurement.

3) Offensive posture and (failure to) institutionalize doubt.

The chapter highlights the prevalence of the offensive (cyber, financial, and clandestine operations) as a parameter of success. This appears to contradict Heuer's conclusions, which emphasize how the quality of intelligence depends on a series of factors related to widespread freedom, such as the acceptance of constructive dissent, the institutionalization of doubt, the positive management of prejudices, the shared analysis of alternative hypotheses, and a leadership that prioritizes accuracy over speed (Heuer, 2010). However, when, as may be the case with North Korea, the ethos remains solely mission-oriented and political loyalty takes on a fundamental role, then the risk is that Heuer's mechanisms could be counteracted, resulting in an apparent increase in tactical effectiveness in the short term, but simultaneously resulting in a deterioration in accuracy in the medium term.

4) Speed/error choices and information bottlenecks.

The combination of operational decentralization and political centralization described in the chapter can lead to a misjudgment, sometimes implicit, of the trade-off between speed and error. Garicano and Posner had already studied this trade-off, highlighting how an inefficient distribution of information can generate systematic errors and coordination failures (Garicano and Posner, 2005). The same result can emerge from an incorrect design of incentive factors. The North Korean model appears to minimize decision-making times, but could generate (unmeasured) errors further down the chain.

II.

Israeli extended intelligence (eco)system as an adhocratic complex network

A discerning heart acquires knowledge, and the ear of the wise seeks knowledge
Proverbs 18:15

1. The structure of the Israeli intelligence system

The intelligence system of the state of Israel is composed first of all by national agencies, reporting to various internal top management, and with different functions (Kahana, 2002).

i) The *ha-Mosád le-Modiʿín u-le-Tafkidím Meyuḥadím* ("Institute for Intelligence and Special Operations", usually known simply as **Mossad**) is the structure in charge of collecting information for national security and its subsequent analysis. The Mossad also operates in the field of psychological warfare, propaganda and disinformation (*Lohama Psichologit*, LAP Department). Furthermore, observers agree in establishing that the Mossad also operates in the execution of "direct actions", i.e. operations that use force to obtain the result, often with the violation of the foreign state in which they take place. The Mossad could be divided into eight departments, but information about them is extremely limited, fragmented, and often the result of willful disinformation (Barucija, 2020).

ii) The *Sherut haBitaẖon haKlali* ("General Security Service", usually known by its acronym – **Shabak** – or simply by the name of **Shin Bet**) is an agency that operates in the field of internal security in relation to counter-espionage and counter-terrorism, as well as the protection of people and sites of government interest (Barucija, 2020). The intelligence activities carried out by this agency have as main objectives those defined above.

iii) The *Agaf HaModi'in* ("Intelligence Section", usually known by its abbreviation **Aman**) is the military intelligence agency of the Israel Defense Force. Aman collects information of direct and indirect military utility, both in the field and from units of the various armed forces, links and analyzes them, and reports directly to the defense staff. State-of-the-art units and programs are active in Aman (Kahana, 2002).

Unit 8200 (*shmone matayim*) is centrally responsible for the collection of information other than that from human sources (HUMINT). This unit therefore deals with the collection and interpretation of electromagnetic signals (SIGINT), decryption of codes, cyberwarfare, cyber espionage, security and surveillance (Reed, 2015). The Unit is mainly composed of very young personnel, in order to make the most of young talents in the electronic and IT fields. It is estimated that this unit consists of at least 5000 units. *Unit Hatzav* was a subunit, now closed, which deals with Open Source Intelligence (OSINT), starting from the monitoring of arabic media in particular.

Unit 81 is an office that has probably existed since before the existence of the state of Israel itself, dealing with the development of new military technologies (Shulman, 2021). He not only deals with ICT and cyberwarfare, but also with quantum technologies, nanotechnology and aerospace. The numerical consistency of this unit is subject to military secrecy and is also difficult to estimate.

Unit 9900 performs IMINT (Imagering Intelligence) and VISINT (Visual Intelligence) by exploiting information provided by satellites and other optical surveillance methods (Ahronheim, 2020). The unit is also involved in the development of technologies related to its sector, including military applications of augmented reality and metaverse. This unit is also responsible for the peculiar *Roim Rachok* program, which aims to exploit the particular abilities of subjects on the autistic spectrum for military intelligence purposes.

Havatzalot Program it is an ambitious path that tries to combine, within three years, two university degree paths simultaneously, a selective training regarding military and leadership skills, as well as an education of excellence in the field of intelligence (Senor & Singer, 2011). The first university path is oriented on political science, focused on the Arab world; the other is optionally oriented towards learning economics, mathematics, computer science or philosophy. To achieve all the objectives of the ambitious program in just three years, the initial phase involves a strict selection, focused on the best and most motivated high school students in the country.

It’s similar to *Talpiot Program*, which the IDF organizes outside the intelligence circle and which is more canonical, though no less prestigious (Shulman, 2021). This program is also aimed at gifted high school students who, while pursuing a bachelor’s degree, also become IDF officers and are usually placed in technology study offices. Many prolong their stays in the military, while others embark on prestigious academic careers, so much so that its former members include winners of the Gödel prize as well as the Fields Medal. However, there seems to be a close correlation between the graduates of this program and Unit 81.

iv) *C4I (Heyl HaTikshuv*, Comunication Corps) is the teleprocessing and communication unit of the Israel Defense Force (Rosenne, 2022). *Unit Matsov* is the subunit responsible for all Israeli Encryption and Information Security.

v) In the Israeli Defence Ministry is active the *Director of Security of the Defense Establishment* (DSDE), which is an intelligence and security agency which deals with the security of Israeli weapon industries and institutions (Barucija, 2020).

vi) There are other intelligence agencies, unrelated to the IDF, with specific tasks (Oren, 2020), like The Center for Political Research (once known as the Intelligence Research Department), which works in a certain way as a bridge between intelligence and diplomacy under the Israeli Ministry of Foreign Affairs; or the police intelligence branches, active also in SIGINT. It is worth mentioning the famous *Lakam* (*ha-Lishka le-Kishrei Mada*, "Bureau of Scientific Relations"). It was an agency, now dissolved following scandals (Oren, 2020), but characterized by a peculiar mission in the field of intelligence agencies: that of collecting secret information in the specific field of scientific and technological innovation.

vii) Finally, the activity of the various agencies is coordinated by the *HaMateh leBitachon Leumi* ("National Security Council" - NSC), a central staff structure with the task of directing national intelligence activity, starting from the requests of the Prime Minister and the Government, and verifying the results (Barucija, 2020). There are also various commissions, committees and control bodies that oversee the work of the intelligence and security structures.

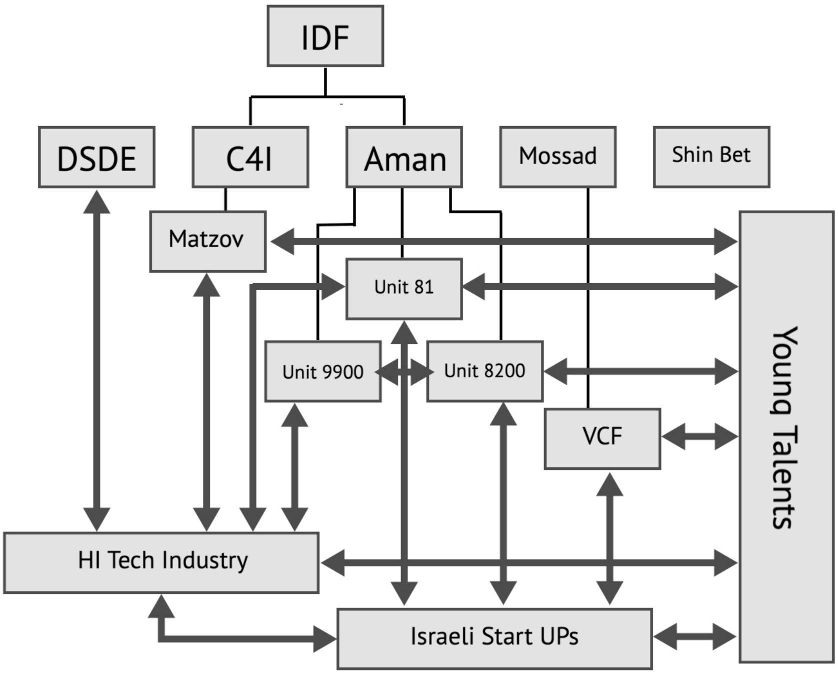


Figure 3: Israeli Intelligence (public and private) ecosystem

2. Israel’s HRM policies

Due to the peculiar secrecy of the intelligence and security services, which involves every aspect of them (from recruitment to the chain of command, from the organization of offices to internal regulations) it is simply impracticable to analyze HRM policies as one would do for a traditional organization. But the Israeli intelligence system has a peculiarity that allows it to be studied indirectly: its peculiar contamination with the private sectors (Senor & Singer, 2011).

Israel, whit only 8 million people, have more companies listed on the NASDAQ than Europe, China, Japan, India and Korea combined (Tendler, 2015). Many of them insist in Silicon Valley, where many leading personalities of the ITC industry are from Israel and specifically from military and intelligence fields (Green, 2016). Technology companies founded by Israeli citizens in the Greater Boston area, from 2013 to 2015, area secured over $1.2 billion in venture capital and contributed to the Massachusetts economy over $9 billion in revenue (Goodtree, 2016). And many of these companies were founded by former IDF officers, who worked in military technical fields (Abigail Klein Leichman, 2017).

This transmigration from intelligence to tech start-ups became public knowledge when *Unit 8200*, whose existence until a few decades ago only its members and military leaders knew about. According to Forbes estimates, former *Unit 8200* operatives have founded more than 1,000 tech companies. One of the reasons for this, can be found in the fact that even within *Unit 8200* work is organized in a similar way to that of technological start-ups: small groups of people working on ambitious projects, without limitations of action and thought, with the explicit favor of divergent thinking, under pressure (due to strict deadlines) but lacking any guidance on how to act (Reed, 2015). To obtain these results, the unit selects possible candidates already during high school, with a view to including them in its staff during the subsequent compulsory period of military service. Furthermore, the recruitment is not carried out by human resources or high-ranking officers, but by the young members of the unit themselves who evaluate, in addition to the general characteristics necessary for the delicate military assignments, also, above all, the technical, creative and mental skills. It is believed that young soldiers, who are faced with high technical level mental challenges on a daily basis, are the most suitable to identify candidates who possess the qualities to be able to replace them (Behar, 2006). Given the young age of the candidates (who do not even know they are as recruitment takes place in a hidden way), the unit considers it more important to evaluate mental qualities such as creativity, ability to adapt and ability to solve problems, rather than good school performance or experience (that such young people cannot objectively possess in any field). The unit furthermore has a 25% annual turnover rate and operators rarely stay past 22-24 years of age. This therefore allows you to constantly have people who tackle problems in a new way, without becoming stuck on the solutions already adopted, even if successful (Cordey, 2019). And at the same time the new recruits are put to work on highly difficult problems, without being informed that many of their predecessors have already faced them, failing. All with the result of solving seemingly impossible problems on many occasions. The mandatory annual military refresher period intervenes as a natural corrective to the problems that could emerge from a system of this type, which affects those who have served military service for three weeks a year, up to forties. In that short annual period, past knowledge and skills, strengthened by subsequent professional activities carried out in the technological sectors, can transmigrate towards young operators.

Other departments are less known to the general public, such as *Unit 81* which deals with innovative technological solutions, also in a very concrete way, i.e. by building upon request materials and mechanisms that do not exist on the market and which the IDF sees as a need (Behar, 2006). For this, it recruits very young but highly gifted operators in certain disciplines (such as ICT, aerospace engineering, quantum computing and other STEM skills). Collectively, companies founded by former Unit 81 members are valued at more than $10 billion (Shulman, 2021). The veterans of this unit are tightly connected in a network (the Alumni Association *Amit*) which also acts as an engine in the technical and financial collaboration between the various start-ups founded by its members.

The requirement of permanence for a period longer than the three years of military service (more two/three years) seems to be mandatory, presumably due to the non-short times of technical planning and related investments, both financial and human resources. Those who stay longer, i.e. until the end of their twenties, and therefore move up the ranks in the units, when entering the world of work possess both the technical skills and those of personnel management in crisis situations, which provides them with a competitive advantage in the market (Shulman, 2021).

Little can be found on the *Matzov* decryption unit, although even personnel outside that facility are explicitly in demand on the market. Furthermore, the unit, active in the most advanced cryptography techniques, including quantum, interacts with the specialist sector also with reports and papers that do not report the authors but indicate the unit itself as "author" (MATZOV, 2022)

Libertad Ventures is the Mossad's Venture Capital Fund, which reverses what has been seen for the other units. In this case, a state agency offers funds to certain selected private start-ups, against a reciprocal exchange. In fact, Mossad will receive in return the license to use developed technologies without any fees (non-commercial, non-exclusive license) and with no restrictions on the intellectual property.

The VCF, founded in 2017, highlights on its website[6] the area of interest: Fintech, Robotics, Data Science, Drones, Personality Profiling, Big-Data, Energy Harvesting, NLP, Voice Analysis, AI, 3D Printing and Scanning, Blockchain, Machine Learning, Synthetic Biology, Smart City Tech, Perfect Online Privacy.

The fund began in 2017 by investing in five companies annually, totaling approximately $3 million annually. The fund's portfolio is kept secret, both for strategic reasons and to guarantee mutual confidentiality between the start-ups (Orbach, 2018).

Human resources management policies are absolutely functional and consistent with the needs of a system, that of intelligence and security, called to operate in a complex, changing, challenging, competitive environment with a high strategic survival value.

The main traits of HRM policy are summarized below:

– the Israeli intelligence system, through specialized Units and structures, recruits very young but highly gifted operators in certain disciplines (such as ITC, aerospace engineering, quantum computing, and other STEM skills). The young age of the resources forming part of the operational core is an element of adaptability of the system, given that age is notoriously inversely proportional to the propensity for innovation;

- it is not the management of the organization, but the young people of the operational core who choose the resources to include in their teams (based on creativity and capacity for innovation, as well as on the basis of very high technological skills)
- the system trains the recruited young people in military and intelligence disciplines, and in the application of their skills to these fields;
- after a period of internal operations, a strong turnover is implemented, and these operators follow other paths. The high turnover allows to avoid the typical problems that emerge when resorting to approaches that have proven successful in the past;
- some of these former agents accept to be hired by large companies in the sector, even abroad (Silicon Valley, Europe, etc.), attracted by the prospects for career development in the private sector with the associated generous earnings;
- others former agents found start-ups in the sectors, cyber, ITC, security, etc. (sometimes helped by State).

[6] (https://www.libertad.gov.il retrived 11 July 2023)

For the whole country, these intelligence units represent a point of contact between the military system, the world of business and the academia (Reed, 2015). This type of system takes the form of a network, a vicious cycle, between the country's young talents, elite military structures, start-ups, the country's economy and national security. With positive benefits for each of the actors involved in the cycle.

This human resources management policy leads to the establishment of an ecosystem where the intelligence recruited and used by the agencies is not lost due to the need for continuous turnover, but is valorized in different contexts, where business is the driver of innovation. This allows agencies to have newer and newer resources to tackle ever-changing problems, and at the same time to maintain connections with the world of ICT companies and related innovations; while it offers the world of private companies, large and small, a precious reservoir for the recruitment of resources not only of very high technical qualification but also with leadership and teamwork experiences and skills, particularly rare and precious in the Hi-Tech sector.

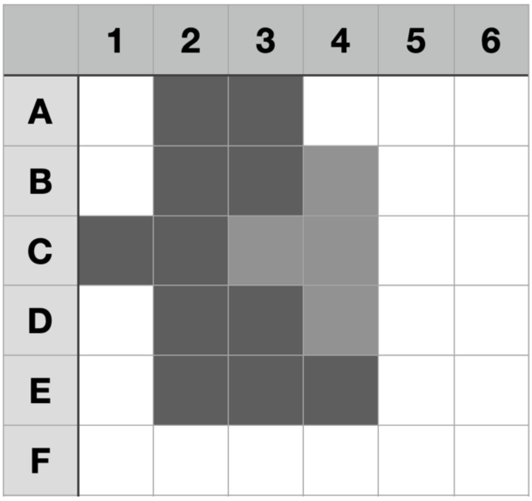
Some observers highlight how the success factors of a start-up are not only linked to the ability to develop an innovative idea, but also to more practical skills, linked to the concrete realization of the company project. In this sense, the military experience of the Israeli technological elite units has an added value, compared to the canonical university courses, as it puts the young student into a world that stimulates the learning of high technical skills as well as soft skills such as teamwork, execution, leadership, anchored to strong values, such as the physical safety of one's community. Personnel leaving these units, usually around 23 years of age, can boast not only considerable technical preparation but also leadership experience that is difficult to find in their European or North American peers who enter the business world after a canonical path university (Tali, 2017).

On the other hand, for the same reasons, the training of these units sometimes lacks in the areas of marketing, product placement, branding, distribution and budgeting. This emerges in general in Israeli start-ups which in fact often do not supply products to the consumer, but focus on technologies, features or intermediate products, for other companies, which use them to create complete products (Green, 2016).

3. Analysis of sources relating to the Israeli intelligence (eco)system

The sources consulted for the analysis of the Israeli intelligence (eco)system include, first of all, a series of statements, analyses, and reviews conducted by professionals in the field with verifiable experience. These analyses are often confirmed by other sources or are at least consistent (C1 C2).

Alongside these, however, it is worth highlighting the widespread use of anonymous or suspicious sources which often provide information which is consistent or compatible with the context (D2 D3 E2 E3), but which just as often goes beyond this into information which appears to conflict with the context, often coming from suspicious sources (E4) and sometimes from higher-level sources (B4 C3 C4 D4).



	1	2	3	4	5	6
A		■	■			
B		■	■	▨		
C	■	■	▨	▨		
D		■	■	▨		
E		■	■	■		
F						

Figure 4: 6x6 Matrix for Evaluating Israeli Intelligence Sources

Studies by public and private research institutions on the Israeli system are numerous, but they fail to adequately permeate the level of secrecy imposed on the actual current functioning of the agencies and units, and are therefore configured as consistent and compatible with the context (A2 A3 B2 B3).

4. The Israeli intelligence (eco)system organizational elements

The analysis of what has been gathered through published literature, gray sources, and indirect analyses, shows the public-private ecosystem of Israeli intelligence and security agencies possesses elements such as high organizational adaptability, low formalization and bureaucracy, small agile units, limited detailed planning, high transversal connections, selective decentralization, centrality of human resources, high staff training, young age of staff, fluidity of turnover of decision makers.

What emerges from the examination of the Israeli intelligence system is that it has peculiar characteristics, here schematized:

- reticular structure based on different units;
- high horizontal specialization of tasks within units;
- blurred differences between line and staff units;

- little formalization of behaviors;
- coordination mechanisms mainly based on mutual adaptation, which favors the integration of resources with different specializations in synergistic project groups;
- both vertical and horizontal decentralization of a selective nature, i.e. the decision-making power relating to the strategies to be pursued distributed along the entire hierarchy.

On the whole, the organization, albeit military in nature, or in any case structured on the basis of military-type hierarchies, manages to remain fluid and adaptive towards the complex environment: the elements above synthetized characterize organizations with exceptional adaptation and innovation capabilities, capable of performing in particularly dynamic and complex contexts such as those in which intelligence agencies operate. These organizations are theorized as "adhocraciers" by Mintzberg in his seminal work on organizational configurations (Mintzberg, 1983). Mintzberg highlights how these organizations often tend to evolve towards more rigid structures, i.e. bureaucracies, which standardize and formalize processes and behaviors. This trend, which is positive in the cases in which the environment tends to stabilize, must be avoided in the case of intelligence, because the environment in which this particular discipline operates has such variability and speed of variation as to make any form of standardization impossible.

Other elements of this complex structure should be highlighted. First of all, the young age of the staff employed in positions of responsibility, burdened with decision-making power according to selective decentralization. The elements of fluidity and laterality of the structure become fundamental for dealing with the environment in which the (eco)system operates. Furthermore, in such a structure the difference between staff and line blurs, and the groups work directly with the aim of operating "on the market", although the operational field of this type of agency is abstract to conceptualize.

5. Conclusions on the Israeli system

The organizational structure of Israel's national intelligence ecosystem represents a sophisticated example of complexity management. A network of connections tightly integrates public and private actors, while highly innovative units, even when embedded in typically rigid environments like the military, operate with an organizational model directly reminiscent of tech startups. Small, highly qualified teams work with high levels of operational autonomy, often under intense time pressure and with ambitious objectives, yet at the same time enjoy almost complete internal freedom in choosing strategies and resolution actions. This approach maximizes individual creativity and adaptability, combined with the ability to work in teams among highly specialized individuals, allowing the Israeli intelligence system to maintain a technological, operational, and strategic advantage.

Another distinctive feature of the Israeli system is the centrality it places on human resources management (HRM). The recruitment process is geared toward finding young talents with extraordinary technical and creative skills, identified and selected during high school. This unorthodox process involves the selection phase being carried out by the operators, themselves once young talents, who will be replaced by these new recruits. This approach is based on intensive staff rotation, which avoids the consolidation of standardized practices and constantly encourages the contribution of innovative ideas and methods. The human resources management strategy is not limited to the mere selection and training of highly qualified personnel, but extends beyond strictly military life, encouraging the natural migration of skills to the private sector. This phenomenon, particularly evident in technological units such as the aforementioned Unit 8200, has created a unique ecosystem in which experience gained in the military and intelligence sectors constantly fuels the dynamism of the Israeli technology industry, which then returns the necessary solutions to strategic challenges to the public sector. This system is further strengthened by the creation of dedicated structures, such as the Mossad's Libertad Ventures, which finances private startups in exchange for access to innovative technologies, thus ensuring a two-way flow of expertise between the public and private sectors.

Organizationally, the Israeli system exhibits elements typical of the adhocratic structures described by Henry Mintzberg, such as a low level of formalization, high decentralization of decision-making, coordination based primarily on mutual adaptation, and strong integration between the various units, each characterized by strong specialization.

However, strong decentralization and operational autonomy, while clear strengths, can also pose challenges. In particular, the limited formalization and fluidity of operational structures, while ensuring agile decision-making, could hinder overall strategic control. Likewise, the presence of a collection of operational units could degrade the quality of integrated information management. Therefore, the presence of such highly specialized units must provide effective and timely coordination and communication systems to avoid the fragmentation and dispersion of otherwise crucial information.

Another critical factor is the long-term sustainability of the continuous turnover model for young, highly specialized personnel. While this mechanism ensures freshness and continuous innovation, it could also lead to a loss of institutional experience, potentially impacting the stability of internal knowledge and the organizational memory capacity of the system.

Despite these challenges, Israel's organizational model is overall extremely effective in highly complex and strategically dynamic environments. This configuration allows the country to successfully address a particularly complex strategic landscape, enabling it to respond rapidly and effectively to emerging internal and external threats, with a co-evolutionary and proactive approach that constitutes a genuine competitive advantage on the international stage. Its ability to synergistically integrate military, technological, economic, and academic expertise is an exemplary example of integrated complexity management, which could serve as a benchmark for other national intelligence systems seeking to successfully address the challenges posed by today's evolving global landscape.

The Israeli extended intelligence (eco)system displays some characteristics that had already emerged in the literature review.

1) Networked adhocracy and small autonomous units.

The Israeli system, which makes extensive use of highly specialized micro-teams (Units 8200/81), is characterized by low formalization and selective decentralization. This solution had already been anticipated, for example, in the simulations of Behrman and Carley, who showed that decentralization, when accompanied by targeted information redundancy capable of exploiting resilience under conditions of uncertainty, maximizes accuracy (Behrman and Carley, 2003).

2) Meta-organization and public/private hybridization.

The ecosystem described is rich in interconnections with universities, startups, and public initiatives. This can be linked to Best's vision of the US intelligence community, which he sees as a meta-organization with varied and overlapping lines of authority, while coordination remains predominantly political-cultural (Best, 2011). Instead, according to Zegart and his ecosystemic vision, US intelligence effectively integrates the public, private and academic spheres (Zegart, 2023).

3) Talent pipeline, early turnover, and learning.

Hiring very young staff, high turnover, and rapid assumption of responsibility foster creativity and problem-solving skills. However, the literature warns that rapid turnover can erode organizational memory and damage long-term reflexivity, especially when feedback is not adequately institutionalized. Dunbar and Weber, in particular, have demonstrated that the lack of stable learning channels (such as self-assessment, inter-agency exchanges, etc.) poses a real risk for organizations to develop error-absorbing behaviors without implementing mechanisms for correcting them (Dunbar and Weber, 2014).

4) Cooperation as a low-integration/high-interdependence network.

The numerous horizontal interfaces between intelligence units and external actors reflect a cooperative model, with little formal integration but high functional interdependence. This dynamic had already been theorized by Lefebvre, according to whom cooperation in the intelligence field operates as an adaptive and negotiated network, with variable nodes (Lefebvre, 2013). The Israeli case appears to be a particularly successful operational example of this structure.

5) Performance metrics: operational vs. forecasting.

In the Israeli system, performance appears to be primarily anchored to technical-operational outputs (positive solutions, IT capabilities, time-to-task). The literature, on the other hand (Tetlock & Mellers, 2014), proposes forecasting capacity as an organizational metric for intelligence analysis. Performance evaluation in particular should be implemented through continuous feedback tools, such as measuring forecast accuracy. The Israeli ecosystem appears to prioritize tangible short- and medium-term results, while the literature argues that a more efficient quality standard is linked to predictive transparency.

6) Oversight: adaptive and multi-level vs. operational agility.

The close integration of intelligence with the private sector, and the broad autonomy of specialized units, pose governance challenges. Van Puyvelde et al. (2017) argue that effective oversight of a system like this must also be a distributed ecosystem (in terms of actors involved, tools, and objectives). Only in this way would it be able to adapt to evolving technologies and threats. The Israeli model therefore requires flexible, multi-actor forms of control to identify any deviations from the standard, while maintaining the necessary balance between secrecy, speed, and accountability (Van Puyvelde, 2017).

III.

The multi-layer network organization of the French economic intelligence system as a complexity mitigatory

It is better to have a bad method than to have none
Charles De Gaulle

1. Economic intelligence

Each national entity has always collected information useful for its functioning and protection. Intelligence activity, as defined scientifically, has the task of collecting, processing and disseminating information that is not easily available because the adversary entity (be it another state, a criminal or terrorist organization, etc.) wants to keep them secret in order to maintain or achieve a strategic information advantage (Moutouh & Poirot, 2018). The content of information collected by intelligence agencies can be the most varied. In fact, if the most attractive issues are military, political and grand national strategy ones, which are in fact prioritized by states, it is equally true that any type of information on the functioning of an adversary entity can be useful for understanding its priorities, its operating methods, its weaknesses, and therefore counter it more effectively (Silberzahn & Guisnel, 1999). Therefore, information of an economic nature is also among those subject to attention by intelligence agencies.

This interest, however, unlike those for other issues that are clearly of national security interest, has fluctuated throughout history. If many nations have underestimated this application of intelligence, others, thanks to the foresight in gathering economic, financial and industrial information, have flourished and prospered (Laïdi, 2016). Without wanting to proceed with a detailed history of economic intelligence, it is worth remembering how European states managed over the centuries to strengthen their economic position thanks to the collection of industrial secrets on the manufacture of silk, porcelain and ceramics in

China, thanks to the work of traders, religious personalities and travelers, who sometimes acted spontaneously (but were well aware of the future support of European nations) and at others were operational agents in the direct service of state entities (Van Ham, 1992).

This work will focus on the French economic intelligence system, which however was born in fairly recent times, following studies and debates that arose in the early 1990s of the twentieth century, and therefore in conjunction with the collapse of the European communist bloc (Denécé & Arboit, 2010). France had nevertheless played a leading role also during the intelligence battle between NATO and the USSR, to which we will return shortly (Gomart & Frank, 2020).

Anyway, well before the French system there were other examples of highly relevant economic intelligence. Great Britain has a very long tradition in this sense, which favored and was favored by the extension of the British empire, which was largely based on commercial capabilities (Bragg, 1996). In the same vein, the USA can also boast a tradition in this sense, especially after its rise to superpower (Fialka, 1997), while other interesting realities in Europe were the systems of Germany and Sweden. Absolutely peculiar and fundamental for the modeling of the French system was the Japanese one, also constituted as a network, which allowed a nation far behind from a technological and industrial point of view compared to Western countries, bowed by the defeat in the Second World War, to become an absolute pioneer of cutting-edge technology and also the second industrial power in the world (Johnson, 1982). This success of Japan was a driving force in pushing many nations to develop an economic intelligence system.

Although economic competition between states has been present in relations between supranational entities since ancient times, with important effects on their respective national securities, the Cold War period was undoubtedly peculiar in intensifying the use of this type of instrument (Guisnel & Korn-Brzoza, 2017). It was also a war between different economic ideas and ideologies, but that was not the reason that brought economic intelligence into vogue, but rather the simultaneous tension between two unprecedented needs. The first was the desire to fight the adversary with all the tools available, including the emerging technologies that were evolving exponentially. On the other hand, the impossibility of fighting the adversary openly, due to the pressing danger of a nuclear escalation which would have led to total mutual destruction. The economic instrument therefore became a powerful lever to gain or maintain a position of geopolitical superiority (Lacoste, 1998).

Post-Cold War globalization has provided a further boost to this trend (Schweizer, 1996). The ability to acquire, store and process raw materials in every part of the world, and then to produce, distribute and sell products without geographical limits, have incentivized the need for information on the part of both governments and private companies (Jackson, 2006). If a system like the British one, being able to benefit from imperial experience, was already structured for this type of challenge, the intelligence of many countries was caught unprepared (Silberzahn & Guisnel, 1999).

For this reason, the Martre Report (1994), which is usually considered the founding point of French economic intelligence, first analyzed the systems of Great Britain, the USA, Japan, Sweden and Germany, in order to acquire their strengths.

Before moving forward, it is necessary to highlight the differences between economic intelligence and two other disciplines that could be considered similar, but which in reality are not.

The first is *Business Intelligence*, a process by which a company acquires information relevant to its strategic decisions (Porter, 1980). The techniques and technologies of this activity are the most varied, and range from classic market investigations to much more invasive methods borrowed from state intelligence, and often feeds on a large amount of structured data (Bouthillier & Shearer, 2003). But business intelligence still remains an activity carried out by a subject (company or aggregation of companies) limited to its own purposes. Although it may appear that economic intelligence is also a sort of national summation of the business intelligence of individual companies, it must immediately be highlighted that economic intelligence constantly intersects with other aspects of the protection of national security, such as military defense, industrial planning, geopolitical relations, political and diplomatic decisions; issues that business intelligence can possibly undergo, but can never determine. Furthermore, economic intelligence is characterized by the fact that it deals mostly with unstructured data, in order to extract information from it (Kahaner, 1997).

The other discipline we will not deal with is *Industrial Espionage*. This term indicates an illegal activity aimed at acquiring confidential information to the detriment of a company (Hou & Wang, 2020). The classic case occurs when a private actor steals information (projects, patents, know-how, industrial processes, prototypes, customer and supplier lists, etc.) from a competing actor on the market. But industrial espionage can also be carried out by a state organization against a company, typically from another nation but not only.

It must be specified that the term espionage, once used as a synonym for intelligence, over time has been confined to the use of activities that constitute a criminal offence. This obviously poses a problem of reciprocity: an operation that, for a nation, is considered a brilliant act to gather economic information against an adversary, for another state will be considered an espionage action and therefore a criminal offence punishable by imprisonment. And vice versa.

Therefore, industrial espionage can sometimes become an instrument of economic intelligence, which however includes a much broader series of methods, techniques, processes and analyses (Faligot et al., 2013).

An example may clarify this relationship between economic intelligence and industrial espionage. Contrary to what many still believe today, the USSR and its satellite countries suffered a very strong technological disadvantage compared to the USA, Western Europe and Japan (Salvatori, 2018). The spectacular successes in the space race and military applications, favored by the presence of Nazi scientists captured during the advance towards Berlin, were cleverly spread and exaggerated during propaganda and disinformation operations whose effects continue today, but at the same time The Warsaw Bloc countries were heavily backward in many areas involving technological processes, information technology and electronics. Throughout the Cold War, and even afterward to the present day, Russian intelligence has used many methods to take possession of Western technological information, from the theft of projects and data in Western companies, to the enlistment of foreign technicians. But the technique most used because it was the simplest was the legal purchase of technological equipment and its subsequent sending to the USSR, where it would be the subject of study and reverse engineering. To block this type of activity, many NATO countries and some neutral ones created CoCom (Coordinating Committee for Multilateral Export Controls), whose headquarters were operative right in Paris (Rue de la Boité) from 1949 to 1994. CoCom, which was responsible for blocking the export of material deemed sensitive to countries considered hostile, including first the USSR, remained in the shadows for decades (Libbey, 2010).

But the body apparently worked with great efficiency, blocking most attempts by Warsaw Pact agents to acquire sensitive material, so much so that after the fall of the Berlin Wall, Mikhail Gorbachev declared in an interview that the CoCom had been largely responsible for the defeat of the USSR.

It is useful instead to analyze a failure of CoCom. In the early 1980s, thanks to a series of falsified documents and bribes given to company managers, USSR was able to buy some numerical control machine tools by the Japanese company Toshiba and software by the Norwegian Kongsberg (Wrubel, 1989). At that time, Russian submarines were very noisy and therefore extremely easy to detect, while Western ones used silent anti-cavitation propellers, which however could only be built with high-tech machinery that surpassed Soviet technological capabilities. Thanks to that CoCom failure, also USSR managed to build anti-cavitation propellers, and a simple purchase of industrial machinery ended up changing geopolitical relations. All this without any act of industrial espionage.

2. Overview of the intelligence agencies of the French system, and their role in economic intelligence

French intelligence has a long-standing tradition, linked to the nation's role as a regional power and its colonial past (Soullez, 2020). In recent years have there been profound reorganizations in French intelligence in general, and in economic intelligence in particular, implemented through the merger of entities, the transfer of skills and the creation of figures of responsibility, always following a logic of simplification combined with interdisciplinarity (Faure, 2007). The most notable reforms occurred in 2008, 2014, 2015, 2016 and 2023.

The French economic intelligence system is structured as an overlap of various actors, at various levels, and we will first try to describe this system.

The large number of entities involved and the mutual relationships can be appreciated from *Figures 4 and 5* (taken from https://cf2r.org) which represent only the first and second circle agencies of French intelligence. *Figure 6* below, developed by the author, focuses on the actors of economic intelligence.

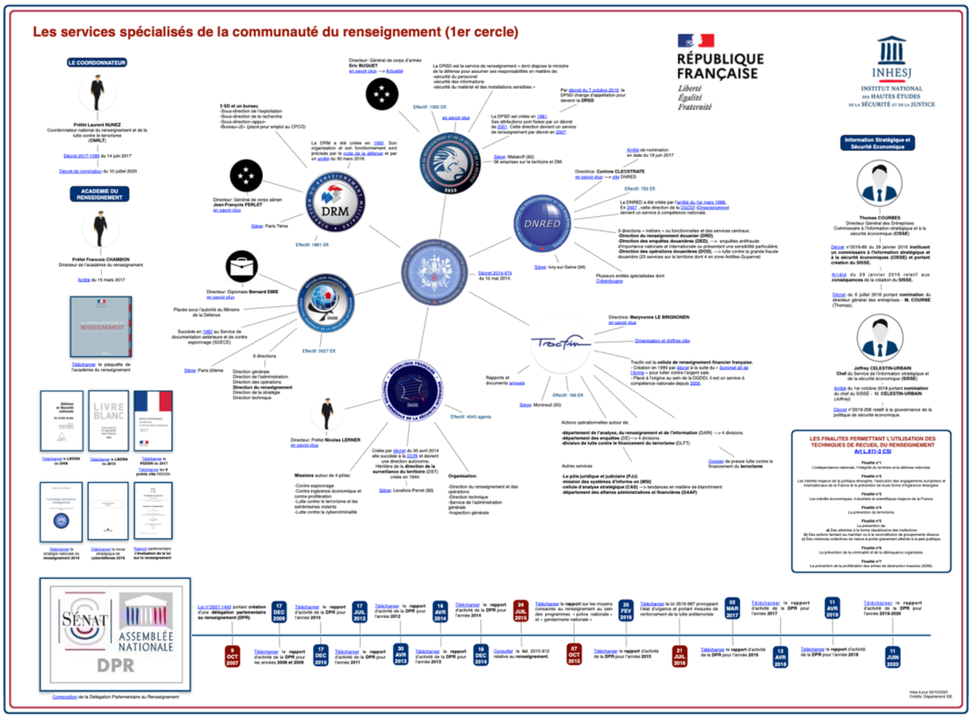

Les services spécialisés de la communauté du renseignement (1er cercle)
LE COORDONNATEUR
ACADEMIE DU RENSEIGNEMENT
RÉPUBLIQUE FRANÇAISE
INHESJ
Information Stratégique et Sécurité Economique
DRM
DNRED
Tracfin
LIVRE BLANC
SÉNAT
ASSEMBLÉE NATIONALE
DPR

Figure 5: *the firs circle of French intelligence actors.*

The state intelligence system in France is made up of a well-defined series of actors, whose most specialized actors are part of the so-called French intelligence community (*Communauté française du renseignement*). The components of the first circle of that community are (Comité d'études de défense nationale, 2018):

i) DGSI (*Direction générale de la sécurité intérieure* - General Directorate of Internal Security), which deals with the collection of information within the French state, on all matters of interest (Jordanov, 2020). This agency reports directly to the Ministry of the Interior and is equipped with local territorial services.

The tasks of this agency in the economic field move along two main lines. The first is the surveillance of international scientific and technological relations in order to prevent French know-how from being used for weapons of mass destruction, the so-called counter-proliferation (Dgsi, 2018). The second axis is the surveillance of foreign infiltrations in both public and private national research laboratories and the defense of French companies against foreign interference. An integral part of the agency's action is the creation of a shared culture regarding these risks, through conferences, dissemination of real cases and relationships with the top management of sensitive companies and laboratories.

ii) DGSE (*Direction générale de la sécurité extérieure* - General Directorate of External Security), which deals with the collection of information outside the French state. This service reports directly to the Ministry of Defence (Dgse, 2018). This agency places economic intelligence among its priority objectives, as demonstrated by the fact that there is an internal directorate completely dedicated to this activity, which would appear to absorb 25% of the budget (Lorho & Lobjois, 2015).

Analyzing the intelligence systems of the world, it emerges that Most of them use a (at least) two main agency system, although there are significant examples of single-agency systems (as in the case of the USSR). The system that caught on most was that of separation (Merlen & Ploquin, 2003) between a security agency (counter-espionage) and an intelligence agency (collection and analysis of information). The French system, however, is based on the geographical separation of the areas of interest: the national territory for the DSGI and abroad for the DSGE. In this way both French agencies operate both in the field of intelligence and counter-intelligence.

iii) DRM (*Direction du renseignement militaire* - Directorate of Military Intelligence)

This agency, due to its eminent orientation towards military intelligence, is one of those that is least involved in the economic intelligence sector (Manificat, 2021). This service reports to the Defense General Staff, and through them to the Ministry of Defence (Drm, 2018).

iv) DRSD (*Direction du renseignement et de la sécurité de la defense* - Directorate of Defense Intelligence and Security)

This agency collaborates on economic intelligence through the protection of defense-related companies, in all the aspects that such defense requires. It is responsible for countering threats that can compromise national defense secrets, scientific and technical potential and interests relating to the tangible and intangible assets of defense-related companies or organizations (Heinrich, 2016). It therefore implements an economic counter-intervention to avoid damage linked to the "economic war" and therefore for example theft of confidential information and materials, sabotage, damage to corporate reputation and more (Drsd, 2018). This agency reports directly to the Ministry of Defence.

v) DNRED (*Direction nationale du renseignement et des enquêtes douanières* - National Directorate of Customs Intelligence and Investigations)

The agency, reporting to the Ministry of Economy and Finance, deals with intelligence regarding customs issues, and therefore acts as a necessary glue with the other agencies when any goods cross the borders of the French customs area.

vi) TRACFIN (*Service de traitement du renseignement et d'action contre les circuits financiers clandestins* - Intelligence processing and action service against clandestine financial circuits)

This agency also depends on the Ministry of Economy and Finance, and is responsible for collecting information regarding money laundering, illicit transfer of funds and other illegal operations involving money (Tracfin, 2018).

All these agencies report to (Cnrlt, 2018):

vii) CNRLT (*Coordination nationale du renseignement et de la lutte contre le terrorisme* - National coordination of intelligence and the fight against terrorism), which reports directly to the government through a director (*Coordonnateur national du renseignement et de la lutte contre le terrorisme*).

The agency staff is trained in a common way by:

viii) Académie du renseignement - Intelligence Academy.

And all the system is under control of

ix) ISR (*Inspection des services de renseignement* - Intelligence Services Inspection), composed of inspectors appointed by the government among senior public administrators. The task of this inspectorate is to verify compliance with the laws by intelligence agencies and respect for citizens' rights.

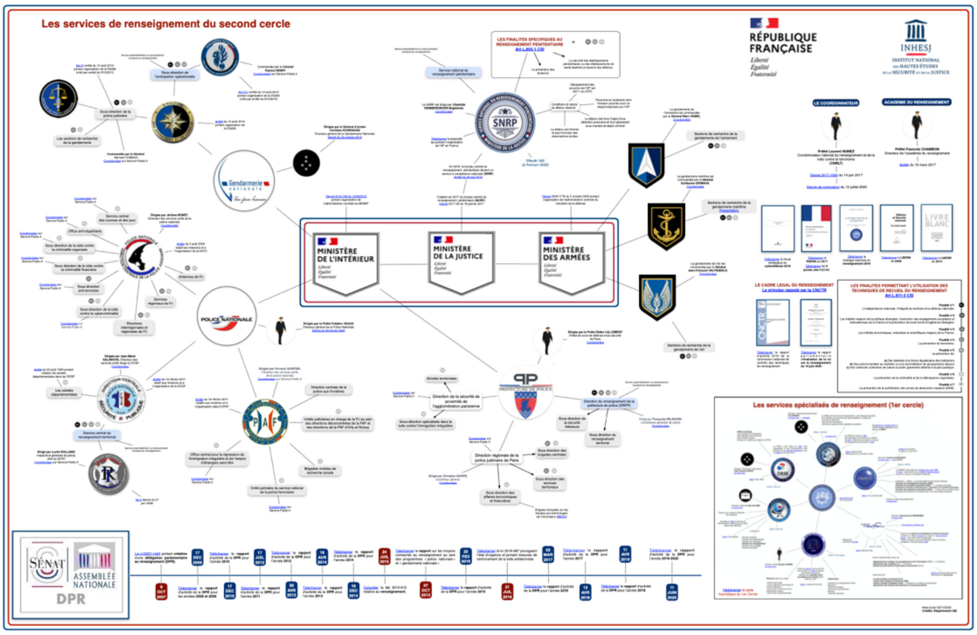


Figure 6*: the second circle of French intelligence actors.*

Alongside this Community there are some other relevant intelligence services which constitute the second intelligence circle.

x) DNRT (*Direction nationale du renseignement territorial* - National Directorate of Territorial Intelligence), placed under the authority of the DGPN (*Direction générale de la Police nationale* - Director General of the National Police), in the Ministry of the Interior. This service operates throughout the territory, thanks to its 255 offices, in which the country's two main police forces collaborate: the national police (civil) and the gendarmerie (military). Its Division number 2 deals with Economic and Social Information.

xi) SDAO (Sous-*direction de l'anticipation opérationnelle* - Operational Anticipation Sub-Directorate) placed under the authority of the DGGN (*Direction générale de la Gendarmerie nationale* - General Directorate of the National Gendarmerie).

The Economic Security and Business Protection sub-section (SEcoPE) of the SDAO is more specifically responsible for proposing the necessary doctrinal developments in the field of intelligence and economic security for the gendarmerie; coordinating and monitoring the activity of the network of local representatives; carring out awareness and prevention actions for the benefit of economic actors; providing training assistance.

xii) DR-PP (*Direction du Renseignement de la préfecture de police de Paris* - Intelligence Directorate of the Paris Police Prefecture). This specific intelligence service deals only with the capital, and is a fairly typical solution in the French panorama, which often reserves different treatments for Paris (Berlière, 2018a). The main focus of this agency, which depends on the Ministry of the Interior through the Préfecture de Police of Paris, is terrorism, given that the French capital often becomes a privileged target for this type of attack.

xiii) SNRP (*Service national du renseignement pénitentiaire* - National Prison Intelligence Service) which reports to the Prison Administration Directorate of the Ministry of Justice.

Intelligence within prisons has over time become fundamental for intercepting terrorist radicalization dynamics or for monitoring organized crime events even outside penal institutions, but in the field of economic intelligence its role is marginal.

The entire intelligence system is then subjected to control and verification by the:

xiv) DPR (*Délégation parlementaire au Renseignement* - Parliamentary Delegation for Intelligence), made up of four deputies and four senators, which meets in unregistered meetings, the minutes of which are subject to state secrecy.

3. The different layers in French economic intelligence

All the agencies we have seen so far report, directly or indirectly, to a ministry, as is normal for intelligence agencies around the world. But mere dependence on a ministry does not mean direct activity of that ministry in intelligence. The French reality, on the other hand, also provides for a direct involvement of ministerial realities, sometimes even in an inter-ministerial manner, in economic intelligence, as a fundamental glue with the productive economic world (Cambon, 2020).

xv) GIC (*Groupement interministériel de contrôle* - Interministerial control group) reporting to the Prime Minister.

The function of this service is very specific and technical, as it deals with the interception of communications outside the judicial context. The very existence of this agency was hidden for 42 years, until the announcement of its existence in 2002 thanks to the issuing of a decree (Laurent, 2009). Its role in economic intelligence is presumably technical, but information on the functioning of the GIC is shrouded in great secrecy.

xvi) CNCTR (*Commission nationale de contrôle des techniques de renseignement* - National Commission for the Control of Intelligence Techniques). It is an independent administrative body with the task of providing a mandatory prior opinion, upon written and reasoned request of some ministers (of Defence, of the Interior, of Justice or of the Economy) fundamental for the French intelligence agencies to be able to activate interceptions of communications. The formal authorization for these activities, after the opinion of the commission, is issued directly by the prime minister.

xvii) IHEMI (*Institut des hautes études du ministère de l'Intérieur* - The Institute of Advanced Studies of the Ministry of the Interior) provides joint training to senior civilian and military leaders from various ministries and administrations, as well as the private sector, in the areas of internal security, justice, crisis management and also economic intelligence. It also trains sub-prefects, prefects and prosecutors in crisis management. The school also involves the academic and university world on the application of theories for forecasting purposes.

xviii) SGDSN (*Secrétariat général de la Défense et de la Sécurité nationale* - The General Secretariat of Defense and National Security) is an inter-ministerial body placed under the authority of the French Prime Minister, with the task of protect national defense secrets, prevent and manage crises and attacks, and protect the State from cyber-attacks.

This last task is also implemented through:

xix) ANSSI (*Agence nationale de la sécurité des systèmes d'information* - National Agency for Information Systems Security), with the task of managing, implementing and coordinating the country's cyber security, including that of its critical infrastructures.

xx) SISSE (*Service de l'information stratégique et de la sécurité économiques* - Strategic Information and Economic Security Service), based in the Ministry of Economy and Finance, has the task of managing the inter-ministerial approach to issues involving security and the economy, in particular on the acquisitions of strategic companies and on the economic security of the state.

This service, which was born from the merger of two previous entities (SCIE *Service ministériel de coordination à l'intelligence économique* - Ministerial coordination service for economic intelligence and D2IE *Délégation interministérielle à l'intelligence économique* – Interministerial Delegation for Economic Intelligence), operates in synergy with the SGDSN, as well as with intelligence agencies and the embassy system. Its strength is the centralized collection of every information collected by the entire intelligence network on economic issues. The service acts in a naturally interministerial manner, organizing cooperation between the numerous actors in the information chain, in order to protect the economic sovereignty of France with particular regard to research laboratories, critical technologies and strategic companies.

A key figure for the operation of the service is the **CISSE** (*Commissaire à l'Information Stratégique et à la Sécurité Economiques* - Commissioner for Strategic Information and Economic Security), heir to the interministerial delegate for economic intelligence.

A further level of economic intelligence, markedly characteristic of the French reality, is attention to the territory (Herbaux, 2007). In fact, internal intelligence was implemented, before the creation of the current DGSI, by the DST (*Direction de la Surveillance du territoire* - Directorate of Territorial Surveillance), within which he operated the Economic

Security and Protection of National Assets. That department had units in the 22 regions of France to protect French technology, not only on behalf of defense industry, but also for manufacturing, pharmaceuticals, automobile and telecoms industry, as well as for the service sector (Delbecque, 2005). Historically, DST has been known to recruit cyber hackers since the late 1980s, to pursue leadership in cybersecurity (Faligot & Krop, 1999).

The primary aims of this type of territorial intelligence are: the protection of the economic system from threats, strategic monitoring and subsequent assistance in critical decisions, the anticipation of long-term trends in order to create a favorable system, training on the previous points (Berlière, 2018b).

If Public economic intelligence policy (PPIE) is part of a system established by a decree of 22 August 2013, the Prime Minister's circular of 16 July 2011 outlined the framework of the territorial economic security system: management and coordination are the responsibility of the **Regional Prefect**, who directs this policy in collaboration with the President of the Region.

The regional prefect periodically chairs the **regional economic intelligence committee** and directs the public policy best suited to the territories.

Most of the agencies seen above operate at a territorial level. In particular *SISSE* has 22 delegates for strategic information and economic security (**DISSE**), located in the regional Directorates of Enterprise, Competition, Consumption, Work and Employment the implementation of the territorial economic intelligence policy.

Furthermore, national gendarmerie, due to its peculiar distribution over the vast French territory, is particularly active in this field and its intelligence service (SDAO), via the SecoPE representatives act in a network and partnership dynamic, integrated in the intelligence chain up to the departmental level of the ministries. They carry out their activity in coordination with the DNRT, responsible for centralizing and transmitting all the information collected in the territory to government and administrative authorities.

A further fundamental actor involved in territorial economic intelligence are the regional councils of the Order of Chartered Accountants (Naftalski, 2004), which acts as a connection with the individual production entities, which are the true protagonist of this territorial intelligence (Guilhon, 2016).

Also other actors are involved: academia, think thanks and journalism. In fact, since its origins, found in the famous Martre report of the 1994, French economic intelligence has aimed at some expressly established objectives:

- to ensure that final private actors, and therefore companies, also achieve awareness relating to the practice of economic intelligence, spreading its culture;

- involve university and higher education networks in general in the creation of this culture;
- take care of the information flow between the private and public sectors, and vice versa.

In general, given the peculiarity of the subject, economic intelligence naturally involves (and requires) greater interaction with private actors compared to other intelligence sectors (Moinet, 2003). This includes, for example, universities and research bodies, both for the education of personnel and for the dissemination of the culture necessary for the management of complex phenomena. Furthermore, research on economic, financial, scientific and technological dynamics is a compelling requirement for this type of intelligence activity. For the same reason, relationships with think tanks are close. However, this type of research body, together with the journalistic sector, also lends itself to further intelligence activity, which in the past has raised doubts about its constitutionality.

In fact, the economic-financial system not only influences the surrounding environment, but is influenced by them (Dasquié, 1999). In the context of the so-called "direct actions" or "active operations" of the intelligence services, the dissemination of targeted news can also heavily influence the economic-financial system (Cousseran & Hayez, 2021). This is why many democratic systems expressly prohibit intelligence agencies from operating with professional journalists.

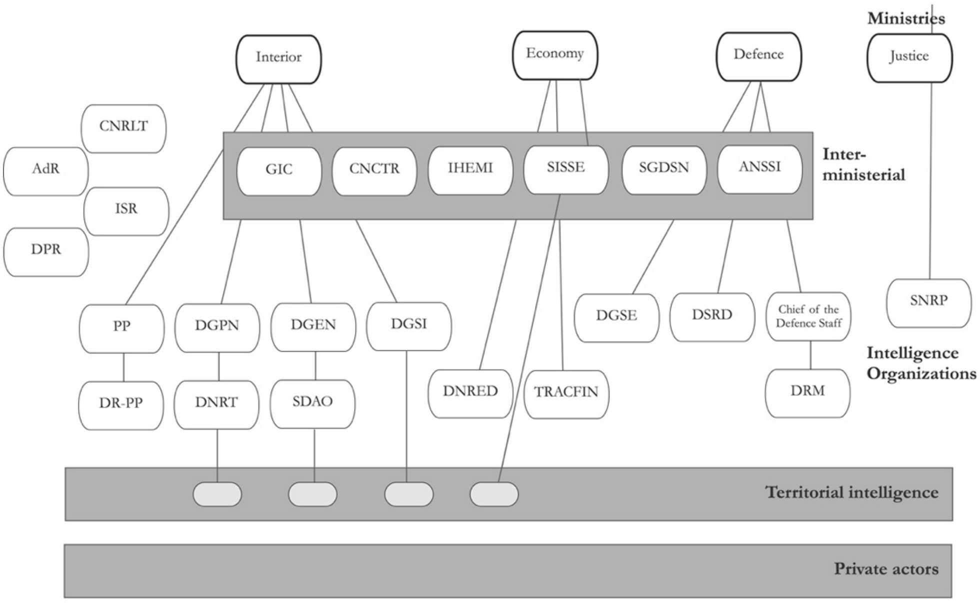


Figure 7: *the whole system of French economic intelligence actors.*

4. Economic intelligence and the challenges of complex systems

The challenge posed by economic intelligence is twofold. In fact, intelligence finds itself, by its very nature, facing a hostile, continually evolving environment, which partly evolves in a chaotic way, naturally hindering the collection of information, and on the other hand moves in a hostile manner. according to precise dictates orchestrated by the opponent's strategy (Warusfel, 2003). Added to this is the economic element, whose components (state decision makers, multinationals, manufacturing and distribution companies, customers, marketing supply chain and various stakeholders) interact in an intertwined and non-linear manner (Smith & Kossoo, 2008).

The union of these two forms of complexity makes economic intelligence operations even more difficult.

The methodological rupture of globalization has required a more flexible, rapid and responsive approach to emerging challenges (Cusset, 2020). This affected, among other things, the organization of structures, both public and private, which had to move from more archaic and stable structures (such as the pyramid one) towards solutions capable of coping with a disorderly, constantly changing world, characterized by fluctuating ties and which requires the constant management of chaotic and random events.

The new post-Cold War economic system was soon characterized by new non-binary relationship methodologies, an incremental increase in the use of the immaterial economy, an abundance of resources and demand, and a technological development impossible to compare with any other period in history. of humanity (Toumoun, 2018). This qualitative and quantitative increase has simultaneously required an increase in information needs, both from the point of view of volume and time ratio.

Another source of complexity to be managed with appropriate methodologies is given by the continuous interaction, in economic intelligence, of public bodies and private actors. This type of interaction is fatally simple in regimes with a low level of democracy, where the State is able to freely apply coercive measures against citizens and the private entities managed by them.

In structured democracies, however, intelligence agencies must submit to the current regulatory system and interactions with private entities and citizens must pass through clear, shared and dialectical methods. This can represent an obstacle when the (typically short-term) objectives of private structures do not coincide with those of protecting national security (Seiglie et al. 2008). For example, the loss of an important foreign customer can represent a source of stress for a company, when on the contrary that same foreign customer may, according to intelligence assessments, belong to hostile nations.

Instead, it becomes an opportunity if it is possible to align the (typically long-term) objectives of all of a nation's private structures with national interests. At that point the collaboration between intelligence and economic reality becomes mutual and helps to reduce the difficulties of adapting to the complex situation of the system.

5. The French network solution with central and peripheral nodes

To achieve this virtuous management, France has used a model that appears to be successful (Wedding & Rose, 2004), based on a multi-layer network system. The intelligence agencies represent a first level of the network, working in a coordinated manner for the entire national security system, but without neglecting the economic sector. the core activity of intelligence agencies is information gathering is, but also the analysis operated by these agencies is fundamental for the system. Analysis that aim to combine and interpreter the data collected by the entire system, in order to obtain structured information for subsequent dissemination to political decision makers.

A second layer is given by the specialized offices in the ministries, fundamental for concretely implementing the results of economic intelligence within the system of ordinary administration of the State. Inter-ministerial coordination, which in this case is part of the network structure of this level, has proven effective over recent years in many areas to address modern challenges, threats and opportunities, which are increasingly complex and difficult to frame in a simple function of the state apparatus as were the classical ministries.

The third level is the territorial network, in which local public bodies such as prefectures and dedicated agencies interface with private actors (Ouassou & Bakour, 2024). Since each regional reality develops, at an economic and financial level, in a different way, it is essential that public-private interaction not only takes place at a centralized level, where only mediated and therefore unrepresentative needs risk appearing, but also punctually throughout the territory.

Other levels complete the complex French model, but the crucial point is the communication capacity of the different layers with each other (Yves Laurent, 2019). The fact that not only homogeneous actors talk to each other in a network, but that different networks talk to each other in a multi-level system, acts as a power multiplier. In this way the flow of structured information, data, requests and needs is able to flow both transversally and vertically, making up for both geographical and regional differences and planning differences.

Precisely in this peculiar system lies the strong point of French economic intelligence, capable as seen of also holding its own against intelligence systems which have historically invested financial and human capital in the intelligence sector that was unthinkable for a small or medium power.

The study of intelligence systems, their organization and functioning, is characterized by a serious methodological difficulty, linked to the fact that their activities are constantly covered by secrecy. Even the reconstruction of an organic map or the understanding of the competences of the various offices are often difficult because they are shrouded in secrecy, and often false news is spread aimed at misinforming the secret services of opposing countries.

In the case in question, which concerns the specific field of economic intelligence, there is strong interaction between the public intelligence sector (subjected to total secrecy), and the public institutional and private sectors (subjected to partial secrecy). This allows for a greater, although not total, possibility of scientific exploration.

The peculiarity of the French system was to combine the classic national intelligence agencies, sometimes even specialized ones, with two parallel networks: the inter-ministerial system, necessary to dialogue with the public system; and the territorial system, capable of connecting with the local industrial and financial fabric, whose events are fundamental to the well-being and economic sovereignty of a nation. All of this is also characterized, at every level, by a strong interaction with private bodies of both an academic nature and a more distinctly economic orientation.

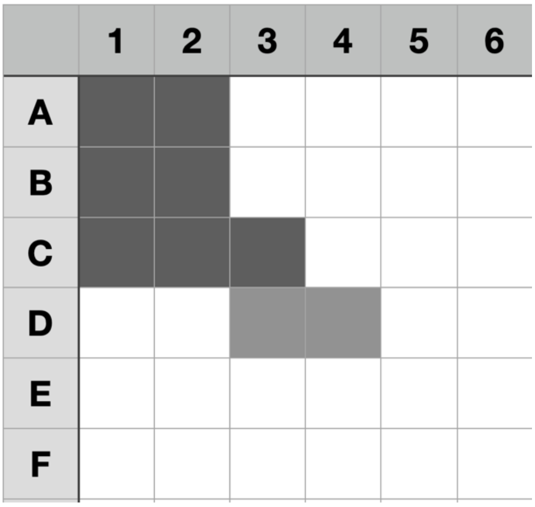
This multi-layered multiple network system has exponentially multiplied the connection possibilities, increasing the degree of complexity of the structure. This has reasonably allowed it to adapt to a complex environment in many ways, due to the presence of: economic competitors inserted in a globalized system; foreign agencies active in the fields of intelligence, industrial espionage, interference, influence and disinformation; an economic and above all financial environment that is increasingly unstable and ready for rapid and sudden collapses and crises; a world in general characterized by rapid changes; a technological level in constant, rapid and sometimes unpredictable evolution.

Dealing with this type of complexity requires organizational adaptations that take into account the factors listed above. In this sense, the multi-layer network type structure, with interactions both between the network of a single layer and between the nodes of the different layers, enable the information and decision-making flows necessary to govern the complexity of the environment.

6. Analysis of sources relating to the French economic intelligence system

The sources relating to the vast network system of French economic intelligence are first and foremost state reports, in large numbers, reinforced by other sources and in any case consistent with the context (A1 A2), supported by research from private and independent institutes which align with the same results (B1 B2).

The reality of French economic intelligence is also revealed by a series of professionals who, in various capacities, have participated in its many facets, which, as we have seen, involve not only agencies but also ministries, other public institutions, academia and research, as well as private companies. The information coming from these sources is confirmed, consistent, or compatible with the context (C1 C2 C3).



	1	2	3	4	5	6
A	■	■				
B	■	■				
C	■	■	■			
D			▒	▒		
E						
F						

Figure 8: 6x6 Matrix for Evaluating French Intelligence Sources

As in any intelligence study, the picture is completed by a series of anonymous or dubious sources, whose information is sometimes compatible and sometimes conflicts with the overall picture (D3 D4).

7. The French economic intelligence as an adhocratic system

The environment in which the different levels of French economic intelligence operate are therefore undoubtedly characterized by high complexity, from the different intelligence and economic points of view. They are also hostile, dynamic, heterogeneous and constantly changing both internally and internationally.

The peculiarity of French economic intelligence, however, acts in this complex environment thanks to the ability to bring together experts in the disciplines of intelligence and economic issues, two very distant macro-sectors, in a harmonious manner. The training of these two families of experts is it is of a high standard: in fact, France has long supported structured training in each other's fields with joint and shared training, which involves leading experts from the two areas, as well as academia and private research. Unlike the Israeli case, a particular predisposition for the valorization of young people, for example by placing them in positions of responsibility, on the basis of their skills, did not emerge in the study. Although the internal details of the French intelligence agencies are not known, from an external survey it seems that the role of young people is comparable to that of many other European countries where the time required to assume important positions in public organizations is much longer compared for example to that necessary in companies of technological excellence.

The multi-layer network structure is configured as fully capable of operating effective but fluid, targeted but decentralized connection mechanisms. The challenges posed to French economic intelligence are posed from the outside: economic competitors, foreign intelligence, foreign national economic interests and asymmetric para-state actors. The structure is therefore structured to contain threats in a local and decentralized manner, while at the same time maintaining a connection between the entire structure, a connection that operates both on the single layer and between different layers.

The multi-layer network structure is configured as fully capable of operating effective but fluid, targeted but decentralized connection mechanisms. The challenges posed to French economic intelligence are posed from the outside: economic competitors, foreign intelligence, foreign national economic interests and asymmetric para-state actors. The structure is therefore structured to contain threats in a local and decentralized manner, while at the same time maintaining a connection between the entire structure, a connection that operates both on the single layer and between different layers. In a structure of this type the difference between line and staff is naturally lost.

8. Conclusions on the French system

France has developed a multilevel network system for its economic intelligence, in which information and decision-making flows can move both horizontally and vertically. This approach, initially inspired by British, American, and Japanese models, has been progressively refined, reaching its current form, which is unique in the global landscape. The fundamental characteristic of the French system lies in the coexistence and interaction of multiple levels, involving both national intelligence agencies and local structures, ministries, and private actors. Each level is called upon to perform specific tasks, yet is simultaneously integrated into a network of relationships that ensures maximum fluidity in communication and cooperation.

At the national level, key agencies such as the DGSI, the DGSE, and the DRM work in a coordinated manner to ensure, in addition to the country's general internal and external security, also the economic dimension, considered of strategic importance to national security. The ministerial level constitutes a second tier, crucial especially for the inter-ministerial coordination function, which often represents a source of enormous bureaucratic bottlenecks. This level collects, integrates, and disseminates information from various agencies.

The territorial level is perhaps the most distinctive element of the French organizational structure. Through a widespread network involving prefectures, gendarmerie, regional delegates, and representatives of the local production system, the system is able to establish a constant dialogue between the public and private sectors. This territorial network allows the system to be extremely responsive and sensitive to signals from the local community, which can then be channeled upward in the information chain, contributing to the effective and proactive protection of national economic resources.

Interaction with private actors, universities, and think tanks is another strength of the French model. This collaboration provides intelligence services with the valuable contribution of highly specialized external expertise, while also enabling the dissemination of economic intelligence culture in otherwise difficult-to-reach environments. Joint training between public and private institutions also enables ongoing and joint capacity development among the various actors, further strengthening the system's resilience.

The French economic intelligence system is ultimately characterized by a highly specialized and decentralized structure, although under central coordination surveillance. The highly trained staff operates in a complex and dynamic environment, and the macrostructure of the system, a multi-layer network, allows mixing vertical and lateral connection mechanisms and selective decentralization.

These elements unanimously indicate that this system is structured as an adhocratic organization.

However, this model, while proving extremely functional and effective in the short and medium term, presents some potential challenges. The complexity of the multilevel network, along with the advantages highlighted, can also lead to confusion in the decision-making process in crisis situations. Furthermore, the presence of such heterogeneous levels, such as inter-ministerial coordination and territorial levels, can actually lead to bureaucratic inefficiencies, especially when there are conflicts of interest or overlapping responsibilities between different agencies.

In summary, the French economic intelligence system represents an innovative and effective organizational model, capable of co-evolving and proactively addressing global economic complexity. The combination of a highly integrated, multi-level network and strong interaction with the private and academic sectors is an example of organizational excellence capable of successfully responding to the challenges posed by the growing complexity of the international economic and geopolitical landscape.

It may also be interesting to compare the findings of the literature review with those emerging from the characteristic elements of French economic intelligence.

1) Multi-layer network as a response to complexity.

We have seen that the French system is constructed as a multilevel network composed of central agencies, inter-ministerial coordination, territorial levels, and connections with universities and businesses. This framework is present in the literature in two forms: both as a meta-organization with multiple lines of command and coordination with more political-cultural than technical characteristics (Best, 2011), and as an organizational structure that evolves from a rigid system of bureaucratic pyramids to a networked and/or adhocratic architecture, typical of knowledge-oriented organizations (Berkowitz & Goodman, 2000). France appears to have implemented these models through the use of a dual network of horizontal and vertical channels for the exchange of information and the transmission of decisions.

2) Public-private ecosystem and “multi-actor” logic.

The strong hybridization of French economic intelligence with private actors, academia, and even think tanks (through elements such as joint training) corresponds to Zegart's ecosystemic vision, according to which contemporary intelligence must adopt governance implemented through a network structure, horizontal cooperation between the public and private sectors, as well as new forms of information exchange that reconcile security and trust (Zegart, 2023).

3) Cooperation as an adaptive network with low integration/high interdependence.

The dual vertical intertwining between levels (central, ministerial, territorial), and the horizontal intertwining between public and private, recalls the networked cooperation described by Lefebvre, which is not fully integrated but nevertheless interdependent in its functioning. This system would seem to confirm that effectiveness does not require a single, omnipotent decision-making center, but rather a series of variable nodes, through which negotiated trust can develop and flow, allowing for informal exchanges regulated only to the extent necessary (Lefebvre, 2013).

4) Multilevel Oversight: Consistency and Stress Tests.

The intelligence system analyzed here is characterized by multiple control tools and authorization procedures arranged at various levels. Van Puyvelde et al. (2017) propose that supervision also occurs in a manner similar to an ecosystem, using multiple actors who apply different tools and objectives, all oriented towards achieving efficiency, legality, and accountability. The potential criticality of the French system, already generally highlighted in the literature, is the risk of losing coordination effectiveness, thus resulting in a loss of interorganizational trust. This risk is exacerbated if the network becomes too dense and technologically complex.

5) Speed/error trade-off and information bottlenecks.

A multilevel network like the one analyzed alleviates bottlenecks, but, the literature warns, each organizational structure is forced to choose between sacrificing speed or precision, and paying the associated costs (Garicano & Posner, 2005). France has opted for selective decentralization, likely hoping to prevent delays in authorization chains and inter-ministerial interactions and thus avoid, especially in times of crisis, bureaucratic delays and friction that could lead to risky failures.

6) Adhocracy, but hybrid.

The text presents France as a networked adhocracy, while acknowledging possible bureaucratic grafts into critical substructures. This ties in with Berkowitz and Goodman's (2000) vision, according to which effective intelligence tends toward networked models, develops efficiency through iterative processes, but retains elements of bureaucracy that allow for the necessary standards of traceability, legality, and control. France's specificity lies in having operationalized this hybridization at multiple levels, including territorial ones.

GENERAL CONCLUSIONS

1. Intelligence agencies and organizational models

The aim of this work was to analyze three peculiar organizational models of "secret" services known for the particularity of their work, in order in the first instance to identify their characteristics. The choice fell on the intelligence and security services for a series of reasons:

- the high level of challenges that these agencies must face, constantly connected with national security;
- the possibility of accessing the best human and technical resources of the country system;
- the possibility of structuring their own organizational chart, their flows and methodologies according to distinct systems compared to the rest of the public administration, including military entities;
- the operation immersed in a complex world from various points of view, in constant change, characterized by continuous challenges and adversaries with investment possibilities unparalleled in other realities;

The selection of the three cases (North Korea, Israel, and France) responds to the need to test the theoretical hypothesis in very different institutional, cultural, and operational contexts. Furthermore, the choice is also fueled by methodological reasons. While, as we have discussed at length, the greatest difficulty in studying intelligence is penetrating institutional secrecy, the three systems chosen share a common trait crucial for indirect observability through open sources and gray literature: intense external contact, implemented by Israel and France through engagement with the private sphere of the economic sector, and by North Korea (as well as Israel) with an operational aggressiveness that the agencies of Western democracies can no longer afford.

North Korea represents the extreme case of an opaque yet highly reactive authoritarian system: frequent restructuring of functional dependencies, selective redundancy, and massive investment in youth skills (especially cyber) produce configurations that, despite the absence of democratic accountability, exhibit the adaptability and modularity typical of adhocracy. Israel, by contrast, constitutes an institutionalized ecosystem of bidirectional permeability between the military, intelligence, universities, and the technology sector:

excellence programs, rapid learning cycles, and public-private "bridge" roles offer a prototype of a planned adhocracy, oriented toward continuous innovation. Finally, France offers a hybrid model: "economic intelligence" is organized across multiple levels (center, ministries, prefectures, business community, training, and research), with formal coordination mechanisms coexisting with task forces and agile operational networks, useful for managing the dual complexity of information and economics.

Together, the three cases cover a spectrum from closed authoritarianism to a highly innovative democratic ecosystem, including an intermediate solution of multilevel governance. This maximized variance allows us to distinguish between the regime and national culture of adhocracy and its functional needs for coordination, rapid decision-making, and learning. At the same time, the shared "outlook" toward external actors increases the triangulation of evidence and inferential robustness. The combination of maximal difference and shared trait therefore offers the best comparative leverage for testing, with indirect but multi-source data, the validity of the working hypothesis.

The analysis first focused on the *North Korean system*, characterized by a high degree of redundancy, which can provide the system with greater robustness, suitable for a challenge full of unknowns and complexity. The organizational system is also characterized by considerable fluidity: organizations change over time, their hierarchical dependencies change, and many organisms respond transversally to different vertices. The agencies also use skills and resources in a hybrid way, shifting them as needed and reassigned as necessities change. The constant state of alert that characterizes the country's international posture also allows the prevalence of the practical function over the theoretical one. All these features highlight how the system of North Korean intelligence agencies is complex, albeit limited by an in-depth knowledge of how the system works. Other elements found were: the high level of training of the staff, whose age is probably low, at least in the technological sectors; the selective decentralization that emerges from the mandatory coexistence of the planning areas with those of execution; the fragmentation and specialization of sub-structures; the notable mutability of dependency relationships over time, even between line and staff bodies.

All these elements make the structure of the North Korean intelligence system compatible with an adhocratic organization, but the elements are not sufficient to make a statement in this sense, due to the scarcity of available material.

The *Israeli system*, on the other hand, which we can define as an eco-system between the public and private sectors, is characterized by elements that make it surely an adhocratic organization according to Mintzberg. Its reticular structure is based on different units, with high horizontal specialization of tasks and blurred differences between line and staff units. There is little formalization of behaviors and the coordination mechanisms is mainly based on mutual adaptation, while the decision-making power relating to the strategies to be pursued is distributed along the entire hierarchy. The Israeli system, like the North Korean one, is complex and adapted to deal with complex systems while remaining immersed in a complex system.

The HMR policies of the Israeli (eco)system also place particular emphasis on the valorization of young talents, both from the point of view of training, career and responsibility. In fact, the young people of the operational core have the responsibility to choose the resources to include in their teams, and then they migrate to large companies in the cyber, ITC and security fields, even abroad, or found start-ups in the sectors, sometimes helped by State.

The framework allows us to establish with certainty that the structure of the Israeli intelligence (eco)system is adhocratic.

Finally, the *French economic intelligence system* is a sub-sector of intelligence with its own peculiarities, both in relation to the rest of French intelligence and in relation to the economic intelligence of the rest of the world. The French system, like the Israeli one, shows strong points of contact between the public and the private, but this is not its peculiar element because in this case, unlike the Israeli one, despite the contact, the public remains public and the private remains private. The interaction between the two worlds is strong, but it represents only one element of the entire system, which is characterized by a multi-layered network structure, in which interactions occur both between nodes at the same level and between different layers, allowing to address the different sources of complexity that emerge from the sources of each different environment.

The highly qualified French economic intelligence system personnel operate in a complex and dynamic environment, and the macrostructure of the system, a multi-layer network, allows for the mixing of mechanisms of vertical and lateral connections

and selective decentralization, in a highly specialized and decentralized structure, even if under central coordination surveillance.

The structure of the French economic intelligence system therefore allows us to establish with reasonable certainty that its organization is of an adhocratic type.

Table 1: adhocratic elements found in the three case studies

	North Korean intelligence	***Israeli intelligence (eco)system***	***French economic intelligence***
Complex environment	Yes	Yes	Yes
Dynamic environment	Yes	Yes	Yes
Heterogeneous environment	Yes	Yes	Yes
Hostile environment	Yes	Yes	Yes
High level of training	Likely	Yes (from inside)	Yes (from inside and outside)
Young people in positions of responsibility	Likely	Yes	
Poorly formalized behavior		Likely	Likely
Lateral connections		Yes	Yes
Selective decentralization	Likely	Yes	Yes (mitigated)
Grouping on a "market" basis and mutual adaptation		Yes	Yes
Staff and line combinations	Likely	Likely	Yes
Type of Adhocracy		Likely operational	

The table contains some elements of the adhocratic systems found in the three national intelligence agencies. As it is possible to see, the quantity of positive findings is notable. The Israeli system stands out as the one most closely aligned with Mintzberg's adhocratic model, thanks to its low formalization, strong horizontal specialization, high decentralization, and mechanisms for mutual adaptation. Israeli intelligence is configured as an operational adhocracy, fostering an agile and innovative response to complex and constantly evolving problems.

The North Korean system, while featuring fluid and adaptable operational elements, differs significantly from the pure adhocratic model due to the excessive centralization of the decision-making process and its hierarchical nature, which severely limits the true autonomy of individual operational units.

Finally, France adopts a hybrid form that combines elements of adhocracy with more bureaucratic and formalized coordination mechanisms. The French multilevel network manages to ensure both stability and adaptability, representing an advanced form of mixed organization, capable of meeting the needs of a complex democratic system.

The study was limited to three intelligence realities and a generalization is not possible in an indiscriminate manner since, as already highlighted, each nation in this field uses different organizational, process and human resources management methods. In fact, it would not be impossible to find highly bureaucratized national intelligence structures. But we will return to this point in the final paragraph of the work.

2. Problems and limits of the adhocratic configuration in case studies

Given that the systems studied are characterized as adhocracies, we can now evaluate whether these systems have advantages and suffer limitations that usually afflict organizations structured according to this model. Again, since we cannot explore the inside of the intelligence agencies except indirectly, we will be limited, and we will limit ourselves to formulating hypotheses that should be confirmed in practice as far as possible. We will first focus on the limitations and problems, and then address the positive factors.

Adhocracies generally suffer from organizational ambiguity. The first level of suffering is the individual one, which affects those with a more structured mentality, who poorly tolerate the fluidity and confusion that an adhocracy can generate. The second level is the system one, in which the effects of the lack of bureaucracy are reflected on all members of the organization, including those who, due to personal predisposition, would be more inclined towards adhocracy.

In the case of intelligence agencies, a significant percentage of the members often have a military or police background and the habit of a highly structured, hierarchical and bureaucratized environment represents an element of intolerance towards adhocracy.

Furthermore, in general, intelligence agencies can also find themselves in situations that require a prompt response to an external threat, such as the outbreak of a military conflict involving their own nation or an imminent terrorist attack. In these situations, any uncertainty regarding responsibilities, skills, command, or any other organizational factor risks lowering the quality of the organization's outcome.

Even the danger of politicization of the organization, theorized by Mintzberg, is more current than ever in the scenario of intelligence agencies, whose activity, it should be remembered, is to provide structured information to the political decision maker.

This element, mixed with the strong individualism of professionals, which also characterizes the adhocratic structure, can lead to potentially traumatic risks of drift for the entire national security structure, which the intelligence agencies must protect. In fact, it should be remembered that the Ego represents one of the main levers (along with money, coercion and ideology) of recruitment by foreign espionage.

A further profile to consider is that adhocracy does not lend itself to carrying out ordinary and repetitive activities, due to its inefficiency and communication difficulties. The intelligence agencies, although often engaged in highly complex and risky operations that have magnified and spread their fame and myth, are also engaged in routine activities on a daily basis. One of these, for example, is the widespread control of all imports of Dual-Use material, i.e. tools, materials or substances that can be used both for legitimate purposes (medical, technological, etc.) and for illicit activities often connected with weapons of mass destruction. This type of activity, in addition to being completely ordinary in nature, is also accompanied by the risk that an error or delay in the control phase could produce devastating effects.

For all these reasons, the correct organizational structure of an intelligence agency should probably combine adhocratic substructures with more bureaucratized ones. But this thesis would require further investigation. For example, by exploiting the theory of High-Performance Organization (HPO), which offers a useful framework for analyzing and improving organizational performance, focusing on the key factors that favor its success, to provide a systematic approach that optimizes operational capacity and strategic contribution, maintaining a high level of adaptability in an evolving global landscape (de Waal, 2012).

3. Comparison of the three systems in addressing the challenges of a complex world

The three systems analyzed in this thesis present organizational models with very distinct characteristics.

The North Korean system has a highly centralized structure, dominated by the single figure of the Supreme Leader, although the model is enriched by elements of operational fluidity and functional redundancy, often attributable to a pragmatic interpretation of adhocracy. However, extreme centralization limits true operational autonomy, relegating peripheral units to subordinate roles aimed at maintaining internal security and political support for the regime.

In contrast, the Israeli model represents the ultimate expression of an adhocratic organization, in which highly decentralized decision-making and the operational autonomy of individual specialized units create a highly flexible and responsive structure. This model, enhanced by extremely dynamic human resources management geared toward developing young talent, allows for an agile and immediate response to emerging threats.

France, on the other hand, adopts a hybrid system based on a multi-level network, combining national agencies, ministries, and local structures. This inter-ministerial and territorial model combines traditional bureaucratic elements with more modern network approaches. While maintaining hierarchical and formalized forms, the French structure allows for a notable degree of adaptability through continuous interactions between public and private sectors, centers and peripheries. The integration of multiple institutional levels thus allows for a more balanced and robust governance of complexity than the North Korean system, although it lacks the extreme flexibility of the Israeli model.

Each model presents significant advantages and disadvantages when faced with the challenge of managing complexity. The North Korean system appears capable of reacting rapidly to threats through its combination of concentrated decision-making power combined with structural elements of fluidity and redundancy. However, the risk is that this speed translates into structural vulnerabilities due to the presence of a single decision-maker on whom all systemic lines converge, thus making the system more rigid in responding to external shocks or significant internal crises.

The Israeli model has proven to be the most efficient in managing complexity. Its adhocratic and highly decentralized nature allows for an immediate response to threats, thanks to a network of specialized units capable of interacting fluidly and dynamically. Israeli governance is also strengthened by the ability to continuously integrate expertise from external sources, creating an ecosystem in which knowledge flows freely between the public, private, and academic sectors, resulting in strong coevolution and continuous innovation.

The French system offers a middle ground, based on the strength of an integrated, multi-level network that effectively manages complexity through continuous and structured interactions between different entities. While this structure makes the French system less immediately responsive than the Israeli one, it allows for greater long-term stability and more harmonious management of relationships between different institutional levels and private economic actors.

Coevolution and adaptation to the challenges of complexity

Thanks to its co-evolutionary and adaptive capacity, Israel emerges as the most effective model. The continuous rotation of human resources, strong public-private integration, and constant technological innovation enable the Israeli system to address the challenges of complexity with dynamism and efficiency. The ability to anticipate change and adapt rapidly constitutes a clear competitive advantage.

France maintains a good level of adaptive effectiveness, guaranteed by a structured network that allows for rapid and targeted information flows. Interministerial and territorial management ensures a good capacity to respond to threats, although its lesser operational autonomy compared to Israel may slightly slow its adaptation times in extreme crisis situations.

North Korea, while capable of rapid and aggressive reactions, displays an adaptive capacity limited by its hierarchical rigidity. This significantly limits its ability to co-evolutionarily adapt to external and internal changes, exposing the system to the risk of instability in the event of systemic crises.

The following table summarizes the strengths and weaknesses of each system in addressing the challenges of a complex world.

Table 2: Strengths and weaknesses of the three intelligence systems

	Strengths	*Weaknesses*
North Korean Intelligence	Quick decision-making, tactical operational fluidity, offensive capacity.	Strategic rigidity, vulnerability due to extreme centralization, little real autonomy.
Israel intelligence (eco)system	High decentralization, continuous innovation, public-private integration.	Risk of dispersion, possible information fragmentation, high staff turnover that could compromise institutional memory.
French Economic Intelligence	Balance between stability and adaptability, multilevel integration, and inter-ministerial coordination capacity.	Greater bureaucratic formalization, slightly slower reaction times in extreme emergency situations.

4. Limits of the research and further possible investigation profiles

The research conducted also presents a series of ***limitations***:

1. The activities of intelligence agencies are covered by secrecy, often also imposed by criminal laws. The limited access to direct data prevents obtaining first-hand information through interviews, surveys or direct observations. The absence of these direct sources limits the depth of the analysis and forces us to rely on indirect and second-hand sources.

2. The use of indirect sources, such as gray literature and information disclosed through investigative journalism, can limit the reliability of conclusions. Indeed, such sources may be biased, incomplete, or even influenced by political agendas. Furthermore, intelligence

agencies tend not to publicly deny information, meaning that much of the information in gray literature may be hypothetical or unverified.

3. The choice to study only three agencies, although necessary for in-depth research, does not allow for the extension of the findings to all types of intelligence agencies, particularly those structurally very different from those discussed. The specific characteristics of each of the three countries studied also influence their approaches to organization and secrecy, and this also hinders the transferability of the findings to intelligence agencies in other countries with very different cultures or organizational structures.

4. Secrecy prevents the use of quantitative methods and access to large data sets, which could strengthen the robustness of the conclusions. The absence of these data makes it difficult to objectively measure adherence to the adhocratic organizational model, leaving many analyses at a qualitative or theoretical level.

5. The choice of cases based on specific characteristics of interaction with the outside world (e.g., the aggressive North Korean context, the Israeli collaborative ecosystem, the French multilevel network) limits the research to a typology of intelligence agencies with similar modes of interaction. This results in limited generalizability to all those intelligence organizational configurations that do not exhibit similar significant external interactions.

6. The research could be influenced by a specific bias, which occurs very rarely in academic research, which is the one originating from a voluntary action of sabotage and disinformation by other human beings. In fact, even gray literature, which constitutes a priority source in studies on intelligence agencies due to the secrecy that surrounds them, can often also be voluntarily manipulated by the agencies themselves in order to spread a fallacious image among adversaries and obtain a strategic advantage. Furthermore, although in some countries it is easier to approach at least some background elements of intelligence activity, thanks for example to parliamentary reports and independent control bodies, in other nations, characterized by more rigid political regimes, this path is precluded. This produces an unavoidable asymmetry in the study of agencies from different countries.

These limitations make this research an indirect and necessarily partial analysis of the organizational structures of intelligence agencies, which should therefore be interpreted as an exploration rather than a conclusive investigation. To expand research on the functioning of intelligence agencies and their organization, ***additional research approaches*** could be developed, aimed at overcoming some of the current limitations and exploring new dimensions of the phenomenon. Some possibilities are:

1. *A comparative analysis extended to other intelligence agencies*. One possible direction is to extend the case studies to a larger number of agencies, including countries with different

structures, cultures, and objectives, such as the United Kingdom, the United States, Russia, and China. This could also include intelligence agencies in medium-sized European countries, or specific contexts in Asia, Africa, or South America. This could identify common organizational characteristics or significant differences between agencies operating in different contexts, making the research more representative (Van Puyvelde, Coulthart, and Bruneau, 2017); (Gill, 2018).

2. *Research on the effects of digitalization and technology*. Another potential focus could be the impact of new technologies on the organizational structures and operational models of intelligence agencies, starting with artificial intelligence and quantum computing (Zegart, 2023); (Berkowitz and Goodman, 2000).

3. *Longitudinal study of the organizational evolution of intelligence agencies*. Research could follow a longitudinal approach to analyze how the structures of these agencies evolve over time, especially in response to external events such as terrorist attacks, scandals, or changes in the geopolitical landscape. This would allow us to understand how agencies adapt their organizational models to external changes, verifying the adoption or rejection of an adhocratic model over the long term (Zegart, 2007); (O'Connell, 2006).

4. *Analysis of interinstitutional relations*. Another interesting aspect concerns the study of the relationships and interactions between intelligence agencies and other national and international institutions, such as ministries, armed forces, private companies, and international partners. A greater understanding of the collaborations and tensions between these entities, especially in contexts where such interaction is more problematic, can shed light on how intelligence agencies manage conflicts of interest and balance secrecy with the demands of transparency and coordination (Lefebvre, 2013); (George & Rishikof, 2017).

5. *Impact of organizational culture and national characteristics*. Studying how national culture and institutional values influence the organization of agencies could provide a useful perspective to understand how different governance traditions, levels of transparency and political values shape the approach to intelligence. This type of research could highlight, for example, how democracies and authoritarian states structure their agencies differently based on institutional trust and internal control (Hastedt, 1996); (Weiss, 2014).

6. *Investigation of transparency and accountability approaches*. Transparency is often limited in intelligence agencies, but it would be worth exploring how some countries (e.g. the Nordic ones) manage to implement forms of control and accountability without compromising operational secrecy. Studying these practices could help identify new governance models that balance the right to security with the needs of accountability and

transparency towards the public (Van Puyvelde, Coulthart, & Bruneau, 2017); (Van Ginkel, 2012).

7. *Developing quantitative models for organizational analysis*. While direct quantitative data is limited, creating quantitative models based on secondary data (e.g. budget data, cyber-intelligence related expenditures, known staff numbers) could provide useful estimates. Statistical models and simulations could offer a rough view of the structure and operations of agencies, especially when combined with theoretical models (Behrman & Carley, 2003); (Axelrod & Cohen, 2000).

8. *Exploring other similar adhocratic structures in fields other than intelligence*. Based on the methodologies explored here, it would perhaps be interesting to apply the methodologies employed in this work in other areas characterized by secrecy, such as those of the military world and in particular the Special Forces, which represent the point of contact between the world of defense and that of intelligence. The research could also be applied to some religious realities and orders, characterized by great secrecy, whose social role has developed for centuries, and which have also recently become famous in the business field due to the lessons learned that they have been able to inspire in the field of leadership (Oleson & Cothron, 2016); (Laloux, 2014).

5. Policy Recommendations

In light of the analyses conducted in this thesis on the organizational structures of intelligence agencies in North Korea, Israel, and France, it is now possible to extrapolate some potential policy recommendations, which will be now exposed.

1. Effectiveness of the adhocratic system in intelligence agencies.

This study has highlighted how the adhocratic system, thanks to its high adaptability, proves to be a choice that significantly increases the operational effectiveness of intelligence agencies. The environment in which these agencies operate, characterized by unpredictability and changeability, is also consistent with the adhocratic choice. The Israeli and French experiences confirm the effectiveness of non-hierarchical and results-oriented organizational models, which allow for rapid and flexible responses. It is therefore desirable that policymakers seriously consider the implementation of adhocratic structures in strategic intelligence areas, such as those related to information technology, economics, and technology.

2. Integration of private sectors without risks for National Security

Integrating private sector expertise into intelligence agencies' activities appears to be an essential strategy for addressing contemporary threats, especially in the emerging fields of information and electronic technologies. At the same time, it is essential to prevent such integration from resulting in breaches of secrecy, which could compromise national security. The Israeli experience shows that it is possible to create a virtuous system of mutual exchange between intelligence and the private sector by applying rigorous protocols, regular security reviews, and careful selection of private partners. It is therefore recommended to encourage public-private partnerships, in order to increase the cultural, technical and self-regulatory depth of the agencies, while establishing clear and transparent governance of public-private relations, including strict rules regarding stakeholder selection, confidentiality, and information sharing.

3. Balancing flexibility and oversight in intelligence agencies

One of the critical points highlighted in the research concerns the importance of finding an optimal balance between operational flexibility and institutional control. Flexibility, typical of adhocratic organizations, while allowing for agile and adaptive responses, risks weakening political and democratic control mechanisms. It is therefore recommended that intelligence agencies' internal, as well as external, mechanisms be strengthened to achieve effective monitoring and control of their activities without compromising rapid decision-making. The French multilevel network model offers a valuable reference as it appears to combine multilevel operational agility with a clear, or at least effective, functional hierarchy.

4. Risks of decentralization of intelligence agencies

A decentralized decision-making process risks significantly increasing the fragmentation of responsibilities, which could lead to a loss of coherence in national strategies, also due to potential internal conflicts between the organization's different operational structures. The experiences of Israel and North Korea suggest that decentralization must be managed in a controlled manner to prevent deviations. It is therefore appropriate that decentralization always be accompanied by a clear command and control system that ensures overall coherence and effectiveness.

5.1. A possible application

To explore a possible practical application of the above, we will now analyze an Italian national security problem, proposing a solution that leverages adhocratic organization to address the complex challenges of a rapidly changing world. This world presents challenges in reconciling the judicial protection of individual rights, as required by the constitutional and legislative principles of democratically advanced states, particularly the Italian system, with the threats posed to national security by the international landscape (Frisia, 2022).

The rationale for this proposal stems directly from the literature review analyzed, which has highlighted three recurring needs in the study of intelligence agencies: (a) adopting organizational theory lenses to explain performance and failures; (b) reconciling secrecy and accountability; and (c) designing structures capable of adapting to highly uncertain environments. But this proposal also benefits from the results obtained by analyzing the three case studies outlined above, taking the appropriate strengths from each of them.

This final chapter seeks to apply these assumptions by translating them into an operational framework for solving the problem that will now be outlined.

The problem (1): The Italian legal system and public administration

The term "legal system" (Losano, 2002) refers to a complex set of concepts, doctrines, procedures, criteria, and actors, variously combined within different theories and primarily aimed—according to prevailing interpretations—at the application of the law rather than its mere understanding.

Numerous commentators have expressed criticism of the Italian legal system, for example accusing the judiciary of discouraging foreign investment due to various factors such as (Phillips, 2016): procedural delays; the pervasive reach of judicial action in virtually every area; the inconsistency of rulings caused by the lack of a hierarchical structure (indeed, as is well known, the Italian legal system does not provide for the systematic use of precedents. Only rulings of the Supreme Court, when sitting in joint session, oblige the individual sections of the Supreme Court to conform, and only then do the precedents acquire factual validity and, in any case, are not binding).

In response, the judiciary has often shifted the blame to other branches of government. The administrative branch is characterized by slowness and bureaucratic complexity, only partially mitigated by privatization, outsourcing, and transparency reforms (Chieppa, 2010). The legislative branch, meanwhile, is criticized for its unclear, ineffective, and multilayered legal framework (Mattarella, 2011).

Furthermore, some (Battini and Decarolis, 2019) argue that the Italian legal system has favored the proliferation of "defensive" legal actions, particularly within the public administration, which is largely staffed by officials with legal training.

Eliminating the dysfunctions of such a complex system—rooted, in part, in the bureaucracies introduced by foreign rulers before Italian unification—is clearly unrealistic in the short term. Nonetheless, there are situations in which rapid, decisive, and, above all, effective responses are essential to safeguarding the overriding national interests.

The problem (2): Threats to National Security on the Legal and Administrative Front

In addition to military, diplomatic, or illegal threats posed through direct action, there are a number of situations in which foreign actors attempt to harm the state's national and international interests through strictly legal means. Indeed, familiarity with the weaknesses of the judicial system and public administration can be exploited by adversaries, both state and non-state, to delay, hinder, or even nullify threat response mechanisms.

While, for example, during the Cold War, CoCom export control decisions could be effectively implemented within the legal systems of the time, today the monitoring and regulation of dual-use goods for non-proliferation purposes (assigned by Article 6, paragraph 2, of Law 147/2007 to the AISE, to which, however, the armed forces, police forces, and the judiciary also contribute, within their respective spheres of competence) must comply with legal requirements, particularly those of contemporary administrative law. The reforms of the 1980s and 1990s and subsequent legislative and case law adjustments introduced transparency, stakeholder participation, and broad protections for private interests in administrative processes. These reforms are essential in modern democracies, as they allow private parties such as citizens, companies, and other stakeholders to defend their rights in court. But at the same time, they allow these tools to be used, in a distorted manner, by individuals intent on undermining national security.

As a result, some of the efforts to protect national security have shifted to a new battlefield: the legal arena, which includes both administrative procedures and potential administrative litigation.

Other areas in which foreign state or non-state actors with interests conflicting with Italian national security could seek to exploit the judicial system include: control of strategic assets, influence operations, interference campaigns, the establishment of operational bases on national territory, and other threats to national interests that may only become visible upon implementation, necessitating a legal-administrative response.

Legal conflicts involving parties with objectives contrary to national security present unique challenges. First, the Italian legal system does not provide adequate confidentiality protections for national security concerns (Sfroza, 2004). Unlike the British procedural tradition, which provides specific mechanisms (Passaglia, 2012) that allow classified information to be presented to a judge without its public disclosure, the Italian legal system enshrines the constitutional principle of due process and its corollary of adversarial proceedings in all proceedings, including administrative ones (Ieva, 2002). These principles are incompatible with the introduction of evidence that is not fully and effectively available to the parties seeking to protect their rights and interests in such proceedings.

Furthermore, the requirement of procedural equality (all parties enter the proceedings in symmetrical and equal positions) and the notion of justice (which rejects any concept akin to the "right of the strongest") prevent state administrations from exercising influence in court. The administration can indeed represent the public interest, but such interest can only enter the process through judicially valid claims (Spuntarelli, 2012). Furthermore, adversarial proceedings prevent the use of undisclosed documents or testimony, including confidential police or intelligence and security reports.

If authorities were tempted to influence the judiciary by submitting classified reports, such a move—in addition to potentially being overturned by higher courts—could have negative consequences, such as:

a) implicitly revealing that the alleged fact cannot be proven otherwise;

b) creating an opening through which the judiciary or the opposing party could attempt to obtain the original documents, either through a court disclosure order (against which the only recourse would be to invoke state secrecy) or through the private party's right of access to administrative records. These documents, although not formally classified, may nevertheless contain information best kept confidential.

A Solution: Strategic Approaches to the Problem

To mitigate the risks to national security arising from the exploitation of vulnerabilities in the legal system and public administration, it is essential to foster a culture of national security among public officials. Although this cultural campaign has been ongoing for some time (Cornei, 1995), its results remain slow and uncertain. Career anxieties—exacerbated by current performance evaluation systems (Linee guida, 2018)—or adverse local case law can present substantial obstacles.

That said, Italian legal culture can also be characterized by considerable creativity (Pascuzzi, 2013), both in the drafting and application of rules.

The strategy proposed here involves a structured and forward-looking approach starting from the embryonic stages of legal disputes, well before the matter reaches the courtroom. For example, in administrative proceedings, key elements such as the communication of rejection, the analysis of the opposing party's arguments, and the reasoning for the preliminary decision must be part of a broader strategic vision. Time is also of the essence, as although legal discussions typically begin with lengthy written exchanges, their decisive phases can escalate rapidly and take the parties by surprise. This context is therefore characterized by a high level of environmental complexity, both by virtue of the considerable variability of the cases that could fall within these categories and by the varied skills required to address these issues, including, for example: knowledge of administrative law, a vision for the protection of national security, knowledge of the functioning of intelligence services, legal creativity, attention to the protection of rights, respect for the skills of the various actors involved (judiciary, state attorneys, perhaps the police, intelligence services, national agencies, public bodies, private companies, etc.).

This operational proposal also finds support in the literature review above. It aims to integrate organizational structures with expertise (Zegart, 2023), addresses the challenges of multilevel oversight in balancing secrecy and accountability (Van Puyvelde, Coulthart, & Bruneau, 2017), and suggests a broad and diverse cognitive framework that draws on multidisciplinary sources (Gill & Phythian, 2018). Such a framework should also resolve the tension between central and distributed authorities (Arquilla & Ronfeldt, 2001) and design its organizational architecture to address current challenges (Behrman & Carley, 2003).

But insightful elements also emerge from monographic cases, which demonstrate that effective solutions emerge when institutional design bridges the gap between law and practice. In Israel, the extensive intelligence-defense-academia-industry network enhances horizontal coordination and agile delegation without losing substantive legality. In France, economic intelligence policy has institutionalized inter-ministerial coordination and information exchange to protect the national interest, reducing procedural friction and decision-making times. This evidence supports the need for flexible organizational tools in the Italian context as well. Finally, the study, albeit partial, on North Korea highlights how structural redundancy and fluidity appear to increase the system's reactivity. Even in a non-democratic regime, this organizational lesson remains useful: when faced with actors capable of exploiting legal and bureaucratic constraints, a rapid and cross-functional response capacity, anchored in streamlined procedures, is necessary.

The proposed solution, therefore, is to create an adhocratic structure that, through the highly skilled members and the use of simplified and streamlined (though law-abiding) procedures, can intervene to protect national security with rapid implementation, adaptability, and multidisciplinary synergy, ideal for addressing the complex challenges of the current socioeconomic context.

One possible model could include an adhocratic structure to support both administrative bodies in issuing decisions (pre-litigation phase) and the State Attorney's Office in strategic planning (actual litigation phase). This structure could be established by ministerial decree (or preferably inter-ministerial) and would be tasked with providing added value through specific sectoral expertise, research, and reflection on how to best protect national security in the legal and judicial sphere.

The structure's mission would be based on the objectives of the individual countermeasures. For example, to counter the export of dual-use goods, it would rely on the surveillance, enforcement, and deterrence obligations established by Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. However, if it were deemed appropriate to grant the adhocratic agency even substitute powers, its existence would have to be based on a law, and the substitute power would be activated only through high-level administrative acts, typically presidential decrees of the Council of Ministers (DPCM).

Such a body could also receive direct reports from intelligence and security services regarding threats to national security requiring immediate attention. Nevertheless, priorities and operational methods should remain firmly within the purview of policymakers.

The most appropriate institutional location for the group would be within the Presidency of the Council of Ministers, where it could serve as a bridge between the Public Administration, the Judiciary, and the national security defense structure. Its membership should include both legal experts in its various branches (lawyers, retired magistrates, university professors) with a focus on creative application, as well as experts in international and diplomatic settings with applied strategic expertise, and experts familiar with issues related to national security, intelligence operations, and the legal management of classified information. The direct involvement of active-duty intelligence officers should be avoided, as their presence could be seen as unlawful interference by intelligence agencies in the work of the judiciary, a circumstance that conflicts with the constitutional principles of modern democracies.

Consistent with the Israeli case, the body's composition could also include, in a purely supportive role, individuals with specific roles (boundary spanners) from public administration, police forces, academia, intelligence, and strategic companies, possibly with rotation cycles and joint training. The French experience with economic intelligence, however, suggests a lean inter-ministerial “control room” for strategic direction and ex ante legitimation of extraordinary actions. From a resilience perspective, the redundancy of critical skills, along the lines of the DPRK model, could take on strategic value and should not be interpreted as mere bureaucratic duplication.

The coordinated use of interdisciplinary skills would allow for the proper identification of objectives, strategy design, and the creation of a motivational framework capable of withstanding judicial scrutiny at all levels. These efforts should remain dynamic and iterative, consistent with the recurring nature of strategic action (Luttwak, 2001), which requires continuous adjustment.

The organization's composition should also incorporate ethical standards and professional culture to align its mission with its values and procedures (Omand & Phythian, 2018) and provide for internal accountability mechanisms in addition to external oversight (Van Puyvelde, 2021).

In addition to direct operational interventions, the organization could devote its remaining time to strengthening its understanding of the legal battlefield through the analysis and systematization of lessons learned, the creative use of legal tools, case study reviews, administrative benchmarking, strategic assessment, and the provision of training, refresher courses, legislative advice, and both classified and public documentation. Overall, both operational and analytical activities would clearly serve the broader interests of national security.

The working group would have to maintain a stable core and a long-term organic perspective, which would make its structure incompatible with that of a simple task force.

The use of task forces is increasingly accepted in Italian legal and ministerial culture. Recent examples include:

- the "Multidisciplinary Expert Group for Data-Based Technological Solutions to Manage the COVID-19 Health, Economic and Social Crisis", established in March 2020 by Interministerial Decree of the Minister for Technological Innovation and Digital Transition, in agreement with the Ministry of Health, it is made up of experts in various fields including: healthcare, economics, big data, technology, privacy legislation, and more;
- the "State Police Task Force for Intelligence and Investigative Operations Related to Unauthorized Maritime Landings", established in 2014 by the Central Directorate of Immigration and Border Police, Department of Public Security, Ministry of the Interior, it currently involves the cooperation of personnel with a wide variety of previous experience: investigative activities on foreign organized crime, border control, counterterrorism, and administrative management of foreigners.

Such bodies offer agility, rapid deployment, adaptability, and multidisciplinary synergy – ideal for tackling the complex challenges of today's socio-economic environment.

But at the same time, the task force is characterized by two fundamental elements:

- the task force's ontologically temporary structure;
- and the permanence of its members within their original administrations, to which they can return at any time for a variety of needs and reasons.

These two elements conflict with the purpose and specifics of this adhocratic structure. Indeed, the temporary nature of a task force would hinder organizational learning, which is crucial here, so that the experiences acquired over time would only fuel the learning process of individual members. The creation of an adhocratic structure would instead allow for the implementation of policies that enhance organizational learning, as well as promoting training and professional development, thus contributing to the creation of a shared knowledge base, useful for national security and benefiting the state as a whole. Furthermore, the permanence of members of a potential task force within their respective administrations would create significant difficulties with any active members of the intelligence agencies, whose presence would be unwelcome in modern democratic systems. Conversely, a stable adhocratic structure would allow for the acquisition of personnel with the necessary skills, allowing them to transition to different administrations.

Conclusions

In summary, the proposed framework builds on the research trajectories identified in the literature review, such as information ecosystems with open metrics (Zegart, 2023), networked governance capable of co-evolution (Arquilla & Ronfeldt, 2001), and multilevel oversight to preserve democratic legitimacy (Van Puyvelde, Coulthart, & Bruneau, 2017).

Furthermore, case studies show that the proposed structure would possess numerous characteristics typical of an adhocracy:

- Networked governance and rapid experimentation (Israel)
- Inter-ministerial coordination and protection of national economic interests (France);
- Selective redundancy and adaptability (North Korea);
- A flexible and adaptable structure, based on multidisciplinary expertise rather than rigid hierarchies (Israel and France);
- A strong focus on innovative and creative solutions to complex problems (Israel and France).

The ability to rapidly assemble multidisciplinary teams capable of dynamically integrating and disintegrating based on contingent needs is precisely what Mintzberg identifies as essential for tackling problems that are unstructured or difficult to categorize according to traditional theoretical frameworks.

The proposed body perfectly meets the need for a complex approach, highlighted by the very nature of the threats described. The complexity of the Italian legal and administrative system and its relative vulnerability in terms of national security require a rapid and adaptive response capacity and he presence of diversified professional skills, capable of interacting synergistically in a non-hierarchical environment, would enable effective management of emerging issues.

At the same time, such a group would be particularly suited to addressing the challenges of an increasingly complex environment, adopting a co-evolutionary and proactive organizational model. Growing complexity requires predictive and adaptive capabilities, intrinsic elements of an organizational structure oriented towards strategic creativity and operational flexibility. The proposed model would enable anticipation of regulatory and administrative developments, rapidly adapting to changes in the operational environment. The organization, thanks to analysis, administrative benchmarking, and ongoing strategic review of its operations, would therefore be able not only to react to events, but also to proactively anticipate them, developing solutions that can co-evolve with the problems themselves and the environment that generates them.

The combination of these characteristics highlights the utility of an interdisciplinary approach to national security management. Interdisciplinarity, the third key aspect of the proposal, emerges as a critical success factor in addressing the complexity of the current landscape. The ability to integrate legal, administrative, strategic, and intelligence expertise is not only desirable, but essential. Hybrid threats that exploit legal and administrative vulnerabilities necessarily require an interdisciplinary understanding that transcends individual disciplines and traditional organizational boundaries.

Therefore, a structure organized according to the adhocracy paradigm would not only be suitable, but it is hoped that it will represent the best possible response to proactively and co-evolvingly address the growing complexity of threats. Adaptability and operational speed, combined with the strengthening of interdisciplinary expertise, would allow to overcome traditional structural rigidities, offering effective and timely strategic responses. This approach would also ensure a continuous process of organizational and institutional learning, which would not only foster individual learning but also develop a shared knowledge base, essential for ensuring the resilience of the country system.

REFERENCES

Allen, P., Maguire, S., McKelvey, B. (2011). The SAGE Handbook of Complexity and Management. SAGE.

Abelson, D. E. (2009). Do Think Tanks Matter? Assessing the Impact of Public Policy Institutes. McGill-Queen's University Press

Abigail Klein Leichman. (2017, 26 ottobre). 12 Israelis making a mark on Boston's tech scene. Israel21C. https://www.israel21c.org/12-israelis-making-a-mark-on-bostons-tech-scene (Last accessed January 20, 2025)

Adam, P. (2013). Assemblée Nationale, XIV Législature, Compte rendu n° 52. Commission de la défense nationale et des forces armées - Audition de M. Jean-Paul Garcia, directeur national du renseignement et des enquêtes douanières au ministère de l'Économie et des finances (DNRED).

Adam, P. (2013). Assemblée Nationale, XIV Législature, Compte rendu n° 55. Commission de la défense nationale et des forces armées - Audition du général Didier Bolelli, directeur du renseignement militaire (DRM).

Adam, P. (2013). Assemblée Nationale, XIV Législature, Compte rendu n° 56. Commission de la défense nationale et des forces armées - Audition du préfet Érard Corbin de Mangoux, Directeur général de la sécurité extérieure (DGSE).

Ahronheim, A. (2020, 2 luglio). Meet the unit behind the scenes of the IDF's precision warfare. The Jerusalem Post. https://www.jpost.com/israel-news/meet-the-unit-behind-the-scenes-of-the-idfs-precision-warfare-633617 (Last accessed January 20, 2025)

Allen-Ebrahimian, B. (2018). Inside China's Surveillance State. Foreign Policy

Alon, U. (2006). An Introduction to Systems Biology: Design Principles of Biological Circuits. Chapman & Hall/CRC

Analysis | An Indian nuclear power plant suffered a cyberattack. Here's what you need to know. (n.d.). Washington Post. https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/ (Last accessed January 20, 2025)

Andreadis, N. (2009). Learning and organizational effectiveness: A systems perspective. Performance Improvement, 48(1), 5–11. https://doi.org/10.1002/pfi.20043

Andregg, M. M. (2013). Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War. Intelligence and National Security, 28(5), 660–678. https://doi.org/10.1080/02684527.2013.820255

Andrew, C. M. (2018). The secret world: A history of intelligence. Allen Lane, an imprint of Penguin Books.

Arquilla, J., & Ronfeldt, D. (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation.

Atkinson, C. (2015). Evaluating counterterrorism performance: A comparative study. Journal of Policing, Intelligence and Counter Terrorism, 10(2), 179–180. https://doi.org/10.1080/18335330.2015.1089647

Axelrod, R. M., & Cohen, M. D. (2000). Harnessing complexity: Organizational implications of a scientific frontier. Basic Books, a member of the Perseus Books Group.

Banks, M. A. (2014). Understanding grey literature and its role in scholarly communication. Oxford University Press.

Barabási, A.-L. (2009). Linked: How everything is connected to everything else and what it means for business, science, and everyday life. Plume print; authorized reprint of a hardcover ed. publ. by Perseus Publ

Barnea, A. (2020). Strategic intelligence: A concentrated and diffused intelligence model. Intelligence and National Security, 35(5), 701–716. https://doi.org/10.1080/02684527.2020.1747004

Barucija, A. (2020). The Historical Evolution of Israeli Intelligence. American Intelligence Journal, 37(1), 178–182. https://www.jstor.org/stable/27087696

Bason, C. (2018). Leading public sector innovation: Co-creating for a better society (Second edition). Policy Press.

Battini, S., & Decarolis, F. (2019). L'amministrazione si difende. Rivista trimestrale di diritto pubblico, (1), 293–320. https://www.irpa.eu/rivista/rivista-trimestrale-di-diritto-pubblico-n-1-2019-gennaio-marzo/ (Last accessed June 16, 2025)

Beer, S. (1979). The Heart of Enterprise. Wiley

Behar, R. (2006, 11 maggio). Inside Israel's Secret Startup Machine. Forbes. https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/?sh=62d571931a51 (Last accessed January 20, 2025)

Behrman, R., Carley, K. M. (2003). Modeling the Structure and Effectiveness of Intelligence Organizations: Dynamic Information Flow Simulation. https://doi.org/10.1184/R1/6623966.V1

Berkowitz, B., Goodman, A. (2000). Best Truth: Intelligence in the Information Age. Yale University Press.

Berlière, J.-M. (2018a). Renseignements généraux. 2. Le service des Renseignements généraux de la préfecture de police (RG-PP). In Polices des temps noirs (pp. 1000–1019).

Berlière, J.-M. (2018b). Surveillance du territoire. In Polices des temps noirs (pp. 1239–1253). Perrin. https://doi.org/10.3917/perri.berli.2018.01.1239

Berman, E., Fox, J. (2016). Learning from Failure in the Intelligence Community: A Framework for the Future. International Journal of Intelligence and CounterIntelligence, 29(1), 1–25. https://doi.org/10.1080/08850607.2015.1083314

Bermudez, J. S. J. (2010). A New Emphasis on Operations Against South Korea. A Guide to North Korea's Intelligence Reorganization and the General Reconnaissance Bureau. 38 North. www.38north.org/?p=920 (Last accessed January 20, 2025)

Best, R. A. (2011). The Intelligence Community: Organizational Chart. Congressional Research Service.

Blancke, S. (2009). North Korean Intelligence Structures. North Korean Review, 5(2), 6–20. https://doi.org/10.3172/NKR.5.2.6

Boardman, C. H. (2006). Organizational Culture Challenges to Interagency and Intelligence Community Communication and Interaction. https://doi.org/10.21236/ADA460017

Boraz, S. C., Bruneau, T. C. (2006). Reforming Intelligence: Democracy and Effectiveness. Journal of Democracy, 17(3), 28–42. https://doi.org/10.1353/jod.2006.0042

Born, H., & Caparini, M. (Eds.). (2009). Democratic control of intelligence services: Containing rogue elephants (Reprinted). Ashgate.

Born, H., Leigh, I., Wills, A. (2015). Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies. Geneva Centre for Democratic Control of Armed Forces (DCAF).

Bouillon, S. (2023). Secrétariat général de la défense et de la sécurité nationale, Rapport d'Activité 2022.

Bouthillier, F., & Shearer, K. (2003). Assessing competitive intelligence software: A guide to evaluating CI technology. Information Today.

Boyd, J. R. (1987). A discourse on winning and losing. http://dnipogo.org/john-r-boyd/ (Last accessed June 16, 2025)

Brady, A.-M. (2008). Marketing Dictatorship: Propaganda and Thought Work in Contemporary China. Rowman & Littlefield

Bragg, M. (1996). Reinventing Influence. London: Pitman Publishing

Brown, S. L., & Eisenhardt, K. M. (1997). The Art of Continuous Change: Linking Complexity Theory and Time-Paced Evolution in Relentlessly Shifting Organizations. Administrative Science Quarterly, 42(1), 1. https://doi.org/10.2307/2393807

Brown, S. L., Eisenhardt, K. M. (1997). The art of continuous change: Linking complexity theory and time-paced evolution in relentlessly shifting organizations. Administrative Science Quarterly, 42(1), 1-34.

Bruneau, T. C. (2007). Challenges to Effectiveness in Intelligence due to the Need for Transparency and Accountability in Democracy. https://doi.org/10.21236/ADA441720

Bruning, P. F., & Campion, M. A. (2018). A Role–resource Approach–avoidance Model of Job Crafting: A Multimethod Integration and Extension of Job Crafting Theory. Academy of Management Journal, 61(2), 499–522. https://doi.org/10.5465/amj.2015.0604

Camazine, S., Deneubourg, J. L., Franks, N. R., Sneyd, J., Theraulaz, G., Bonabeau, E. (2001). Self-organization in biological systems. Princeton University Press.

Cambon C. (2020). Délégation Parlementaire au Renseignement. Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020.

Capra, F. (1996). The Web of Life: A New Scientific Understanding of Living Systems. Anchor Books

Carayon B. (2003). Intelligence économique, compétitivité et cohésion sociale (p. 103). https://www.vie-publique.fr/rapport/26501-intelligence-economique-competitivite-et-cohesion-sociale (Last accessed January 20, 2025)

Carayon B. (2006). A armes égales: Rapport au Premier ministre. https://www.vie-publique.fr/rapport/28581-armes-egales-rapport-au-premier-ministre (Last accessed January 20, 2025)

Casarini, N. (2012). The Role of Think Tanks in China. Europe China Research and Advice Network

Cavelty, M. D., Wenger, A. (2020). Cyber Security Meets National Security: Organizational Responses to Cyber Threats. Contemporary Security Policy, 41(1), 5–29. https://doi.org/10.1080/13523260.2019.1677322

Center for Strategic and International Studies (CSIS). Intelligence, Surveillance, and Reconnaissance. https://www.csis.org/programs/intelligence-surveillance-and-reconnaissance (Last accessed January 20, 2025)

Chanlett-Avery, E., Campbell, C. E., Manyin, M. E., Mackey, W., & Nikitin, M. B. D. (2018). North Korea: U.S. Relations, Nuclear Diplomacy, and Internal Situation (Congressional Research Service Report No. R41259). https://crsreports.congress.gov/product/pdf/R/R41259 (Last accessed January 20, 2025)

Chanlett-Avery, E., Rosen, L. W., Rollins, J. W., & Theohary, C. A. (2017). North Korean Cyber Capabilities: In Brief (Congressional Research Service Report No. R44912). https://sgp.fas.org/crs/row/R44912.pdf (Last accessed January 20, 2025)

Chieppa, R. (2010). Il codice del processo amministrativo alla ricerca dell'effettività della tutela. In Il Codice del processo amministrativo. Commento a tutte le novità del giudizio amministrativo. Milano: Giuffrè.

Chilton, P., Ilchman, W. F. (1983). Knowledge, politics, and public policy. Lexington Books.

Cnrlt. (2018). La CNRLT et la communauté française du renseignement: Revue Défense Nationale, N° 813(8), 9–13. https://doi.org/10.3917/rdna.813.0009

Commission nationale de contrôle des interceptions de sécurité: 21e rapport d'activité 2012-2013. (2015). La documentation française.

Commission nationale de contrôle des interceptions de sécurité: 22e rapport d'activité 2013-2014. (2015a). La documentation française.

Commission nationale de contrôle des interceptions de sécurité: 23e rapport d'activité 2014-2015. (2015b). La documentation française.

Commission nationale de contrôle des techniques de renseignement. 7^ Rapport d'activité 2022.

Cordey, S. (2019). Trend Analysis: The Israeli Unit 8200 – An OSINT-based study. Center for Security Studies (CSS).

Corneri, A. (1995). Intelligence diffusa e cultura dell'intelligence. Per Aspera ad Veritatem, (1). https://gnosis.aisi.gov.it/sito/Rivista1.nsf/servnavig/1 (Last accessed July 20, 2025)

Cornut Gentille F. (12/10/2017). Assemblée Nationale, Constitution du 4 Octobre 1958, Quatorzième Législature, N. 273. Rapport fait au nom de la Commission des Finances, de l'Economie Générale et du Contrôle Budgétaire sur le Projet de loi de Finances pour 2018 (n° 235). Annexe n° 13, Défense: préparation de l'avenir.

Cousseran, J.-C., & Hayez, P. (2021). Chapitre 12. La tentation de l'économie pour le renseignement. In Nouvelles leçons sur le renseignement (pp. 329–351). Odile Jacob. https://www.cairn.info/nouvelles-lecons-sur-le-renseignement--9782738154569-p-329.htm (Last accessed January 20, 2025)

Creemers, R. (2017). China’s Concept of Cyber Sovereignty: Rhetoric and Realization. Hague Journal on the Rule of Law, 9(1), 25–42

Cusset, F. (2020). Une histoire (critique) des années 1990: De la fin de tout au début de quelque chose. La Découverte.

Dahl, E. J. (2019). Intelligence and surprise attack: Failure and success from Pearl Harbor to 9/11 and beyond. Georgetown University Press.

Dasquié, G. (1999). Secrètes affaires: Les services secrets infiltrent les entreprises. Flammarion.

De Toni, A. F. (2021a). L’auto-organizzazione quale strumento di gestione della complessità. L’Arco di Giano, (108), 75–87

De Toni, A. F. (2021b). Rifondare il management sulla prospettiva della complessità. FOR - Rivista per La Formazione, 3, 13–16. https://doi.org/10.3280/FOR2021-003004

De Toni, A. F. (2024). Decalogo della complessità. Agire, apprendere e adattarsi nell’incessante divenire del mondo. Guerini e Associati

De Toni, A. F., De Zan, G. (2020). Il dilemma della complessità. Metodologie di assessment e casi aziendali. Guerini Next

De Toni, A. F., Pessot, E., Matarazzo, L., Cisilino, C. (2022). La nave e l’aliante: Apprendimento organizzativo come risposta sistemica alla complessità dei progetti. Guerini Next.

de Waal, A. A. (2012). “What Makes a High Performance Organization: Five Validated Factors of Competitive Advantage That Apply Worldwide”. Global Professional Publishing.

Delbecque E. (2005). L’intelligence territoriale: Portrait d’un concept opérationnel. Défense Nationale, 11(680), 122–130.

Denécé, E., & Arboit, G. (2010). Intelligence Studies in France. International Journal of Intelligence and CounterIntelligence, 23(4), 725–747. https://doi.org/10.1080/08850607.2010.501694

Dgse. (2018). La DGSE au cœur des cinq fonctions stratégiques: Enjeux et perspectives: Revue Défense Nationale, N° 813(8), 14–19. https://doi.org/10.3917/rdna.813.0014

Dgsi. (2018). DGSI, chef de file de la lutte antiterroriste en France: Revue Défense Nationale, N° 813(8), 20–22. https://doi.org/10.3917/rdna.813.0020

Dombrowski, P., Gentry, J. A. (2018). Evaluating Intelligence Performance: Balancing Metrics and Mission. Intelligence and National Security, 33(6), 789–805. https://doi.org/10.1080/02684527.2018.1436604

Dorsey, J. M. (2021). China and the Middle East: Venturing into the Maelstrom. Palgrave

Doz, Y. L., Kosonen, M. (2008). Fast Strategy: How Strategic Agility Will Help You Stay Ahead of the Game. Pearson Education

Drm. (2018). Quels défis et quelle stratégie pour la DRM dans la décennie qui s'ouvre ?: Revue Défense Nationale, N° 813(8), 23–27. https://doi.org/10.3917/rdna.813.0023

Drsd. (2018). Deux facettes de la contre-ingérence de défense: Protection des forces en opérations extérieures et sécurité des salons d'armement: Revue Défense Nationale, N° 813(8), 28–32. https://doi.org/10.3917/rdna.813.0028

Dukalskis, A., & Joo, H.-M. (2021). Everyday Authoritarianism in North Korea. Europe-Asia Studies, 73(2), 364–386. https://doi.org/10.1080/09668136.2020.1840517

Dumas, F., & Buffet, F. N. (2021). Rapport public fait au nom de la Délégation Parlementaire au Renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021.

Dunbar, C., Weber, T. (2014). Organizational Learning in U.S. Intelligence Agencies: Pitfalls and Prospects. Public Administration Review, 74(6), 741–753. https://doi.org/10.1111/puar.12255

Eisenhardt, K. M., & Brown, S. L. (1998). Competing on the Edge: Strategy as Structured Chaos. Long Range Planning, 31(5), 786–789. https://doi.org/10.1016/S0024-6301(98)00092-2

European Union. (2009). Council Regulation (EC) No. 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009R0428 (Last accessed January 20, 2025)

Europol. (2017). Handling Codes and Source Evaluation System. European Union Agency for Law Enforcement Cooperation.

Fair, C. C. (2014). Fighting to the End: The Pakistan Army's Way of War. Oxford University Press

Faligot, R., & Krop, P. (1999). DST Police secrète. Flammarion.

Faligot, R., Guisnel, J., & Kauffer, R. (2013). Histoire politique des services secrets français: De la seconde guerre mondiale à nos jours. La Découverte.

Faure, C. (2007). Bref historique des services de renseignement et de sécurité français contemporains: Revue Historique Des Armées, n° 247(2), 70–81. https://doi.org/10.3917/rha.247.0070

Federal Bureau of Investigation. (2012). Source and information evaluation manual. U.S. Department of Justice.

Fernandez, S., Cho, Y. J., & Perry, J. L. (2010). Exploring the link between integrated leadership and public sector performance. The Leadership Quarterly, 21(2), 308–323. https://doi.org/10.1016/j.leaqua.2010.01.009

Fialka, J. J. (1997). War by other means, Economic Espionage in America. New York: W. W. Norton & Co.

Fitsanakis, J. (2015). North Korean Intelligence and the Making of a National-Security State. In S. Blancke (Ed.), East Asian Intelligence and Organised Crime: China, Japan, North Korea, South Korea, Mongolia (1. Aufl, pp. 317–320). Köster.

Friedman, J. A., & Zeckhauser, R. (2012). Assessing Uncertainty in Intelligence. Intelligence and National Security, 27(6), 824–847. https://doi.org/10.1080/02684527.2012.708275

Friedman, J. A., Zeckhauser, R. J. (2015). Handling and Mishandling Estimative Probability: Likelihood, Confidence, and the Weighting of Evidence. Intelligence and National Security, 30(1), 1–30. https://doi.org/10.1080/02684527.2013.820259

Frisia, M. (2017). Strategia e intelligence. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/strategie-intelligence-Frisia.pdf (Last accessed January 20, 2025)

Frisia, M. (2022). Pubblica Amministrazione, Sistema Giuridico italiano e Sicurezza Nazionale: Una proposta di approccio strategico. In CASD (Ed.), Documento finale di sintesi Dibattito sulla Difesa e Sicurezza Sistemica (pp. 409–416). CASD, Centro Alti Studi Difesa. ISBN 978-88-31203-80-7

Garicano, L., Posner, R. A. (2005). Intelligence Failures: An Organizational Economics Perspective. Journal of Economic Perspectives, 19(4), 151–170. https://doi.org/10.1257/089533005775196723

George, A. L., Bennett, A. (2005). Case studies and theory development in the social sciences. MIT Press.

George, R. Z., Rishikof, H. (2017). The National Security Enterprise: Navigating the Labyrinth. Georgetown University Press.

Gill, P. (2007). Evaluating intelligence oversight committees: The UK Intelligence and Security Committee and the 'war on terror.' Intelligence and National Security, 22(1), 14–37. https://doi.org/10.1080/02684520701200756

Gill, P. (2018). The way ahead in explaining intelligence organization and process. Intelligence and National Security, 33(4), 574–586. https://doi.org/10.1080/02684527.2018.1452566

Gill, P., Phythian, M. (2012). Intelligence in an Insecure World (2nd ed.). Polity Press.

Gill, P., Phythian, M. (2018). Intelligence in an insecure world. Polity Press.

Gokhale, S. (2018). The role of grey literature in academic research. Information Today.

Goldman, J. (2015). The US Intelligence Community: An Introduction. Rowman Littlefield.

Gomart, T., & Frank, R. (2020). Double détente: Les relations franco-soviétiques de 1958 à 1964. Éditions de la Sorbonne.

Goodtree, D. (2016). The Massachusetts Israel Economic Impact Study. NEIBC.

Green, T. (2016, August 23). Why spies make the best entrepreneurs. Insider. https://www.businessinsider.com/israeli-cyber-spies-are-becoming-top-entrepreneurs-2016-8?r=US&IR=T (Last accessed January 20, 2025)

Guilhon, A. (2016). Intelligence économique: S'informer, se protéger, influencer. Pearson.

Guisnel, J., & Korn-Brzoza, D. (2017). Au service secret de la France. Éditions de La Martinière.

Haggard, S., & Noland, M. (2010). Reform from below: Behavioral and institutional change in North Korea. Journal of Economic Behavior & Organization, 73(2), 133–152. https://doi.org/10.1016/j.jebo.2009.09.009

Hamel, G., Zanini, M. (2018). Humanocracy: Creating Organizations as Amazing as the People Inside Them. Harvard Business Review Press.

Hammond, T. H. (2010). Intelligence Organizations and the Organization of Intelligence. International Journal of Intelligence and CounterIntelligence, 23(4), 680–724. https://doi.org/10.1080/08850601003780987

Harju, L. K., Kaltiainen, J., & Hakanen, J. J. (2021). The double-edged sword of job crafting: The effects of job crafting on changes in job demands and employee well-being. Human Resource Management, 60(6), 953–968. https://doi.org/10.1002/hrm.22054

Hastedt, G. P. (1996). CIA's organizational culture and the problem of reform. International Journal of Intelligence and Counterintelligence, 9(3), 249–263. https://doi.org/10.1080/08850609608435317

Heifetz, R. A., Grashow, A., Linsky, M. (2009). The Practice of Adaptive Leadership: Tools and Tactics for Changing Your Organization and the World. Harvard Business Press

Heinrich, J. (2016). Le renseignement militaire après la guerre du Golfe: Après-demain, N ° 37, NF(1), 18–19. https://doi.org/10.3917/apdem.037.0018

Herbaux, P. (2007). Intelligence territoriale: Repères théoriques. Harmattan.

Heuer, R. J. (2010). Psychology of Intelligence Analysis. Central Intelligence Agency.

Heuer, R. J., Pherson, R. H. (2014). Structured analytic techniques for intelligence analysis. CQ Press.

Heylighen, F. (2008). Complexity and self-organization. In M. J. Bates, M. N. Maack (Eds.), Encyclopedia of Library and Information Sciences (pp. 1215-1224). CRC Press.

Holland, J. H. (1995). Hidden order: How adaptation builds complexity. Addison-Wesley.

Hou, T., & Wang, V. (2020). Industrial espionage – A systematic literature review (SLR). Computers & Security, 98, 102019. https://doi.org/10.1016/j.cose.2020.102019

Hulnick, A. S. (2020). Keeping Intelligence Ethical: The Role of Accountability and Professional Norms. International Journal of Intelligence and CounterIntelligence, 33(1), 12–30. https://doi.org/10.1080/08850607.2020.1687567

Ieva, L. (2002). Riflessioni sul principio costituzionale del "giusto processo" applicato al giudizio amministrativo. Rivista amministrativa, (4), 311 ss.

INSS. Publications on Intelligence and National Security. https://www.inss.org.il (Last accessed April 11, 2025)

Institute for Security Studies (ISS). Research on Intelligence and Counter-Terrorism. https://issafrica.org (Last accessed June 14, 2025)

Istituto Affari Internazionali (IAI). Sicurezza e Difesa. https://www.iai.it/it/ricerche/sicurezza-e-difesa (Last accessed June 14, 2025)

Jackson, P. (2006). Intelligence and the state: An emerging 'French school' of intelligence studies. Intelligence and National Security, 21(6), 1061–1065. https://doi.org/10.1080/02684520601046408

Jasper, S. E. (2019). North Korea's Cyberspace Aggression. International Journal of Intelligence and CounterIntelligence, 32(1), 194–198. https://doi.org/10.1080/08850607.2018.1524247

Javorsek II, D., & Schwitz, J. G. (2014). Probing Uncertainty, Complexity, and Human Agency in Intelligence. Intelligence and National Security, 29(5), 639–653. https://doi.org/10.1080/02684527.2013.834218

Johnson, C. (1982). MITI and the Japanese miracle: The growth of industrial policy, 1925-1975. Stanford University Press.

Johnson, L. K. (2018). Handbook of intelligence studies. Routledge.

Johnson, S. (2002). Emergence: The connected lives of ants, brains, cities, and software. Scribner.

Johnston, K., Toft, M. (2021). Risk, Error, and Organizational Culture in British Intelligence. Intelligence and National Security, 36(3), 401–420. https://doi.org/10.1080/02684527.2020.1837642

Johnstone, I. (2016). Between Bureaucracy and Adhocracy: Crafting a Spectrum of UN Peace Operations. Center on International Cooperation. https://cic.nyu.edu/resources/between-bureaucracy-and-adhocracy-crafting-a-spectrum-of-un-peace-operations/ (Last accessed January 20, 2025)

Jong-il, K. (2015). On the Juche idea. Foreign Languages Publishings House.

Jun, J., Center for Strategic and International Studies, LaFoy, S., & Sohn, E. (2015). North Korea's cyber operations: Strategy and responses. Center for Strategic & International Studies.

Kahana, E. (2002). Reorganizing Israel's Intelligence Community. International Journal of Intelligence and CounterIntelligence, 15(3), 415–428. https://doi.org/10.1080/08850600290101686

Kahaner, L. (1997). Competitive intelligence: How to gather, analyse, and use information to move your business to the top (1. ed). Simon & Schuster.

Kang, D. C. (2013). Securizing Transnational Organized Crime and North Korea's Non-Traditional Security. In K.-A. Park (Ed.), Non-Traditional Security Issues in North Korea (pp. 75–99). University of Hawai'i Press. https://www.degruyter.com/doi/book/10.21313/9780824837822 (Last accessed January 20, 2025)

Kauffman, S. A. (2011). The origins of order: Self-organization and selection in evolution (Nachdr.). Oxford Univ. Pr.

Kent, S. (2016). Strategic intelligence for american world policy. Princeton University Press.

Khalaji, M. (2015). Iranian Think Tanks: The Anatomy of Influence. The Washington Institute

Kim, S. C. (2020). North Korea 2019–2020. East Asian Policy, 12(02), 68–79. https://doi.org/10.1142/S179393052000015X

Korea, North. (2021). In The World Factbook. Central Intelligence Agency. https://www.cia.gov/the-world-factbook/countries/korea-north/#military-and-security (Last accessed January 20, 2025)

Kotter, J. P. (1996). "Leading Change". Harvard Business Review Press.

La communauté française du renseignement. (2018). Comité d'études de défense nationale.

Lacoste, P. (Ed.). (1998). Le renseignement à la française. Economica.

Lagourgue, M. J.-L., & Cambon, M. C. (n.d.). Proposition de loi permettant à tout médaillé militaire ayant fait l'objet d'une citation à l'ordre de l'armée de bénéficier d'une draperie tricolore sur son cercueil – Examen des amendements.

Laïdi, A. (2016). Histoire mondiale de la guerre économique du XVème au XXIème siècle. Perrin, Lyon.

Laloux, F. (2014). Reinventing Organizations: A Guide to Creating Organizations Inspired by the Next Stage of Human Consciousness. Nelson Parker.

Lankov, A. (2006). Bitter Taste of Paradise: North Korean Refugees in South Korea. Journal of East Asian Studies, 6(1), 105–137. http://www.jstor.org/stable/23418172

Larrivé, G. (2020). Assemblée Nationale, Constitution du 4 Octobre 1958, Quatorzième Législature, N. 3069. Rapport d'information déposé en application de l'article 145 du règlement par la mission d'information commune, sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement.

Larsonneur J.C. (19/10/2022). Assemblée Nationale, Constitution du 4 Octobre 1958, Quatorzième Législature, N. 369. Avis fait au nom de la Commission de la Défense Nationale et des Forces Armées sur le Projet de loi de Finances pour 2023 (n° 273). Tome II: Défense Environnement et Prospective de la Politique de Défense.

Laurent, S. (2009). Politiques de l'ombre: État, renseignement et surveillance en France. Fayard.

Lawrence, A. (2012). Electronic documents in a print world: Grey literature and the Internet. Journal of Electronic Publishing, 15(1), 1-12. https://doi.org/10.3998/3336451.0015.103

Lefebvre, S. (2013). The Difficulties and Dilemmas of International Intelligence Cooperation. International Journal of Intelligence and CounterIntelligence, 26(4), 617–640. https://doi.org/10.1080/08850607.2013.806559

Les Guerres de l'ombre de la DGSI: Plongée au coeur des services secrets français (con Jordanov, A.). (2020). Nouveau Monde éditions.

Les services secrets (2e édition) (con Soullez, C.). (2020). Eyrolles.

Li, C. (2009). China's New Think Tanks: Where Officials, Entrepreneurs, and Scholars Interact. Brookings Institution

Libbey, J. (2010). CoCom, Comecon, and the Economic Cold War. Russian History, 37(2), 133–152. https://doi.org/10.1163/187633110X494661

Linee guida per il Sistema di misurazione e valutazione della performance dei Ministeri. (2018). Dipartimento della Funzione Pubblica. https://performance.gov.it/linee-guida-il-sistema-di-misurazione-e-valutazione-della-performance (Last accessed August 20, 2025)

Lorenz, E. N. (1963). Deterministic nonperiodic flow. Journal of the Atmospheric Sciences, 20(2), 130–141

Lorho, T., & Lobjois, P. (2015). Profession caméléon: De la DGSE à l'intelligence économique. Fayard.

Losano, M. G. (2002). Sistema e struttura del diritto. Milano: Giuffré.

Lowenthal, M. M. (2019). Intelligence: From secrets to policy (8th ed.). CQ Press.

Luttwak, E. N. (2001). Strategy: The logic of war and peace. Cambridge, MA: Harvard University Press.

Mahdavi, P., & Ishiyama, J. (2020). Dynamics of the Inner Elite in Dictatorships: Evidence from North Korea. Comparative Politics, 52(2), 221–249. https://doi.org/10.5129/001041520X15652680065751

Mallory, K. (2021). North Korean sanctions evasion techniques. RAND Corporation.

Manificat, P. (2021). Renseignement et action: De la "drôle de guerre" aux opérations spéciales, 80 ans de renseignement militaire en France. Sophia Histoire & Collections.

Manyin, M. E., Nikitin, M. B. D., & Smith, K. (2020). North Korea: A Chronology of Events from 2016 to 2020 (Congressional Research Service Report No. R46349). https://crsreports.congress.gov/product/pdf/R/R46349 (Last accessed January 20, 2025)

Marrin, S. (2016). Improving Intelligence Analysis: Bridging the Gap Between Scholarship and Practice. Routledge.

Marrin, S. (2018). Evaluating intelligence theories: Current state of play. Intelligence and National Security, 33(4), 479–490. https://doi.org/10.1080/02684527.2018.1452567

Martre H. (1994). Intelligence économique et stratégie des entreprises, Rapport du groupe de travail du Commissariat Général du Plan (p. 167). https://www.vie-publique.fr/rapport/29146-intelligence-economique-et-strategie-des-entreprises (Last accessed January 20, 2025)

Matovski, A. (2020). Strategic Intelligence and International Crisis Behavior. Security Studies, 29(5), 964–990. https://doi.org/10.1080/09636412.2020.1859128

Mattarella, B. G. (2011). La trappola delle leggi. Molte oscure, complicate. Bologna: Il Mulino.

Maturana, H. R., Varela, F. J. (1987). The Tree of Knowledge: The Biological Roots of Human Understanding. Shambhala

MATZOV. (2022). Report on the Security of LWE: Improved Dual Lattice Attack. Zenodo. https://doi.org/10.5281/ZENODO.6493704

Mazet, P. (2017). L'Intelligence économique: Un enjeu de sécurité nationale. Harmattan.

McChrystal, S., Collins, T., Silverman, D., Fussell, C. (2015). Team of teams: New rules of engagement for a complex world. Penguin.

McEachern, P. (2010). Inside the red box: North Korea's post-totalitarian politics. Columbia University Press.

McGann, J. G. (2020). 2020 Global Go To Think Tank Index Report. University of Pennsylvania

McKelvey, B. (2016). Complexity ingredients required for entrepreneurial success. Entrepreneurship Research Journal, 6(1), 53-73.

McMillan, E. (2004). Complexity, organizations and change. Routledge.

Melkonian, T., & Picq, T. (2011). Building Project Capabilities in PBOs: Lessons from the French Special Forces. International Journal of Project Management, 29(4), 455–467. https://doi.org/10.1016/j.ijproman.2011.01.002

Menkveld, C. (2021). Understanding the complexity of intelligence problems. Intelligence and National Security, 36(5), 621–641. https://doi.org/10.1080/02684527.2021.1881865

Merlen, E., & Ploquin, F. (2003). Les entreprises et le renseignement économique. Revue Défense Nationale, 2, 35–48.

Meyer, C. (2019). Intelligence économique et stratégie nationale: Une nouvelle approche du renseignement. Revue Défense Nationale, 3, 81–90.

Michel, R. (2020). Le renseignement économique. Éditions des Équateurs.

Miller, G. (2019). The Shadow War: Inside Russia's and China's Secret Operations to Subvert America. Simon Schuster.

Miller, J. H., & Page, S. E. (2007). Complex adaptive systems: An introduction to computational models of social life. Princeton Univ. Press.

Mintzberg, H. (1983). Structures in Fives. Designing Effective Organizations. Englewood Cliffs, Prentice-Hall.

Mintzberg, H. (1985). Strategy Formation in an Adhocracy. Administrative Science Quarterly, 30(2), 160-197.

Mintzberg, H., Quinn, J. B. (1996). The Strategy Process: Concepts, Contexts, Cases. Prentice Hall.

Mitchell, M. (2009). Complexity: A Guided Tour. Oxford University Press

Mitleton-Kelly, E. (2015). Effective policy making: addressing apparently intractable problems. In Geyer, R., Cairney, P. (Eds.), Handbook on Complexity and Public Policy (pp. 111-128). Edward Elgar Publishing.

Moinet, N. (2003). Les batailles secrètes de la science et de la technologie: Gemplus et autres énigmes. Lavauzelle.

Montin, J. (2013). L'intelligence économique à l'ère de l'information. L'Harmattan.

Morgan, G. (2016). Images of Organization (Updated edition). SAGE.

Morin, E. (2014). Complexity and organization. Routledge.

Morin, E. (2020). La Via. Per l'avvenire dell'umanità. Raffaello Cortina Editore.

Morin, Y. (2019). Intelligence économique et stratégie d'entreprise. Dunod.

Moural, A. (2008). The role of espionage in the U.S. economy. National Defense University.

Moutouh, H., & Poirot, J. (Eds.). (2018). Dictionnaire du renseignement. Perrin.

Naftalski. D. (2004). Les entreprises françaises et l'intelligence économique. Défense Nationale, 12(670), 27–39.

Négrier, É. (2008). L'intelligence économique en France: Revue Défense Nationale, N° 67(1), 16–25.

Némo, L. (2011). Intelligence économique: Le cadre juridique et ses impacts. Revue Internationale de Droit Comparé, 63(2), 341–362. https://doi.org/10.3917/ridc.632.0341

Némo, L. (2018). La lutte contre le financement du terrorisme: Une approche historique et comparative. Revue de Droit Pénal et de Criminologie, 1(2), 69–90. https://doi.org/10.3917/rdpc.182.0069

Norton, B. (2022). U.S. intelligence and economic policy: The role of CIA in trade. Stanford University Press.

Nowak, M. A. (2006). Evolutionary Dynamics: Exploring the Equations of Life. Harvard University Press. https://doi.org/10.2307/j.ctvjghw98

O'Connell, A. J. (2006). The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World. Social Science Research Network. https://doi.org/10.2139/ssrn.887249

Office of the Secretary of Defense. (2017). Military and Security Developments Involving the Democratic People's Republic of Korea (Report to Congress No. 9-600987B). https://media.defense.gov/2018/May/22/2001920587/-1/-1/1/report-to-congress-military-and-security-developments-involving-the-democratic-peoples-republic-of-korea-2017.pdf (Last accessed January 20, 2025)

Oleson, P. C., & Cothron, T. (2016). Leading and Managing Intelligence Organizations. 33(1).

Omand, D., Phythian, M. (2023). How Spies Think: Ten Lessons in Intelligence. Penguin.

Orbach, M. (2018, March 12). Mossad’s Venture Arm Selects Startups for its Secretive Portfolio. CTECH. https://www.calcalistech.com/ctech/articles/0,7340,L-3733822,00.html (Last accessed January 20, 2025)

Oren, I. (2020). Between Intelligence and Diplomacy: The Information Revolution as a Platform for Upgrading Diplomacy. 23(3).

Ouassou, S., & Bakour, C. (2024). Territorial intelligence: State of the theoretical art. International Journal of Accounting, Finance, Auditing, Management and Economics, 5(4), 597-613.

Pacher, L. R. (2000). The Nature of Future Intelligence Organizations: Defense Technical Information Center. https://doi.org/10.21236/ADA393418

Park, Y. S. (2014). Policies and Ideologies of the Kim Jong-un Regime in North Korea: Theoretical Implications. Asian Studies Review, 38(1), 1–14. https://doi.org/10.1080/10357823.2013.868864

Pascuzzi, G. (2013). La creatività del giurista. Tecniche e strategie dell’innovazione giuridica. Bologna: Zanichelli.

Passaglia, P. (2012). Il segreto di Stato e l’attività giurisdizionale. In Studi e ricerche di Diritto comparato. Corte Costituzionale. https://www.cortecostituzionale.it/documenti/convegni_seminari/CC_SS_SegretoStato_28032012.pdf (Last accessed August 20, 2025)

Pavard, J. (2018). Le renseignement économique: Une intelligence au service des entreprises. L'Intelligence Economique et la Sécurité.

Phillips, J. R. (2016, April 21). The judicial system is the first reason why (many potential investors) decide not to invest in Italy. Speech given at Università Bocconi. https://www.unibocconi.it/en/news/american-lesson (Last accessed August 20, 2025)

Phythian, M. (2021). Intelligence in an Insecure World (3rd ed.). Polity Press.

Pinkston, D. A. (2020). North Korea’s Objectives and Activities in Cyberspace. Asia Policy, 27(2), 76–83. https://doi.org/10.1353/asp.2020.0031

Plowman, D. A., et al. (2007). Radical change accidentally: The emergence and amplification of small change. Academy of Management Journal, 50(3), 515-543.

Porter, M. E. (1980). Competitive strategy: Techniques for analyzing industries and competitors (52. printing). Free Press.

Prigogine, I., Stengers, I. (1984). Order out of Chaos: Man's New Dialogue with Nature. Bantam

RAND Corporation. Research Areas. https://www.rand.org/topics/intelligence.html (Last accessed April 15, 2025)

Rapport d'activité 2022. (2023). Secrétariat général de la défense et de la sécurité nationale.

Rapport sur les perspectives de la politique de renseignement. (2017). Commission nationale de contrôle des interceptions de sécurité.

Reed, J. (2015, July 10). Unit 8200: Israel's cyber spy agency. Financial Times. https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c (Last accessed January 20, 2025)

Reed, W. J., & Hughes, B. D. (2002). From gene families and genera to incomes and internet file sizes: Why power laws are so common in nature. Physical Review E, 66(6), 067103. https://doi.org/10.1103/PhysRevE.66.067103

Regourd, M. (2020). La défense nationale à l'ère du numérique: Revue Défense Nationale, N° 813(8), 83–91. https://doi.org/10.3917/rdna.813.0083

Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.

Riehle, K. P. (2015). A Counterintelligence Analysis Typology. 32(1), 55-60.

Roberts, A. (2013). The Logic of Discipline: Global Capitalism and the Architecture of Government. Oxford University Press.

Rochester, C. (2005). The Rise and Fall of the French Intelligence Community: A History of the DGSE. International Journal of Intelligence and CounterIntelligence, 18(4), 554–573. https://doi.org/10.1080/08850600500289173

Rosenau W. (Eds.), Confronting the "Enemy Within" (Vol. 58, pp. 17–23). RAND Corporation. http://access.portico.org/stable?au=phzphd07j (Last accessed January 20, 2025)

Rosenne, D. (2022). Heritage of the IDF C4I Corps. The Association for the Commemoration of the Fallen Soldiers of the IDF Signal Corps.

Rotenstreich Y., & ì Tsur T. (1987). Israel Intelligence & Security: Report of an Investigation Commission on the Pollard Case. Ministerial Committee on National Security Affairs (NSAC- National Security Affairs Committee. https://www.jewishvirtuallibrary.org/israeli-report-of-an-investigation-commission-on-the-pollard-case-may-1987 (Last accessed January 20, 2025)

Roth, M. (2022). Une histoire politique des services secrets en France. Presses Universitaires de France.

Roul, D. (2018). Le renseignement économique: État des lieux. Revue Défense Nationale, N° 813(8), 99–100. https://doi.org/10.3917/rdna.813.0099

Rouvin, G. (2020). The Political Economy of Intelligence and Counterintelligence: Understanding the French Approach. Security Studies, 29(4), 685–703. https://doi.org/10.1080/09636412.2020.1764088

Roux, A. (2016). Espionnage et renseignement économique: une histoire d'hier à aujourd'hui. Éditions du Cerf.

Royal United Services Institute (RUSI). Technology, Security and Intelligence. https://rusi.org/explore-our-research/topics/technology-security-and-intelligence (Last accessed January 20, 2025)

Saïd, A. (2019). The Impact of Intelligence on Decision-Making in France. European Journal of Political Research, 58(4), 1079–1101. https://doi.org/10.1111/1475-6765.12341

Salvatori, P. (2018). Spie? L'intelligence nel sistema di sicurezza internazionale. La lepre edizioni.

Scharmer, O., Kaufer, K. (2013). Leading from the Emerging Future: From Ego-System to Eco-System Economies. Berrett-Koehler Publishers.

Schöpfel, J. (2010). Towards a Prague definition of grey literature. In D. Farace, J. Schöpfel (Eds.), Grey Literature in Library and Information Studies (pp. 11–22). De Gruyter Saur.

Schwartz, P. (2020). The Art of the Long View: Planning for the Future in an Uncertain World. Currency Doubleday.

Schweizer, P. (1996). The Growth of Economic Espionage: America Is Target Number One. Foreign Affairs, 75(1), 9. https://doi.org/10.2307/20047464

Seiglie, C., Coissard, S., & Échinard, Y. (2008). Economic intelligence and national security. In Contributions to Conflict Management, Peace Economics and Development (Vol. 6, pp. 235–248). Emerald (MCB UP). https://doi.org/10.1016/S1572-8323(08)06014-1

Senor, D., & Singer, S. (2011). Start-up nation: The story of Israel's economic miracle (1st trade ed). Twelve.

Serscikov, G. (2024). Grey literature in the intelligence domain: Twilight or revival? Intelligence and National Security, 39(6), 1028–1050. https://doi.org/10.1080/02684527.2024.2372119

Sforza, L. (2004). Sicurezza nazionale, segreto e giurisdizione. Per Aspera ad Veritatem, (28). https://gnosis.aisi.gov.it/sito/Rivista28.nsf/servnavig/9 (Last accessed August 20, 2025)

Shambaugh, D. (2002). Modernizing China's Military: Progress, Problems, and Prospects. University of California Press

Shulman, S. (2021, January 8). Unit 81: The elite military unit that caused a big bang in the Israeli tech scene. CTECH. https://www.calcalistech.com/ctech/articles/0,7340,L-3886512,00.html (Last accessed August 20, 2025)

Silberzahn, C., & Guisnel, J. (1999). Au cœur du secret: 1500 jours aux commandes de la DGSE (1989 - 1993). Fayard.

Smelser, N. J., & Reed, J. S. (2012). Usable Social Science. University of California Press. https://doi.org/10.1525/9780520954144

Smith, J., & Kossou, L. (2008). The emergence and uniqueness of competitive intelligence in France. Journal of Competitive Intelligence and Management, 4(3), 63–85.

Snowden, D. J., Boone, M. E. (2007). A Leader's Framework for Decision Making. Harvard Business Review, 85(11), 68-76.

Socialist Constitution of the Democratic People's Republic of Korea. (2017). Foreign Languages Publishing House.

Spuntarelli, S. (2012). La parità delle parti nel giusto processo amministrativo. Roma: Dike Giuridica.

Stacey, R. D. (2001). Complex Responsive Processes in Organizations: Learning and Knowledge Creation. Routledge

Stacey, R. D. (2010). Complexity and organizational reality: Uncertainty and the need to rethink management after the collapse of investment capitalism. Routledge.

Steinhart, A., & Avramov, K. (2013). Is Everything Personal?: Political Leaders and Intelligence Organizations: A Typology. International Journal of Intelligence and CounterIntelligence, 26(3), 530–549. https://doi.org/10.1080/08850607.2013.780556

Stiftung Wissenschaft und Politik (SWP). Security and Defense. https://www.swp-berlin.org/en/topics/security-and-defense (Last accessed August 20, 2025)

Stone, D. (2007). Think Tanks and Policy Advice in Countries in Transition. Asian Development Bank Institute

Su-yong, H. (2016). Undestanding Korea: Defence. Foreign Languages Publishing House.

Sussman, D. (2005). Intelligence and War in the Modern World: The Case of France. Intelligence and National Security, 20(2), 214–230. https://doi.org/10.1080/02684520500068257

Svendsen, A. D. M. (2015). Contemporary intelligence innovation in practice: enhancing “macro” to “micro” systems thinking via “System of Systems” dynamics. Defence Studies, 15(2), 105–123. https://doi.org/10.1080/14702436.2015.1033850

Tali, T. (2017, June 5). 8200 graduates aren’t like 23 year-olds in Texas or Norway. Globes. https://en.globes.co.il/en/article-8200-graduates-are-not-like-23-year-olds-in-texas-or-norway-1001191294 (Last accessed August 20, 2025)

Tama, J. (2017). The politics of strategy: Why government agencies conduct major strategic reviews. Journal of Public Policy, 37(1), 27–54. https://doi.org/10.1017/S0143814X15000148

Tan, A. T. H. (2018). Evaluating counter-terrorism strategies in Asia. Journal of Policing, Intelligence and Counter Terrorism, 13(2), 155–169. https://doi.org/10.1080/18335330.2018.1473628

Teirila, O. (2016). Intelligence and Media. American Intelligence Journal, 33(2), 137–143. JSTOR. https://www.jstor.org/stable/26497098

Tendler, I. (2015, March 20). From The Israeli Army Unit 8200 To Silicon Valley. TC. https://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley/ (Last accessed August 20, 2025)

Tetlock, P. E., Mellers, B. A. (2014). Expert Political Judgment and Good Judgment Project: How to Improve Decision Making in Intelligence. Psychological Science, 25(5), 1445–1452. https://doi.org/10.1177/0956797614532915

The Council of the EU. (2016). COUNCIL DECISION (CFSP) 2016/849 of 27 May 2016 concerning restrictive measures against the Democratic People’s Republic of Korea and repealing Decision 2013/183/CFSP. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D0849&from=EN (Last accessed August 20, 2025)

The Council of the EU. (2017). COUNCIL REGULATION (EU) 2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People’s Republic of Korea and repealing Regulation (EC) No 329/2007. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1509&from=IT (Last accessed August 20, 2025)

The Council of the EU. (2018). COUNCIL IMPLEMENTING REGULATION (EU) 2018/602 of 19 April 2018 implementing Regulation (EU) 2017/1509 concerning restrictive measures against the Democratic People’s Republic of Korea. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0602&from=EN (Last accessed August 20, 2025)

The Council of the EU. (2021). COUNCIL IMPLEMENTING REGULATION (EU) 2021/478 of 22 March 2021 implementing Regulation (EU) 2020/1998 concerning restrictive measures against serious human rights violations and abuses. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0478&from=EN (Last accessed August 20, 2025)

Thurner, S., & Hanel, R. (2009). Generalized-generalized entropies and limit distributions. Brazilian Journal of Physics, 39(2a). https://doi.org/10.1590/S0103-97332009000400011

Thurner, S., Klimek, P., & Hanel, R. (2018). Introduction to the Theory of Complex Systems (Vol. 1). Oxford University Press. https://doi.org/10.1093/oso/9780198821939.001.0001

Tims, M., & Bakker, A. B. (2010). Job crafting: Towards a new model of individual job redesign. SA Journal of Industrial Psychology, 36(2), 9 pages. https://doi.org/10.4102/sajip.v36i2.841

Toumoun, A. (2018). Autonomie stratégique et politique industrielle: Un défi national et européen: Revue Défense Nationale, N° 813(8), 101–107. https://doi.org/10.3917/rdna.813.0101

Tracfin. (2018). Tracfin et la lutte contre le financement du terrorisme: Revue Défense Nationale, N° 813(8), 38–42. https://doi.org/10.3917/rdna.813.0038

Tranquillo J. (Ed.). (2018). An introduction to complex systems: Making sense of a changing world. Springer Science+Business Media, LLC.

Trent, S., Patterson, E. S., Woods, D. D. (2007). Challenges for Cognition in Intelligence Analysis. Journal of Cognitive Engineering and Decision Making, 1(1), 75–97. https://doi.org/10.1177/155534340700100104

Treverton, G. F., Gabbard, C. B. (2014). Assessing the Tradecraft of Intelligence Analysis. RAND Corporation. https://www.rand.org/pubs/research_reports/RR382.html (Last accessed August 20, 2025)

Ulrichsen, K. C. (2014). The Gulf States and the Arab Uprisings. Oxford University Press

UNESCO. (1998). Transdisciplinarity: Stimulating synergies, integrating knowledge. DRG.98/WS/05. International Symposium on Transdisciplinarity, Val-d'Oise, France.

United Nations Security Council. (2013). Resolution 2094 (2013). Adopted by the Security Council at its 6932nd meeting, on 7 March 2013 (S/RES/2094 (2013)).

United States & Defense Intelligence Agency. (2021). North Korea military power: A growing regional and global threat. https://purl.fdlp.gov/GPO/gpo172971 (Last accessed August 20, 2025)

UNODOC (United Nations Office on Drugs and Crime Vienna) (2011). Criminal Intelligence, Manual for Analysts. UN, New York.

Urvoas, J. J. (2015). Délégation Parlementaire au Renseignement. Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014.

Urvoas, J. J., & Verchère, P. (2013). Assemblée Nationale, Constitution du 4 Octobre 1958, Quatorzième Législature, N. 1022, Rapport de la Commission des lois Constitutionnelles, de la Législation et de l'Administration Générale de la République sur l'évaluation du cadre juridique applicable aux services de renseignement.

Valette-Valla, G. (2023). Ministère de L'économie, des Finances et de la Souveraineté Industrielle et Numérique. L'activité de Tracfin Bilan 2022.

Van Ginkel, B. (2012). Towards the Intelligent Use of Intelligence: Quis Custodiet ipsos Custodes? Terrorism and Counter-Terrorism Studies. https://doi.org/10.19165/2012.1.10

Van Ham P. (1992), Western Doctrines on East-West Trade. Theory, History and Policy, St. Martin's Press, New York.

Van Puyvelde, D. (2021). Out of the Shadows: The Ethics of Intelligence. Oxford University Press.

Van Puyvelde, D., Coulthart, S., Bruneau, T. C. (2017). Comparative Intelligence Oversight: A Framework for Analysis. Intelligence and National Security, 32(2), 162–180. https://doi.org/10.1080/02684527.2016.1202080

Warusfel, B. (2003). Le renseignement, dimension majeure de l'action publique dans une société d'information.

Wedding, D., & Rose, S. M. (2004). Security Intelligence in France. In P. Chalk & W. Rosenau (Eds.), Confronting the "Enemy Within" (Vol. 58, pp. 17–23). RAND Corporation. http://access.portico.org/stable?au=phzphd07j (Last accessed August 20, 2025)

Weiss, J. C. (2014). Authoritarian Signaling, Mass Audiences, and Nationalist Protest in China. International Organization, 67(1), 1–35

West, M. A. (2012). Effective Teamwork: Practical Lessons from Organizational Research. Wiley-Blackwell

Wey, A. L. K. (2018). Japanese intelligence and covert operations: A strategic evaluation of Fujiwara Kikan in the invasion of Malaya and Singapore, 1941–1942. Journal of Intelligence History, 17(1), 52–64. https://doi.org/10.1080/16161262.2017.1397398

Wheaton, K. J. (2009). Evaluating Intelligence: Answering Questions Asked and Not. International Journal of Intelligence and CounterIntelligence, 22(4), 614–631. https://doi.org/10.1080/08850600903143122

Williamson, M. (2017). Socializing Intelligence: The CIA and Professional Identity Formation. Intelligence and National Security, 32(6), 769–785. https://doi.org/10.1080/02684527.2017.1285240

Wirtz, J. J., Gelles, M. G. (2020). Intelligence and Mental Health: Addressing Psychological Challenges in National Security. International Journal of Intelligence and CounterIntelligence, 33(4), 762–778. https://doi.org/10.1080/08850607.2020.1754247

Wise, C. R. (2006). Organizing for Homeland Security after Katrina: Is Adaptive Management What's Missing? Public Administration Review, 66(3), 302–318. http://www.jstor.org/stable/3843912

Wrubel, W. A. (1989). The Toshiba-Kongsberg Incident: Shortcomings of Cocom, and Recommendations for Increased Effectiveness of Export Controls to the East Bloc. American University International Law Review, 4(1), Article 8.

Xinhua. (2015). China to build new-type think tanks with Chinese characteristics. Xinhua News Agency

Yves Laurent, S. (2019). La gouvernance supérieure du renseignement: Un défi culturel pour la technostructure d'État. Journée d'études Sur Le SGDN.

Zaccaro, S. J., Gilbert, J. A., Thor, K. K., & Mumford, M. D. (2001). "Leadership and Social Intelligence: Linking Social Perspectiveness and Behavioral Flexibility to Leader Effectiveness". The Leadership Quarterly, 2, 317-342

Zegart, A. (2007). Spying Blind: The CIA, the FBI, and the Origins of 9/11. Princeton University Press.

Zegart, A. (2023). Spies, Lies, and Algorithms: The History and Future of American Intelligence. Princeton University Press.

Zegart, A. B. (2000). Flawed by design: The evolution of the CIA, JCS, and NSC (Nachdr.). Stanford Univ. Press.

Zhang, X. (2019). Chinese Think Tanks, Policy Advice and Global Governance. Routledge

9 791255 151234