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

Juan Carlos ESTARELLAS y LÓPEZ
Army Captain (VR) and Terrorism, Bioterrorism and Counterintelligence Analyst (Structured Analytic Techniques). Information Operations (ROI I).
Associate Member of the "Juan Velázquez de Velasco" University Research Institute for Security and Defence Intelligence (UC3M).
Lecturer at the International Campus for Security and Defence (CISDE)

E-mail: capest22@gmail.com

Offensive counter-intelligence as a suitable disrupter to counteract Russian foreign intelligence

Abstract

The activities developed by the intelligence services are aimed at providing information, analysing it, preparing intelligence products and disseminating them to political decision-makers, in order to support their decision-making in the face of threats, risks and opportunities. On the other hand, the counter-intelligence operations, as a specialised intelligence discipline, have a double dimension: the offensive counter-intelligence, which aims to penetrate the enemy services and use the figure of double agent ; and the defensive counter-intelligence, which leads to the identification of designated service officials, the knowledge of the methods used and the identification of their sources of information. In this essay we will delve into the origin and importance of counter-intelligence operations, aimed at fighting counterinformation, espionage and subversion, and how to improve the counter-intelligence analysis using the structured analysis techniques.

Keywords

Offensive counter-intelligence, Defensive counter-intelligence, Double agent, Penetration, Structured analytic techniques.

Cite this article:

Estarellas López, J. C. (2023). Offensive counter-intelligence as a suitable disruptor to counteract Russian foreign intelligence *Revista del Instituto Español de Estudios Estratégicos*, no. 21, pp. 333-366.

1. Introduction

The term "intelligence" as we know it today has its roots in the 16th century and even earlier. Renaissance Venice was an ideal setting for the emergence of intrigue and the exchange of information and secrets. The city's canals, bridges, stately homes and palaces facilitated this activity, creating an environment conducive to the emergence of the espionage networks woven by European diplomacy during the 16th and 17th centuries. And within these networks, subtly differentiated profiles and terms emerged, such as envoys, residents, plenipotentiaries, agents and intelligentsia. However, in the military sphere, the preferred terms were "spy" and "espionage", for the employment, in return for financial reward, of those who were informants and people close to treasonous, conspiratorial or despicable activities (Navarro, 2009:106-108).

There is now a widely accepted definition of the term intelligence and espionage activities, and although scholars of these disciplines continue their discussions, the differences are credulous and have to do with the scope of definitions centred on the function of providing information, analysing it, devising an intelligence product and providing it to the decision-maker to support their decision.

We aim to deepen the counter-intelligence approach as a discipline to make intelligence work to our advantage. Not only is mistrust the basis of counter-intelligence, but its exercise reinforces mistrust, which ultimately becomes a problem (Taylor, 2007:10). An instinctive cycle that feeds back on itself and degenerates into paranoia. Thus, the act of counter-intelligence fuels feelings of apprehension and suspicion which, in turn, generates further scepticism (Taylor, 2009: 35).

In the following sections, we will discuss the role of counter-intelligence, highlighting its offensive disruptive nature in countering the threat of espionage and infiltration, as well as the degree of influence and impact on other areas of relevance to any modern state. These includes national security strategies and the neutralisation of espionage; the objectives of counter-intelligence and the structure, operation and activities of opposing intelligence services; the successes of Soviet-Russian intelligence and the reason for Western mistakes; and finally, the importance of counter-intelligence analysis and the use of structured analytic techniques.

2. Counter-intelligence in Spain's National Security Strategy

The Spanish National Security Strategy, with the objective of guaranteeing security, sets out a plan for political action through three fundamental axes: "*protect*", "*promote*" *and*"*participate*". The third chapter, on risks and threats, focuses on identifying strategic targets for preventive action by drawing up a risk map to combat hybrid strategies, disinformation campaigns and espionage. And in the field of counter intelligence, there is a willingness to adopt measures in defence of Spain's strategic, political and economic interests, with the aim of preventing, detecting and neutralising covert

aggression by hostile intelligence services that seek to obtain information and state secrets by means of illegal or criminal procedures[1].

The strategic review warns about hybrid strategies executed by hostile services, including espionage operations as a form of intimidation against Spain's security[2].

2.1. The search for a homogeneous, analogous definition of counter-intelligence as a discipline

One of the modern definitions for counter-intelligence was drawn from the arguments contained in Samuelson and Nordhaus's economics textbooks, in which they stated: "Economics is the study of how societies use scarce resources to produce valuable commodities and distribute them among people" (Samuelson and Nordhaus, 1992: 53).

Thus, for an initial definition based on the theories of Samuelson and Nordhaus, we can state that (Ehrman, 2004:44): "Counter-intelligence is the study of the organisation and behaviour of the intelligence services of foreign states and entities, and the application of the resulting knowledge". It is a definition that enjoys a number of qualities. Firs, it assumes that counter-intelligence is a broad analytical discipline that encompasses all ntelligence service, whether domestic, foreign or military. Secondly, the definition avoids transforming the study of intelligence services into a simple research exercise (Ehrman, 2009: 4-5).

A second definition of counter-intelligence is found in the US National Security Act of 1947, as amended by 50 USC 401a of the National Security Act of 1949 (Ehrman, 2009: 4):

> "The term 'counterintelligence' means information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities".

A third definition can be found in Executive Order 12333 passed by Ronald Reagan, President of the United States (Ehrman, 2009: 4): "Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities".

1 The National Security System. National Security Department (DSN). Available at: https://www.dsn.gob.es/es/sistema-seguridad-nacional/qué-es-seguridad-nacional/ámbitos-seguridad-nacional/contrainteligencia

2 Spying and interference from abroad. 2021 National Security Strategy. Royal Decree 1150/2021 of 28 December, approving the National Security Strategy (Spain). Available at: https://www.boe.es/boe/dias/2021/12/31/pdfs/BOE-A-2021-21884.pdf

A fourth definition comes from the *National Counterintelligence Strategy 2016* (Evanina, 2016: 1-6), which states:

> "Counterintelligence is the activity of identifying and addressing foreign intelligence threats to the United States. Its main concern is foreign intelligence services and similar organisations of non-state actors, such as transnational terrorist groups. Counterintelligence has a defensive mission, to protect sensitive national assets against foreign intelligence infiltration, and an offensive mission, to identify what foreign intelligence organisations are planning in order to thwart their objectives".

From other regions, specifically the USSR, we discovered a practical definition of counter-intelligence provided by Vasili Mitrokhin, a defector from the KGB (Ehrman, 2009): 5), who argued: "Counterintelligence activity is an activity carried out by special state agencies against foreign intelligence services and organisations and individuals being used by them".

In the light of the above explanations and when taking the definition of counter-intelligence in Spain into comparison, we find counter-intelligence fell within the purview of the SECED, the espionage and counter-espionage agency that was the precursor to the CESID and later the CNI (National Intelligence Centre). The Spanish secret service of that time had its own counter-intelligence unit attached to the Second Section of the High General Staff (Bardavio *et al.*, 2000: 12). Colloquially known as "the High One. Or the origins" (Urbano, 1997: 34). It was a group specialised in counter-espionage activities (Bardavio *el al.*, 2000: 12). However, the most significant change came with the enactment National Intelligence Centre (CNI) Act,[3] in which we can note similarities in terms of the information gathering that allows for the prevention, detection and neutralisation of competing intelligence services.

2.2. *The duty of intelligence services: neutralising espionage*

The powers to neutralise espionage and guarantee the protection of classified information lie exclusively with the CNI, as set out in Article 4(b) of the CNI Act:

> "Prevent, detect and enable the neutralisation of those activities of foreign services, groups or individuals that jeopardise, threaten or attack the constitutional order, the rights and freedoms of Spanish citizens, the sovereignty, integrity and security of the state, the stability of its institutions, national economic interests and the welfare of the population".

3 Chapter I. General provisions. Article 4. Functions of the National Intelligence Centre. Law 11/2002 of 6 May 2002 regulating the National Intelligence Centre. Available at: https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628

It should be pointed out that not only are counter-espionage and infiltration as *disruptive actions* against hostile intelligence services essential for an intelligence agency, but also analysis activities (Navarro and Esteban, 2004: 35), and more importantly, structured analytic techniques. These latter techniques are aimed at providing support to the analyst for the purpose of increasing his capabilities in the planning and implementation of clandestine actions and covert operations, focused on counter-espionage and offensive intelligence.

Today, the strategic dimension of knowledge management takes on special relevance at a time when there is no doubt that it is considered a fundamental strand in decision-making processes (Navarro and Esteban, 2004: 56).

it must also be stressed that analysts cross minefields everty day to know the present and from it guess every future, sustained by the valuable secrets intelligence gathering reveals. In the same way, counter-intelligence cannot be understood if it does not provide protection for the concealment of secret information by means of *cryptography (kripto*, hidden, and *grafía*, writing) or, on the contrary, through *cryptanalysis,* as a discipline linked to the study of the various methods for decoding encrypted information produced by other services (Ribagorda, 2015: 313).

2.3. The Spanish position on counter-intelligence

In one of the definitions linked to the discipline of counter-intelligence (Navarro, 2009: 377), the researcher Navarro Bonilla argues:

> "Counterintelligence is, so to speak, the inherent reverse of intelligence, and as old as intelligence itself. Indeed, a historical analysis of the one in isolation from the other is not understandable. This concept encompasses all the means and resources available to a state, which are capable of identifying and neutralising the action of agents or spies of a foreign or enemy power who are seeking to carry out aggressive operations against any interest of that sovereign state, whether located inside or outside its national territory".

The activities carried out by the Spanish counter-intelligence were divided into two two categories: firstly, counter-information i.e the actions aimed at disabling the informational effectiveness of foreign powers in matters related to the nation itself; and, counter-subversion, i.e the actions aimed at identifying, neutralising and counteracting the subversion of hostile powers, understood as activities that provoke disorder in the general interest, security and defence of the nation (Navarro, 2009: 377).

Accumulated experience led to other complementary specialities being included under the term counter-information. Counter-espionage, as a speciality, is aimed at identifying, detecting, tracking and neutralising spies and operatives active within the jurisdiction of another state. It has its own methods of action: firstly, the intelligence cycle which involves gathering as much information as possible about a possible aggression by agents of an enemy intelligence service; secondly, the complete identification of the

network operating in the country, which requires the initiation of counter-intelligence operations to disarm it; and thirdly, allowing the spy to continue his illegal activity but under surveillance with his movements tracked, and checked in order to obtain as much information as possible (Navarro, 2009: 377). Therefore, deception and lies are very powerful weapons in the war against spies (Navarro, 2009: 385).

Currently, the meaning of counter-intelligence must be interpreted in the light of the CNI Act, which states:

> "Counterintelligence is none other than the set of actions aimed at preventing, detecting and enabling the neutralisation of those activities of foreign services, groups or individuals that put at risk, threaten or attack the constitutional order, the rights and freedoms of Spanish citizens, the sovereignty, integrity and security of the state, the stability of its institutions, national economic interests and the welfare of the population"[4].

After analysing the index of terms in the "glosario de intelligencia" [intelligence glossary], we looked at the similarities in an analogous definition for counter-intelligence (Esteban *et al.* 2007: 68), which offers us a scientific interpretation of what the discipline represents (Esteban *et al.* 2007: 64): [...] activities aimed at nullifying the knowledge that foreign intelligence services seek to acquire about essential aspects of the state in the political, economic or security fields.

At the same time, it is worth highlighting the relevant role played in military counter-intelligence (competences and missions) by the personnel belonging to the Armed Forces Intelligence Centre (CIFAS), who advise both the Chief of Defence Staff (CHOD) and the Chiefs of Staff of the Spanish Army and Navy[5].

3. Counter-intelligence objectives

Before describing the objectives of counter-intelligence, we must define what we mean by counter-intelligence.

It "is the specialised discipline of intelligence operations", and when successful it generates endless feedback loops. Initiating an operation requires the application of previously gathered and analysed counter-intelligence information (Ehrman, 2009: 5-20). Thus, counter-intelligence operations, as a disruptive tool, are aimed at obtaining additional information on how the competing service operates, including many details of its operations. It can be classified as offensive or defensive counter-intelligence.

4 Chapter I. General provisions. Article 4. b) Functions of the National Intelligence Centre. Law 11/2002 of 6 May 2002 regulating the National Intelligence Centre. Available at: https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628

5 Organisation of the Defence Staff. Article 8 The Armed Forces Intelligence Centre. "*It also advises the CHOD and the Army and Navy Chiefs of Staff on military counterintelligence...*". Available at: https://www.defensa.gob.es/Galerias/ministerio/organigramadocs/ORDEF-2020-710-organizacion-basica-EMAD-.pdf

3.1. Offensive counter-intelligence activity: penetration of opposing intelligence services

The scientific perspective provides a precise definition of the penetration agent (Esteban *et al.* 2007: 80): "An agent recruited or implanted as a member of an opposing organisation, engaged in obtaining and supplying information in a clandestine and regular manner to the intelligence service to which he belongs or with which he collaborates. Unlike an informant, this agent actively seeks information".

Consequently, a successful raid would provide the identification of spies in the designated competing service working for it or others, and even if the raider did not know their identities, it would provide information that would lead to unmasking them.

When it comes to infiltrators, they know the organisation and can provide biographical information on their colleagues, revealing possible internal friction, training received, relevant details of their operational methods, or the ability to climb career ladder and gain access to relevant information within the service.

Mid-level infiltrators can be devastating to an intelligence service, as former CIA counter-intelligence analyst Aldrich Hazen Ames demonstrated (Ehrman, 2009: 5-20). For nine long years, Ames betrayed his country after offering his services to the KGB (Andrew, 2018: 709).

William J. Casey, former CIA director under Ronald Reagan, consistently pressed Soviet division officials time and again to make efforts to recruit human sources (Woodward, 1981: 274-275).

3.2. Offensive counter-intelligence activity: double agents

The most complex discipline of intelligence is counter-intelligence, but the most challenging subspecialty of counter-intelligence is the "double agent".

The scientific perspective again provides us with a definition: "[...] a double agent is an intelligence agent or officer of one service who is recruited by another foreign intelligence service or services to carry out clandestine activities, usually supplying information about his or her first service" (Esteban *et al.*, 2007: 51).

An example of a double agent is "one who has been sent by one intelligence service to volunteer to another service" or "an asset of a service who has been discovered by another service and turned(flipped), i.e. sent back to spy on the original handlers" (Ehrman, 2009: 61).

3.3. Defensive counter-intelligence activity: identification of foreign intelligence officials

A third type of counter-intelligence operation is one aimed at identifying the officers of a designated service who are engaged in espionage activities and then, through field

agents and physical and technological surveillance, revealing their operations, contacts and sources of information (Ehrman, 2009: 62).

In Spain, in the summer of 1996, an episode took place in Madrid's Parque del Retiro involving officers from two intelligence services. The main protagonist was a Russian citizen named Sergei Viktorovich Skripal, who was supposed to be carrying out diplomatic activities in the city as First Secretary of the Embassy, focusing on science and technology companies. However, his real hobby was espionage (Urban, 2018: 7-12). Skripal was a military intelligence (GRU) colonel at the Russian diplomatic legation, whose mission focused on recruiting human sources and obtaining information of military interest for onward transmission to Moscow. But his regular strolls through the Retiro were being studied by a young British Foreign Intelligence (MI6) officer named Richard Bagnall, based in Gibraltar. Bagnall deployed an operation in the centre of Madrid aimed at recruiting a veteran of Russian military intelligence, persuade him to defect and, together with his family, travel to the UK.

4. Understanding the organisation, structure, functioning and activities of foreign intelligence services

Counter-intelligence is ingenuity aimed at discovering and learning about the intelligence efforts of the opposing service. The task involves understanding and exploiting the competitor's dependency, and requires the use of detailed detective work in the operational detail of the clandestine world, winning meetings, appointments and interviews, setting up locations where messages and intelligence can be exchanged as if they had never occurred (Hitz, 2004: 5-7).

One of the activities carried out by counter-intelligence is the sacrosanct study of rival services and constitutes an analysis-oriented procedure. In other words, it is an analytical process to reveal or unmask the adversary's behaviour and how they define and fulfil their goals.

4.1. The intelligence services of the Russian Federation

The Soviet security apparatus has evolved very little over the last hundred years. The KGB (Committee for State Security) of the past and today's agencies that make up the conglomerate of the Russian intelligence services (the FSB, SVR and GU), were and are the Russian state's tools to intervene in the lives of its citizens and to conduct foreign policy (Barron, 1974: 391).

Founded in 1917, as a state surveillance, investigation and security apparatus, the "Cheka" was established itself as a terrorist organisation with the aim of exterminating and eliminating citizens who expressed their opposition to communist policies. It became an army of 31,000 civil servants and an institution geared towards the performance of a set of skills and attributes that, to this day, endure in Russian society (Barron, 1974: 392).

Image 1. Evolution of the USSR Intelligence Service (KGB).
Source: Author's own elaboration based on the work of Christopher Andrew and Vasili Mitrokhin (1999: xi).

In February 1922, the State Political Directorate (GPU) replaced the Cheka. A new body subordinate to the People's Commissariat for Internal Affairs (NKVD), with functions of militia control and conventional police (Lucas, 1966: 269). The following year, the GPU would become the Joint State Political Directorate (OGPU) (Barron, 1974: 393). Subsequently, by Stalin's order of July 1934, the OGPU would be transformed (Barron, 1974: 394) into the Main Directorate of State Security (GUGB), under the aegis of the NKVD.

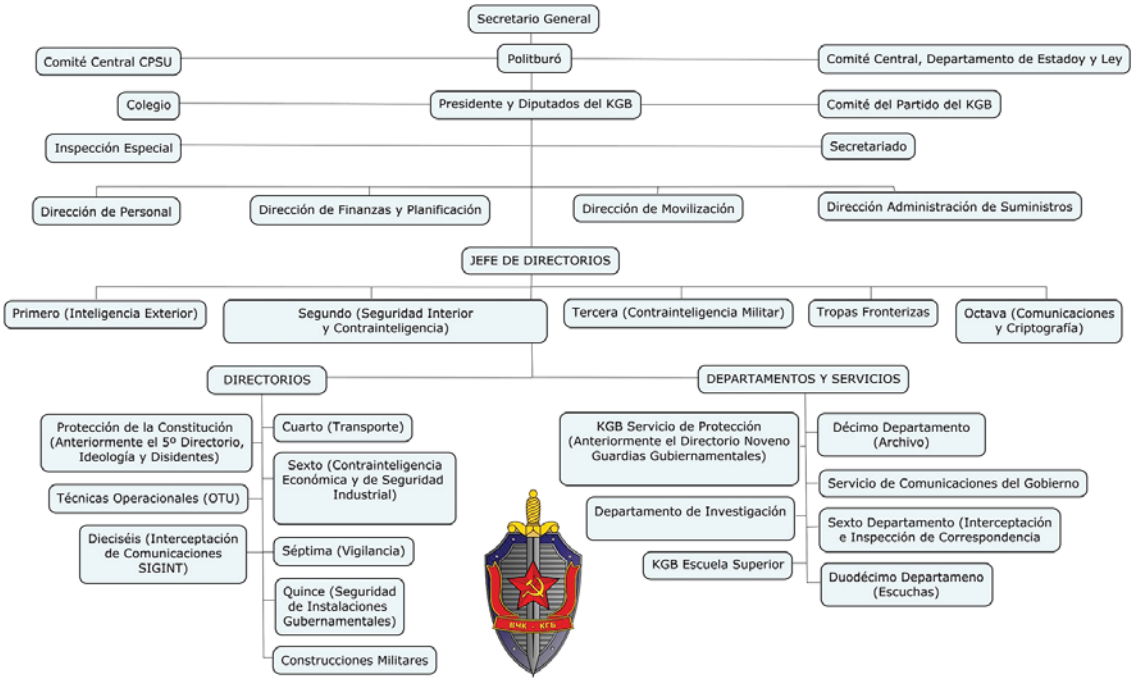


Image 2. Organisation of USSR's Domestic Intelligence (KGB).
Source: Author's own elaboration based on the work of Christopher Andrew and Vasili Mitrokhin (1999: 741).

In 1936, the first secret unit dedicated to ethnic cleansing and torture was established within the NKVD's Directorate for Special Tasks (Andrew, 2018: 654). The unit was tasked with carrying out targeted assassinations on the orders of the Kremlin (Richelson, 1995: 252-253). It remained in operation until 1954 (when it was reassigned to the 13th Department of the first KGB Directorate).

In 1941, the political police was transformed into the People's Commissariat in Charge of State Security (NKGB) (Barron, 1974: 394). And shortly afterwards, in 1946, the NKGB intensified its clandestine activities abroad (Lucas, 1966: 269), and especially in the United States (US), albeit as Ministry of State Security (MGB).

In 1947, the Committee of Information (KI) was created, taking over the responsibilities of of the MGB overseas section (Lucas, 1966: 269) and incorporated units of the Ministry of Foreign Affairs and the Military Intelligence Service (Barron, 1974: 395).

After Stalin's death in 1953, the Soviet security apparatus was restructured into a new entity, the Committee for State Security (KGB), which was assigned the functions of political police, clandestine operations and the surveillance and control of the USSR's borders (Lucas, 1966: 269), except for the illegal and covert operations of the Military Intelligence Service (GRU) (Barron, 1974: 395-296).

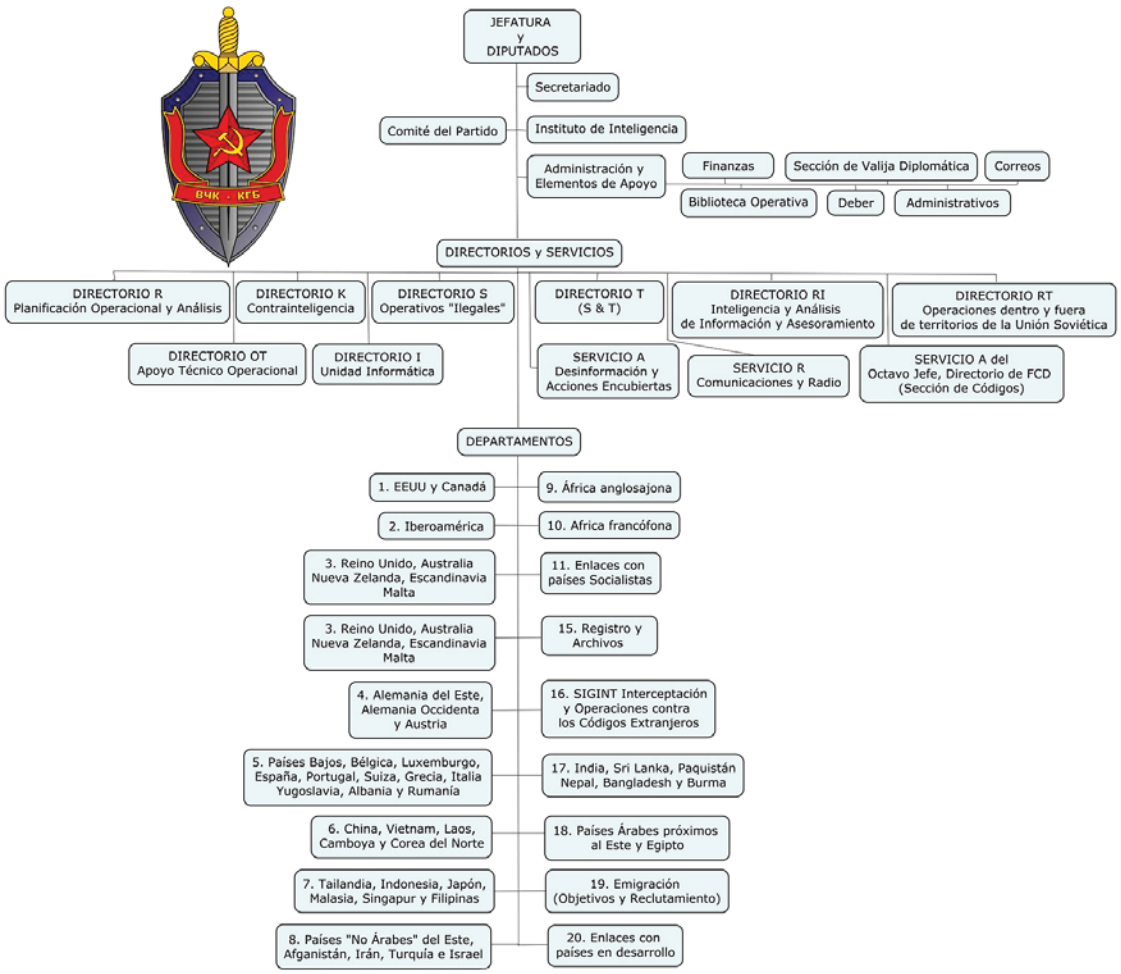


Image 3. Organisation of USSR's Foreign Intelligence (KGB).
Source: Author's own elaboration based on the work of Christopher Andrew and Vasili Mitrokhin (1999: 742).

From its inception, the KGB exercised effective control over land and sea borders (Barron, 1974: 25), the surveillance and investigation of citizens, as well as the residences and offices of Communist Party leaders (Barron, 1974: 25-26). The KGB not only monitored the interior of the USSR, but had a network of spies that eventually reached the fridges of Russian society, from the General Staff of the Red Army to the humblest village.

Such was the control exercised that it was very difficult for foreigners arriving in the USSR to escape the shadow of the security apparatus (Barron, 1974: 27). The KGB embedded its officers in key positions after deploying them in the colossal Soviet bureaucratic apparatus and in the Communist Party hierarchy (Barron, 1974: 26).

The power attained by the KGB and the trust placed in its officers led to it being entrusted with the custody of the USSR's nuclear warheads (Barron, 1974: 25).

4.2. Federal Security Service (FSB)

The current Federal Security Service of the Russian Federation (FSB) inherited its functions from the defunct KGB, although a considerable part of its human capital came from the Border Guard Service (PFS) (Riehle, 2022: 65), which had become the main agency of the internal security apparatus of the communist regime. Its resources and human capital are devoted to domestic intelligence and counter-intelligence activities.

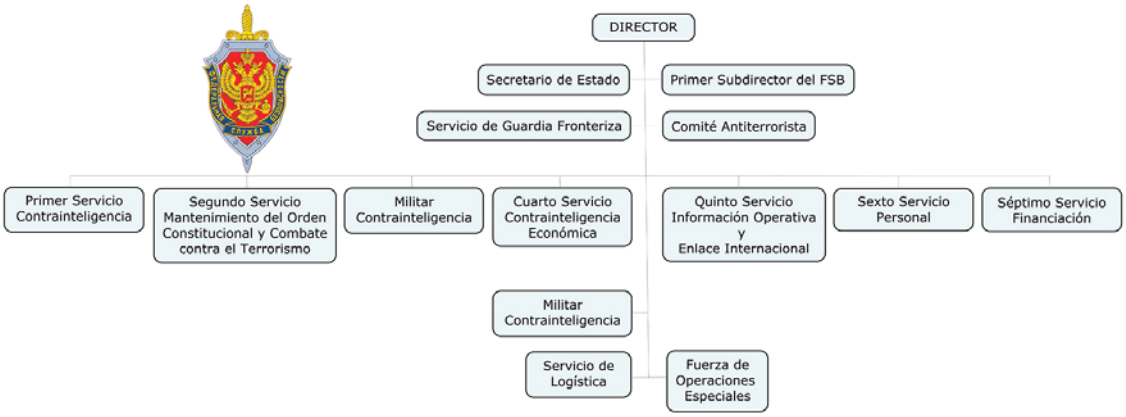


Image 4. Organisation of the Domestic Security and Intelligence Service (FSB).
Source: Author's own elaboration based on the work developed by Kevin P. Riehle (2022: 66).

It could be argued that the FSB's counter-intelligence unit is, in fact, the remnant of what used to be second main directorate, and one of the main units, of the KGB. Its activities are aimed at thwarting the operations of foreign intelligence services operating on the territories of the federation, penetrating foreign legations, harassing their diplomatic staff and investigating Russian citizens with whom foreign diplomatic staff come into contact .

The FSB also has its own military counter-intelligence service, a remnant of the KGB's third main directorate, which monitors the loyalty of the armed forces and conducts investigations within military units (Remnick, 1991).

Finally, it inherited the KGB's "Alpha" and "Vympel" units[6] (the latter, an assassin squad that could be deployed around the globe) dedicated to the execution of covert special operations abroad (Andrew, 2001: 389).

4.3. Foreign Intelligence Service (SVR)

The SVR is Russia's foreign intelligence service, the apparatus in charge of developing intelligence activities abroad (Riehle, 2022: 61), and the direct descendant of the first main directorate of the KGB.

Russian foreign intelligence has a human capital of approximately 12,000 to 14,000 employees, a quarter of whom, just over 3,000, operate abroad. Its organisational structure is divided into three areas: "operational actions", "analysis" and "functional activities".

– Directorate PR (Political Intelligence) is responsible for developing political intelligence operations (Riehle, 2022: 62), and draws on personnel who were part of the KGB's main directorate.

– Directorate NTR (Scientific-Technical Intelligence) is in charge of the production of scientific-technical intelligence aimed at gathering operations and acquiring technologies to preserve security and defence against modern Western weapon systems (Riehle, 2022: 63), a successor to the former KGB T-Directorate.

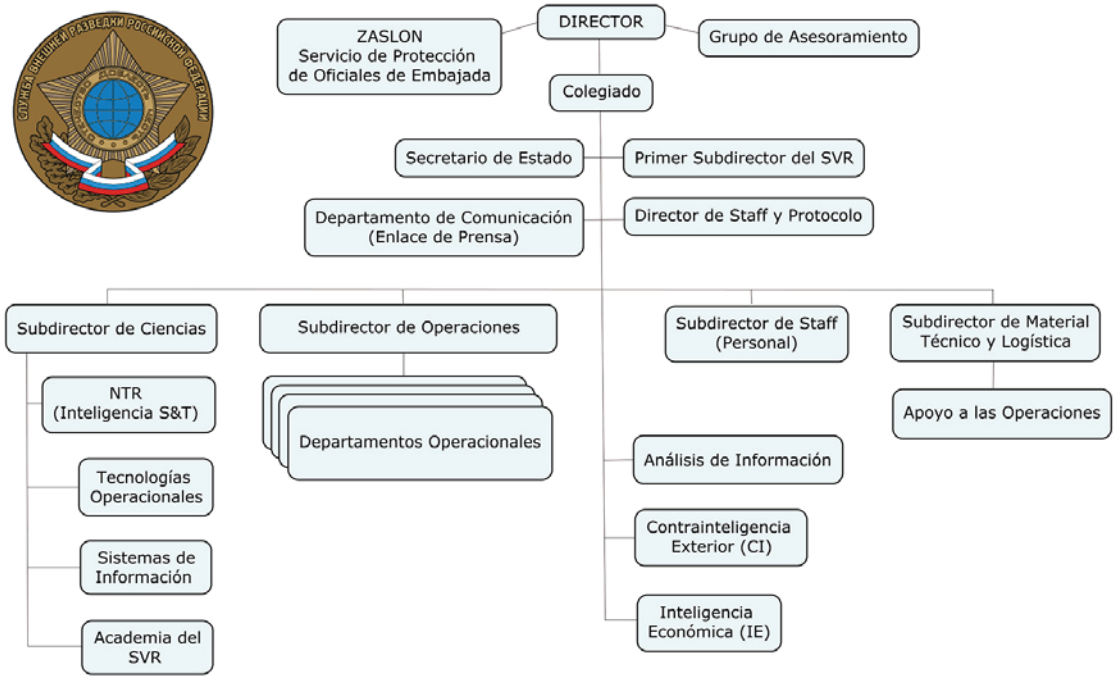


Image 5. Organisation of Foreign Intelligence (SVR).
Source: Author's own elaboration based on the work developed by Kevin P. Riehle (2022: 62).

6 Navruzbekbekov, Emran. FSB counter-intelligence (defected senior lieutenant of counterintelligence service). Available at: https://igorsushko.substack.com/p/fsb-counterintelligence-senior-lieutenant
https://igorsushko.substack.com/p/fsb-counterintelligence-senior-lieutenant-160

- Directorate ER (Economic Intelligence) is responsible for producing intelligence linked to the functioning of Western economic systems, with the task of influencing and interfering with them (Riehle, 2022: 63), with offices in the SVR's diplomatic stations abroad.
- Directorate S (Illegal Intelligence) is in charge of undertaking illegal operations and conducting missions in wartime environments, including war scenarios such as, for example, the "special military operation against Ukraine". To this end, it has a number of departments: the international area; recruitment and training of illegal operatives; and planning, financing and logistics for transport abroad. Missions are directed from overseas *rezidenturas* or stations (Riehle, 2022: 63).
- Directorate KR (Foreign Counter-intelligence) directs counter-intelligence operations and plans the penetration of foreign intelligence and security services, managing the missions from stations (Riehle, 2022: 64).
- Directorate MS (Support Measures) is in charge of developing support activities and undertaking "active measures", exploiting the intelligence gathered for the design and execution of influence operations in support of Russian foreign policy priorities (Riehle, 2022: 64).

Finally, the foreign intelligence service also has Zaslon teams (Riehle, 2022: 65), responsible for executing special operations and covert missions, with operational bases in diplomatic missions abroad.

4.4. Main Directorate (GU)

In totalitarian regimes, military intelligence structures coexisted with services of a political and police nature, and overlapped with other espionage organisations (Navarro, 2009: 49).

Similarly, the Russian Federation can count on the Main Directorate (GU), a military intelligence service that until 2010, operated under its former acronym "GRU" for Main Intelligence Directorate (Riehle, 2022: 73). It reports to the General Staff. Its primary mission is to gather information on military secrets related to military strategy, tactics and techniques, as well as to participate in intelligence operations (Barron, 1974: 397) aimed at the strategic defence industry of NATO countries.

The GU has military personnel in all embassies, from where they plan and execute operations and report back to Moscow through their own security channels and encryption methods. Most military attachés posted to diplomatic missions abroad are members of the GU (Barron, 1974: 397).

Military intelligence is also involved in clandestine operational arrangements (Barron, 1974: 397), although their targets include attacks directed against power transmission lines, oil pipelines, undersea cables and communications systems, as well

as large strategic technological and industrial complexes for the defence of NATO allies (Riehle, 2022: 179).

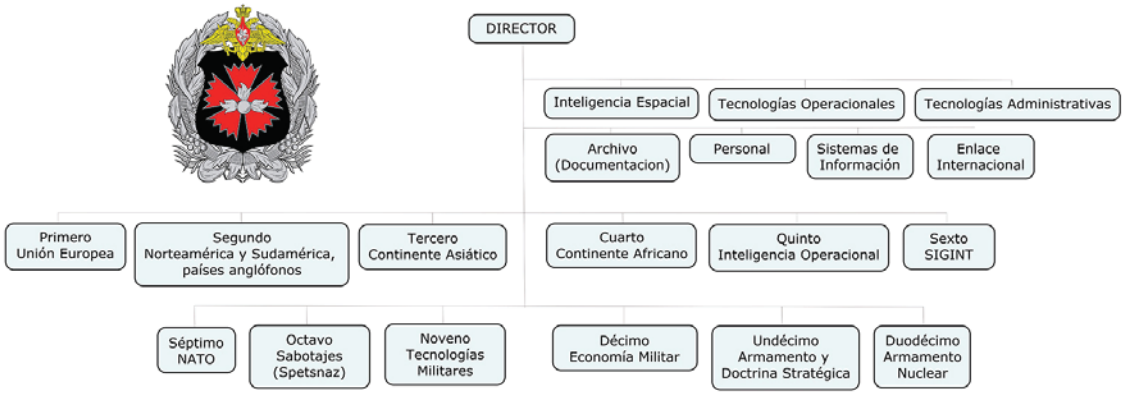


Image 6. Organisation of the Military Intelligence Service (GU).
Source: Author's own elaboration based on the work developed by Kevin P. Riehle (2022: 74).

It should be pointed out that GU activity revolves around three key focal points. The first is aimed at obtaining intelligence on the basic elements of a specific military force, which it might face in the future in a war. The second is directed at obtaining information and intelligence on strategic forces and nuclear and missile defence capabilities. The third is focused on intelligence gathering, analysis and planning of attacks on the critical infrastructure of countries that would support military intervention against the Russian Federation (Riehle, 2022: 165).

Intelligence gathering for military decision-making is a genuine GU activity (Riehle, 2022: 166), irrespective of whether the SVR manages the sources that provide information relaed to the Russian military from abroad.

5. A brief review of counter-intelligence errors: casuistry

In counter-intelligence, errors are a major concern for intelligence services. It is tempting to assume that foreign intelligence agencies will behave in a friendly manner, especially when they intervene in foreign countries they regard as adversaries. The basis of counter-intelligence work therefore consists of a thorough and individual examination of rival services (Ehrman, 2009: 46). This discipline is set out as a technical-analytical process whose goal is to understand the behaviour of the opposing service and to discern how it designs, plans, defines and executes its operations, because each service has different actions, as evidenced by the comparative study. Learning about their behaviour offers enormous potential for interpreting and guessing a wide variety of useful penetrations.

It is advisable to consider the following questions: should we know the history of counter-intelligence? Is it worth examining, analysing and learning from counter-intelligence failures and mistakes? Is it essential for counter-intelligence officers to be trained in casuistry?

James M. Olson, in his work *To catch a spy: the art of counterintelligence* (Olson 2019: 50), and "*he ten commandments of counterintelligence* (Olson, *et al.* 2004a: 251-258), states:

> "I find it inconceivable that any counterintelligence practitioner today could ply his or her trade without an in-depth knowledge of the Angleton era. Have our officers read Mangold? Have they read Legend and Wilderness of Mirrors? Do they know the Loginov case, HONETOL, MHCHAOS, Nosenko, Pollard, and Shadrin? Are they familiar with Aspillaga and the Cuban double-agent debacle? Have they examined our mistakes in the Ames and Howard cases? Are they staying current with recent releases like The Mitrokhin Archive and The Haunted Wood? I believe it is an indispensable part of the formation of any American CI officer... to study the CI failures of the past, to reflect on them, and to make sure they are not repeated".

Markus Wolf (Wolf, 1997: 232-235), considered communism's greatest spymaster and the top intelligence officer of the Eastern Bloc, expressed that:

> "The Union of Soviet Socialist Republics (USSR) was a sorry creature, poorly coordinated and doomed from birth, inferior in many ways to its arch-rival the United States. But, in truth, the Soviet services were able to achieve the best successes in the United States and Europe, before and during World War II, when they relied on the communist party and the intelligentsia in many countries, such as Germany, the United Kingdom and the United States, because the agents recruited during that period were the best and offered the USSR advantages in the nuclear race. Nobody betrays their country for money alone, although the Americans used money as a recruiting tool, and the KGB did the same".

5.1. Russian foreign intelligence successes

The success achieved by Russia's purely offensive foreign intelligence has shown that it has been excessively aggressive and violent. In reality, the recruitment and penetration of their illegals takes precedence if we equate this with the disparity of regular information gathering and disinformation propagation (Olson, 2004b: 67), in their infiltration of European Union and NATO countries. And one of the most recent episodes took place in the Netherlands, where seventeen Russian foreign intelligence and military intelligence officers (eight SVR spies together with nine GU spies) planned operations for the recruitment and penetration of their illegal agents[7].

Here, very briefly, are five events that we consider to be notable successes of Russian foreign intelligence in the West.

7 *NL TIMES.* (2022). Russians expelled from NL were spying on high-tech sector, recruiting informants: report. (Netherlands). Available at: https://nltimes.nl/2022/10/14/russians-expelled-nl-spying-high-tech-sector-recruiting-informants-report

The first case occurred in 1951, when Harry Frederich Houghton, a Royal Navy military attaché stationed at the British embassy in Warsaw, Poland, committed treason. The secret information provided to the Russians (delivered in London on the first Saturday of every month) focused on submarine weapons, antisubmarine warfare systems information, and British nuclear submarine technology (Andrew, 2015: 564-565). Houghton provided Russian intelligence with a significant amount of secret information.

The second case occurred in 1978, and involved Glenn Michael Souther, a US Navy sailor-photographer stationed on the *USS Nimitz* based in Naples, Italy. While at the Neapolitan naval base, Souther married an Italian woman named Patrizia di Palma. However, in collusion with his wife, he maintained a life far removed from a conventional marriage by engaging in frenetic pro-communist activity and expressing admiration for the USSR. What is surprising is that his superiors never reported the countless episodes in which Souther publicly and repeatedly expressed his dissatisfaction and disapproval of US government policies. The situation worsened in 1980, after he visited the Russian embassy in Rome to claim Soviet citizenship. He was recruited by the KGB and he began to bleed information and make a significant amount of documentary material available to Russian foreign intelligence (Olson, 2019: 157-164).

The third event occurred during the 1980s, perpetrated by Clayton Lonetree, a US Marine Corps sergeant stationed at the US embassy in Moscow. Sergeant Lonetree was recruited by the KGB through Violetta Seina, a 25-year-old intelligence officer who managed to seduce Lonetree. The marine sergeant's collaboration with Soviet foreign intelligence began after his transfer to the US embassy in Vienna, Austria, and consisted of providing them with the blueprints of the US diplomatic missions in Moscow and Vienna, including the identities of undercover agents operating in the USSR (Olson, 2019: 113-116).

A fourth case of treason came from Earl Edwin Pitts, an officer in the FBI's counter-intelligence office in New York City. Agent Pitts' activity focused precisely on Soviet intelligence operations in New York State. But in mid-1987, after being the victim of several episodes of humiliation due to demanding working conditions and family financial difficulties, he ended up betraying his country by offering his services to the KGB (Olson, 2019: 127-132). The documentation provided to Soviet foreign intelligence consisted of counter-intelligence operations, surveillance and observation methods, double agents and information that the New York FBI office had on KGB personnel who could be recruited.

Finally, the most outlandish case occurred in Italy in 2018, in the shadow of NATO's Allied Joint Force Command and the US Navy in Naples (Italy), at the hands of Maria Adela Kuhfeldt Rivera (known as Olga Kolobova), an SVR officer acting illegally in Europe. After settling in Naples, she used a jewellery design and the luxury goods trade business (Serein SRL) as a front to prove her residence in Italy. Maria Adele penetrated various social circles in Naples after forming a network of contacts that included US Navy officials who provided her with graphic documentation of the base and files containing confidential information and secrets. When her cover was blown,

Kuhfeldt fled to Moscow, using a passport with a serial number from a list of passports commonly used by Russian foreign military intelligence officers[8].

5.2. The use of double agents

From a skill-set point of view, the most challenging discipline of intelligence is counter-intelligence, and the most complex subspecialty of counter-intelligence is the double agent.

James M. Olson, former head of the CIA's Counterintelligence Division, and who held a position of enormous responsibility within the Directorate of Operations (Olson, 2019: 86), argues that: "Double agent actions are the caviar of counterintelligence operations, because there is nothing more delectable for a counterintelligence professional than to dupe his or her adversary, particularly one that prides itself on being clever and sophisticated, with a controlled case".

It is necessary to define what a double agent is, as the concept is very often misinterpreted and misused by journalists, writers and even officials themselves. And likewise, in terms of its terminology, when it is used to describe people such as Edward Lee Howard, Aldrich Hazen Ames, Harold James Nicholson, Edwin Earl Pitts, Jonathan Pollard and many others. Thus, the use of the term double agent is erroneous (Olson, 2019: 86-87).

No one can be a double agent without first being an agent. The FBI, CIA or any other US agency official is not an agent the sense of intelligence because CIA agents are case officers and FBI agents are special agents. The situation in Spain is very similar. On the other hand, the controversy arises when the term "agent" is used. Its use is enormously confusing because, in intelligence terms, "an agent is someone recruited by a foreign intelligence service". Accordingly, Robert Hanssen as well as Aldrich Hazen Ames were Russian agents, Jonathan Pollard was an Israeli agent, and Joey Chun was a Chinese agent, but "they were not double agents". They would have been if their recruitment by Russians, Israelis or Chinese was a ruse and they remained loyal and responsive to US intelligence (Olson, 2019: 86-87).

The double agent is used to provide the opposing service with false information, although this is a rare target. Deceiving the enemy with this methodology requires excellent planning and great subtlety because the opposing service is not stupid and often has the means to verify the validity of the double agent's reports.

We must emphasise how valuable it is for Spanish counter-intelligence to know how adversary intelligence services, such as Russian foreign intelligence, operate. And it is an essential step towards defeating them. Defectors and field penetrations can be

8 Grozev, C. (2022). Socialite, widow, jeweller and spy: as a GRU agent she charmed NATO circles in Italy. *Bellingcat* (UK). Available at: https://www.bellingcat.com/news/2022/08/25/socialite-widow-jeweller-spy-how-a-gru-agent-charmed-her-way-into-nato-circles-in-italy/

of great help, but there is no better position to know what is happening on the ground than to have a cleverly infiltrated double agent.

In parallel, we have methods for initiating a double agent operation, although the most classic method is for the agent to enter a foreign embassy, ask to speak with the security or intelligence officer, and volunteer to cooperate (Olson, 2019: 104).

Ultimately, the ideal double agent should have good, but not spectacular, access. If that agent has significant access to an area considered a high priority for the opposing service, the agent will be enthusiastically recruited but will subsequently be required to provide an output that exceeds our willingness to hand over. Thus, double agent operations are extremely sensitive lines of action, so the material to feed the opposing service must match the claimed access to the double agent and be good enough to sustain the operation, but not too damaging to the service itself.

5.3. Active measures (political warfare): disinformation and deception

For decades the USSR sponsored large-scale hoaxes aimed at disorienting, confusing and inflaming international public opinion. Sometimes the subterfuges employed produced far-reaching effects, but in other situations they produced unpredictable consequences (Barron, 1974: 197). So the launching of such unpredictable activities, aimed at creating confusion and disorientation, ultimately harmed Soviet interests, making it yet another victim of its own fallacies.

Disinformation and deception originated in early Leninism, following the emergence of a contemporary concept called "*dezinformatsiya*" or disinformation, also defined as the "dissemination of false and provocative reports". Over the years, the KGB refined the practice and disinformation became much more complicated than what disinformation was defined as. It entailed providing forged or fabricated documentation, including letters, manuscripts and photographs of the like, and spreading false or ill-intentioned rumours and misinformation using outside agencies. Moreover, those visiting the country would be deceived, and other material actions were perpetrated to exert a psychological effect (Barron, 1974: 199). The techniques were exploited in a variety of ways to influence the policies of Western governments, thereby disrupting relations between countries and undermining people's trust in their leaders and institutions.

It should be stressed that the KGB conducted covert political operations that were initially labelled as "active measures" (political warfare) (Riehle, 2022: 190), focusing on covert political manipulation during the Cold War period (Andrew, 2015: 292). And the United States has been the primary target of active measures led by Russian foreign intelligence, which are at the non-violent end of the active measures spectrum: "influence operations designed to discredit the adversary" (Andrew, 2015: 293).

The extent of "active measures" became known to us thanks to information provided by Ladislav Bittman, a former Czech intelligence officer and defector,

who was deputy head of the "department of active measures and disinformation". Bittman described in detail how during the 1960s "entire bureaucracies in the Eastern Bloc administration were developed with the aim of confusing adversary countries and manipulating the facts", and how such projects were proposed and authorised. In his daily work, Bittman was required to acquire new professional skills as he had to learn how to gather, combine and entangle precise details. In order for disinformation to be successful, it had to respond partially to reality or at least to accepted views. For half a century, the leaking of stolen documents was standard procedure for the implementation of disinformation activities (Rid, 2020: 5-8).

Disinformation reached its peak in the mid-2010s, in the midst of the fourth wave of disinformation, having been reshaped by the use of new technologies and the internet (Rid, 2020: 14-15). The old art of slow, highly skilled, short-range and laborious psychological influence gave way to a new psychological influence that had become hasty, indiscriminate, remote and unconnected.

There is controversy about the difficulty of recognising an active measure because disinformation, when done well, is very difficult to detect, and especially when it is first made public. So it will be very useful to clarify what is an active measure and what is not. First of all, active measures are not spontaneous lies of politicians, but the methodical production of huge bureaucratic apparatuses. Disinformation was, and in many ways continues to be, the domain of intelligence services, albeit enhanced and professionally managed, being employed against foreign political opponents. Second, most active measures contain an element of disinformation: content may be falsified; sources may be imitated; the method of acquisition may be covert; specialist influencers may be something they are not; and online accounts involved in the appearance or amplification of an operation may not be real. Finally, an active measure aims to achieve an objective, such as weakening an adversary, but the means used can vary: creating divisions between allied nations; driving wedges between ethnic groups; creating friction between individuals in a political party or group; or undermining the confidence that certain groups have in their institutions. At the same time, active measures may be aimed at achieving a very specific purpose, such as eroding the legitimacy of a democratic government, destroying the reputation of an individual, or affecting the deployment of a weapons system (Rid, 2020: 10-11). Ultimately, projects are designed to facilitate a defined policy decision.

In 1992, the British Secret Intelligence Service (SIS) told the historian Christopher Andrew about the vicissitudes that led to the defection and extraction from Russia of Vasili Mitrokhin, an intelligence officer specialising in archives and documentation (Andrew, 2015: xxii-xxxix). The spy provided a wealth of top-secret documentary material from the third department of the KGB's foreign intelligence directorate (Andrew, 2015: 742), revealing the identities of "hundreds of illegal spies" then operating in the West. In other words, the documentation provided by Mitrokhin facilitated the task of tracking down and identifying true legends of Russian foreign espionage (Andrew, 2015: xxii-xxxix).

The meaning of the definition "active measures" (also offered by Mitrokhin to British intelligence) was as follows:

– The activity carried out by an operational agent aimed at influencing the domestic and foreign policies of target countries in the interests of the USSR (Riehle, 2022: 190). It was to weaken the political, military, economic and ideological positions of capitalism and undermine its aggressive plans, in order to create favourable conditions for a successful implementation of the foreign policy of the USSR, today the Russian Federation.

– It would involve one or more actions carried out clandestinely by intelligence officials, or the use of agents or other means on their own account, aimed at completing intelligence or counter-intelligence tasks (Mitrokhin, 2002: 11).

5.4. Quiet measures: covert operations

Intelligence has dual disruptive function. First, it is an operational activity in the sense of gathering, collecting and capturing information and intelligence; and second, it is the design, planning and execution of covert operations.

While knowledge-generating intelligence activities are developed through information collection to support the regime's decision-making process, clandestine and covert operations implement that very political decision (Riehle, 2022: 187).

It should be clarified that the definitions "clandestine" and "covert" do not mean the same thing. The clandestine conceals the operation, while the covert conceals the operator.

Thus, the definition "covert" means that the sponsoring government does not want to reveal its involvement, and such a methodology includes covert sabotage in which a target is damaged, such as when a bomb is detonated or when the service provided by a computer system is permanently disabled. The main element of covert activities is defined by the term "plausible deniability", whereby the action is visible but the identity of the perpetrator remains hidden and out of sight.

When it comes to covert operations in times of war, it is actually military officers who are responsible for carrying out incursions into enemy territory (e.g., the military invasion of Ukraine by the Russian army) in order to carry out various activities and operations. And it was defected intelligence officers during the Soviet era who provided an insight into the extent to which the armed forces were able to carry out their covert activities effectively.

Judging by the information provided by KGB defectors Oleg Lyaling, Oleg Kalugin and Vasily Mitrokhin, it was the DRG (Distraction Intelligence Groups) who, during the war, obtained the intelligence gathered on the adversary's targets and those who executed operations against them (Riehle, 2022: 188), with the aim of:

- Stirring up disorder in the enemy's rearguard functions.
- Disabling transport and communications.
- Spreading panic among enemy troops and the civilian population.
- Gathering intelligence on movements, armaments, militarily significant industrial facilities and their means of transport and communications.
- And assassinating the enemy's top and middle management, including political and administrative officials.

In July 2015, John B. Emerson,[9] as US ambassador to Berlin (Germany), opened the *Exposing Russian Disinformation in the 21st Century* conference, hosted by the Atlantic Council, the European Council on Foreign Relations and the Heinrich Böll Foundation, at which he argued that historical and current disinformation operations show a pattern of activity that can be described as "the 4D" approach:

- *Distort*. They twist real information; they hold on to a truth and reframe it in a different light to make it seem more or less appealing. Russian-driven activity using the World War II narrative, an undeniable talking point that they twist to achieve their political goals.
- *Distract*. They divert attention from real information, as happened in 2014 after the downing of Malaysia Airlines flight MH17 while flying over Ukraine. The Russian propaganda media conceived and disseminated multiple contradictory stories that lacked credibility, but all emphasised that responsibility did not lie with the Russian Federation. A similar case occurred with the Russian operations that leaked information on athletes from several countries who had allegedly violated doping rules. This was done to divert and take public attention away from the Russian doping programme.
- *Dismiss/Deny*. In March 2018, Vladimir Putin was able to boldly deny that Russian troops were involved in the seizure of Crimea and supporting insurgents in Ukraine, and deny that the Kremlin had any responsibility for the attempted assassination of Sergei Skripal (former GU officer).
- *Dismay*. They stir up fear, hatred or revulsion. Such as the claims that were spread in Russia in 2016 that German troops raped a girl in Lithuania.

Another category of "covert activities" that had been professionalised was kidnapping, and used as a weapon of last resort since the creation of the KGB's First Directorat . The *modus operandi* of kidnapping abroad remained largely unchanged. After locating political opponents or traitors of interest to the Kremlin, special

9 Emerson, John B. (2015). *Exposing Russian disinformation*. Atlantic Council Ukraine Alert. 29 June. (Berlin, Germany). Available at: https://www.atlanticcouncil.org/blogs/ukrainealert/exposing-russian-disinformation

teams would carry out abductions and assaults, and people would be transported hidden inside vehicles with diplomatic protection plates or driven to Czechoslovakia under false arrest. Once there, the final outcome depended on orders from Moscow (Richterova, 2023: 12-13).

The operations to eliminate people became an important issue for political and journalistic discussion in the West after the reported killings inside and outside Russia. The August 2020 attempt on the life of opposition leader Aleksei Navalny brought the plot into the spotlight.

Russia currently differentiates its covert assassination operations into three categories: "military targets", "political targets" and "traitors". At the same time, it divides the scenarios for such operations into two location types: "those perpetrated in the interior of the country" and "those executed elsewhere in the world" (Riehle, 2022: 201-202). Accordingly, the approach to eliminating opponents differs significantly whether they are perpetrated inside or outside Russia. Within the federation, military targets are by far the most important category, and the North Caucasus is a case in point (Riehle, 2022: 202). Military targets outside the federation are a relevant category, although generally speaking they are lower than those perpetrated inside the country. Political targets would be next on the list.

6. Use of structured analytic techniques by the counter-intelligence analyst

Before discussing the use of modern structured analysis techniques and their application to the discipline of counter-intelligence, we need to clarify some aspects related to the analysis of the behaviour of other services, as well as those related to counter-intelligence analysis itself.

As we have explained, from a scientific point of view, we must highlight the importance of the "intelligence cycle" and "the analyst's working methodology" as a system (Esteban *et al.*, 2007: 59), which has been defined as:

> "The process of generating and communicating new, accurate knowledge tailored to the needs and requirements of a user by obtaining and processing appropriate information. That is, a sequence of activities by which information is obtained and converted into knowledge (intelligence) and made available to a user".

Thus, intelligence production can be presented as a set of organised sequences over several stages and, at the same time, within its analysis, which consists of (Esteban *et al.*, 2007: 52): "[...] the systematic examination of available information by establishing relations and inferences in order to identify the most significant facts and elements of a phenomenon or situation".

6.1. The counter-intelligence analyst's tasks

As a scientific method, the analysis has a taxonomy and knows what it represents as a classification of the elements that make up a field of information, by identifying, naming and cataloguing the various objectives that it comprises and then organising them into groups based on common factors, in addition to the existing categories of methods. (Heuer and Pherson, 2015: 45). These include: "expert judgement"; "quantitative methods using expert-generated data"; "quantitative methods using empirical data"; and finally "structured analytic techniques". It is necessary for the counter-intelligence analyst to know the processes of deductive and inductive reasoning, the development and elaboration of diagrams, mind maps, concept maps and diagrams, besides making, confirming or dismissing assumptions. They also need the ability and knowledge to measure the degree of association between data sets and variables through the use of correlation and regression techniques, the elaboration of scenarios, the use of theoretical and mathematical models, or the use of software tools and programmes and computer, statistical and information mining support (Esteban *et al.*, 2007: 52.53).

Image 7. Taxonomies of analytical methods. Author's own elaboration (2022).
Source: Richards J. Heuer Jr. & Randolph H. Pherson. SAGE Publications, Inc. (2015).

The work of the counter-intelligence analyst is focused on a very specific type of analysis, adapted to the deductive and inductive method and the validation or rejection of hypotheses, and includes the possibility of relying on other specific analytical methods such as structured analysis techniques.

6.2. Reasons for using structured analytic techniques

The duties of the counter-intelligence analyst can be described as the effort to protect operations from penetration, attack from hostile nations, and the protection of state secrets by studying and analysing opposing intelligence services and the many and varied factors that determine the behaviour of those services.

As the researchers Pherson and Heuer argue, it is one thing to advocate that analysts use structured analytical techniques in order to overcome the cognitive traps that lead to analytical failure (Pherson and Heuer, 2021): 17-22), but it is quite another to learn how to select, understand and use structured analytical techniques correctly. (Heuer and Pherson, 2015: 32-33). However, one of the main criticisms from the analysts themselves relates to the fact that they do not have enough time to use these techniques.

Consequently, we must rely on two common methodological models to address limitations in our memory functions (Heuer and Pherson, 2015: 32-33). The first has to do with decomposition, i.e. dismantling or deconstructing a problem into its component parts. So that each of these can be considered separately or independently. The second focuses on creating an orderly visualisation by placing the different parts on paper, a multimedia screen, tablet, or other device. This will allow us to understand how the different pieces of certainty relate to each other.

6.3. The most useful structured analytic techniques for counter-intelligence

Out of a total of sixty structured analytic techniques, we have selected eleven of them which are included in the following categories: "decomposition and visualisation techniques"; "idea-generating techniques"; "scenario techniques and indicators"; "hypothesis generation and testing techniques"; "cause-and-effect evaluation techniques"; "challenge analysis techniques"; and finally "decision support techniques".

Then, through a brief introductory presentation of the methodologies of interest, we will emphasise when to use them, what value they add, and what methodology should be used in each case.

Decomposition and visualisation techniques:

- Initial checklist: this is a methodological tool that allows us to initiate new projects, as long as long as we put them on the right track from the beginning, avoiding changes later on. The methodology saves time and increases the quality

of the final product (Heuer and Pherson, 2015: 70-71), and consists of answering a set of questions before starting the project (Hibss and Pherson, 2021).

- Chronologies / Timelines: two methodologies aimed at obtaining a graphical representation of time, allowing us to place events in the order in which they took place and the period elapsed between them, and can be used in cases where it is necessary to interpret times, the sequence of events and the identification or absence of key events, whether or not they have a cause-and-effect relationship (Heuer and Pherson, 2015: 75-78).

  In counter-intelligence, they are of great help in identifying patterns and correlations between the occurrence and relationship of unrelated events. It can provide an overview, identify significant changes, uncover trends, emerging issues and anomalies, portray influences, set out hypotheses about unknown events and, finally, organise data in an understandable visual format.

One. Idea-generating techniques:

- Structured brainstorming: a tool composed of a total of seven rules and twelve basic moves that allow us to identify a list of variables, driving forces, a wide range of hypotheses, stakeholders, indicators, sources of information, potential solutions to problems, outcomes and scenarios, suspects, and lines of enquiry (Pherson and Heur, 2021: 36). It is a tool designed to stimulate team thinking and creativity through a set of ideas that bounce from one place to another generating multiple perspectives and different points of view (Heuer and Pherson, 2015: 113-116).

- Nominal group technique: a methodology similar to structured brainstorming, which prevents a single person (a manager or senior executive) from dominating the discussion (Heuer and Pherson, 2015: 118-201).

Matriz de Impacto Cruzado

	Variable 1	Variable 2	Variable 3	Variable 4	Variable 5	Variable 6
Variable 1			+		-	
Variable 2			-	+	+	+
Variable 3	+			+		-
Variable 4		+			+	-
Variable 5	-	+		+		
Variable 6	-	+	-	-	-	

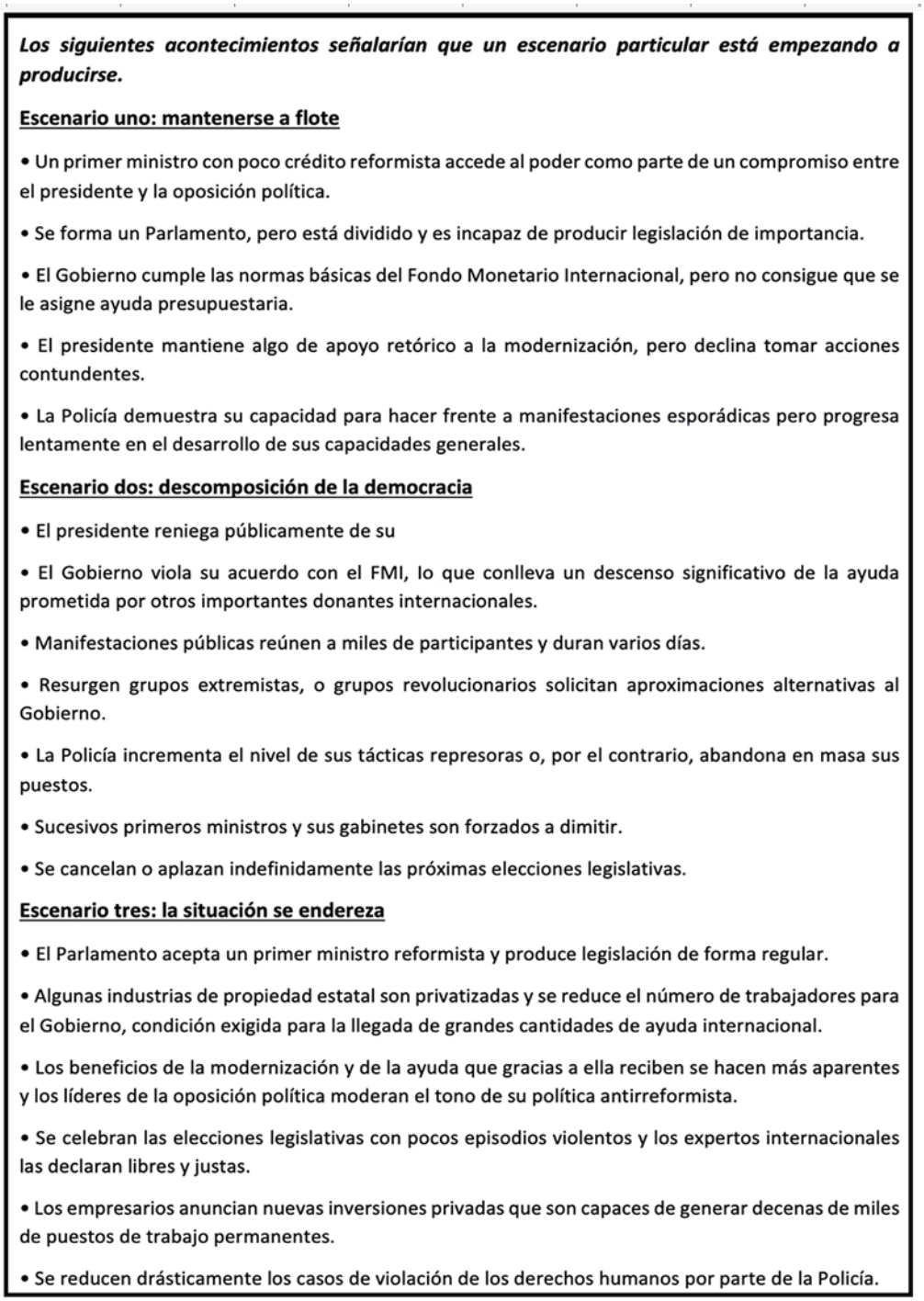
Direccion y magnitud del efecto:

+	Strong Positive
+	Positive
	Neutral
-	Negative
-	Strong Negative

Las variables 2 y 4 de la Matriz de Impacto Cruzado arriba mostradas tienen el mayor efecto sobre las otras variables, mientras que la variable 6 es la que tiene un mayor efecto negativo.

Image 8. Example of analysis using the cross-impact matrix. Author's own elaboration (2022). Source: Richards J. Heuer Jr. & Randolph H. Pherson. SAGE Publications, Inc. (2015).

- Starbursting: a methodological tool similar to structured brainstorming (Heuer and Pherson, 2015: 121-122). The starburst technique is designed to raise and generate questions rather than to elicit answers and ideas, by asking the following questions: Who? What? How? Where? When? Why?
- Cross-impact matrix: an extremely useful methodology to implement after structured brainstorming or the nominal group technique. Its use allows us to manage complex problems, especially when everything is connected to everything else (Heuer and Pherson, 2015: 122-126).



Los siguientes acontecimientos señalarían que un escenario particular está empezando a producirse.

Escenario uno: mantenerse a flote

• Un primer ministro con poco crédito reformista accede al poder como parte de un compromiso entre el presidente y la oposición política.

• Se forma un Parlamento, pero está dividido y es incapaz de producir legislación de importancia.

• El Gobierno cumple las normas básicas del Fondo Monetario Internacional, pero no consigue que se le asigne ayuda presupuestaria.

• El presidente mantiene algo de apoyo retórico a la modernización, pero declina tomar acciones contundentes.

• La Policía demuestra su capacidad para hacer frente a manifestaciones esporádicas pero progresa lentamente en el desarrollo de sus capacidades generales.

Escenario dos: descomposición de la democracia

• El presidente reniega públicamente de su

• El Gobierno viola su acuerdo con el FMI, lo que conlleva un descenso significativo de la ayuda prometida por otros importantes donantes internacionales.

• Manifestaciones públicas reúnen a miles de participantes y duran varios días.

• Resurgen grupos extremistas, o grupos revolucionarios solicitan aproximaciones alternativas al Gobierno.

• La Policía incrementa el nivel de sus tácticas represoras o, por el contrario, abandona en masa sus puestos.

• Sucesivos primeros ministros y sus gabinetes son forzados a dimitir.

• Se cancelan o aplazan indefinidamente las próximas elecciones legislativas.

Escenario tres: la situación se endereza

• El Parlamento acepta un primer ministro reformista y produce legislación de forma regular.

• Algunas industrias de propiedad estatal son privatizadas y se reduce el número de trabajadores para el Gobierno, condición exigida para la llegada de grandes cantidades de ayuda internacional.

• Los beneficios de la modernización y de la ayuda que gracias a ella reciben se hacen más aparentes y los líderes de la oposición política moderan el tono de su política antirreformista.

• Se celebran las elecciones legislativas con pocos episodios violentos y los expertos internacionales las declaran libres y justas.

• Los empresarios anuncian nuevas inversiones privadas que son capaces de generar decenas de miles de puestos de trabajo permanentes.

• Se reducen drásticamente los casos de violación de los derechos humanos por parte de la Policía.

Image 9. Example of an indicator list for monitoring emerging scenarios.
Source: Richards J. Heuer Jr. & Randolph H. Pherson. SAGE Publications, Inc. (2015). Revised (2022).

The technique of cross-impact analysis makes it possible to systematically examine how each factor, in a given context, influences other factors that appear to be linked or related. It provides an understanding of the complex situation that the analyst faces when forecasting future events, taking into account the dominant forces and potential future events that would influence a given outcome.

Three. Scenario techniques and indicators:

- Indicator list: a very useful tool in counter-intelligence, aimed at obtaining and detecting tactical alerts, operational alerts and even strategic alerts against future developments which, if they were to occur, would have a huge impact. It consists of a set of indicators that constitute observable and reviewable phenomena in order to assist in monitoring developments, identifying possible emerging trends or warning of unanticipated changes.
- The indicator list can provide us with an objective basis by tracking developments and introducing rigour into the analytical process and strengthening credibility (Heuer and Pherson, 2015: 150-156).
- This is done through a pre-established set of observable actions, conditions, facts, circumstances or events that, if they were to occur, would clearly indicate that an event has been triggered or that there is a possibility that it could occur (Pherson and Heuer, 2021:38).

Four. Hypothesis generation and testing techniques:

- Analysis of competing hypotheses (AHC): a tool for making judgements in cases where mutually exclusive alternatives are required. The AHC tool aims to eliminate errors in matters that are controversial by identifying the precise areas of disagreement and looking for traces of evidence, as well as showing how the analyst reached their conclusions (Heuer and Pherson, 2015: 175-180).

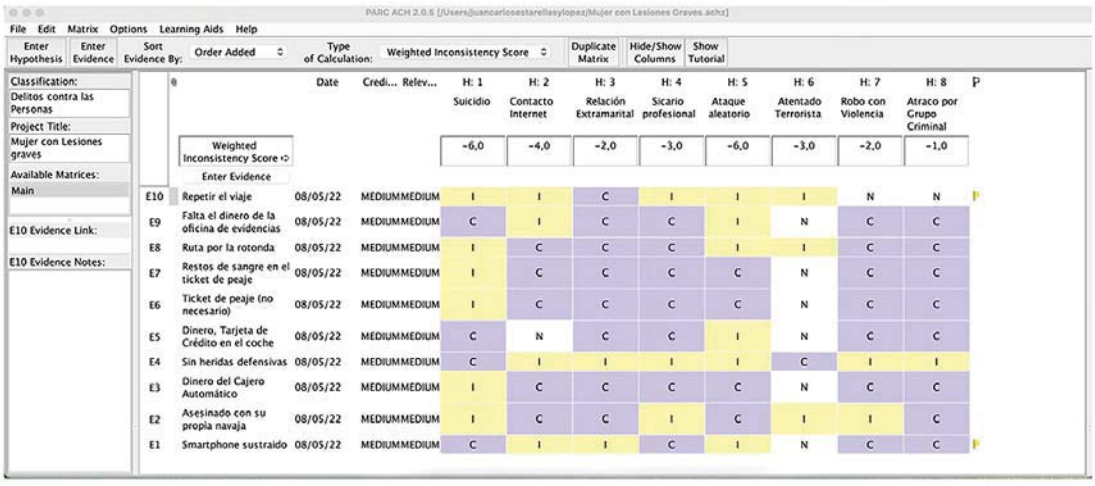


Image 10. Example of the analysis of competing hypotheses technique (software "PARC ACH v.2.0.5").
Source: Richards J. Heuer Jr. & Randolph H. Pherson. SAGE Publications, Inc. (2015). Own revision (2022).

It is useful when dealing with potential deception, and in particular effective in providing feedback on technical issues, enabling better analytical results (Pherson and Heuer, 2021:37.

A simultaneous assessment of multiple competing hypotheses without analytical help is complicated, as retaining three, five or seven hypotheses in memory, and recording how each piece of information fits into each of the hypotheses, is beyond the capabilities of most analysts. It requires greater mental agility than the usual practice of looking for evidence in order to test a hypothesis that is considered the most likely answer (Heuer and Pherson, 2015: 175-180).

Five. Cause-and-effect evaluation techniques:

- Key assumptions checklist: a methodology of combining evidence and assumptions and preconceived ideas, which influence the way evidence is interpreted, allowing to question and make explicit the assumptions that guide the analyst in interpreting the evidence and reasoning on a problem (Pherson and Heuer, 2021: 37).

  The technique requires a list of working assumptions to be drawn up at the start of the project in order to: identify specific assumptions that underpin the basic line of analysis; gain a better understanding of the fundamental dynamics at play; gain insights and new ideas; discover hidden relationships and links between key factors; identify developments that would result in the abandonment of an assumption; and, finally, avoid surprises when information emerges that invalidates old assumptions (Heuer and Pherson, 2015: 198-203).

Six. Challenge analysis techniques:

- What-if analysis: a tool to alert the command or decision-making body to an event that might occur. It is used to analyse unexpected scenarios that would have consequences if they were to occur. It is based on the existence of a supposedly sudden or random event accompanied by a potential conflict (Pherson and Heuer, 2021: 37-38).

  The analyst perceives and represents how the event would occur and what its consequences would be (Heuer and Pherson, 2015: 242-246).

Seven. Decision support techniques:

- SWOT analysis: a tool used by large companies, multinationals and business organisations due to its ease of use, which can be exploited by a single analyst.

What is its purpose? Assessing and scaling strengths, weaknesses, opportunities and threats inherent in any plan or project. It enables useful information to be generated with little effort, and brings it together in a framework that serves as a basis for further analysis (Heuer and Pherson, 2015: 299-231). In short, it is about designing and elaborating a plan to achieve a specific objective.

Análisis DAFO (SWOT)

	Positivas	*Negativas*
Internas	**Fortalezas**	**Debilidades**
	• Confecciona una lista con los atributos de la organización que resulten útiles para consecución del objetivo.	• Confecciona una lista con los atributos de la organización que sean perjudiciales para la consecución del objetivo.
Externas	**Oportunidades**	**Amenazas**
	• Confecciona una lista con las condiciones externas que sean útiles para la consecución del objetivo.	• Confecciona una lista con las externas que podrían ser perjudiciales para alcanzar el objetivo.

Image 11. Example of the SWOT analysis technique.
Source: Richards J. Heuer Jr. & Randolph H. Pherson. SAGE Publications, Inc. (2015). Own revision (2022).

7. Conclusions

The lack of trust within societies is a problem for modern states because it ends up feeding grounds for suspicion back into society. In such an environment, mistrust becomes the main basis of what counter-intelligence theory is all about. If all people were trustworthy, the work and activities of counter-intelligence units would be unnecessary. For these reasons, counter-intelligence is considered the most laborious, complex and difficult intelligence activity.

Nevertheless, counter-espionage was one of the most important and active dimensions of the rivalry and confrontation between the two main opponents, the West and the communist bloc, with Russia taking the lead.

It is important to underline the disruptive task of counter-intelligence departments as an offensive tool to counter threats. And following this line, we have described the main functions of the intelligence services whose mission is to detect and neutralise espionage intrusions perpetrated by adversary services operating on their own territory. In order to carry out these capabilities, but above all to face the challenge that Russia represents, it is necessary to have trained human capital and suitable instruments to counter the threat posed by its offensive intelligence and counter-intelligence.

We highlighted the transcendence of the double agent in counter-intelligence activities as he or she constitutes a disruptive offensive instrument against the thrust

of espionage, and who has the necessary ingredients to achieve successful penetrations into the ranks of rival services that intend to operate in Spain.

However, if we look the known counter-intelligence case load compared to the West's, we can note that the most successful incursions came from the Eastern Bloc. However, the lessons learned in each case provide relevant and pedagogical knowledge.

Finally, the more expert knowledge we have about the workings of Russian intelligence and foreign espionage in our country, the greater our chances of success.

We must conclude by stressing that counter-intelligence analysis has never been more necessary for political leaders and decision-makers. Recommendations are made in a highly technological global environment (in contrast to the bipolar dynamics between the Soviet Russian and Western blocs), with a significant number of failed states, proliferation, regional crises and international differences, emerging threats and the participation of non-state actors on the ground, in a context conducive to important transformations in complex areas such as technology and society. Our proposals are addressed to the analyst with the aim of overcoming criticisms of failure and increasing his or her analytical skills by studying and implementing a set of procedures for improvement via the use of structured analytic techniques.

Bibliography

Andrew, C. and Mitrokhin, V. (2001) *The sword and the shield*. USA, Perseus Books Group.

Andrew, C and Mitrokhin, V. (2015) *The Mitrokhin archive. The KGB in Europe and the West*. UK, Penguin Books.

Andrew, C. (2018) *The secret world. A history of intelligence*. UK, Penguin Random House.

Bardavio, J., Cernuda, P. and Jáuregui, F. (2000) *Servicios secretos* [Secret services]. Spain, Plaza & Janés Editores.

Barron, J. (1974). *KGB la labor clandestina de los agentes secretos soviéticos* [KGB: the clandestine work of Soviet secret agents]. Mexico, Editorial Diana.

Ehrman, J. (2004). *¿De qué hablamos cuando hablamos de contrainteligencia? [What are we talking about when we talk about counterintelligence?]* Manual Básico de Contrainteligencia. Volume 4. TIEV de la SHCP. Mexico.

—. (2009) *What are we talking about when we talk about counterintelligence? Studies in Intelligence*. Vol. 53, No. 2, 2009 (USA). Available at: https://www.cia.gov/static/867934afc1db19abcfcc5ced4193b676/toward-a-theory-of-ci.pdf

Emerson, J. (2015). *Exposing Russian disinformation*. Atlantic Council Ukraine Alert. 29 June (Berlin, Germany). Available at: https://www.atlanticcouncil.org/blogs/ukrainealert/exposing-russian-disinformation

Esteban Navarro, M. Á. *et al.* (2007). *Glosario de Inteligencia* [Intelligence Glossary]. Ministry of Defence (Spain).

Evanina, W. R. (2016). *National counterintelligence strategy of 2016*. Director of the National Counterintelligence and Security Center (NCSC), USA. Available at: *https://www.dni.gov/files/NCSC/documents/Regulations/National_CI_Strategy_2016.pdf*

Grozev, C. (2022). Socialite, widow, jeweller and spy: how a GRU agent charmed her way into NATO circles in Italy. *Bellingcat*, 25 August UK. Available at: https://www.bellingcat.com/news/2022/08/25/socialite-widow-jeweller-spy-how-a-gru-agent-charmed-her-way-into-nato-circles-in-italy/

Heuer J. R., Richards J. and Pherson, R. H. (2015) *Structured analytic techniques for intelligence analysis. Studies in Intelligence*. Spain, Plaza y Valdés Editores.

Hibss 'Pherson', K. and Pherson, R H. (2021) *Critical thinking for strategic intelligence*. USA, SAGE Publications Ltd.

Hitz, F. P. (2004). *The great game. The myth and reality of espionage*. First Edition.USA, Alfred A. Knopf.

Lucas, N. (1966) *The great spy ring.* UK, Arthur Barker Limited.

Maik Baumgärtner, F. B. (2022) How Putin's agents are infiltrating Germany, (p.13) *SPIEGEL* .International section, 9 September 2022. Available at: https://www.spiegel.de/international/germany/hackers-spies-and-contract-killers-how-putin-s-agents-are-infiltrating-germany-a-2cc6c24c-16ac-43d4-97fa-103081414acc

Mitrokhin, V. (2002) *KGB Lexicon. The Soviet intelligence officer's handbook.* UK, Frank Cass & Co. Ltd.

Navarro Bonilla, D. (2009). *¡Espías! Tres mil años de información y secreto [Spies! Three thousand years of information and secrecy].* Spain, Plaza y Valdés Editores.

Navarro Bonilla, D. y Esteban Navarro, M. Á. (2004) *Gestión del conocimiento y servicios de inteligencia [Knowledge management and intelligence services].* Monografías no. 47. Spain, Instituto Español de Estudios Estratégicos. Ministry of Defence.

Navruzbekbekov, E. (2022). *FSB Counterintelligence*. Lieutenant Major of the FSB counter-intelligence service, defector and political asylum seeker in Europe (Parts I and II). Available at: https://igorsushko.substack.com/p/fsb-counterintelligence-senior-lieutenant

https://igorsushko.substack.com/p/fsb-counterintelligence-senior-lieutenant-160

Olson, J. M. *et al.* (2004) *The ten commandments of counterintelligence.* Intelligence and the National Security Strategist: Enduring Issues and Challenges, Sherman Kent Center for Intelligence Studies.

—. (2004). *Los diez mandamientos de contrainteligencia. [The ten commandments of counterintelligence]* Manual Básico de Contrainteligencia, volume 4 (Basic Lecurtes). TIEV de la SHCP, 2004 (Mexico).

—. (2019). *To catch a spy: the art of counterintelligence*. Georgetown University Press (USA).

Pherson, Randolph H. and Heuer JR, Richards J. *Structured analytic techniques for intelligence analysis*. SAGE Publications Ltd, 2021 (USA).

Remnick, David. *KGB Targeted for major reforms*. Washington Post, August 27, 1991 (USA). Available at: https://www.washingtonpost.com/archive/politics/1991/08/27/kgb-targeted-for-major-reform/6bf9c712-2e63-45b8-b2ed-5a3affab734c/

Ribagorda Garnacho, A. (2015) *Criptografía y criptoanálisis [Cryptography and cryptanalysis]. Guía de Seguridad CCN-STIC-401*. National Cryptology Centre (CCN-CNI), 2015 (Spain). Available at: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html

Richelson, J. T. (1995). *A century of spies. Intelligence in the Twentieth Century.* UK, Oxford University Press.

Richterova, D. (2023). *Hunting traitors. Anatomy of a Cold War kidnapping campaign. Cambridge Intelligence Seminar 2022-2023*. Senior Lecturer in Intelligence Studies, Department of War Studies, King's College of London, UK.

Rid, T. (2020). *Active Measures. The secret history of disinformation and political warfare.* Farrar, New York, Straus and Giroux.

Riehle, K. P. (2022). *Russian intelligence. A case-based study of Russian services and missions past and present*. USA, National Intelligence Press.

Samuelson, P. and Nordhaus, W. (1992) *Economics, 14th Edition*. USA, McGraw-Hill Publishers.

Taylor, S. A. (2007). *Definitions and theories of counterintelligence. Strategic Intelligence.* Vol. 4. USA, Loch K. Johnson PSI.

—. (2009). *Definiciones y teoría de contrainteligencia [Definitions and theory of counterintelligence]*. Manual Básico de Contrainteligencia. Volume 4. TIEV de la SHCP, Mexico.

Urban, M. (2018) *The Skripal files. The life and near death of a Russian spy*. UK, MacMillan Editor.

Urbano, P. (1997). *I joined CESID*. Spain, Plaza & Janes Editores.

Wolf, M. and McElvoy, A. (1997) *El hombre sin rostro. El gran maestro del espionaje comunista [The man without a face. Communism's greatest spymaster]*. Spain, Javier Vergara Editor.

Woodward, B. (1981) *VEIL: The secret wars of the CIA.* USA, Ediciones B

Article received: 09 February 2023
Article accepted: 27 April 2023