BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Information operations, rivalry projects in the information arena

Lect. Cristinel-Marius AMZA, Ph.D.*

*"Carol I" National Defense University, Bucharest, Romania
e-mail: amza.marius@unap.ro

Abstract

The organization and conduct of intelligence operations in the Intelligence Arena involves a real rivalry and confrontation among the Intelligence Services, conducted in order to gain some advantages at the expense of others. Nothing is surprising in the fact that these rivals are constantly trying on the one hand to thwart each other's efforts to know the other, and, on the other hand, to mislead, misinform, or deceive.

Keywords:
intelligence operations; ISR; counterintelligence; clandestine; confidential; secret.

Article info
Received: 2 October 2024; Revised: 1 November 2024; Accepted: 13 December 2024; Available online: 17 January 2025

Citation: Amza, C.M. 2024. "Information operations, rivalry projects in the information arena."
Bulletin of "Carol I" National Defence University, 13(4): 221-233. https://doi.org/10.53477/2284-9378-24-60

At this point, we can say that the vast majority of security or defense strategies developed by the vast majority of the world's states refer, particularly, to national interests, which determine their actions on the international stage, ensuring their survival.

Gathering information about adversaries has been and still is essential to developing these military strategies since the emergence of rivalries. Knowing your opponents' capabilities, order of battle, and intent can make the difference between victory and defeat. Whether through human sensors and interception of communications or by observation from a hilltop or, in the modern age, from the highest level of space, the ability to know what the adversary is doing is essential to understanding and ultimately to aiming for victory.

In the current security environment, the dependence of national power on intelligence is obvious and it requires specialized structures to be capable of supporting the foreign policy desired by strategic decision-makers. Dominant states create and configure their intelligence services to enhance their power in international relations and, from this perspective, they are essential "arenas for power relations" (Morgenthau 2007; Evans and Wilson 1992, 330).

Intelligence means understanding the security environment, actors (NATO AAP-6 2021) and forces that pose a threat to a state. Knowledge means supporting the political and military actors and it is a part of the decision-making process and the result of collecting, processing, exploiting, integrating, and interpreting available information about the current security environment and threat.

Intelligence has two broad objectives: the first is to reduce uncertainty by providing accurate, timely and relevant information, threat and environmental knowledge and the second is to protect the homeland and citizens by conducting counterintelligence activities and actions.

The interests and the divergences of geopolitics, geostrategy, economics, and ideology among state actors will never allow decision-makers at the strategic level to have a clear picture of the security environment; that is why intelligence deals with the greatest number of unknowns and has to provide answers in order to know their true intentions. Almost always there will be gaps in the information and knowledge provided and the degree of detail desired will be lacking because information cannot provide absolutely everything with certainty. It uses probabilities but it tries to reduce uncertainty by confronting the competitor by gathering relevant information, placing in the context to provide knowledge, and passing it on to form the complete picture and improve its understanding; therefore, the execution of intelligence and counterintelligence operations by the intelligence services is extremely relevant.

From the point of view of intelligence operations, the approach to the intelligence arena is that it can be divided into three broad categories. The first category refers to the collection of data and information for processing, transforming it into intelligence, and disseminating it to decision-makers. The second category refers to those intelligence operations undertaken to influence the course of events, sometimes called clandestine or secret operations. Finally, the third category refers to counterintelligence operations that are executed to counter-intelligence operations, regardless of who the rival is. All those types of intelligence operations will have an impact on any state's foreign policy. This impact will vary in both scope and degree of involvement because it is the political factor that approves the planning and execution of intelligence operations (Westwood 1977, 86).

An intelligence operation is a unique and complex project that is planned and executed over a medium to a long period of time, with experienced human resources and a huge consumption of material and financial resources to accomplish the objectives. Such a project consists of a varying number of phases, subphases, tasks, and collective and individual actions executed in a unified concept and the execution is possible only through the coordination and interrelation by a multidisciplinary group of intelligence personnel (collectors, analysts, technical, IT, etc.) of the phases, activities and tasks. The main objective of implementing the operation's project is to ensure the required performance and quality with the lowest achievement risk and in the most reasonable time.

Intelligence operations for the collection of data and information for processing and transforming it into finished intelligence products are necessary for military actions because they clarify the strategic, operational, and tactical environment, clarify the adversary's intentions, and are essential for the commander's decision-making. Intelligence encompasses the organizations, capabilities, and processes used to task, collect, process, analyze, and exploit information from multiple sources, with an ongoing focus on satisfying intelligence requirements of the joint force commander's (JFC), and intelligence operations are conducted in and from all domains throughout the competition (U.S. Air Force Doctrine 2023).

Intelligence enables leaders at all levels to make decisions based on intelligence to apply combat power. Success in operations requires timely and effective decisions based on the application of judgment and available knowledge. As such, commanders and staff seek to build and maintain ongoing situational understanding throughout the operation.

Intelligence operations encompass intelligence collection in all domains with the full spectrum of sensor capabilities, processing, exploitation, integrated analysis, and intelligence production activities at the large-unit level, operations centers (air, naval, and ground) distributed to beneficiaries, and national production centers. These operations produce and disseminate intelligence to tactical, operational, and strategic users through the intelligence cycle: planning and targeting; collection, processing, analysis, and production; dissemination; and evaluation and feedback. Importantly, evaluation and feedback are continuous and facilitated throughout the cycle through collaboration and dialogue with all stakeholders.

Joint Intelligence, Surveillance, and Reconnaissance (JISR) services are vital to all military operations and provide decision-makers and headquarters with better situational awareness of the operational environment. To enable the collection of information and to ensure that intelligence is analyzed and produced for decision-makers, there are several primary actors involved, including collection, surveillance, and reconnaissance assets (e.g. Alliance Ground Surveillance and Airborne Warning Aircraft & Control System, which uses radars, observation satellites, electronic assets, and reconnaissance structures to gather information), intelligence analysts and decision-makers.

Special reconnaissance is reconnaissance and surveillance conducted as a special operation in hostile, difficult-to-access, or politically and/or diplomatically sensitive environments to collect or verify information of strategic or operational importance, avoiding discovery and direct combat with the enemy. Special reconnaissance is carried out by small structures, such as a detachment or reconnaissance team, consisting of highly trained military personnel, usually from special forces units or military intelligence structures.

Special reconnaissance is different in purpose and its role, from commando actions, but both are usually carried out by the same type of structures. The special reconnaissance role includes direct support of air operations strikes by providing imagery, enabling aircrews to adjust flight strategy, as well as that of artillery and ground-based missile systems, in areas of operations deep within the enemy's air defense, the placement of remotely operated and monitored sensors, and specific preparations for the actions of other special forces or military intelligence structures. The myriads of missions that can be performed by special reconnaissance structures include direct actions on targets, as well as unconventional warfare, including guerrilla operations. In addition to being highly trained, special reconnaissance units are also equipped and weaponized with high-quality technology and weaponry, as they have to fight in difficult conditions, often with an unfavorable force ratio, when they are discovered and when the extraction elements are delayed in reaching them. During the first Gulf War in 1991, British SAS and US Air Force units were initially deployed deep into the Iraqi battlefield to find Scud Missile Launchers and direct air strikes. When air actions were delayed, the patrols attacked the critical infrastructure of the Scud systems with their weapons and equipment.

Following the execution of a special reconnaissance operation, structure debriefing might be done with HUMINT personnel who are most familiar with intelligence-gathering techniques. The information resulted is likely to contribute to the support of HUMINT intelligence collecting, but depending on the mission may also contribute to IMINT, SIGINT, MASINT, and TECHINT. Some of these techniques and procedures are highly sensitive and confidential and are managed on a "need to know" basis within the structures coordinating the special reconnaissance operation, including for members of the all-source intelligence cell.

Discreet, covert, or secret intelligence operations of a government, seeking to influence events in other countries, are only a small part of international relations, but they exist precisely to support decision-makers. Planning and execution of those types of operations have the distinct advantage of accomplishing policy without jeopardizing the national aspect, and regardless of their nature, when intelligence structures fail, they do not leave the bitter taste of defeat as in a confrontation.

The long-considered axiomatic doctrine that even if a state's involvement in a covert action becomes known, the head of state should be able to deny that he authorized or even had knowledge of it is closely related to the aforementioned. He should be able to state, quite plausibly, that the operation was carried out by his subordinates who acted without his knowledge or authorization (Shulski and Schmitt 2008, 151). Intelligence operations aimed at influencing events can be categorized into the following types of operations: "discreet", "undercover", "clandestine" and "false flag". In this article, I will use the term "discreet" operations to differentiate it from "covert" and "clandestine" operations.

A black operation is a covert operation by a government agency, a military entity, or a paramilitary organization and may include activities, including those of private entities, with the primary objective of clandestine or covert entry into a competitor's target structures to obtain information using human sources. This is obviously the best situation in the case of information gathering since access to secret documents or fragments of useful or necessary information is gained. The basic characteristics of a discrete operation are that it is confidential and cannot be attributed to the organization conducting it (Smith Jr. 2003). This type of intelligence operation has been planned and executed by most specialized services such as MI6, MI5, Mossad, CIA, KGB, FSB, and ISI, as well as intelligence structures of other states (Intelnews 2008).

The major difference between a discreet operation and a secret one is that a discreet operation involves a significant degree of deception to hide who is behind the operation or to make it appear that another agency or entity is involved. A well-known example dates back to May 2007, when ABC News and, later, The Daily Telegraph reported that US President George W. Bush had authorized the Central Intelligence Agency (CIA) to undertake "discreet operations" in Iran to promote regime change and sabotage the nuclear program. Subsequently, ABC News was criticized for reporting the discreet operation, with 2008 presidential candidate Mitt Romney saying he was "shocked to see the ABC News report on the discreet action in Iran", but ABC said the CIA and the George W. Bush knew of their plans to publish the information and raised no objections (Montopoli 2007). In June 2007, the CIA declassified some of the documents and made them public detailing illegal surveillance, assassination plots, kidnappings, and other "discreet" operations undertaken during the 1950s and 1970s because they offered insight over a very difficult period and showed a different profile of a different intelligence agency on how to go about accomplishing its tasks.

A clandestine operation is an intelligence or military operation conducted in such a way that actions and activities go undetected by the local population or by the adversary's intelligence and counterintelligence structures. Until the 1970s, clandestine operations were primarily political in nature, generally aimed at supporting groups or nations that another entity favored. Examples include US intelligence involvement with German and Japanese war criminals after World War II or the failed Bay of Pigs Invasion, in 1961. Today, those operations are part of the modus operandi of many intelligence structures around the world and are carried out in a variety of ways depending on the technology available.

Most clandestine operations involve information gathering, usually by both humans and sensors placed in strategic areas or camouflaged in important locations. The placement of underwater or land-based communications cables, cameras, microphones, traffic sensors, monitors such as sniffers, and similar systems requires that the mission remain undetected and undetected. Clandestine sensors may also be mounted on unmanned underwater vehicles, reconnaissance satellites, unmanned aerial vehicles (UAVs), or unmanned detectors, or manually placed by clandestine human sources.

The terms clandestine and hidden are not synonymous. As stated in the definition (which has been used by the United States and NATO since World War II), in a covert operation the identity of the sponsor is concealed, while in a clandestine operation, the operation itself is hidden. In other words, clandestine means "stealth procedure", where the operation is not intended to be discovered. The term "stealth" refers to both a broad set of tactics designed to provide and maintain the element of surprise and to reduce the enemy's resistance to information gathering. Hidden means "deniable" so that if the operation is discovered, it is not attributed to a group or entity. Some operations may have both clandestine and hidden aspects, such as the use of hidden sensors located at great distances or human observers who can direct artillery and ground-based missile strikes and air strikes. The attack is obvious, but the component that was used to locate the target may remain stealthy.

In World War II, targets identified and located by cryptanalysis of radio communications were only attacked if aerial reconnaissance of the areas was also carried out or, in the case of the downing of Admiral Isoroku Yamamoto's plane, an observation which was the responsibility of the Coastwatchers (Coast Watch Organization, Combined Field Intelligence Service were Allied military intelligence agents stationed on remote Pacific islands). During the Vietnam War, the drivers of the truck attacked on the Ho Chi Minh Trail were unaware of the capabilities of US-owned sensors such as the Black Crow airborne device that pinpointed their trucks' location by engine heat.

At this moment in the North Atlantic Area, there is a vast critical infrastructure of undersea communication cable networks between Europe and North America, and sites such as TeleGeography have detailed maps of the layout of cables with civilian uses (power, internet, etc.), but there are also military systems that are not the subject of such postings, as they contain essential data for all forms of communication between Alliance members. Relatedly, electronic reconnaissance vessels of the Russian Navy (e.g. Yantar – officially classified as an auxiliary general oceanographic research vessel with underwater rescue capabilities, which is subordinate to a separate structure from the military navy of the Russian Ministry of Defense) sometimes operate covertly (deactivation of the satellite identification system), in the vicinity of vital submarine cables, raising concern among military and intelligence officials for possible interception of secret communications.

A covert operation is an operation carried out by military or police structures that involves an undercover agent or troops acting under a supposed cover to conceal the identity of the responsible party (Carson 2018). Under US law, the Central Intelligence Agency (CIA) is able to conduct covert operations. The legislative framework has defined covert action as special activities, both political and military, that the US government can legally deny (Daugherty 2004). The effect of this legislative framework is reflected in the special attention that the US Congress gives to the CIA compared to other intelligence structures.

According to a 2018 study by University of Chicago political scientist Austin Carson, covert operations can have the beneficial effect of preventing differences from escalating into conflict or war. He argues that keeping military operations secret can limit the dynamics of escalation, as well as insulate leaders from domestic pressures, while simultaneously allowing them to communicate to the adversary their interest in maintaining a limited war (Carson 2018, 45).

When these operations are carried out by police structures, the term "undercover" means to avoid detection by monitoring personnel with duties and especially to conceal one's own identity (or use an assumed identity) in order to gain the trust of the persons or organization, to learn or confirm confidential information or to gain the trust of data subjects in order to gather information or evidence. Undercover operations are traditionally carried out by law enforcement agencies, and those who perform such roles are commonly referred to as undercover agents.

The first actions were carried out in 1883 on the territory of Ireland, they were aimed at combating the bomb-planting actions that the Irish Republican Brotherhood had started a few years earlier, and the agents who acted were for the first time trained in counter-terrorism techniques and tactics. In 1906 a similar activity was carried out across the United States when the "Italian squads" were established to combat and intimidate the crime of aggressive elements in poor Italian neighborhoods.

There are two main issues that can affect undercover agents. The first is maintaining their identity, and the second is reintegrating back into their normal work after

accomplishing the operational objectives. Living a double life in a new environment presents many challenges, as undercover work is one of the most stressful jobs a special agent can undertake. The biggest cause of stress identified is the agent's separation from friends, family, and his normal environment. The lifestyle of undercover agents is very different from that of normal police officers and after the mission is over it is difficult to reintegrate into the everyday tasks. After such a free lifestyle, agents may have problems with subordination, and discipline or feel uncomfortable, may have strange sometimes even paranoid views about the world and life, and may be constantly on alert.
Throughout history, there have been many covert intelligence operations aimed at gaining information about potential adversaries as early, as peacetime. In this context, it can be said that such operations are part of the mode of action of the intelligence services for the purpose of early warning of the political-military leaders (Piroșcă 2020).

A false flag operation is an act committed to disguise the real source of responsibility and place the blame elsewhere. The term has been used to describe a trick in naval warfare whereby a ship flew the flag of a neutral or friendly country in order to hide its true identity. The tactic was originally used by pirates and corsairs to trick other ships into allowing them to approach them before attacking them. Later, it was considered an acceptable practice during naval warfare under international maritime laws, provided the attacking ship displayed its true flag once the attack had begun (Ruis and Nilsson 2022).

At present, the term also stands for the organization of attacks by some nations against themselves and makes them appear to be of enemy nations or terrorist groups targeting them, thus providing a pretext for internal repression or triggering military aggression. In-ground military action, such operations are generally considered acceptable under certain circumstances, such as deception of the enemy, provided that deception is not perfidious and that all deception is eliminated before opening fire on the enemy.

Intelligence operations of this kind were used as a pretext for starting wars. Thus, the Gleiwitz incident on the night of August 31, 1939, had Reinhard Heydrich as the protagonist by fabricating evidence of a Polish attack against Germany in order to mobilize German public opinion for war and to justify war with Poland. Alfred Naujocks was a key organizer of the operation on Heydrich's orders which resulted in the death of several victims in some Nazi concentration camps who were dressed as German soldiers and then shot by the Gestapo to make it appear that they had been shot by Polish soldiers. This, along with other false flag operations in Operation Himmler, would be used to mobilize the support of the German population for the start of World War II in Europe (Lightbody 2004). The operation was unsuccessful because it failed to convince international public opinion of German claims, and Britain and France declared war two days after Germany invaded Poland.

In February 2022, intelligence structures of some Western governments warned about the possibility that the Russian Federation might be conducting a false flag operation to make the case for an invasion of Ukraine. The run-up to the February 24 invasion revealed an intensified disinformation and misleading campaign by the Kremlin and the Russian media by promoting "false flags" almost hourly, purporting to show the attack on Russia by the Ukrainian armed forces, in an attempt to justify an invasion of Ukraine. Many of the videos posted on social media were for disinformation having poor and amateurish quality, the metadata did not match as it showed incorrect data, and the evidence and arguments presented by Bellingcat specialists and other independent journalists made it clear that the claimed attacks, explosions and evacuations in Donbas were staged by Russia.

Similarly, in naval warfare such deception is permissible, provided the false flag is lowered and the true flag raised before engaging in combat (Squires 2008). A notable example was the German cruiser (formerly merchant ship) Kormoran of World War II, which surprised and sank the Australian cruiser HMAS Sydney in 1941 while disguised in a Dutch merchant ship, causing the highest loss of life on an Australian warship. While Kormoran was fatally damaged during the battle and her crew captured, the result was a considerable morale victory for the Germans.

In espionage, the term "false flag" describes the recruitment of agents by intelligence officers posing as representatives of a cause to which potential agents are sympathetic, or even the agents' own government.

In order to ensure the success of a state's international relations and military operations, strategic decision-makers must also arrange for the necessary measures to be taken to deny the adversary the possibility of carrying out acts of terrorism, espionage, subversion, sabotage, organized crime or attacking own communications and IT networks. In order to achieve this, it is necessary to identify the vulnerabilities of one's own entities to the execution of the adversary's intelligence operations, and the results of the analysis will be forwarded to the counterintelligence structures.

Counterintelligence (CI) includes those activities that relate to identifying and countering the threat to security posed by hostile intelligence services or organizations by persons engaged in espionage, sabotage, subversion, or terrorism (NATO Standard AJP-2 2016; UK Ministry of Defence JP 2-00 2023), and the best defense against attacks by foreign actors on the national territory, against the citizens of the country or the infiltration of intelligence services are active and flexible measures, having the ability to quickly choose counterintelligence techniques, depending on the evolution of the situation against those hostile services regardless of their affiliation. This defense is usually referred to as counter-espionage, i.e. measures taken to detect enemy espionage or physical attacks against friendly intelligence services, to prevent damage and loss of information, and where possible to turn the attempt against its originator. Counter-espionage goes beyond being reactive and actively seeks to undermine the hostile intelligence service by recruiting agents into the foreign service, by discrediting personnel actually loyal to their service, and by taking resources that would be useful to the hostile service. All of these actions apply to non-national threats as well as national organizations.

If the hostile action takes place in one's own country or a friendly or allied country with the cooperation of police structures, the hostile agents may be arrested or, if they are diplomats, declared persona non-grata. From an intelligence service perspective, exploiting the situation to the party's advantage is usually preferable to arrest or actions that could lead to the death of the threat. The intelligence priority sometimes conflicts with the instincts of one's law enforcement organizations, especially when the foreign threat combines foreign personnel with the country's citizens.
In some circumstances, arrest can be a first step where the detainee is given the choice to cooperate or face serious consequences up to and including the death penalty for espionage. Cooperation may consist of telling all that is known about the other service, but preferably actively assisting in deceptive actions against the hostile service.

The protection of intelligence services is achieved by organizing defensive counterintelligence and involves assessing the risks to their culture, sources, methods, and resources. Risk management must constantly reflect those assessments because effective intelligence operations are often risk-takers. Even when taking calculated risks, services need to mitigate the risk with appropriate countermeasures, especially to discover the specific methods of the art of information sharing. Today's intelligence services are developing capabilities to explore other intelligence entities believed to be open and be able to undermine individuals within the intelligence community. Offensive counterintelligence is the most powerful tool for finding penetrators and neutralizing them, but it is not the only tool.

So, it is generally understood that governments engage in covert actions (as they engage in espionage), these are often illegal under the laws of the state on whose territory they take place. They may also be contrary to international laws, which is underpinned by the principle of non-intervention in the internal affairs of sovereign states, although this principle has increasingly gained weight in international jurisprudence since the end of the Cold War (Shulski and Schmitt 2008).
Decision-makers need information that is not controlled or manipulated by hostile forces. Because every intelligence discipline is subject to manipulation by adversaries, the veracity of information and the credibility of all means of collection are essential. Consequently, each counterintelligence organization will validate the reliability of sources and methods that relate to the counterintelligence mission following common standards.

When a foreign threat combines foreign personnel with a country's citizens, we are dealing with intelligence operations called the "fifth column". In common parlance, the term refers to those who betray their homeland, acting from within, usually in favor of an enemy group or another nation. In fact, the Petit Robert dictionary defines the phrase as "enemy's secret intelligence services in a territory", and the Larousse as "an element working in a territory for the benefit of the adversary (under this name were designated in 1940 the agents of the German secret services who they acted in France)". The term also applies to actions organized by military personnel. The activities of a fifth column can be overt or clandestine. All persons and material and financial means established in secret can be coordinated to directly support an attack from outside the country. Clandestine activities for a fifth column can be materialized through terrorism, espionage, sabotage and disinformation. These actions are carried out exclusively on the national territory or even within the combat device (during the established or decreed states of emergency) by the secret sympathizers of an outside force.

The term "fifth column" originated in Spain (originally quinta columna) during the run-up to the Spanish Civil War. Its first known appearance is in a secret telegram dated September 30, 1936, which was sent to Berlin by the German charge d'affaires in Alicante, Hans Hermann Völckers. In the telegram, he referred to an unidentified "alleged Franco statement" circulating (apparently in the Republican or Republican-held Levantine area). This "alleged statement" claimed that Franco claimed that four nationalist columns were approaching Madrid and a fifth column waiting to attack from within (the term first appears in a Spanish publication after which the following day, on 4 October 1936, is taken up in the French publication Le Journal (Le Journal 1936).

The first identified public use of the term is in the October 3, 1936 issue of the Madrid communist daily Mundo Obrero, and by mid-October, the media was already warning about the famous fifth column. By the late 1930s, as American involvement in the war in Europe became more likely, the term "fifth column" was commonly used to warn of potential rebellion and disloyalty within US borders. Fears of betrayal were heightened by the rapid fall of France in 1940, which some blamed on domestic weakness and a pro-German fifth column, and in the United Kingdom in a speech to the House of Commons, Winston Churchill assured MPs that he would act as a strong hand against the activities of the fifth column.

Conclusions

The instruments of national power consist of assemblages of sources of power that must constantly adapt to changes in the international security environment or even those in the domestic environment of a particular state. The informational instrument is also exercised through specialized institutions and is designed to provide the leadership of states, and other institutions that are responsible for other instruments of power, with the data necessary to make the most appropriate decision. Like the diplomatic instrument, the information instrument is used both in times of peace and in crisis or war.

In this respect, intelligence operations are seen by the Intelligence Services as methods and means of using agents, infiltrating agents into foreign environments of interest, incursions into enemy territory, as well as actions to prevent acts of sabotage or terrorism on its own territory.
Intelligence is vulnerable not only to external threats but also to internal ones. Subversion, betrayal, and leaks expose vulnerabilities, government and military secrets, intelligence sources, and methods. The insider threat is a source of tremendous damage to national security, especially when agents have access to information about major, discrete, covert, or clandestine activities.

To plan, organize, and conduct intelligence operations, intelligence structures must continuously adapt their activities to the requirements of their commanders and the harsh and often changing conditions of the intelligence arena. This particularly involves mental and organizational agility underpinned by resilience, adaptation, and flexibility. It is normal for success to come later and therefore requires perseverance in actions, adapting quickly, and seizing opportunities as they arise. For each intelligence operation, an agency must develop a project-specific methodology, thus ensuring the uniqueness and complex nature of the activities, in order to successfully fulfill the intended purpose. The rapid adaptation of intelligence working methods to the operational environment obliges secret agents to improve the efficiency of intelligence gathering and the flexibility of working procedures, in order to cope with changing circumstances and to avoid the idea that there is only one way of working.

At this point, we can say that intelligence operations are a common action that is part of the tactics, techniques, and procedures of action of the intelligence services around the world, for the purpose of permanent knowledge of the intentions of the competitors or to the states in which hostility is manifested towards the state initiating such an operation, as well as for the support of military actions and early warning of political and military leaders at the strategic level.

In conclusion, the organization and conduct of intelligence operations in the "Intelligence Arena" involves a real rivalry and confrontation between the intelligence services, conducted to gain some advantages at the expense of others. Nothing is surprising in the fact that these rivals are constantly trying, on the one hand, to thwart each other's efforts to know the other and, on the other hand, to mislead, misinform, or deceive one another.

References

Carson, Austin. 2018. *Secret Wars: Covert Conflict in International Politics.* Princeton University Press.

Daugherty, William J. 2004. *Executive Secrets: Covert Action and the Presidency.* University of Kentucky Press.

Evans, Tony, and Peter H. Wilson. 1992. "Regime Theory and the English School of International Relations: A Comparison." *Millennium - Journal of International Studies* 21: 329 - 351.

Intelnews. 2008. *Tallinn government surveillance cameras reveal black bag operation.* https://intelnews.org/2008/12/16/04-11/.

Le Journal. 1936. "La Passionaria preche la terreur."

Lightbody, Bradley. 2004. *The Second World War: Ambitions to Nemesis.* Routledge.

Montopoli, Brian. 2007. *Știri CBS.* http://www.cbsnews.com/8301-500486_162-2842625-500486.html.

Morgenthau, Hans J. 2007. *Politica între națiuni, Lupta pentru putere și lupta pentru pace.* Iași: Editura Polirom.

NATO AAP-6. 2021. "NATO Glossary of Terms and Definitions ."

NATO Standard AJP-2. 2016. "Allied Joint Doctrine for Intelligence, Counterintelligence and Security." Edition A Version 2. https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf.

Piroșcă, Valerică. 2020. "Operații de intelligence." *Colocviu Strategic* 6 (173): 2-3. https://cssas.unap.ro/ro/pdf_publicatii/cs06-20.pdf.

Ruis, Carlos Diaz, and Tomas Nilsson. 2022. "Disinformation and Echo Chambers: How Disinformation Circulates in Social Media Through Identity-Driven Controversies." *Journal of Public Policy & Marketing* (no. 42): 18-35.

Shulski, Abram N., and Gary J. Schmitt. 2008. *Războiul tăcut.* București: Editura Polirom.

Smith Jr., W. Thomas. 2003. *Encyclopedia of the Central Intelligence Agency.* New York: Facts on File Inc.

Squires, Nick. 2008. *HMAS Sydney found off Australia's west coast.* https://www.telegraph.co.uk/news/worldnews/australiaandthepacific/australia/1581972/HMAS-Sydney-found-off-Australias-west-coast.html.

U.S. Air Force Doctrine. 2023. "Air Force Doctrine Publication 2-0 - Intelligence." https://www.doctrine.af.mil/Doctrine-Publications/AFDP-2-0-Intelligence/.

UK Ministry of Defence JP 2-00. 2023. "Joint Doctrine Publication. Intelligence, Counter-intelligence and Security Support to Joint Operations." https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf.

Westwood, James T. 1977. "A contemporary political dilemma: the impact of intelligence operations on foreign policy." *Naval War College Review* 29 (4): 86-92. https://www.jstor.org/stable/44641751.