CHAPTER 5

Intelligence and Military Disinformation and Its Impact on Information Security: Theoretical, Practical, and Legal Aspects

We live in a network society where a significant part of our personal and professional activities take place in cyberspace (Castells, 2011). The rapid socio-economic changes and technological advancements in recent decades have transformed the way we function in our everyday lives, communicate, acquire knowledge, and perceive the world. The internet has made it possible to shop, learn, work, make friends, and communicate without limitations of time zones or distance, and it allows us to stay updated on events from around the world. Churches conduct their missionary activities, terrorists recruit fighters, and states wage their conflicts – all online.

This widespread use of the internet has caused many users to lose their sense of critical distance, self-control, and distrust toward the content published on it. The situation has created opportunities for foreign intelligence services to conduct disinformation operations that target decision-makers and entire societies. Furthermore, the information and technology revolution has altered the nature of military information warfare at the strategic, operational, and tactical levels. State institutions, armed forces, and societies must therefore develop effective defense mechanisms to combat falsehood and manipulation.

1 State Information Security

In today's world, information is considered a strategic asset, whether it is viewed from the perspective of an individual, society, the state, or the international community. Access to information and the ability to process, transmit, secure, and store it determines cognitive security. These conditions are essential for effective decision-making, management, and operation of all entities, including states, institutional systems, private sector entities, societies, and individuals. In contemporary times, knowledge and information technologies have become one of the primary factors of production. It is estimated that the IT sector is already responsible for creating over 15% of global economic growth, showing an upward trend (Henry-Nickie et al., 2019).

In the 21st century, the world's economy and global politics are heavily reliant on information, its accuracy, timing, and uninterrupted flow. The consequences of long-term disconnection from telecommunication networks, also known as internet blackouts, could be severe. Such a situation would bring about the paralysis of most employment sectors, stock market crashes, stop in financial flows, and disruption of the functioning of critical infrastructure that sustains vital areas of state responsibility. Inevitably, it could lead to social unrest, chaos, riots, bankruptcies, and even the collapse of governments.

Because of this, it is hardly surprising that in reflections on the future of international conflicts, cyber threats and offensive network scenarios are now more seriously considered than traditional military clashes. In 2015, as a result of internet blockades, the global economy suffered losses amounting to USD 2.4 billion (Waddell, 2016). In 2019, this amount grew to USD 8 billion before dropping to USD 5.5 billion in 2021 (Woodhams & Migliano, 2021).

From the state's perspective, information, its accessibility, and the possibility of safe processing are critical components of its power. It is also a crucial element for its functioning in politics, security and defense, the economy, as well as in the social and cultural dimension. Sensitive information containing data that requires special protection against unauthorized access must therefore be adequately protected from the moment of acquisition, during processing (analysis), transfer, storage, and usage, with appropriate standards implemented at each stage. State information security is ensured when:

- Information resources are not at risk.
- State institutions make decisions on the basis of true, relevant and accurate information. This does not guarantee the quality of the decisions themselves but provides conditions for rational and optimal actions.
- Information flows and the functioning of the information and communication technology (ICT) networks that make up the state's critical infrastructure are undisturbed.
- State structures effectively ensure the protection of classified information.
- Public institutions do not violate citizens' right to privacy and the protection of their personal data.
- Citizens, non-governmental organizations (NGOs), and the media have access to public information.
- Society is resistant to disinformation and propaganda activities (Aleksandrowicz, 2018, pp. 33–35).

Information security is a trans-sectoral area that encompasses the information environment, including the state's cyberspace. A threat arises when state structures are unable to provide effective protection, making society susceptible to falsehood and manipulation. The core of the problem is securing the

functioning of the state (and social order) and protecting its interests in the information space.

The above approach to the problem emphasizes three issues:

1. Protection of the state's information resources. This particularly applies to protecting sensitive and classified information that is crucial for its functioning and of strategic importance against unauthorized access (e.g., espionage). This also requires protection against disruptions of its functioning due to cyber-attacks, acts of sabotage, etc.
2. Protection of state institutions and society against the impact of disinformation and propaganda. These disinformation activities may be aimed at causing social unrest or internal destabilization of the state; interfering in political processes like elections; or shaping internal, foreign, or security and defense policies.
3. Retaining offensive capabilities against the information resources of potential opponents. This involves pursuing tools to be able to influence their societies in an informative way.

To protect sensitive information against unauthorized access, state institutions impose secrecy clauses on it. These commonly fall into classifications such as "restricted", "confidential", "secret", and "top secret". NATO also has classification categories indicating the originator/owner or nature of the protected information, with symbols such as "cosmic top secret" or "atomal top secret". The content of information protected by these categories is strictly regulated by law, and administrative proceedings are instituted for persons applying for access to them. Access is granted through a limited, strictly personal admission to a certain level of sensitive data, which does not entail automatic access to all such information. To ensure protection, states restrict access to only the group of people who need the information to perform specific task; they also increase the physical and technical security of their processing systems.

They do this through complex and detailed office systems, which include conditions for storing a given type of knowledge, accessing it, and learning about it. This takes place, for instance, in government institutions, the armed forces, the defense sector, the arms industry, the organs and services of the state security system, public administration, and other elements of critical infrastructure. Specialized counterintelligence institutions, referred to in NATO terminology as National Security Authorities, are responsible for guarding state secrets and preventing their unauthorized disclosure to unauthorized persons. The tasks of these institutions include:

– Controlling classified information and ensuring compliance with the applicable rules and regulations.

– Securing ICT systems of institutions that have access to classified information.
– Conducting verification and control procedures as well as proceedings within the scope of industrial security.
– Ensuring the protection of the exchange of classified information with other states and international organizations (e.g., within NATO and the EU).
– Providing advice and training in the field of classified information protection.

Access to classified information, or a security clearance, is only granted to trusted and authorized persons who have undergone complex vetting proceedings confirmed by the National Security Authority. Classified information must be processed under conditions that prevent its unauthorized disclosure, and this is regulated by relevant provisions specifying the requirements for secret offices, ICT system security, material circulation, and physical security measures. The "need-to-know rule" states that classified information is made available only to authorized persons to the extent necessary for the performance of their official duties. This means that not everyone with a security clearance up to the "secret" level has the right to access all information within that classification. The principle of adequate protection of information also applies to the person who comes into possession of it. Institutions and companies with industrial access to classified information are subject to control regarding how they protect it, and counterintelligence services work closely with the divisions responsible for protecting classified information in individual institutions. The unauthorized disclosure or use of such information is a punishable crime.

2 Intelligence Disinformation

Against this background, it is worth noting the category of "intelligence disinformation" as a special type of manipulation of cognitive processes and international communication. Although similar to "classical" disinformation, its differentiation lies in the specialized nature of the institutions carrying out such activities, as well as their organization and goals. Intelligence disinformation can be defined as "the process of influencing the behavior of a disinformed subject by distorting their perception of reality, leading to taking actions consistent with the deformed image, and at the same time corresponding to the interests of the disinforming entity" (Świerczek, 2020, p. 33).

By delivering prepared information to the opponent, foreign intelligence services aim to make the target of disinformation believe in the credibility of

the information provided to them, leading them to draw conclusions and make decisions that are inconsistent with the actual state of affairs but consistent with the goals of the entity conducting the operation. These decisions may result in actions that are detrimental to the interests of the disinformed entity, such as improper allocation of resources and forces, errors in the assessment of threats or opponent intentions, or a false sense of security, such as when the aggressor misinforms about its hostile intentions. The purpose of intelligence disinformation may involve:

– The falsification of knowledge about the state's military, diplomatic, intelligence, or economic capabilities.
– Concealing the actual strength and integrity of the state's subsystems, as well as its strategies and intentions.
– Ensuring the political, social, and economic stability of the disinforming entity and at the same time concealing problems. This could include economic issues, internal disputes, factional struggles, crises, or social unrest.
– Influencing the implementation of the policy of a disinformed state (e.g., in the area of security and defense or allied policy).
– Building foundations for further psychological and disinformation operations.
– Distorting real information in such a way that it becomes useless for decision-makers.

When conducting disinformation operations, secret services engage in deliberate, planned, and covert actions with assistance from various entities that use different channels of information transmission but are subject to the supervision of a centralized directing center. Disinformation is not only the domain of intelligence services; it also used by counterintelligence services as part of their 1) active counterintelligence operations, which involve disinformation operations; 2) offensive counterintelligence, which is carried out with the help of a network of double agents. Disinformation is the primary operational tool in both cases.

Intelligence and counterintelligence disinformation activities, carried out in a specific environment with set goals, usually consist of the following stages:

– Selection of channels for transmitting disinformation. These can include political and military elites, state-owned companies, an analytical and expert base, journalists and commentators, influence agencies, "useful idiots", trolls, and bots.
– Determination and possible elimination of alternative sources of obtaining and verifying information by the targets.

– Masking of actions that lead to operational initiatives. Maintaining secrecy ensures that the disinformed object believes their decisions, successes and failures are the result of their own actions or mistakes only and not external influences (Hosaka, 2020).

Politicians, business people, government officials, journalists, bloggers, vloggers, commentators, experts or individuals who use a fabricated identity can act as inspirers or transmitters of disinformation. They may utilize their accounts on popular social media platforms such as Facebook, Twitter, YouTube, Instagram, Tik Tok, or Russian vKontakte and Telegram. Another category of relays and information producers on the internet are "machine bots", which are computer algorithms that automatically create and duplicate false information, posts, comments, or other content after appropriate programming.

"Agents of influence" are individuals recruited by foreign intelligence and consciously acting on its behalf. They follow instructions for which they may receive specific benefits (e.g., financial); their activities can also be ideologically motivated or the result of blackmail or psychological and personality traits. The motivational model used by secret services to obtain human assets is commonly referred to as MICE (Money, Ideology, Coercion, Ego). The agent of influence's task is to covertly support narratives, opinions, and actions that are beneficial to the country they work for, for which they establish contacts in politics, business, military, science, and media. Agents of influence operating in the public space aim to create a debate on specific political, social, or security and defense issues in such a way as to trigger the desired reaction (e.g., change of opinion or attitude) or action (e.g., protests, riots, or revolutions) in line with the client's expectations.

The task of the influence agent who operates within the structures of the state administration is to influence analytical and decision-making processes in such a way as to make it impossible to properly assess the situation and make appropriate decisions. This activity can also take the form of inspiration, in which the disinformed subject is directed to make a specific decision. This goal is achieved, for example, by creating an image of reality that aligns with the interests of the disinformer or by diverting attention from essential matters and replacing them with secondary ones (Świerczek, 2020).

Influence agentry has been one of the main methods of operation for Soviet/Russian intelligence since the Cold War, and there have been several high-profile cases of unmasked agents of influence from Soviet secret services during that time. These include Alger Hiss, an American official in the Department of State and the United Nations; Pierre-Charles Pathé, the founder of the "Synthesis" newsletter read by the French journalistic and political elite, who

worked for the KGB from 1959; Arne Treholt, who joined as a young journalist and activist of the Norwegian Labor Party in 1967 then served as an advisor to the Minister of Trade and an official in the Ministry of Foreign Affairs; and Hirohide Ishida, a Japanese politician who was a close associate of two prime ministers and served as the minister of labor and transport.

In the 1990s, Richard Gott, a journalist for the British newspaper *The Guardian,* known for his radical views and sympathies for Ernesto "Che" Guevara, was accused of working for Russian intelligence as an agent of influence (Williams, 1994). He denied having connections to the KGB, HOWEVER, and was not convicted due to a lack of evidence. It is worth noting that the British were not only targeted by Soviet/Russian influence operations but also used similar methods in their fight against the Irish Republican Army (IRA). British intelligence believed that by supporting the leaders of organizations that preferred negotiations over armed struggle and cooperating with them, they could stabilize the situation in Northern Ireland at a lower cost (Edwards, 2021).

The relationship between an agent of influence and a "case officer" may be informal and not raise suspicion. In practice, the person used as a tool in the influence operation may not even receive direct instructions but only be subtly guided or inspired. This is particularly true for those who are motivated not by material gain or fear but by a sense of mission or ideology. This method is often used with journalists who, during meetings with intelligence officers disguised as "state officials", are intentionally provided with information, such as that pertaining to a particular country's internal situation.

There is a mechanism of triple addiction at work here. The first addiction is to inspire the agent of influence in everyday situations. The second addiction is if the recipient of the information finds it appealing, which increases the chances of publishing it in a newspaper or TV station. Finally, the third addiction is gratitude. The recipient of the information, in return for being provided with it, may offer repayment by disseminating it. As a result, the recipient becomes a proxy in a disinformation operation, inspired but not openly ordered by foreign intelligence.

The literature on this subject outlines three types of influence agents:

– Trusted contact. This is a person who holds a high position in a state institution, expert center, or media and maintains close relations with representatives of another state's structures, but only cooperates with them to a limited extent.
– Controlled agent of influence. This refers to a person who has been recruited by a foreign intelligence agency to carry out specific tasks in exchange for financial gain. These controlled agents of influence are typically identified

at a relatively young age, such as during their studies, and are provided with the necessary training before being deployed for operational purposes. In order to increase their chances of a successful career in state structures and avoid detection by local counterintelligence agencies, they may remain dormant for many years. These "sleeping agents" are activated when they reach a suitable status.

– Special contact. This refers to situations where the recruitment of a "controlled agent" is limited due to political reasons, such as allied relations between states. In this case, a special contact is used instead of an official agent of a foreign intelligence agency. The special contact does not work for the foreign intelligence agency but rather performs favors under the guise of "common interests of both countries" (*Active Measures*, 1986, pp. 81–83).

The Polish legal system does not have a specific categorization for "agent of influence" activities. However, such activities may fall under the category of espionage according to Article 130 of the Polish Penal Code. This article stipulates that "anyone who participates in the activities of foreign intelligence against the Republic of Poland shall be subject to imprisonment for one to ten years". In practice, however, obtaining a conviction under Article 130 for influence operation activities is more challenging than for classic espionage, such as in the case of stealing state secrets. This is because it requires demonstrating that a person was in regular contact with a foreign intelligence officer and accepted and carried out tasks on their behalf. This is relatively difficult to prove in a democratic state with the rule of law and freedom of speech.

The case of Mateusz Piskorski, the leader of the pro-Russian political party *Zmiana* (Change), provides an example of the procedural difficulties related to the classification of influence operation activities under Article 130 of the Polish Penal Code. Piskorski has been commenting on political events for Russian propaganda media such as *RT* and *Sputnik* for years. Since 2015, he has been the chairman of an openly pro-Russian group that describes itself as the "first non-American political party" in Poland. Members of *Zmiana* work with the Eurasian Movement, founded by one of Russia's main theorists and practitioners of information warfare, Alexander Dugin. Piskorski also created a "think-tank", the European Center for Geopolitical Analysis (ECAG), to promote a clearly anti-Western, anti-Ukrainian, and pro-Russian rhetoric that complies with the Kremlin's narrative, goals, and interests. In 2011, Piskorski participated in a propaganda conference organized by Libyan dictator Muammar Gaddafi. Two years later, he was invited by Bashar al-Assad to Syria and afterwards, he published a series of articles criticizing U.S. policy in the Middle East and North Africa. His organization, ECAG, also recruited "election observers" in unrecognized quasi-states that would not exist without Russian military

interference. These include Transnistria in Moldova, Abkhazia and South Ossetia in Georgia, and Donetsk and Luhansk in Ukraine. Piskorski himself led an "observation mission" for the illegal referendum in Crimea in 2014.

Two years later, he was arrested and accused of working for Russian and Chinese intelligence. Despite compelling evidence of his role in Russian disinformation and propaganda activities, he was not convicted. After three years in custody, he was released and continues to engage in public activity, acting as a commentator and "Polish expert" for Russian propaganda media outlets (Wenerski & Kacewicz, 2017, pp. 27–30).

Piskorski is the most well-known example of an individual involved in disinformation activities in Poland inspired by the Kremlin, but he is not the only one. In May 2021, the Internal Security Agency detained Janusz Niedźwiedzki, who had ties to the leader of the *Zmiana* group. He attempted to establish contacts with Polish and foreign politicians on behalf of Russian intelligence. According to Polish law enforcement authorities, "his activities were part of Russian propaganda and disinformation projects aimed at weakening Poland's position in the EU and in the international arena" (*Janusz N,* 2021). Like Piskorski, he participated in influence operations by commenting on political events for Russian propaganda media outlets, spreading the Kremlin's narratives in Poland, and participating in "election observation" missions in Ukraine and Russia. His role was to undermine the results of the Dnipropetrovsk elections, which ended with the defeat of the pro-Russian candidate, and to legitimize undemocratic elections in Russia. His activities were financed by the Russian Peace Foundation, headed by Leonid Slutsky, Chairman of the Russian State Duma's International Affairs Committee. Niedźwiedzki also has connections with pro-Russian organizations in Poland and Europe, including the Night Wolves motorcycle gang, which is engaged in Russian influence operations (Shekhovtsov, 2021).

A similar role to that of agents of influence is played by "useful idiots", that is individuals who spread disinformation and propaganda messages thoughtlessly or unconsciously. Their activities are not usually the result of being tasked or inspired by a foreign intelligence officer but rather stem from their personal views, knowledge (or lack thereof), sympathy, beliefs, and ideology. Another category of disseminators of disinformation are trolls. These are individuals who are commissioned and paid for their activities, which a focus on posting and commenting on social media in line with the "needs of the disinformer".

The most well-known Russian "troll factory" is the Internet Research Agency (IRA), which has operated from Saint Petersburg since 2013. Its owner, Yevgeny Prigozhin, is a close associate of Vladimir Putin. The IRA's monthly budget exceeds 1 million euros, which allows it to employ around 1,000 people who

spread Russian narratives and false information, reinforcing extreme social and political attitudes abroad (Legucka, 2019). According to a former IRA employee, the troll farm is divided into departments responsible for specific social media platforms (such as Facebook, Twitter, or YouTube) and specialized forms of disinformation, such as creating memes or collecting compromising materials (i.e., *kompromats*). According to the British organization of investigative journalism Bellingcat, the Russian Ministry of Defense and the military intelligence (GRU) are responsible for the operations conducted by the IRA (*Putin Chef's*, 2020).

Bots perform the same task as trolls in disseminating disinformation but are accounts created and managed by computer algorithms. They are widely used on social media to automate the spreading of disinformation. According to research conducted by the NATO Center of Excellence for Strategic Communications, following NATO's decision to deploy multinational allied battalions to Poland and the Baltic States, 84% of tweets in Russian and 46% in English that negatively referred to the presence of NATO troops on the Eastern flank were produced by bots (Fredheim, 2017–2021). Despite a downward trend since 2017, largely due to actions taken by social media owners, bot activity remains high. This demonstrates the increasing use of modern technologies for automated social engineering as part of information warfare in cyberspace. Social media platforms still struggle to detect and remove false content produced by bots, particularly in the case of non-English languages. An experiment conducted by NATO StratCom CoE showed that the effectiveness of individual websites in detecting and combating inauthentic accounts was as follows: 35% for Twitter, 21% for Facebook, 14% for Instagram, and 11% for YouTube (Bay & Fredheim, 2019, p. 22).

The credibility of the source providing manipulated or false information is critical to the success of an intelligence disinformation operation. Therefore, at the initial stage, the source provides only true information to build its reputation. Once it has gained the trust of recipients, it changes its approach by mixing true information with manipulated or completely fabricated information. In such operations, the following methods are used:

- Distraction, or the provision of specially prepared information to redirect the subject's interest to other areas.
- Misleading, or the creation of a false image of reality to influence the perception of a disinformed entity.
- Convincing, which involves efforts aimed at the authentication of disinformation by raising its credibility among public opinion.
- Disinformation by suggestion, or the indirect shaping of an image of a phenomenon in a way that is favorable to the disinformer (Rusbridger, 1993, p. 66).

The distinguishing feature of disinformation carried out by intelligence services is its secret nature. This applies to influence operations directed at state institutions as well as those targeting entire societies. Specialized methods, techniques, and tools are used to mislead the recipient(s) and make messages more credible. To mask the involvement of the inspirer of the disinformation, a system of intermediaries is put in place. In the case of Russia, this system can be called a "matryoshka system" (Świerczek 2018, pp. 210–228), which allows the actual sender of the manipulated message to be hidden many times over. The effect of this type of action is to evoke a specific reaction from the recipient in line with the intentions and interests of the disinformer. The true art of it is to ensure that the object of manipulation remains unaware of it.

3 Military Disinformation

The use of disinformation as a tool in politics, diplomacy, trade, or warfare is an age-old strategy. The advantage of information is an indispensable component of success in times of war and peace, as well as in "gray zone" or "hybrid" conflicts. The essence of these conflicts is the use of a combination of military and non-military means to keep the confrontation under the threshold of war (Hoffman, 2009; Piotrowski, 2015, pp. 7–38). In such a context, disinformation is an element of information warfare (infowarfare), which is defined as "actions aimed at protecting, using, damaging, or destroying information or its resources, as well as contradicting information in order to achieve significant benefits, goals or victory over an opponent" (Schwartau, 1996). It encompasses offensive and defensive actions necessary to gain an information advantage over the enemy and to achieve the intended military and political goals. Military deception (MILDEC) is one of the tools of infowarfare and is understood as the deliberate transfer of specially prepared (manipulated or fake) information (e.g., via documents or demonstrations of military actions) aimed at misleading the opponent regarding real intentions, plans, and undertakings to achieve military advantage. Its application is crucial for obtaining the element of surprise, securing actions, and minimizing the losses of the used forces and resources.

Military disinformation is a tool of strategy that has been known to strategic theorists and practitioners since ancient times. Its operational use, however, was significantly developed during the Second World War. For instance, in 1942 the Allies conducted "Operation Torch", which suggested that they were preparing a landing in Norway or France. The aim was to deceive the French collaborationist government and prevent the strengthening of German forces in North Africa, while the real target was Algeria and Morocco. Another

well-known example is "Operation Mincemeat" (1943), a two-tier disinformation operation conducted by British intelligence. The operation name suggested that the planned Allied landing on Sicily ("Operation Husky") was a sham and that the real targets were Sardinia and Greece ("Operation Brimstone"), which led to a change in German and Italian defense plans. The actual landing target was Sicily, and the strikes against Greece and Sardinia were simulated. In 1944 operations "Bodyguard" and "Fortitude" suggested preparations for Allied forces landing in the Pas de Calais area and off the coast of Belgium, while the real target of "Operation Overlord" was Normandy. The purpose of this disinformation was to force Germany to disperse its activities held in various theaters (Hughes-Wilson, 2002).

Military disinformation aims to cause chaos in the enemy's command and control system (C2) by providing false information, leading to the adversary's incorrect assessment of the situation. It has a specific goal and implementation plan, such as prompting the opponent to change their defense concepts, shifting the location of military groups, or redirecting the enemy's forces and resources to a mock strike area. The success of disinformation activities is determined by the opponent's actions, which align with the deliberately created picture of the operational situation. The following methods are used in the implementation of MILDEC operations:

- Disinformation by intelligence assets. This involves providing fabricated information to the enemy (such as documents, operational plans, orders, reports, decisions, diagrams, and maps) through the use of human intelligence assets (such as agents, double agents, and offerors).
- Disinformation through inspiration from the environment. This is the process of disseminating false information by spreading rumors among the enemy troops, armed groups like rebels, resistance forces, guerilla fighters, and the local population.
- Disinformation via the mass media. This involves spreading false information to the press, radio or television or on social media.
- Radio-electronic disinformation. This refers to the transmission of false commands, orders, and reports through information and communication technologies (ICT), as well as the use of fake radio-electronic and digital communications to simulate activities (such as preparation to start operations in a different direction). It also involves emitting misleading electronic, audible, and visual signals to authenticate disinformation.
- Operational masking. This tactic is aimed at hindering the enemy's ability to make informed decisions and conduct effective military operations. It involves concealing troops and defense infrastructure from enemy reconnaissance capabilities and using dummies and mock-ups.

Military disinformation plays a supporting role and is one element of military information operations (INFOOPS). It is also a component of strategic communication (StratCom), which is defined in NATO as the "integration of communication capabilities and infoops with other military activities, in order to understand and shape the information environment" (MC 0422/6, p. 6). These capabilities include public diplomacy and military public affairs. INFOOPS also include measures such as military reconnaissance, operational security (OPSEC), electronic warfare (EW), psychological operations (PSYOPS), and the physical destruction of the opponent's information systems.

According to NATO standards, tools for strategic communication and information operations involve:

- Strategic communication. This is the coordinated and tailored communication activities and capabilities that serve two functions. Firstly, it integrates coalition information efforts to secure vital interests and goals and promote coalition cohesion. Secondly, it provides advice and coordination for undertakings that affect information and information systems, including the behavior and capabilities of these systems, to achieve the desired effect.
- Public diplomacy. This involves activities in the field of civil communication, which is supplemented by activities and supporting tools that promote awareness and build understanding and support for NATO policies and operations.
- Public affairs. This involves the timely, accurate, active, and reactive involvement of NATO's civilian sector in reporting through the media about Alliance policies and ensuing activities and operations.
- Military public affairs. This aims to promote the impact of NATO's military objectives among the facilities to raise awareness and promote a better understanding of the military aspects of the Alliance's functioning. It includes the planning and implementation of appropriate relations with the media, internal communication, and relations with society.
- Information operations. These ventures are coordinated by a staff cell and rely on analyzing the information environment, planning, integrating, and evaluating information activities to achieve the desired effects of influencing the will to act. They also rely on an understanding of the situation and the capabilities of the opponent and other approved objects of influence. They support the achievement of the operation's objectives and strategic communication.
- Psychological operations. These involve a scheduled process of transmitting prepared content using various methods and means of communication to selected targets to bring about the desired change in perception, attitudes, and behavior, which will facilitate the achievement of intended political

and military objectives. The PsyOps units' tasks include: (1) weakening the enemy's morale and its abilities, including combat abilities; (2) consolidation of friendly/neutral attitudes of groups and communities not directly involved in the conflict; (3) establishing cooperation with indecisive or neutral circles and gaining their support; (4) participating in undertakings related to operational masking and operational security (OPSEC); (5) collecting, analyzing, processing and disseminating data about the enemy and the area of operations within the integrated reconnaissance system; (6) supporting undertakings carried out by cells of the strategic communication system preventing the opponent's psychological operations; and (7) developing and improving one's own and allied database.

- Military reconnaissance. This involves gathering, processing, and disseminating information about the enemy.
- Operational security. This refers to ensuring sufficient protection for military operations or activities through passive or active means to prevent the enemy from accessing critical information on the deployment, capabilities, and intentions of one's own troops. For this purpose, disinformation is also used to mislead adversaries and conceal the actual intentions and actions of one's own troops.
- Electronic warfare. This involves military operations that aim to identify and disrupt enemy electronic systems and emissions, while also ensuring optimal conditions for the use of electronic systems by friendly troops. Electronic warfare is a crucial component of information activities, involving reconnaissance, electronic countermeasures (interference), and targeting the enemy's command, communication, IT, and reconnaissance systems.
- Physical destruction of information systems. These are strikes performed to deprive the combat capability of the key elements of the enemy's command, control, communication, computers, intelligence, surveillance, and reconnaissance systems (C4ISR).

The above definitions primarily represent the Western perspective on the elements of information warfare. They may not align with how authoritarian regimes interpret and apply them. Russian theorists of information warfare distinguish its two components: (1) information-technical and (2) information-psychological. The former involves integrated actions against the adversary's entire ICT infrastructure, including communication channels, radio-electronic means, and command and control systems of their armed forces (Thomas 2010; Giles 2016). The latter refers to a set of activities aimed at gaining and maintaining an information advantage over the enemy during military operations.

The purpose of Russian information-psychological operations is to disrupt the enemy's information resilience by maintaining constant psychological pressure on the adversary (Nowacki, 2004, pp. 144–147). Russian theorists do not distinguish between military and non-military, technological (cyberspace) and social (information space) order, or times of peace and war (Darczewska & Żochowski, 2017). Unlike the Western approach, Russians do not consider cyberspace as a separate strategic theater of military operations alongside air, sea, land, and space. Instead of using the term "cyberspace", they use the term "information space". Russia's cyber-capabilities are just another tool of information warfare alongside intelligence, counterintelligence, disinformation, propaganda, electronic warfare, disruption of communication and navigation, psychological pressure, and destruction of enemy ICT resources.

Military disinformation can be either "passive" or "active". Passive disinformation aims to hide the adversary's real intentions and abilities, while active disinformation provides fabricated "evidence" of alleged intentions and abilities. Disinformation can also be based on ambiguity (type "A" deception) or on misleading (type "M" deception) (Caddell 2004, pp. 6–7). In the case of type "A" deception, the aim is to cause general confusion in the enemy's headquarters through simulated military or diplomatic activity, increased radio communication, or simulated negotiations in order to gain time to prepare an armed operation. An example is Japan's diplomatic activity during the preparations for the attack on Pearl Harbor in 1941, which made it difficult for American military analysts to assess the situation and Tokyo's real intentions (Wohlstetter, 1962). In the case of type "M" deception, the goal is to mislead the opponent about the planned course of action and to reassure them that they are correctly assessing the situation. An example is "Operation Bodyguard", which masked the preparations for the Normandy landings in 1944 (Howard, 1990).

Disinformation can also be classified as "offensive" or "defensive". Offensive disinformation aims to mislead the opponent about future intentions and force them to fight under unfavorable conditions. Its goal is to achieve surprise and gain initiative. Defensive disinformation activities, on the other hand, are aimed at opponents who have the advantage (initiative) and aim to divert their attention and efforts from the actual goals and plans of the operation. The main goal is to improve the security of one's own activities and create conditions for the successful completion of assigned tasks (Wrzosek, 2005, pp. 75–76). Disinformation can also be carried out at different levels of command within an operation. In this order, its division is as follows:

– Strategic disinformation. This is carried out to mislead the enemy regarding the time, place, strength, and intention of a campaign or operation.

It encompasses matters related to the training system, organizational structure, deployment, level of combat readiness, methods and timing of mobilization, operational and strategic development of the armed forces, composition, equipment, and combat readiness of deployed troops during peacetime, as well as the command and control system.

– Operational disinformation. This involves activities and measures to mislead the enemy regarding the conduct of operations. They should be consistent with, and a logical consequence of, false information communicated at the strategic level. The main purpose is to conceal the preparations and intentions to conduct the operation. This applies particularly to the readiness of separate components of the armed forces planned for use, areas of operational and strategic reserve dislocation or mobilization, as well as the readiness of precision destruction means, areas for the development of command posts, and the operating mode of ICT systems. It also includes directions of military maneuvers and the movement of logistic support shipments.
– Tactical disinformation. This refers to all activities and measures used to mislead the enemy in the area of operations. Actions at this level include protecting critical information, masking, concealing, and simulating (Modrzejewski, 2015, pp. 92–93).

Military disinformation is a specialized form of deception primarily directed at the enemy's armed forces, especially its command, communication, information, computer, and reconnaissance systems. Its aim is to create a credible but false picture of the strategic, operational, and tactical situation. Military disinformation employs methods typical of intelligence activities, such as the use of agents and mass media. It is also understood as one of the forms of INFOOPS or PSYOPS and considered an element of a broader set of strategic communication tools aimed at the enemy's armed forces, decision-making centers, and society. The success of military operations often depends on the attitude of the population living in the war zone, making the informational "struggle for hearts and minds" crucial in the era of asymmetric, unconventional, and hybrid conflicts (Lennon et al., 2003; Stubbs, 2004). In the 21st century, information should therefore be regarded as a weapon.