INFORMATION WARFARE, SECURITY INTELLIGENCE AND MILITARY INTELLIGENCE. – A SHORT THEORETICAL APPROACH –

Teodor BADIU

National Intelligence Academy, Bucharest

In research, discussions from public space and materials designed and disseminated by media trusts, the issue of hybrid warfare/hybrid threats is often analysed either as a phenomenon or as a specific factor of an event. However, due to the complexity of the subject, confusion is often made or the concepts are mixed as the subject becomes even more ambiguous. In addition, the excessive use of simple terms such as "information manipulation", "propaganda", "misinformation", "influence", in the public space, has led to an alteration of their meaning and an ambiguity of the effects that these terms have on the perception of threat. On the other hand, in this context, the role and relevance of security and military intelligence in the management and limitation of hybrid warfare/hybrid threats has been little discussed. Thus, this paper tries to detail in a succinct manner (due to the complexity of the topics), at a theoretical level, the concepts of security intelligence, military intelligence and information warfare.

Keywords: information warfare; security; deception; multinational exercises; asymmetrical confrontations;

INTRODUCTION

Starting from the Ukrainian experience and the situations of information interference in the internal affairs of other states, *hybrid warfare/hybrid threats* represent the factor of instability and insecurity that acts according to the specifics of the operations, regardless of the nature of the actors. Hybrid warfare has enveloped the international security environment, especially in the European space, because of the actions of the Russian Federation, starting from 2014, which reminded the EU and NATO that the Russian Federation was willing to use all means to achieve its strategic objectives, including regaining its sphere of influence over the Eastern European states.

In this regard, we can consider *hybrid warfare* as the factor that establishes the context of information warfare and reduces the distance between security intelligence – its role is to secure the elements that operate the national system such as society, economy, political environment, infrastructure etc. and military intelligence – whose function is to gather information about the armed forces of the opponent or a possible one, disseminating the information obtained to a *military decision maker* who can formulate strategies or organise/reorganise the military forces as needed. Traditionally, their activity gets intensified when there is a declared state of conflict between at least two actors, but, at present, *hybrid warfare* exists without states declaring their actions and without any declared conflict. A major problem of *hybrid warfare* is that it makes the origins and forms of threats ambiguous, which has led to the necessity of increasing activities such as monitoring, preventing or repelling by institutions specialised in military and security intelligence. In addition, in the issue of information warfare, the context of *hybrid warfare* has produced some changes: information warfare has traditionally been a component of armed conflicts between actors (such as asymmetric or irregular confrontations, unconventional approaches, active measures etc.); its scope has extended to the civil one, without requiring the official declaration of the beginning of hostilities.

Next, we will approach, from a theoretical point of view, the relevance of information warfare, security intelligence and military intelligence to understand some of their peculiarities.

DEFINING INFORMATION WARFARE, SECURITY INTELLIGENCE AND MILITARY INTELLIGENCE

Hybrid warfare is an operational concept that integrates a wide range of elements, and in this sense, it is predictable that it affects domains from the economic, political and military to the social and cultural ones. However, events of recent years since 2014 – the annexation of the Crimean Peninsula and the emergence of separatist forces in eastern Ukraine, the political rise of extremist groups in Europe, foreign involvement in elections and referendums, the proliferation of conventional arms between NATO and the Russian Federation, the wargames[1] initiated during the multinational exercises, the disinformation and de-legitimisation campaigns initiated by the Russian Federation, the attempted assassination of the defector Sergei Skripal, the need to rethink CBRN protection measures (context of the international spread of COVID-19 virus) – demonstrate the need to include security intelligence and military intelligence in a common and inclusive approach. Overall, these events can be understood as segments that make up hybrid warfare. Until recently, the role and objectives of security intelligence and military intelligence were seen as something limited. Nowadays, the mutations of threats have led to an amalgam of information and military actions whose effects have been felt especially in Eastern Europe.

In this equation, *information warfare* has an essential role in the degradation of security environment. This is a term associated with hybrid warfare (but not only, being connected with asymmetric, irregular and unconventional warfare, active measures, public diplomacy etc.) (Theohary, 2018, pp. 4-5), which has dual valence, offensive and defensive, and which has distinct forms of manifestation depending on the state of war or peace. NATO defines the concept in strictly military terms, from the perspective of cyberwar where information warfare consists of *"undertaking actions to obtain computer field superiority through deterioration of enemy information technology systems and protect own devices"*. (AAP-6, 2018, p. 430). However, as we talked about the context, we notice that the information warfare is not only manifested in the military sphere, but it can also extend to the social and political area or can be interdisciplinary.

The broad spectrum in which information warfare can operate makes it a much more effective weapon, due to the fact that (Molander et al., 1996, pp. 15-29):

- the cost-benefit ratio can be maximised due to relatively low costs. Unlike the maintenance and deployment of an army whose existence poses

[1] Wargames are an analytical form that simulates tactical, operational and strategic aspects of a conventional confrontation. They are usually used to examine the concepts of combat, to train analysts and commanders, to develop scenarios and to evaluate the effects of subsequent or ongoing ones.

a threat or leads to a security dilemma, the infusion of an information environment with rumours, partially true or ambiguous information, can lead to misperceptions and an escalation of fear. Also, the support and organisation of the information warfare can be provided by a small number of individuals, being quite accessible;

- the blurring of traditional borders due to economic, social, political and military interdependencies has led to an alteration of the individuality of state actors. The connection of states and private actors to the global information system (via the Internet, for example) has amplified the difficulty of distinguishing between external and internal threats in the context of information warfare;
- their perceptions and management can be problematic in the sense that the flow of information abounds with official, unofficial, sequential, conspiratorial, erroneous, false, ambiguous information etc., making the society vulnerable to alterations of reality or information intoxications. Manipulation of information through techniques and technologies can allow a wide range of actors to undermine the authority and even the legitimacy of institutions, states or international organisations;
- the difficulty of early warning and rapid impact assessment determines a major vulnerability to surprise information attacks, the actors being limited as a possibility of prevention or response. Doubled by the difficulty of seeing, in the shortest time, which was the target, the evaluation of the effects may require additional time and costs;
- the interoperability between allies or members of an international organisation leads to the synchronisation of C4I systems to ensure coherence, but even if their own systems are well secured, the weakness of an allied system can lead to the penetration of the overall system.

With regard to information warfare, it should be noted that its pillar consists of *information operations* (IO), which can be defined as the integrated employment of information capabilities in accordance with other lines of operations to influence, interrupt, corrupt or usurp the decision-makers of opponents while own systems are protected (*Dictionary of Military and Associated Terms*, 2020, p. 104). In principle, IOs serve the purpose of making the opponent/target behave, or not, in a certain direction by using segmented information (extracting information from a specific context), propaganda and intentional (determined by a deliberate and organised action) or unintentional misinformation (caused by erroneous actions, misunderstanding or involuntary degeneration of information). The following types of operations are subcategories of IOs (Theohary, Ibid., p. 3):

- Psychological operations (PSYOPS) – involve the type of operations initiated, in order to influence and exploit the emotions, motivations, perception and behaviour of the target at the cultural and cognitive level;
- Security operations (OPSEC) – represent actions and measures taken for defensive purposes, which identify and analyse essential information, disruptors of an ongoing operation and the protection of all elements that contribute to the operation. For offensive purposes, it means gathering information to facilitate the understanding of the opponent, being also the process of slowing down the possibility of making a decision in a timely manner by the opponent's decision-makers;
- Electronic warfare (EW) – is defined as the accumulation of military technical actions, carried out using electromagnetic waves and signals to support ongoing operations, protect their own equipment and attack the computer systems of opponents. As more well-known activities, we can mention the jamming of communication systems, encryption and decryption of channels, the use of satellite positioning systems (GPS) etc.;
- Cyber operations – are the actions carried out in cyberspace that can range from system interruption and viruses to support for integrated systems and protection of own systems;
- Deception – can involve all or a large part of the types of operations presented in order to misleading the opponent. By *"accidentally"* sending false reports and documents to foreign agents, falsifying radio channels that are intercepted, organising misleading displays etc. (Herman, 1996, p. 170), and depending on the information that the opponent has, could be exploited opportunities that, in the end, lead to confusion at the decision-making level.

Considering the typologies of operations, we notice that information operations could have a coercive character that can be translated by influencing the adversary's decision-makers or the civil environment in guided directions through covered operations. Hence, if we talk about the soft approach, information operations can contribute by creating a positive image in relation to other actors to determine legitimacy or long-term advantages, or just to support public diplomacy.

Though IOs are generally initiated and planned by specialists from the military field or intelligence services, their applicability extends also to the civilian area. So that, in recent years, discussions about *information disorder* (Wardle et al., 2017, p. 20) – a concept much broader encompassing fake news, false news, misinformation and grey propaganda **–** spreading in the media, mainly in key moments such as elections, referendums, major protests, crisis situations etc. have intensified because of their effects that affect relations between authorities and their own citizens or between different social groups. We can say that the spectrum of information disorder can contribute to the process of deception because it delivers to a target certain information that is partially true or false. It means that it must create a specific perception or make the target act in a particular direction. Seen from a psychological perspective, the essence of information disorder lies in the subjectivism of the target, where it is not important how the story is presented, but the story as such, which can favour a given context.

To exemplify, we can address the issue of social media platforms as Facebook and Twitter, which are increasingly confronted with information disorder that uses their infrastructure. As a result, since 2016 they have tried to initiate some more austere regulatory actions and measures like stopping the spread of fake information through posting and distribution of content, and elimination of accounts that are dubious and disseminate erroneous and contradictory information (Polyakova, Fried, 2019, p. 12). On the other hand, other companies such as Google and YouTube have shown little transparency regarding the measures taken. More exactly, Google has allowed known disruptors such as Sputnik or RussiaToday to remain in the top of search engines, while YouTube has changed only the terms and conditions for extremist and insulting videos without supporting a solid campaign to remove them (Ibid., pp. 13-14). In this regard, the 2019 attack from Christchurch in New Zealand, when a radicalised individual broadcast the attack on two mosques on the internet can be approached as an example of the platforms' inability to stop the spread of toxic information. Only after this incident YouTube did remove from its platform the video Remove Kebab, considered to be an anti-Muslim propaganda song from the Yugoslav wars. It is worth mentioning that the killer on the way to the two mosques listened to this song in his car.

Social media tries to block, in different proportions, the tools and effects of *information operations*, but they will not be able to cope because of the distinct specificity. IOs have a military origin, based on a military doctrine where civilian and military personnel conduct planning and execution. Due to this fact, private companies in the social media sphere are at a disadvantage because their response is from a strictly technical perspective, and from a cultural point of view, they are related to the principles of economic markets. Organising an adequate and efficient response would involve the establishment of a specialised department composed of staff trained in intelligence domain that would probably not be legal and sustainable in terms of costs and benefits.

Thus, we note that with regard to IOs and implicitly the information warfare, states are the ones that must react because they are the only ones with qualified personnel in execution and combat, moral and legal legitimacy, consistent material resources, complex bureaucratic apparatus and specialised institutions. In this respect, the state may have a monopoly and in the context of international competition, the need for security could enhance the significance and activity of security and military intelligence.

After World War II, Sherman Kent introduced in the specialised literature the notion of *security intelligence* as a distinct form by the military intelligence. He defines it in two directions: as the intelligence work behind the police activities that deals with the protection of the state and citizens; and as an activity designed to identify those internal disruptors such as clandestine agents, traitors, elements of organised crime and violations of the (federal) law (Kent, 1965, pp. 209-210). This perspective on security intelligence tends to be closer to police work, but if we compare the institutions of several countries that deal with security intelligence we will see that they have developed a specificity related to culture, the past and tradition of the institution, the regime they belong to, the importance of the institution in relation to other institutions, the financial resources available, the degree of qualification and the number of staff etc. In general, the interest subjects of security intelligence consist in counterterrorism, combating subversive operations carried out on the national territory, counterintelligence and combating organised crime activities. Security intelligence, in theory, excludes activities in the political, economic, tactical and military fields, and is considered different from *information security*, interspersed only with counterintelligence – security intelligence and information security would aim jointly at preventing/combating information leaks and protecting information systems (Robinson, 2010, pp. 113, 207). Moreover, although in theory institutions accredited in the area of security intelligence should deal only in the area of internal protection, in practice, there are particularities of institutions in various states that lead to notable differences.

Taking as an example MI5 (Security Service) from the UK, FBI from the USA and FSB from the Russian Federation, we can notice distinct approaches to national security, each including activities that go beyond the area of internal security or focusing on specific areas. We can exemplify the situation of the FSB, which, after its merge with FAPSI – Federal Agency of Government Communications and Information – began to extend its attributions from internal security to a mix of defence and offense by undertaking activities specific to electronic warfare. In comparison, MI5 offers an increased attention to counterterrorism and extends its area to the defence of economic welfare and the democratic parliamentary regime – as an ideological/identity component (Ibid., pp. 92, 209). Michael Herman explains security intelligence as a separate entity from decision-makers whose role should be to provide information rather than advice. Although security intelligence has to deal with internal threats, they, however internal they may seem, have an external origin so it is vital to inform decision-makers through analysis and forecasts that also include external elements (Herman, p. 34). This adaptation is due to the transition of the security paradigm from the Cold War system, based on an ambivalent conflict between the Warsaw Pact and NATO, to a multipolar system marked by the uncertainties of the hybrid warfare. If in terms of intelligence work, the Cold War period was focused on gathering information, organising and destructuring subversive operations, espionage and counterintelligence, to understand the intentions of the opponent, now we are witnessing a paradox. It is not uncommon when external intelligence is also collected from the national territory, while security intelligence is collected from outside national borders, and the targets may consist more in subjects than in the actors themselves, especially in the context of dilution of the meaning of security intelligence as a strictly internal process (Ibid., pp. 47-49).

Regarding military intelligence, it can be said that there is a long tradition, as a result of the need for armed forces to know vital information such as capabilities, number, specialisations, morale, troop disposition, strategies, command centres etc. of opposing forces. Thus, the definition of military intelligence begins with the perspective of Carl von Clausewitz who described the collection of information in time of war as necessary, but contradictory. Either there is a situation when some of the information is false, and another part consists in uncertain information that at some point will contradict each other, or the information supports each other and in the whirlwind of a decision that seems appropriate proves to be wrong due to erroneous, false or exaggerated information (Clausewitz, 2014, p. 38). In short, military intelligence is that component of intelligence that is concerned with issues specific to the military area, the capabilities of states, foreign organisations, or ongoing multinational military operations (DoD, p. 91). We can add that the military intelligence tries to discover the weaknesses of enemy military architecture, offering the Command the chance to streamline its combat actions with minimal risks. On the other hand, it tries to analyse and discover the weak points in own and the allies' defence system. However, in light of the proliferation of conventional weapons and wargames in recent years, the topics of defence intelligence seems to remain in the spotlight of security institutions. *Defence intelligence* can be considered a subcategory of military intelligence, whose topics are also of interest to the political environment. The object of activity is focused on the supervision of external military actions and local or regional wars, this including autonomous or sustained by external aid insurrections; situations in which combined politics, violence and subversive operations lead to the use of armed forces; the failure of states as a result of inter-ethnic, religious, ideological conflicts, etc. (Herman, p. 50). Moreover, as topics of interest to defence intelligence there are also defence industries, arms exports, technological developments in military technology, the proliferation of weapons of mass destruction (tactical and ballistic) etc.

A fundamental aspect of intelligence, which cannot be neglected, whether we are talking about security or military intelligence, is deception. NATO defines it as *"those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests"* (AAP-6, p. 272). This is not a new practice, leaders and generals have used it since Antiquity in achieving their goals, but conceptually, the complex variant of deception is military deception (MILDEC). Strictly speaking of its operational nature, military deception could not be considered part of intelligence, given that it coagulates specific elements and activities such as OPSEC, PSYOPS, EW, intelligence gathering, counterintelligence etc. However, it can be considered as a defensive means in the case of security intelligence, and offensive in the case of military intelligence. Although it seems strange that it is assigned to the first category, in the context of information warfare, MILDEC can generate various forms of perception of politicians, military personnel and civilian targets, causing erroneous actions or inopportune inaction of governments, or causing civil society to put pressure on governments in a certain direction. In particular, we note that MILDEC's spectrum of soft activities is composed of influencers, information operations, covered financing operations of political groups or media trusts; and the hard spectrum consists in covert support for opposition groups, resistance, insurgency or terrorist forces, and sabotage and paramilitary operations (Herman, p. 55).

Regarding military deception, the literature is abundant and includes comprehensive details, from deception targets and objectives to the conduits, networks and filters used in deception. The subject MILDEC represents in itself a vast research topic, which combines theoretical and practical aspects in a subtle art, but for this study, we will highlight some fundamental theoretical aspects.

MILDEC's role is to create a *story of deception* that the opponent can take as such, and all the evidence related to the story look veridical. The story of deception is a narrative or a brief statement, constructed according to the perspective and specificity of the target – like mental structure, values, specific culture and its expectations – and which is strengthened by misleading events (Field Manual 3-13.4, 2019, p. I-5). Regarding the types of deception, two categories can be identified:

1) ambiguity-increasing, which aims to generate confusion and internal conflict over adverse decision-makers through a continuous flow of seemingly plausible information, drawing their attention from a set of activities to another;

2) ambiguity-decreasing, which involves the manipulation and exploitation of pre-existing thinking and beliefs of adverse decision-makers, by guiding the target to the wrong place at the wrong time, in conditions of maximum vulnerability (Ibid., pp. I-6-17). Alternative terms such as Type-A (ambiguity-increasing) deception, to amplify ambiguity, and Type-M deception (misleading deception), to reduce ambiguity, can also be found in the literature, and passive and active forms of deception can be identified. The passive form is based on the actions of covering and camouflaging one's own intentions and/or capabilities towards the opponent, while the active form consists of one's own deliberate actions, to present to the opponent the intentions or capabilities he does not possess (Shaw, 2014, p. 3). MILDEC uses a narrow range of tactics to concretely serve to different missions objectives as follows:

- *Ruse* – deliberate actions to alter reality through information;
- *Diversion* – intentional distraction of the opponent from a subject/objective of interest or from carrying out an attack;
- *Feint* – offensive actions that involve direct contact with the opponent and whose purpose is to mislead the opponent regarding the place and/or time when an attack will take place;
- *Demonstration* – show of strength initiated in order to determine the opponent to choose the most disadvantageous course of action;
- *Cover* – actions aimed at masking the preparations or initiating an offensive operation, depending on the situation associated with conditioning;
- *Display* – actions organised to support the story of deception by simulating, disguising and/or highlighting the capabilities and composition of allied forces (Ibid., p. 6).

It must be reaffirmed that at the heart of these actions is the story of deception, which is a product of the imagination. This requires organised and disciplined thinking, so that the logic of the story is not interrupted and the target can perceive it visibly – the exaggeration of its subtlety can make the target to ignore the story of deception. The deception operation must be done from the perspective of the target, and his ensemble must be a general description of the whole deception. Thus, the story of deception must be verifiable (the target can confirm it through its own channels or with the help of his allied intelligence structures), executable (the existence of the necessary authority and resources), credible (diminishing suspicions and doubts on the part of the target) and consistent (initiators of deception must know the degree of training of the target to not exaggerate or diminish the complexity of the story) (Field Manual 3-13, 4, pp. II-10-II-11). For this reason, field-specific maxims are often used in misleading processes to facilitate the organisation and execution.

Thus, we detail only a few maxims (CIA, pp. 5-20, 22-26, 32-33) that are relevant to this study:

a) *Magruder's principle* aims to capitalise the opponent's beliefs, using them in altering reality and examining the possibilities that may be to his disadvantage. This principle can be exemplified by the planning of the invasion of Normandy, where information showed that the Germans were expecting an Alliance offensive in the Pas de Calais region, being a setback of German plans to invade Britain.

b) *Limitations to human information processing* are processes of human cognition that, almost universally, in specific situations present syncope of processes. In this sense, syncopes can be exploited, which leads us to the law of small numbers and the predisposition to *conditioning*. The law of small numbers refers to the human tendency to generalise in the case of small data sets. Conditioning is the accustoming of the opponent to a certain situation or will, which was carried out over time by transmitting repetitive stimuli. Another limitation is the human tendency to omit small changes or small details.

c) *The multiple forms of surprise* consist of location, force capabilities, intention, specific style and timing. Although not all can be achieved in an operation, the emphasis must be on limiting a number of relevant elements. The use of false alarms is one of the main elements of surprise by conditioning the opponent not to respond immediately to the apparent imminent threats and by misleading as the opponent directs his attention, resources and staff where false alarms indicate.

d) *A choice among the types of deception* is necessary due to the fact that their extensive use can lead to distrust of the target in the appearances that are served to him. Thus, in this situation we opt to reduce the ambiguity, although if the target already has some real information, it may be recommended to increase the *"noises"* – increase the target's access to false alternative information and/or evidence that prove the authenticity of the false information that has been delivered.

e) *A sequencing rule* refers to the need for misleading activities to be successive and sustained as much as possible in order to reinforce the story of deception.

It should be noted that the process of deception is a constant one, due to the exchange of information that takes place between the analysis and organisation teams, and the operational ones. However, probably, gathering information about the opponent, analysing and interpreting it can be considered the fundamental actions of the whole operation of misleading. In order to influence the behaviour of the target, it is vital to have help from intelligence structures, and to maintain a constant flow of information on how it perceives the environment, how it processes the information delivered and how it makes decisions, and then analysing the variables in the political, military, economic, social and information environments of the target that can influence it (Field Manual 3-13.4, pp. II-3, II-14).

Another important clarification is how the target perceives, at the cognitive level, the threat and we notice that there is a tendency of individuals to perceive things because of their own expectations, where they are also shaped by context. Their way of thinking can present some vulnerabilities which consist in:

a) the tendency to form hasty reasoning, which can later be changed only by a considerable deliberate psychological effort;

b) assimilation of new sets of information, which may be contradictory, and their use in strengthening the initial reasoning;

c) prolonged exposure to ambiguous or unclear information determines that a subsequent exposure to a new set of information requires a sum of additional information, even if they may be clear from the first moment (Heuer, 1999, pp. 7-14). Although there may be solid evidence that show the inaccuracy of the original reasoning, mental processes make the reorganisation of data and the assimilation of information a difficult task in changing perceptions. Although the dynamics of events indicate other trends, there is an inner resistance of the perception to new changes. Even if the individual is psychologically willing to reanalyse the data and information, the different perspectives he reaches will still be related to the initial reasoning, and cannot be totally changed or eradicated (Ibid., p. 125).

Given these details, the ambiguity of the relationship between information warfare, security intelligence and military intelligence seems to be diminishing. Information warfare is offensive in itself, but it tends to engage actors of their own free will or as victims. As a result, security intelligence needs to adapt to new challenges and respond in a timely manner to threats that, in the current context, are not easy to spot and anticipate. However, the uncertainties of the security environment of the 21st century have led to an expansion of the area of security intelligence, and practically, have led to the narrowing of the boundaries between it and military intelligence. The projection of one state's power on another through information and the deception over the existence or non-existence of significant national capabilities also raises security dilemmas. All this produces perceptions as a result of deliberate actions or as an incalculable effect, but the risk that perceptions will degenerate and turn into fear is very real.

CONCLUSIONS

As we have seen, information warfare, and especially deception, tries to change the perception of individuals in a certain direction. Perception can embody the misunderstanding of a real situation, causing: one state to act hastily in relation to another; a government not to perceive the needs of its own population correctly and to act to its detriment; or the population, influenced by negative feelings and shortcomings, to resort to massive protests against the central authority, up to the civil war. The erroneous perception of a particularly important factor, or a possible or in progress event, can generate unfounded panic and fear, inopportune actions, harmful passivity, disproportionate aggression etc., causing national security problems. In addition, the perception of reality is not a standardised thing, it is different depending on the information that individuals assimilate and interpret, using filters such as personal experience, education, culture, spatial and temporal context, affiliation with a group or a set of rules and specific values etc.

On the other hand, adding the context that hybrid warfare establishes, it causes maximisation of ambiguity on the origin, nature and the initial impact of information and military threat. Corroborated with strategic surprise and deception, there is a risk that decision-makers will be unable to act efficient or could act inopportunely at key moments, as a result of the information flows to which they have been subjected in accordance with their own perceptions. The most relevant example in this regard is the case of Ukraine where the cumulation of military and non-military actions of the Russian Federation led to the annexation of Crimea and the destabilisation of eastern Ukraine (the emergence of armed conflicts in the Donetsk and Luhansk regions), which led to a strategic surprise. Kiev leadership had not foreseen these events and that made it impossible for them to respond in a timely manner.

Because of the changes in security environment the role and relevance of security and military intelligence grow exponentially for two reasons:

a) they can be a source of distortion of information and deception, especially that specialised intelligence institutions have the ability to perform offensive and defensive actions;

b) due to their complexity, they can carry out a wide range of protection measures ranging from strategic objectives to political and military decision-makers who, being part of society, are connected to information flows.

Finally, we can say that technological and theoretical developments and geopolitical evolutions affect the form of concepts of information warfare and security and military intelligence because the dynamics of the security environment emphasise the need for an unexpected, intelligent and surprising approach. Regardless of the state of peace or war and regardless of the target, the combatants (declared or not) will try to obtain, by all means, strategic advantages and gains as an alternative to the direct and mass use of force.

BIBLIOGRAPHY:

1. Clausewitz, von C. (2014). *Despre război*. Editura Antet.
2. Herman, M. (1996). *Intelligence power in peace and war.* Royal Institute of International Affairs.
3. Heuer, J.R.Jr. (1999). *Psychology of Intelligence Analysis*. Central Intelligence Agency: Center for the Study of Intelligence.
4. Kent, S. (1965). *Strategic Intelligence for American World Policy*. Connecticut: Archon Books. Hamden.
5. Molander, C.R., Riddile, S.A., Wilson, A.P. (1996). RAND: *“Strategic information warfare: a new face of war”*.
6. Polyakova, A., Fried, D. (2019). Atlantic Council: *“Democratic Defense against Disinformation 2.0”*.
7. Robinson, P. (2010), *Dicționar de securitate internațională*. Translated by Monica Neamț. Cluj-Napoca: Editura CA Publishing.
8. Shaw, J.E. (2014). *“Military Deception at the Operational Level War”*. The United States Naval War College: Joint Military Operations Department.
9. Theohary, A.C. (2018). *“Information Warfare: Issues for Congress”*. Congressional Research Service.
10. Wardle, C., Derakhshan, H. (2017). *“Information Disorder”*. Council of Europe.
11. AAP-6, *Glosar de termeni și definiții NATO* (English, French and Romanian). (2018). Agenția de Standardizare NATO (ASN).
12. Central Intelligence Agency, *“Deception Maxims: Fact and Folklore”* (1981). Washington: Office of Research and Development.
13. Clark, M.R., Mitchell, L.W. (2019). *Deception. Counterdeception and Counterintelligence*. Washington D.C.: CQ Press.
14. Department of Defense (DoD) (US), *Dictionary of Military and Associated Terms*. (2020). Joint Publication (JP).
15. Field Manual 3-13.4, *Army Support to Military Deception* (2019). Washington: Headquarters, Department of the Army.