CONCEPTUAL APPROACHES ON INFORMATION WARFARE AND SOME OF ITS COMPONENTS

Teodor BADIU

graduate of the civil master's degree in International Relations and Intelligence Studies from the "Mihai Viteazul" National Intelligence Academy in Bucharest

In the case of information warfare, it no longer exists a demarcation line between the state of pace or the state of war, this type of war being used by the state and non-state actors because of its effectiveness and the difficulty of being traced and repelled. In addition, it is known that the Russian Federation used information activities against Western and Eastern European countries. To see the specificity of information operations, we must define the concepts and components that underlie information warfare and the perspective Russian military thinkers have on information activities. Even if the paper does not describe in detail all the components of the information warfare, it is important for us to clarify the role of information operations and its components as part of information warfare, as well as the terms that are often used in the public and academic area, such as disinformation, manipulation, propaganda, fake news etc. To better understand the Russian information activity, the paper provides some specific examples from Poland, the Czech Republic and Slovakia.

Keywords: information warfare; psychological operations; information disorder; alternative media;

INTRODUCTION

Although the issue of information warfare – and, implicitly, of information operations – is found in the public and academic space through approaches to misinformation and disinformation, fake news, manipulation of information, propaganda, information taken out of context, the emergence of *"alternative media"*, etc., in few cases the issue was approached more deeply.

The European public space and its citizens have been severely assaulted in recent years by conspiracy or radical narratives, confusing and biased messages, misinformation and disinformation that provoked emotions and rumors, all producing social reactions that hindered the efficient functioning of states. It should be noted that there are many actors who have contributed to the dissemination of false information, like state actors, such as the Russian Federation, Iran, China, North Korea (Nemr, Gangware, 2019, pp. 14-25), and non-state actors such as terrorist organisations. Focusing on state actors, we note that the common element of these states is the purpose of the information operation to promote their own national agendas, with different operating modes. More specifically, the Russian Federation is revitalising the spectrum of active measures; China is launching campaigns to influence public perceptions of economic, political and bilateral personal relations; Iran prefers a classical approach to disseminating false information, similar to Russian and Chinese, focusing on pro-Palestinian and anti-Israeli narratives, and North Korea uses a mix between influence and propaganda operations to alter reality and get rid of sanctions (Ib.). The channels used by these states are diverse, ranging from printed materials to the dissemination of information in the online space, depending on objectives, target groups and their capabilities.

The European public space and its citizens have been severely assaulted in recent years by conspiracy or radical narratives, confusing and biased messages, misinformation and disinformation that provoked emotions and rumors, all producing social reactions that hindered the efficient functioning of states.

On the other hand, the information operations executed by these states have certain particularities that consist in their strategic culture, experience and tradition use of information operations,

in the operating modes, doctrines etc. However, in order to analyse the information actions carried out by these states, it is necessary to define, even briefly, the concepts and terms used when referring to the context of the information warfare. Following the various approaches from the public and academic space, there are sometimes ambiguities regarding the understanding of how this information operations works, what concepts and tools are used or what are the links between components and concepts.

Thus, this paper will try to clarify a number of features of information warfare, especially since this topic develops a whole theoretical and practical approach. Also, we will start from the conception that, in peacetime, information warfare is part of the hybrid warfare/hybrid threats, where the information warfare is included likewise among the spectrum of asymmetric, irregular and unconventional warfare, active measures, public diplomacy and so on (Theohary, 2018, pp. 4-5). It should be noted that we will describe some examples from Poland, the Czech Republic and Slovakia, focusing on the information activity of the Russian Federation on these states.

In order to analyse the information actions carried out by these states, it is necessary to define, even briefly, the concepts and terms used when referring to the context of the information warfare.

THEORETICAL APPROACH

Regarding *information warfare*, there are two main approaches that try to define it: one focuses on the technical specifics of information warfare, where information activities take place in cyberspace and/or the electronic area, and the other approach concerns information warfare comprehensively, from the intelligence perspective.

For the first approach, we can take as an example NATO's perspective on information warfare, which classifies it as *"Undertaking actions to obtain computer field superiority through deterioration of enemy information technology systems and protect own devices"*. (AAP-6, 2018, p. 430). However, regarding the second approach, information warfare is an accumulation of organised actions in the information environment that tries to use all means to have control over the flow of information and its interpretation (Robinson, 2010, p. 169). The target can be a decision-maker, a public opinion of a state or the international one.

Michael Herman writes that *"Warfare is becoming 'information warfare'; 'war begins and ends with intelligence… Information is a critical resource in war, and the same applies increasingly to international competition in peace"* (Herman, 1996, p. 347), thus the conflict becomes constant in the context of international competition and the logic of information warfare becomes universal, involving methods and tools that, in the past, were limited to the military sphere.

In this sense, Edward Waltz defines the concept of information warfare as *information-based warfare* where the ultimate goal is to achieve information superiority through the acquisition, processing and exploitation of information, resulting in knowledge, which will subsequently be protected by defensive actions (information warfare-defend) or offensive actions (information warfare-attack) against the enemy's knowledge (Waltz, 1998, pp. 20-21). Definitions regarding information warfare may continue, but if we simplify this concept, we could define it as the combination of separate or integrated, interdisciplinary actions, carried out by at least two fighters/competitors whose goal is to gain a strategic advantage over the other, using available channels, opportunities and own means by collecting and disseminating data and information.

Edward Waltz define the concept of information warfare as information-based warfare where the ultimate goal is to achieve informational superiority through the acquisition, processing and exploitation of information.

The space in which the information war takes place is the *information environment*, which is defined as *"The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information".* (DoD, 2020, p. 104). In turn, the information environment is composed of three dimensions (Waltz, Ib., p. 27):

- *the physical dimension*, where the actions aim at the protection; physical destruction and/or theft of equipment, materials/ documents, databases, communication nodes, facilities for collecting, processing and disseminating information;
- *the information dimension*, where the actions seek the protection, destruction, interception, alteration and/or dissemination of false information, and this dimension represents the link between the physical and the cognitive dimension. From the perspective of opponents, this field offers more opportunities, as it can affect the opponent's C4 infrastructure without involving the physical risks of an operational action of their own forces. On the other hand,

the conduct of misleading operations or strategic surprises may have an increased efficiency in the field of information infrastructure, due to the possibility of intercepting data and information, parasitizing a channel and inserting false/partially true data and information or the possibility of taking actions act punctually, depending on the vulnerabilities of the opponent;

- *the dimension of human cognition/perceptions*, where actions seek to influence and exploit the emotions, perceptions, trends, motivations and behaviours of targeted social groups, decision-makers or the population by using tools specific to information disorder.

Information operations should be perceived as a particular element (or pillar) in the information warfare, through which actions are taken, at a specific level, in the field of psychological operations (PSYOPS), security operations (OPSEC), cyber operations, military deception (MILDEC), electronic warfare (EW) or operations that support activities like subversion, counterintelligence.

In another train of thoughts, *information operations* should be perceived as a particular element (or pillar) in the information warfare, through which actions are taken, at a specific level, in the field of psychological operations (PSYOPS), security operations (OPSEC), cyber operations, military deception (MILDEC), electronic warfare (EW) or operations that support activities like subversion, counterintelligence, etc.

Information operations can be defined, from a military perspective, as an activity that integrates its own information capabilities in close connection with other lines of operations, with the ultimate goal of interrupting, corrupting, usurping or influencing adverse decision makers, while the systems of the initiator are protected. (DoD, Ib.). Information operations optimize information elements in the context of data and information flow and focus actions specifically on certain topics and targets. Another approach classifies information operations as actions of governments or non-state actors to distort internal or external opinion, in order to achieve a strategic and/or geopolitical result, using a spectrum of methods composed of disinformation, false information or false amplifiers – accounts on social platforms that try to manipulate public opinion (Wardle, Derakhshan, 2017, p. 6).

In information operations, we can identify *information disorder* as a relatively new concept, subordinated to information operations, which seeks to provide a comprehensive understanding of what is considered in the public space as fake news. The need to use this concept is due to: 1) the abusive use – and sometimes inappropriate – by politicians

and journalists, of the term in various contexts, causing the alteration of its meaning; and 2) due to cultural differences between the West and the Eastern space. For example, when we refer to fake news, we understand that the term refers to false or misleading information. In contrast, in Russian culture, there are terms such as *"lozh"* (Hamilton, 1986, p. 43), *"dezinformatsiya"* and *"maskirovka",* which refer to forms of falsehood and misleading, but each of these terms differs in meaning depending on the particularities as linguistic, cultural and contextual. Thus, in order to correctly understand the development of information activities by an initiating actor, it is necessary to analyse them in terms of their cultural particularities. In this light, the use of a concept as comprehensive as possible, which diminishes these cultural differences between the initiator and the target, becomes a necessity.

Information disorder includes tools and techniques such as misinformation, disinformation, malinformation, but due to the role of the concept in altering reality, we can include other techniques and tools such as propaganda, manipulation of information, spread of rumors, use of "alternative media".

Information disorder includes tools and techniques such as misinformation, disinformation, malinformation (Ib., p. 20), but due to the role of the concept in altering reality, we can include other techniques and tools such as propaganda (white, gray and black[1]), manipulation of information, spread of rumors, use of *"alternative media"*, mystification of reality, use of memes, spread of political-historical exceptionalism on target groups to radicalize them. It is important to note that information disorder generally works better in *echo chambers* (Wardle, Derakhshan, p. 50), which are the spaces through which individuals or groups targeted by information disorder can share and disseminate their own perspectives and opinions. The main vulnerability of these chambers is that the exchange of information is generally subjective and presents cognitive biases that can later be used by infiltrated external factors to direct the emergence of trends, to excite the target(s) on certain topics or to determine/stimulate acceptance, refusal or action towards an idea, a symbol or an event.

Information operations can be viewed in the context of the hybrid war/hybrid threats, which, in Europe, had significant implications on the cognitive dimension/perceptions, especially when elections, referendums, protests, etc. were organised. In general, it turned

[1] Other approaches define propaganda as a distinct activity within psychological operations, being an action covered and specific to joint military operations (Col. Frank L. Goldstein, Col. Daniel W. Jacobowitz, *"Psychological Operations. An Introduction",* in Psychological Operations: Principles and Case Studies; col. Frank L. Goldstein (ed.), col. Benjamin F. Findley (ed.), Air University. Press Maxwell Air Force Base, Alabama, 1996, p. 6).

out that the Russian Federation carried out, in European states, information operations that tried to determine the formation of trends in the societies of states or to influence them in various directions depending on the civilisational particularities of European nations and as a part of the conflict between the Russian Federation and the West (Darczewska, 2014, p. 12). They also sought, using information disorder, the constant dissemination in public and social media of conflicting messages and narratives that were intended to convince audiences of multiple versions of truths, eventually confusing them (Wardle, Derakhshan, p. 30).

Thus, regardless of the way we define information operations, their theoretical approach will adapt to the specifics of Russian military thinking and strategy, where the conceptual essence will have its origins in military thinking, but the applicability will extend beyond the military sphere to civilians.

The Russian Federation carried out, in European states, information operations that tried to determine the formation of trends in the societies of states or to influence them in various directions depending on the civilisational particularities of European nations and as a part of the conflict between the Russian Federation and the West.

In this sense, taking as an example of the Russian perspective the vision of Ivan Vorobev, Major General with a long military career and expert in military theory, relevant in a conflict are not only the dynamics of the attack and manoeuvring space, but also the means to stop the opponent's access to correct information. He defines the concept of information attack or information shock in three directions: the initiation of psychological offensive and misleading operations, the use of special measures for psychotronic attacks and the attack of computers in order to affect adverse command and control systems (Franke, 2015, p. 23). He added that, during the information war, coordination of counterintelligence, electronic warfare, physical destruction of C2 points and nodes through precise bombing and the use of deception must be coordinated. Other approaches describe information operations/information warfare (Ib., pp. 25-26)[2] beyond

[2] Like in the West, also in the case of the Russian Federation, the theoretical perspectives on information warfare and information operations are multiple and present a combination of approaches ranging from classical (specific to Soviet military thinking) or unconventional to those based on technical-military ones or trying to find a special relevance to a particular military specialty. Because of this, as Major General Charis Saifetdinov mentioned, certain concepts – especially those in the field of information warfare – can be understood and interpreted subjectively, due to the lack of solid expertise, well-defined principles and/or terminology that is not clearly understood. Although there may be explanations to argue that the theoretical basis of Russian information warfare/information operations is the experience of active measures, according to KGB defector Yuri Bezmenov, active measures are limited to the spectrum of actions specific to psychological warfare/psychological operations (PSYOPS), so they are a component of information warfare and, implicitly, of information operations.

the military sphere, as in the case of Colonel Anatoly Streltsov, who leads the information war in the political and governmental sphere. He considers that the main task of the government, in this context, is to counter the attempts of illegitimate actors to use information warfare in the area of political ideology, in the technical area and in terms of government policies. In the information war in the political sphere, he emphasises three main tasks: identifying and stopping harmful ideological propaganda, stimulating civil society to counter adverse propaganda, and stopping disinformation about state policy (Ib., pp. 28-29).

We note that the Russian perspective on information operations takes into account, to a significant extent, the experience of active measures – psychological operations -, which leads us to include in the discussion the relevance of the PSYOPS component.

Psychological operations are activities undertaken in order to influence, in a direction favourable to their own forces, the emotions, thoughts and behaviour of target groups or decision makers, being carried out in time of peace and war.

Psychological operations are activities undertaken in order to influence, in a direction favourable to their own forces, the emotions, thoughts and behaviour of target groups or decision-makers, being carried out in time of peace and war. It is important to mention that the activity of psychological operations is thought and carried out in reverse, more precisely the design of the action plan and its implementation depend on the cognitive and behavioural characteristics of the target – group or individual – and the quality of intelligence products (Robinson, p. 137). If, in the other components of information operations, the use of information disorder is minimal or optional, in the case of PSYOPS, we can say that it is maximum, being used all the tools and techniques that can contribute to the successful completion of operations. From the perspective of the process, psychological operations can be divided into three categories (Findley, 1996, p. 54): a). strategic psychological operations aim at achieving long-term objectives, in order to create a subsequent environment favourable to their own actions and objectives; b). operational psychological operations aim at obtaining medium-term benefits, at the level of military and non-military campaigns, regional or global; and c). tactical psychological operations aim to achieve short-term, immediate goals, having more of a supporting role than the development of independent and large-scale psychological operations.

Although psychological operations are a vast and complex topic, which has its own methodology and approach, in this paper, it is relevant to highlight some common features that psychological operations must take into account when planning and conducting (Ib., pp. 55-59):

❖ *Cultural differences* – when setting the target, the cultural specificity and the environment from which it comes must be analysed. The cultural environment to which the target belongs can determine perceptions and preconceptions, its perspectives on life and the world, behaviour and inclinations towards certain systems of values and ideas. It is essential that the granting of psychological operations is tailored to the cultural specificity of the target to produce effects.

When setting the target, the cultural specificity and the environment from which it comes must be analysed. The cultural environment to which the target belongs can determine perceptions and preconceptions, its perspectives on life and the world, behaviour and inclinations towards certain systems of values and ideas. It is essential that the granting of psychological operations be tailored to the cultural specificity of the target to produce effects.

❖ *Social influences* – depending on the social affiliation to a class or group, the target may have certain habits or preferences regarding the acceptance or rejection of an idea or perspective promoted by opinion formers. In this sense, the expertise on a target can be done in the opposite direction, starting from the environments it frequents and the opinion formers it pursues.

❖ *Motivations* – there is a close link between the needs, motives and behaviour of a target, all ranging from primary needs to the need for self-determination. Although the reasons are usually the result of satisfying or not satisfying basic needs, they can lead to the conceptualization of one's own existence based on feelings, perceptions, experiences, the environment, interactions and, finally, self-assessment. These can be very useful for PSYOPS analysis, because, through its motivations, the target acts in a certain direction, providing significant clues about who it is or what it wants to be and what it wants to achieve.

❖ *Perceptions and attitudes* – target's understanding of the individuals, the context and the environment is achieved through its own perspectives on life and the world, the set of values it assumes, experience and trends it adheres to, all of which determine the perception of the individual to be selective and subjective. Attitude is the predisposition of the individual to act in a certain direction, being conditioned by the cognitive, affective and behavioural dimension, directly affecting the perceptions of individuals. In this sense, psychological operations can act on: a) changing attitudes

and perceptions by using a constant flow of new information and narratives that are repetitive, follow a narrative logic and be carried out over long periods of time; and b) the change of emotions determined by an action, idea, fact or event through the use of information, through any channel, which would be contradictory to the initial reasoning – preconceived perceptions –, ultimately causing the triggering of emotional impulses.

It should be noted that significant help in the operation of psychological operations consists in intelligence, as it can provide useful information to help calibrate and refine operations and provide analysis of the compatibility between the effects of psychological operations and the desired result. In the case of psychological operations (but not limited to them), intelligence (Waltz, p. 219) can warn in advance when an enemy information action is underway, can provide a real perspective on a situation, perceive subtle indicators, can investigate, analyse and make recommendations where a vulnerability has been exploited, etc.

Significant help in the operation of psychological operations consists in intelligence, as it can provide useful information to help calibrate and refine operations and provide analysis of the compatibility between the effects of psychological operations and the desired result.

Even if, so far, we have highlighted briefly the role and significance of information operations, some subdivisions and related activities that engage in achieving an objective, it is worth noting the high degree of complexity and synchronization throughout the process. Starting from factors that are independent from the target such as culture, environment, social influences, it reaches the motives, feelings, perceptions and attitudes of a target. And after all the parts are in place, the psychological operations aim to use the analysed information to influence the target, in a specific way.

Given the above, the definition of information warfare and information operations highlights a much more comprehensive perspective on the current information environment, which is more than just a disinformation campaign and fake news or propaganda. Also, the inclusion of several Russian approaches to information warfare highlights the military origins in terms of conception and action, especially in the sense that, through psychological operations, the spectrum of active measures is revitalised on essential elements of societies. Especially when those operations try to influence the opinion formers or groups whose actions can cause destabilisation, chaos or can favor actions contrary to national interests of their states.

EXAMPLES

The cases presented are not isolated, and the examples in which the Russian Federation used the range of information warfare on key moments in the domestic policy of European states are not few. But unlike Western Europe, Russian information activity was somewhat more felt at the level of the former socialist bloc states, as a result of Marxist-Leninist legacies, cultural ties, common origins (in some cases) and historical interactions. Thus, we took as examples, to highlight the activity of Russian information operations, Poland, the Czech Republic and Slovakia.

Russian information operations on Poland aimed at fracturing the unity of Polish society through the use of information disorder, more precisely by intoxicating the information environment with memes aimed at deepening tensions between different factions, such as xenophobes, nationalists and pro-Europeans.

Poland

Although Poland can hardly be oriented to a perspective that is at least a little *"warmer"* toward the Russian Federation, it is still subject to the information warfare. Even if it does not present vulnerabilities that could generate any direct link with the Russian Federation, in reality, there is a range of opportunities that are exploited by the Russian Federation. In the case of Poland, the attempt to introduce a pro-Russian narrative into public opinion would be an action doomed to failure, which means that the approach here must be a complex one. Russian information operations on Poland aimed at fracturing the unity of Polish society through the use of information disorder, more precisely by intoxicating the information environment with memes aimed at deepening tensions between different factions, such as xenophobes, nationalists and pro-Europeans (Lucas, Pomerantsev, 2017, p. 23). Given that Russian information operations seek to support and exacerbate Polish nationalism, we note that in this regard, they use the cultural component of psychological operations to determine radical groups to promote ethnocentrism and anti-Western sentiment (along with the anti-Russian one). In some respects, obscure sites (falanga.org.pl, konserwatyzm.pl) have tried to praise the actions of extremist groups in Poland's past and compare their effectiveness, determined by the lack of political correctness and constraints, with current times. For example, the news portal kresy.pl had established a regular flow, which repeatedly commemorated the massacre of Poles in western Ukraine, carried out by the Ukrainian Insurrectionary Army (UPA) during World War II (Gajos, Rodkiewicz, 2016, p. 264).

Thus, the information disorder generates a beautification of Polish personalities with ethnocentric and radical inclinations, promoting them also at the societal level it tries to determine some anti-EU and anti-NATO trends, based on negative criticism, nostalgia for the communist regime, anti-Semitism, anti-Catholicism and anti-democratic ideologies (Ib., p. 24). The emotions and perceptions of Poles about their existence as a nation and their past are the most significant vulnerabilities, being susceptible to information flows that can radicalize them, especially in the context of the Polish political environment – which is beginning to be characterised by ultraconservatism – fuels ethnocentrism and anti- feeling.

Czech Republic and Slovakia

In the Czech Republic, the media is the main channel for conducting Russian information operations, and due to this fact, there are four trends: the traditional media; the new online media; online media and online journals.

At the information level, the case of the two states is a remarkable one, because they are deeply penetrated by the Russian information operations and can become a working point for the dissemination of the elements of the information warfare.

In these two states, Russian information operations seek to highlight, in general, the presence of anti-Western currents, and in particular, of anti-American currents, within the two societies, in an attempt to generalize them. Using information disorder here as well, the primary narrative is based on antagonizing the opponent (the West) and, depending on the context, it tries to create an image of the Russian Federation, if not favourable in the sense of an alternative for these two states, at least acceptable as a partner. While mainstream media usually acts as a correction element for information disorder within social media and the mass-media, in the case of the two states, an *"alternative"* media with strong pro-Russian influences has recently developed (Lucas, Pomerantsev, p. 25). Thus, in the Czech Republic, the media is the main channel for conducting Russian information operations, and due to this fact, there are four trends (Vit, 2016, pp. 279-280): 1) the traditional media, established after the transition period, which resists the pressures of Russian information influences and which is underfunded and gradually deprofessionalised; 2) the new online media, connected to the main news flow that was formed mainly in the period 2012-2014, being equally resistant to Russian informational influences; 3) online media, published after 2010,

which niches on political and social topics, disregarding the main news flow, and which includes in its articles also Russian *"alternative"* narratives; and 4) online journals, which claim to present uncensored perspectives on the world and base their articles on arguments focused on the right to opinion (subjectivisation of reality in accordance with the preconceptions of the target audience), including conspiracy theories. Another very interesting aspect is the action mode of the Russian information operations in the Czech space, because overt and covert operations are carried out, where the overt ones have the role of distraction. As an example, the *Aeronet* website (Lucas, Pomerantsev, p. 26), originally founded by aviation lovers in 2001, changed owners several times, until 2014, when it published its first pro-Russian article. This site may be included in the area of covert information operations, due to the difficulty of tracking the owners of this domain, the title of the site is not suggestive for the content it distributes, being difficult to intercept; and the authors are anonymous or use pseudonyms and the contents have questionable or fictitious sources. The sum of these covered sites, which disseminate pro-Russian narratives and elements of information disorder such as conspiracy theories, gray or black propaganda, fake news, etc., may exceed that of overt sites, which would aim to mislead and influence (Sputnik, Russia Today, TASS etc. can be framed in the sphere of open channels through which the main objective is to influence the perceptions of the target audience).

In contrast, in Slovakia, Russian information operations mainly exploited two vulnerabilities of the state: the Slovak state's dependence on oil/gas imports from the Russian Federation, which led to a deepening of relations (especially diplomatic) between the two states – in contrast to the Czech Republic, which diversified its sources – and the existence of socio-economic problems, which generated a tendency of the Slovak society to appreciate and have nostalgic feelings for the Marxist-Leninist past. This time, the Russian information activity on the Slovak public focused on the use of psychological operations, due to the fact that it tries to determine, at a cognitive level, perceptions and attitudes nostalgic and favorable to anti-capitalist or anti-Western trends. Also, along with the constant and repeated flow of messages that positively subjectivise the memory of Czechoslovak communism, the theme of pan-Slavism is introduced, in an attempt

to substantiate the perception of the Slovak public on a cultural, historical and ethnolinguistic link with the Russian Federation (Fischer, 2016, pp. 295, 301).

A major problem of the information warfare in the Czech Republic and Slovakia is that information operations have led to political subversion (Rosenau, 2007, pp. 6-7) by creating an information environment favourable to the infiltration of subversive factors in key institutions, and in the situation where they are exposed, in whole or in part, to benefit from the support or indifference of the public. For example, in the Czech Republic, Russian information operations have created an entire infrastructure which, according to the Czech Counterintelligence Service (BIS) (EURACTIV, 2016), consisted in the infiltration of agents of influence and the information monopolisation of the media and social media. The distortion of information also generated an *"alternative reality"* to Miloš Zeman, which significantly contributed to his election as President of the State for the second time. Milos Zeman (Santora, 2018), as a vector of influence, did not hesitate to manifest, over time, ethnocentric tendencies and affinity for the Russian Federation and China, to the detriment of Western partners and allies, developing pro-Russian and anti-Western rhetoric.

A major problem of the information warfare in the Czech Republic and Slovakia is that information operations have led to political subversion by creating an information environment favourable to the infiltration of subversive factors in key institutions, and in the situation where they are exposed, in whole or in part, to benefit from the support or indifference of the public.

From this point of view, we notice a link between information operations and subversion, because, along with Zeman, there are two other personalities who have external links or intentions contrary to the national interests of the Czech Republic (PBJ, 2020): Vratislav Mynář, who was Head of the Presidential Office since 2013, but without a security clearance from the Office of National Security (NBU), and businessman Martin Nejedlý, who has ties to Lukoil and the Russian political environment, and who holds a position in the Presidential Office, without being paid from public funds, but who often accompanies the President on foreign trips. In Slovakia, a form of political subversion is being tried, which can be exemplified by the work of former Prime Minister Jan Čarnogurský, president of the Slovak-Russian Association, based in Bratislava, who in 2015 tried to gather signatures for a referendum on whether Slovakia should remain in NATO. Instead, at the societal level, Russian information operations are trying to spread pan-Slavism both inside Slovakia and abroad, by promoting an information vehicle, such as the Slovak motorcycle club

"Night Wolves" (Gotev, 2018). The elements that characterise this motorcycle club[3] are the fact that some members actually contributed to the process of annexation of the Crimea in 2014, are promoters of Russian nationalism and supporters of Vladimir Putin, and in 2018 initiated the project *"Slavic World"*, which involved a tour to promote the project through most Eastern European states and probably to send a message of support or excitement to individuals and groups followers of pan-Slavism, ultranationalism or supporters of the actions of the Russian Federation. It is worth mentioning that,such in the case the example of *"Night Wolves"*, Russian information and subversive activities use any vehicle that can help them achieve their objectives/ mission and is not limited to the classic activities of intelligence services.

CONCLUSIONS

As we have seen, the dynamics of the security environment are changing and, if until recently, elements related to military threats were treated as such, the infusion of these elements in the civilian area may be due to hybrid warfare and the threats it generates. The information warfare can be perceived as a hybrid threat, because, as we have seen in the case of Poland, the Czech Republic and Slovakia, its targets consist of specific groups (with certain religious and ideological preferences, from certain social classes, with certain cultural particularities, etc.). and the ambiguity of the timing, form and practices used makes it difficult to prevent and stop.

It is interesting that the threat of information warfare molds to the particularities of states and hunts down its vulnerabilities. For example, in Poland, we have seen that it focuses on the scourge of radicalism from the Polish society.

In this sense, history and geopolitics can offer many opportunities for exploitation in the case of several states, being difficult to interpret

[3] The Motorcycle Club (MC) is both a formal and informal organization, composed of motorcycle enthusiasts, who develop their own lifestyle and customary rules. The ties between the members are strong, and within the organization, there is a well-established hierarchy, usually based on military ranks recognized and applied only within the organisation. Due to its libertine and sometimes anti-system character, some motorcycle clubs have been involved in activities specific to organised crime, such as human trafficking, drugs and weapons, blackmail and threats, money laundering, custom crimes, etc.

whether the information actions are determined by an aggressor state or only belong to groups that have their own interests. There is also the dilemma of protecting political and military decision-makers who, as part of society, are connected to the flow of information on social media and the mass-media, and their regular exposure to information degeneration leads to conditioning and, subsequently, to altering the correct perception of the reality in which they live.

Thus, defining and providing operational concepts to clarify the role and significance of information warfare and information operations, together with its components, become essential. Given the current context in which confrontations in the information environment no longer distinguish between peace and war, it becomes imperative for states to clarify their concepts and develop their own strategies and information weapons – as in the case of conventional weapons and doctrines –, by which to obtain advantages, to protect or to limit the opportunities of the opponent. Although the literature has been mentioning, since the 1990s, the increasingly significant role that information will play for citizens and decision-makers, today, there are still perspectives that classify information warfare and information operations as taking place only within the military universe and intelligence services. Here again, the superficial use of terms and techniques of information disorder determines the need to resort to new concepts and resize the way we perceive information activities, especially in the context in which approaches, concepts and techniques that once belonged to the military and intelligence began to extend to the civilian environment.

Given the current context in which confrontations in the information environment no longer distinguish between peace and war, it becomes imperative for states to clarify their concepts and develop their own strategies and information weapons – as in the case of conventional weapons and doctrines –, by which to obtain advantages, to protect or to limit the opportunities of the opponent.

Finally, we can say that what gives the information warfare the perspective to develop consists in its effectiveness due to the ambiguity and unpredictability with which it acts, regardless of the target. However, the most interesting fact is that information warfare is a concept based on military thinking that produces effects beyond the military sphere.

BIBLIOGRAPHY:

1. Čižik, T. (ed.). (2017). *Information Warfare – New Security Challenge for Europe*. Bratislava: Centre for European and North Atlantic Affairs (CENAA).

2. Darczewska, J. (2014). *"The Anatomy of Russian Information Warfare: the Crimean Operation, a Case Study"*. Warsaw: Centre for Eastern Studies.
3. Findley, B.F., *"Blending Military and Civilian PSYOP Paradigms"*. In *Psychological Operations: Principles and Case Studies*, Goldstein, L., Frank, col., (ed.), col. Findley, F. Benjamin (ed.). (1996). Alabama: Press Maxwell Air Force Base. Air University.
4. Franke, U. (2015). *"War by non-military means: Understanding Russian information warfare"*. Swedish Defence Research Agency (FOI).
5. Goldstein, L., Frank, col., (ed.), col. Findley, F. Benjamin (ed.). (1996). *Psychological Operations: Principles and Case Studies*. Alabama: Press Maxwell Air Force Base. Air University.
6. Gotev, G. (2018). *"Slovak President Sees Security Risk in 'Putin's Motorcycle Club' Activity"*. In *EURACTIV*, published on 01.08.2018, republished on 02.08.2018, https://www.euractiv.com/section/global-europe/news/slovak-president-sees-security-risk-in-putins-motorcycle-club-activity/, retrieved on 28 March 2021.
7. Hamilton, L.D. (1986). *Deception in Soviet Military Doctrine and Operations*. California: Naval Postgraduate School Monterey.
8. Herman, M. (1996). *Intelligence Power in Peace and War*. Royal Institute of International Affairs.
9. Lucas, E., Pomerantsev, P. (2017). *"Winning the Information War Redux. Techniques and Counterstrategies to Russian Propaganda in Central and Eastern Europe"*. Center for European Policy Analysis (CEPA).
10. Nemr, C., Gangware, W. (2019). *"Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age".* PARK ADVISORS.
11. Pynnöniemi, K. (ed.), Rácz, A. (ed.). (2016). *Fog of Falsehood. Russian Strategy of Deception and the Conflict in Ukraine*. The Finnish Institute of International Affairs.
12. Robinson, P. (2010). *Dicționar de securitate internațională*. Translation by Monica Neamț. Cluj-Napoca: CA Publishing.
13. Rosenau, W. (2007). *"Subversion and Insurgency".* RAND Corporation: National Defense Research Institute.
14. Santora, M. (2018). *"Czech Republic Re-elects Milos Zeman, Populist Leader and Foe of Migrants"*. In *The New York Times*, 27 January 2018, https://www.nytimes.com/2018/01/27/world/europe/czech-election-milos-zeman.html, retrieved on 21 February 2021.
15. Theohary, A.C. (2018). *"Information Warfare: Issues for Congress".* Congressional Research Service.
16. Waltz, E. (1998). *Information Warfare: Principles and Operations*. Boston, London: Artech House.

17. Wardle, C., Derakhshan, H. (2017). *"Information Disorder"*. Council of Europe.
18. AAP-6 (2018). *NATO Glossary of Terms and Definitions (English, French and Romanian)*. NATO Standardization Office (NSO).
19. Department of Defense (DoD) (2020). *Dictionary of Military and Associated Terms*. Joint Publication (JP).
20. *EURACTIV* (2016). *"Russian Secret Services Wage Information War, Says Prague"*, 2 September 2016, https://www.euractiv.com/section/global-europe/news/russian-secret-services-wage-information-war-says-prague/, retrieved on 28 March 2021.
21. *Prague Business Journal (PBJ)* (2020). *"Zeman's Dream Team: VratislavMynar and Martin Nejedly"*, 31 January 2020, https://praguebusinessjournal.com/zemans-dream-team-vratislav-mynar-and-martin-nejedly/, retrieved on 28 March 2021.