OPINIONS ON THE DEFINITIONS AND INTERPRETATIONS OF SOME CONCEPTS FROM RUSSIAN MILITARY THINKING AND THEORY

Teodor BADIU

"Mihai Viteazul" National Intelligence Academy, București

DOI: 10.55535/RMT.2022.2.01

There is an abundance of perspectives and interpretations about the practices and actions of the Russian Federation on states and individuals, especially at the information level. However, in some respects, Western perspectives tend to simplify Russian actions and categorise them as zero-sum games. In this respect, the paper tries to interpret the actions of the Russian Federation, especially at the informational level, by defining key concepts, as well as to provide a perspective on how Russian military theorists use the notion of "hostile actions" in the context of designing peacetime operations. Moreover, the complexity of the Russian military theoretical background is highlighted, with brief comparisons between the theoretical forms of some concepts from the Soviet period and the present. The paper also reviews some conceptions of the hybrid form of Russian action, attempts to synthesise certain views of Russian military theorists and, based on Russian strategic culture, to show the levels of action in the context of a series of operations. Finally, the paper proposes an orientation model that addresses a holistic perspective on how the subversive and informational actions of the Russian Federation can influence the policy and security of a state targeting the individual, society and the political system.

Keywords: indirect approach; information warfare; non-military and asymmetric means; active measures; maskirovka;

INTRODUCTION

From 2014 until now, the literature on hybrid/asymmetric threats and hybrid warfare has flourished, attempting in various ways to describe, explain and interpret the ways in which the Russian Federation operates openly and covertly in the international arena. However, in recent years, voices have begun to emerge that introduce the idea that the Western perspective tends to turn the subject of hybrid warfare/hybrid threats into a closer approach to Western strategic culture.

On the other hand, this observation should not be exaggerated in view of the fact that the scientific and analytical papers that approach this subject, publicly, are based on the collection of information from open, unclassified sources. In this regard, the large volume of information and the quality of public information (which may be incomplete, false or compromised) generates the risk of a dichotomy between the directions of research or analysis and the objective reality. Also here, another handicap is given by the impossibility to verify the certainty of the public research or analysis with information obtained from classified sources (HUMINT, SIGINT, IMINT etc.) due to the restrictions related to information protection. Moreover, obtaining an information product relevant to a particular topic (analysis or scientific paper) depends not only on information, but also on a number of personal characteristics such as experience, skills, abilities, knowledge about the topic (Chiru, 2019, p. 71).

Obtaining an information product relevant to a particular topic (analysis or scientific paper) depends not only on information, but also on a number of personal characteristics such as experience, skills, abilities, knowledge about the topic.

All these considered, the present paper expresses some views on the definitions and interpretations of Russian military theoretical concepts and perspectives with the intention of generating an overview. Thus, it will focus on the forms and methods of Russian action, with more emphasis on the specifics of the strategic culture of the Russian Federation and on the ways a conflict would unfold, from a Russian perspective, especially in the information environment. Therefore, we will be interested in observing how Russian theorists perceive the role of information in a conflict, what the targets of a Russian information operation could be, when it can be used and how information is integrated as a weapon in a series of operations (staged or synchronised). In the paper we will not only focus on the informational element, but we will also explain other concepts such as information warfare, indirect approach, asymmetric and non-military operations. At the same time, we will try to explain the modes of action of Russian military deception (*maskirovka*) along with active measures and reflexive control as part of a series of operations. Finally, we will highlight an orientation model about the Russian action that aims to affect the information environment (informational and cognitive dimension) in order to achieve a change of regime or change the social and political structure.

INDIRECT/NON-MILITARY OPERATIONS OR HYBRID WARFARE/HYBRID THREATS?

In the Russian military thinking we can identify three stages in which a state can be found: peace – general state, internally and externally; hostile actions – an ambiguous conflictual state; war – a social-political state.

Regarding Russian military art and thinking related to hybrid warfare, both military and civilian theorists prefer to avoid using the concept of *hybrid warfare* in favour of other terms such as *indirect approach/strategy*, *non-military measures/operations*, *asymmetric/ indirect actions*, *attrition warfare*. From their point of view, hybrid warfare is one of the options when it comes to possible military action. After analysing the particularities of the possible theatre of operations and the context of the conflict, the military action is designed in such a way as to allow, in a fluid way, the switching to various modes of action for the fulfilment of military and/or political goals (Kabernik, 2019, p. 59). In this regard, in the Russian military thinking we can identify three stages in which a state can be found (Ib., pp. 60-61): a) peace – general state, internally and externally, characterised by the absence of hostile actions; b) hostile actions – an ambiguous conflictual state, characterised by the intention to eliminate or suppress an opponent through violent measures or indirect or covert actions whose purpose is to change the social, political or cultural structure; c) war – a social-political state, defined as a combative form of hostile activities (originating in the thinking of Clausewitz and Lenin), internally and externally, where violence is openly and directly used through military operations.

The Western equivalent of *"hostile actions"* would be the spectrum of undercover actions that could be defined as *"... activities such as secretly providing aid to political supporters in other countries,* *misinformation, black propaganda and other types of psychological operations, provocations, sabotage, subversion, assassinations and the support of insurgents, coups and terrorism"* (Robinson, 2010, p. 14). However, traditionally – in Western military art and thinking – covert actions are carried out during a declared conflict[1], being cumulated with the direct actions of the armed forces. On the other hand, Russian military theorists add to the two classic states of peace and war, the mentioned state of *"hostile actions"* that does not fit into the logic of the classical war, but which is more than just competition between states, suggesting that states are always malicious (mainly during peacetime), one of the *realpolitik* type. Therefore, hostile actions seek to change the social, political and cultural structure in a certain direction. We can assume that this reasoning shows the Russian Federation's concern about the outbreak of *"coloured revolutions"* and the tendency of the exacerbated centralisation of power internally.

Hostile actions seek to change the social, political and cultural structure in a certain direction. This reasoning shows the Russian Federation's concern about the outbreak of "coloured revolutions" and the tendency of the exacerbated centralisation of power internally.

In Russian military thinking and theory, we can identify a number of opinions, concepts and theoretical approaches that are not always clear, and sometimes they act as a *"fog"* in identifying a pattern of Russian action. This is also stated by Major General (r.) Charis Saifetdinov, who considers that there are certain areas that research and subsequent decisions of the decision-maker (in the Russian Federation) should establish, more specifically a universalisation of terminology is needed (in the context of information warfare), objectives should be clearly defined, the principles of how to achieve the objectives should be substantiated, and finally, the necessary units and resources should be identified and allocated (Franke, 2015, p. 25). Even if some of these issues have been rectified, corrected and/or adjusted by the Russian Federation, it is still unlikely that there will be a complete standardisation of concepts and terms.

Continuing in the sphere of *"hostile actions"* we can notice that, in peacetime, the battle is carried out mainly in the information environment – except for the involvement of special forces

[1] Although there is a rather thin line between the covert action carried out by the security structures in peacetime and war, they need to be differentiated according to context and purpose. For example, in times of war, the common effort of all institutions is focused on gaining victory or just deter the opponent by all means, while in peacetime (in the context of international competition), covert actions are carried out, exclusively, by intelligence organisations and include espionage, the use of psychological or information operations, provocations, subversion, financing and supporting insurgent/separatist/guerrilla forces etc.

and subversive factors –, including offensive and defensive actions in the field of HUMINT, electronic operations, cyber operations, psychological operations, information operations, misleading of the decision-makers and so on.

In support of this idea, we can highlight some (compressed) ideas of military and civilian theorists such as:

- *Colonel (r.) Sergei Chekinov* and *Lieutenant-General (r.) Sergei Bogdanov*: they focus on actions in the information environment (information warfare), where non-military and indirect means dominate. The two argue the relevance of the indirect approach in the current context as a tool of the best strategies. They conceptualise the indirect approach as an action aimed at hitting the opponent in its weaknesses, using strategic surprise, quick manoeuvring and exploiting attack opportunities. They consider that while military deception is a common element used in conflict, information influence has reached a level that would allow them even to perform strategic tasks (Ib., pp. 38-39);

Colonel (r.) Sergei Chekinov and Lieutenant-General (r.) Sergei Bogdanov conceptualise the indirect approach as an action aimed at hitting the opponent in its weaknesses, using strategic surprise, quick manoeuvring and exploiting attack opportunities.

- *Major General Ivan Vorobev*: from his perspective, beyond the kinetic attacks and the room for strategic manoeuvre, own ability to deny the opponent's access to correct information also counts. Vorobev separates the concept of information attack or information shock in three directions: a) psychological-information attacks that seek to misinform and deceive the opponent; b) psychotropic attacks that have the function of affecting the opponent's psyche by special means[2]; c) attacks on the opponent's computers to affect C2 systems. With this separation in mind, the general emphasises the importance of carrying out these attacks in a synchronised and coordinated manner (Ib., pp. 23-24);
- *Colonel Yurii Starodubtsev and Lieutenant-Colonels Vladimir Bukharin and Sergei Semenov*: they, in the context of the information warfare, identify two directions of action: a) influencing the civilians or military personnel of another country by disseminating certain information (probably refers to information distortion) targeting groups or decision-makers;

[2] Although we do not yet have the conclusions of an inquiry on *"Havana Syndrome"*, the description of Major General Ivan Vorobev shows some similarities with this case.

b) gaining informational superiority over the adversary by decommissioning information processing and information gathering systems (probably referring to the electronic warfare part) (Ib., p. 40);

- *General Makhmut Akhmetovich Gareev*: he believes that the threats to the Russian Federation are related to information and subversive operations conducted from within the state. In this regard, the main effort of the Russian Federation should focus on destroying the information environment, sources of information and adverse navigation, guidance and C3 systems. To accomplish this goal, Russian forces can use indirect actions to influence the adversary, targeting the political, economic and psychological realms through disinformation. Here, too, the general includes indirect actions in the arsenal of non-military means, corroborating them with information distortion, stratagems, intelligence and counter-intelligence (Thomas, 2016, p. 15).
- *Colonel-General Andrei V. Kartapalov*: he adds to the classical armed forces (ground, air and naval) a fourth related to the information space. From the American theoretical perspective, the general pays close attention to the asymmetric operations performed by a weaker adversary who, facing the problem of limited resources, acts by economic, diplomatic, informational (including *"informational blows"*) and indirect (e.g., military nature) means. Also, from his perspective, the arsenal of combative approaches of the Russian Federation can include asymmetric measures that include the use of special forces, foreign agents, various forms of information weapons and other non-military forms. On the occasion of each conflict, an asymmetric operation will be generated (probably according to the specifics of the conflict) (Ib., pp. 19-20);

Colonel-General Andrei V. Kartapalov pays close attention to the asymmetric operations performed by a weaker adversary who, facing the problem of limited resources, acts by economic, diplomatic, informational and indirect means.

- *Major General (r.) I. N. Vorobyov and Colonel (r.) V. A. Kiselev*: the two consider that the strategy of the indirect approach is gaining ground against the strategies that use force, where the indirect approach is characterised by a diversity of forms and methods specific to military action – including information warfare, electronic strikes, anti-satellite operations etc.

They pay special attention to the psychological-information weapons, which are categorised as special weapons and which act on the human psyche in order to influence it (Ib., pp. 30-31);

- *Andrew Koribko*: He attempts to develop a complex and pretentious theory based on the assumption that hybrid warfare has a Western theoretical basis and defines it as an *"indirect adaptive approach"* designed to cause regime change. His thesis revolves around the practices of unconventional warfare and the *"making of coloured revolutions"*. Here, too, he explains how the success of a *"coloured revolution"* involves recruiting individuals using ideological, psychological and informational techniques, and how this process depends on the specifics of the country, the characteristics of leaders, and the power (capability) of government and its subordinate security institutions (Koribko, 2015, pp. 29-30). In his view, *"coloured revolutions"* are the result of information campaigns targeting the population of a state, and *"they must be persuasive in order to reach as wide of an audience as possible (in some cases, it may be more strategic to only reach a certain demographic in order to have them <rise up> and exacerbate existing ethnic fractures within society, for example)".* (Ib., p. 29).

Andrew Koribko explains how the success of a "coloured revolution" involves recruiting individuals using ideological, psychological and informational techniques, and how this process depends on the specifics of the country, the characteristics of leaders, and the power (capability) of government and its subordinate security institutions; "coloured revolutions" are the result of information campaigns targeting the population of a state, and "they must be persuasive in order to reach as wide of an audience as possible".

Perspectives and approaches may continue, especially as some military theorists give particular significance in this context to the SIGINT component or to cyber/information systems; others focus on the initial period of war[3], on the ability to forecast future trends or on the forms and means to be used in carrying out an operation; and others gives more value to high-tech weapons, the continuous training of troops or the possession of weapons of mass destruction (nuclear, chemical, biological or radiological). All of them are relevant and give clues about the real course of action of the Russian Federation, but we must mention that for a more accurate understanding, each theoretical approach would be worth being researched in itself.

[3] A Russian military theorist who has a significant influence on Russian military art and thinking, especially in deep battle theory, is Alexander A. Svechin (1878-1938) who considers that before the outbreak of hostilities the priorities are the understanding of the historical background, setting realistic goals and intensifying troops training. He also argues that each war is a special (or unique) case that requires the development of a specific strategic behaviour that is based on the particular logic of that conflict, avoiding the application of stereotypical models (Sinclair, 2020, pp. 13-14).

However, at certain points we can identify similarities with the Western conceptual approaches, especially in terms of the efficient use of information, both within our own systems and as a weapon against adversaries. In the case of conflict concepts, we are dealing with a theoretical set consisting of the reuse and updating of Soviet concepts and the results of Western research in the field of military theory (Kabernik, p. 54) and intelligence.

What is interesting is that certain key concepts are highlighted and attract our attention, more precisely *indirect strategy/approach*, *information warfare/attack/shock*, *non-military means*, *asymmetric operations/measures*, thus deserving particularisation.

In the case of the *indirect strategy/approach,* we can say that it is an adaptation of the theory of the strategy of indirect approach of B. H. Liddell Hart (1895-1970). Hart's theory addresses the need for a change in the way of conducting conflicts. Instead of direct fighting between opposing forces, he advocates for a *"strategy of indirect approach which seeks to dislocate the enemy's balance in order to produce a decision"* and to lure or capture him in a moment where *"his own [adversary's] effort is turned into the lever of his overthrow"* (Hart, 1929, 2008, pp. 19, 123). Hart's strategy of indirect approach encourages the exploitation of minimum resistance lines and the limitation of the use of armed forces, where the key element is the high degree of mobility which is doubled by the ability to respond quickly (Ib., p. 138). Also, at the tactical or strategic level, the strategy of the indirect approach seeks to have *"... a plan that can be easily varied to fit the circumstances met; to keep such adaptability, while still keeping the initiative ..."* (Ib., p. 133). Hart considers that in a confrontation *"... the dislocation of the enemy's psychological and physical balance was the vital prelude to a successful attempt at his overthrow"* (Ib., p. 15). In this regard, the strategy should be designed in such a way as to diminish the opponent's resilience by exploiting the (strategic) surprise and manoeuvrability and, in the event of a conflict with several opponents, it would be advantageous to focus efforts on to the weak allies of the adversary rather than to attempt a singular, constant, and weary effort to bring down the strongest adversary in the hope that the others around him will give up the fight (Ib., pp. 128, 123).

Hart's theory addresses the need for a change in the way of conducting conflicts. Instead of direct fighting between opposing forces, he advocates for a "strategy of indirect approach which seeks to dislocate the enemy's balance in order to produce a decision" and to lure or capture him in a moment where "his own [adversary's] effort is turned into the lever of his overthrow".

Even if Hart was Western, we cannot say that the presence of some of his ideas in Russian military theory is a coincidence, especially since, as one author wrote in 1986, Soviet military art was based on the principles of: a) speed and shock (the use of mobility and manoeuvre space), b) concerted effort (the use of superiority in the right place and time), c) surprise and securing, d) maintaining initiative, e) maintaining efficiency in combat, f) compliance with the purpose/objective, g) coordination between forces (Hamilton, 1986, p. 63).

Although, the presented aspects represent only a part of Liddell Hart's perspective, we can notice the similarities between the theory of strategy of indirect approach and the indirect strategy/approach that the Russian military theorists talk about. For example, in the context of the exploitation of the minimum resistance points, the strategic surprise, the dislocation of the opponent's balance and the maximisation of manoeuvrability, the episode of the invasion of Crimea in 2014 highlights these similarities. Taking advantage of the strategic surprise, the Russian forces acted with great speed and flexibility, first by transporting special small units to the peninsula, in the context in which they were part of an exercise carried out on the eastern border of Ukraine, which inspected their ability of quick response. Once in the enemy territory, some units even pretended to be part of the local militia by misleading the local population and occupying the Crimean Parliament (Kofman et. al, 2017, pp. 12-13). This surprise, in practice, had both physical and psychological effects, giving the Russian Federation a tactical, operational and strategic advantage, while Ukraine's response was gradually cancelled. Another example related to the economy of the use of armed forces is the Russian military intervention in Syria in 2015. In this case, the Russian Federation operated (Sinclair, 2020, pp. 15-17): politically, by influencing the Syrian government to refuse access by Western-funded NGOs to territory under the control of government forces; diplomatically, by blocking a UN resolution which could favour the United States of America and expanding partnerships with countries in the region such as Turkey, Saudi Arabia, Iraq and Israel; and militarily, by providing air support, security, weapons supply, specialised training and logistics. In this respect, the troops in the field were limited and composed of naval, air, special forces and independent contractors, also the direct ground clashes were avoided as much as possible, and to compensate for the economisation of use of own forces, the Russians focused on a common, robust, command and control ground system (Ib.).

In the episode of the invasion of Crimea, taking advantage of the strategic surprise, the Russian forces acted with great speed and flexibility, first by transporting special small units to the peninsula, in the context in which they were part of an exercise carried out on the eastern border of Ukraine, which inspected their ability of quick response. Once in the enemy territory, some units even pretended to be part of the local militia by misleading the local population and occupying the Crimean Parliament.

Given these examples (not to mention the examples we can draw from recent Russian military exercises), we note that Russian indirect strategy/approach is a conceptual hybrid that integrates Russian/Soviet strategic culture and Western military theory, and that Russian military theorists will continue to develop and improve according to the new technological developments.

Regarding the *information warfare/attack/shock,* we note that, although there are different terminologies in Russian and Western conceptual approaches, the intention will be similar: in the information dimension, the purpose is to destroy, corrupt, usurp the adversary's information and/or the information environment; and in the cognitive dimension it is aimed at affecting human networks and systems that can influence decision-makers, manipulating the content and structure of information and influencing systems that can affect the decision process (FM 3-13, 2016, pp. 1-4). In short, it is about gaining informational superiority over the adversary while own systems are protected.

Russian indirect strategy/approach is a conceptual hybrid that integrates Russian/Soviet strategic culture and Western military theory; Russian military theorists will continue to develop and improve it according to the new technological developments.

From this point on, the similarities between Western and Russian thought patterns dissipate because of differences in terminology, structure and role. In Western military thinking (NATO dictionaries, strategy papers, manuals etc.) we find the use of the term *information operations* to describe the capabilities and development of activities that affect the information environment, and the term *information warfare* is used when referring to adverse tactics, activities and capabilities (Giles, Seaboyer, 2019, pp. 6-7). In contrast, Russian military thinking attributes to the concept of information warfare a much wider and more dynamic applicability, using information as a tool, field of operations, or being the target/object to be affected. According to the Russian theoretical approach, information warfare is an umbrella concept under which are subsumed cyber operations, psychological operations, strategic communication, influence operations, electronic warfare, information distortion (disinformation and misinformation, information falsification, propaganda etc.), domains of intelligence (HUMINT, SIGINT, IMINT, GEOINT, OSINT etc.), counter-intelligence, maskirovka (the western equivalent being military deception – MILDEC) and alteration/destruction of equipment (Ib., p. 6). In addition, the organisation and conduct of information warfare is the responsibility of the Russian intelligence community (GRU, FSB, SVR etc.)

and the security forces (specialised structures on security and internal order), and the activities of analysis, gathering and dissemination of information are combined with direct actions such as subversion, sabotage and assassination; all this activity aiming civilians, military and decision-makers (Ib., p. 7). In order to identify and exploit the vulnerabilities of the state's media, the Russian Federation has formed *"intelligence troops"* that are composed, along with intelligence and military officers, of hackers, specialists in strategic communication and psychological operations, journalists and linguists (Giles, 2016, pp. 35-36). One of their important roles is to understand the linguistic and cultural peculiarities of the states targeted by the information warfare. Here, too, it must be said that depending on the objectives and targets, the Russian information warfare is divided into (Ib., p. 9): a) psychological-information warfare, whose target is the armed forces and opposing populations; b) technological-informational warfare, the target of which is the technical systems for collecting, processing and transmitting data and information. It should be noted that both typologies include the use of cyber activities because, in their view, cyber warfare refers to the transmission and transfer of information by any means and in this regard the Russians attribute similar meanings to the action of parasitising/infecting a computer and the action of distorting reality through classical media or social media (Ib., p. 10).

As we can see, the character of the Russian information warfare is an offensive one, but it is also doubled by a defensive one in terms of the domestic information environment. Basically, the theoretical (and practical) approach of Russia is a defensive-offensive one, and domestically it keeps a strict control of the information flows coming from outside the Russian Federation. The Russian Federation has the capacity to disconnect itself from the external information environment and can influence the pieces of information leaking from the outside so that the Russian population should not have an objective perception of events, both domestically and externally, and thus be vulnerable to the propaganda of its own state (Ib., pp. 29-30).

The theoretical (and practical) approach of Russia is a defensive-offensive one, and domestically it keeps a strict control of the information flows coming from outside the Russian Federation. The Russian Federation has the capacity to disconnect itself from the external information environment and can influence the pieces of information leaking from the outside so that the Russian population should not have an objective perception of events, both domestically and externally, and thus be vulnerable to the propaganda of its own state.

This defensive-offensive approach can be interpreted as an information security system, where the emotions and attention of Russian citizens are channelled to external opponents designated by the Russian Federation in an attempt to prevent riots against the abuses of the authorities, the morale of troops is kept high, and C4I systems remain protected. At the same time, externally, the perceptions, attitudes and emotions of the populations of other states are exploited through the information warfare in an attempt to generate destabilisation or to change governments or regimes; decision-makers are influenced; key personalities from the targeted states are determined to defect through blackmail, threats or bribery; and the aim is to penetrate, corrupt or decommission the military and governmental systems.

We can approach *non-military means* and *asymmetric operations/ measures* together because, although they are discussed as separate terms by Russian military theorists, in practice, we notice that these are concepts that complement each other.

In this regard, Russian military theorists start from the theory of the sixth- generation warfare[4] where the main objectives are: 1) defeat of the adversary's armed forces on its own territory, 2) destruction of the opponent's economic activity and potential, 3) change or subversion of the opponent's political system (Mattsson, 2015, p. 62). In order to achieve these objectives, an indirect, remote, approach is evident, which will materialise through non-military and asymmetric measures. In support of this idea, they believe that the first step is to take the initiative in launching a psychological warfare, information warfare and recruiting or introducing agents of influence (non-military component) destabilising the victim state from within and create optimal conditions. Subsequently, asymmetric operations are carried out by launching a coordinated attack using special forces, ranged weapons, volunteers and militias to penetrate deep into the enemy territory (Ib., pp. 62-63). However, there are situations in which the use of any armed forces, in any form, can cause greater risks than benefits, so that non-military means are accentuated as part of asymmetric operations, being expressed by:

Russian military theorists start from the theory of the sixth-generation warfare where the main objectives are: defeat of the adversary's armed forces on its own territory, destruction of the opponent's economic activity and potential, change or subversion of the opponent's political system.

- discrediting and delegitimising key institutions and decision-makers through constant information flows highlighting the limitations and inability of authorities to manage issues and governance;

[4] Sixth-generation warfare is a theoretical approach of Russian origin about the phenomenon and trends of war and it refers to the increasingly informational nature of conflicts, the increasingly significant role of high-precision weapon systems, compaction of troops and maximising their mobility etc., but also includes abstract issues such *as "contactless warfare", "cultural warfare"* or *"existential warfare".* For a perspective, see: https://jamestown.org/program/russian-sixth-generation-warfare-and-recent-developments/.

- actions to induce chaos among the population that will cause the sensation of rapid degradation of order and stability and the cause of an anti-system trend among the population;
- deception/misleading actions aimed at distracting the opponent or determining it to act or not to act at a certain moment;
- monitoring and evaluation actions that remotely track the opponent's capabilities, mode and time of reaction and reveal its possible vulnerabilities (Duțu, 2013, p. 36).

In this regard, this perspective of emphasising non-military means carried out under the umbrella of asymmetric actions seeks to achieve strategic objectives by substituting the classic use of armed forces, and thus the opponent – not subject to a military threat – cannot provide a symmetrical response (Renz et al., 2016, p. 54). It must be said that we are facing a paradox in the context of non-military means and Russian asymmetric operations/measures because no matter how much they tend to exclude the military component, all these actions are organised and carried out under the auspices of Russian military structures. The arsenal of *"remote-controlled weapons"* may be composed of organisations, groups or individuals receiving funding and instructions from the Russian Federation, acting against the security interests of the state in which they operate (Ib., pp. 56, 57).

The perspective of emphasising non-military means carried out under the umbrella of asymmetric actions seeks to achieve strategic objectives by substituting the classic use of armed forces, and thus the opponent – not subject to a military threat – cannot provide a symmetrical response.

In the Russian military theory of sixth-generation warfare, we note that significant attention is being paid to the use of non-military means. According to the Russian military approach, the role of non-military means would be to weaken and corrupt the adversary before the attack, as part of the initial period of the conflict/war, deploying them in a covered manner and aiming to undermine or diminish the ability of the state to resist (Göransson, 2021, pp. 86, 88). However, this idea lies in the main security obsessions of the Russian Federation, namely the regime changes through *"coloured revolutions"*. In this regard, the Russian authorities have repeatedly accused the United States of America and NATO of carrying out subversive activities in support of *"coloured revolutions"* in the Middle East and Eastern Europe. The Russians classified Western actions as *"multidimensional hybrid operations"*, consisting of political, diplomatic, information, propaganda, financial, economic and military measures acting through political parties, NGOs, migration and private military companies (although their role as part of non-military measures is not explained) (Ib., p. 89). We must keep in mind that, empirically, what the Russian Federation classified as risks to its security were indications of the actions it had taken against other states, overtly or covertly. There is also ambiguity and conceptual confusion, intentional or unintentional, about non-military means and asymmetric operations/measures that, to some extent, mislead scholars and analysts, generating different interpretations and perspectives without being able to clarify the true forms and methods of Russian actions. We find such an example in the interpretation given by various Western specialists (Mark Galeotti, Roger McDermott, Pavel Felgenhauer etc.) regarding the existence of a *"Gerasimov Doctrine"* or the underestimation of the Russian Federation's intentions to be able to project its power in the international arena. In fact, the intentions of General Valery Gerasimov do not seek to deepen the non-military, asymmetric, informational etc. means by the army to the detriment of other branches/specialties, but points out that *"... Russia needs to create doctrinal and material capability of a highly professional intervention force with the potential to act worldwide, under the protection of a highly effective, modernised nuclear umbrella"* (Fridman, 2019, p. 109) to protect its external interests.

The intentions of General Valery Gerasimov do not seek to deepen the non-military, asymmetric, informational etc. means by the army to the detriment of other branches/ specialties, but points out that "... Russia needs to create doctrinal and material capability of a highly professional intervention force with the potential to act worldwide, under the protection of a highly effective, modernised nuclear umbrella" to protect its external interests.

Following this synthesis, we notice an expanding conceptual diversity which, in some cases, represents adaptations of Western military concepts, and in other ones, consists in taking over and improving Soviet concepts. It appears that the tendency of the Russian armed forces is to emphasise interoperability, mobility, technologization, flexibility and the economic use of force, in direct proportion to the characteristics of the theatre of operations. Also, to the classical Russian military forces are added the informational and non-military components that can be carried out jointly with military operations or as independent actions (using military techniques with civilian means), with the aim of destabilising a state from inside.

However, caution and carefulness are required in the interpretation of Russian military theory and thinking, because: a) the available strategic documents are abstract and the access to classified documents belongs to a small portion of specialists; b) differences in language and strategic culture are a barrier to understanding their mode of action; c) some Russian approaches may be tainted by biases and conspiracy theories resulting from reminiscences of Marxist-Leninist ideological heritage and errors developed by the small circles of Soviet communists from the security structures (Andrew & Mitrokhin, 1999, 2000, 2018).

ACTIVE MEASURES, MASKIROVKA AND REFLEXIVE CONTROL

When we introduce the *indirect approach, information warfare, non-military means or asymmetric operations*, we must keep in mind that *active measures*, *maskirovka* and/or *reflexive control* are carried out within the lines of operations or in an auxiliary manner. The inclusion of these terms in the spectrum of Russian military actions, overt or covert, is mandatory due to their role, tradition and evolution in the Soviet/Russian strategic culture.

According to a special report declassified by the CIA in 2006, the active measures refer to Soviet operations aimed at affecting the domestic policy of the targeted states, being distinct from espionage actions, and aimed at affecting relations between states, discrediting opponents of the Soviet Union and undermining external leaders, institutions, and values.

Starting with the *active measures*, from a historical point of view, they were designed by Service A, which was the active measures specialised branch of the KGB Foreign Intelligence Directorate, and the execution was assigned to PR Line (KGB's political intelligence department) officers, who worked from legal (part of diplomatic missions) and illegal residences located in the territories of the states, which were supposed to give the active measures, in theory, 25% of the total activities undertaken (Ib., p. 292). According to a special report declassified by the CIA in 2006, the active measures refer to Soviet operations aimed at affecting the domestic policy of the targeted states, being distinct from espionage actions, and aimed at affecting relations between states, discrediting opponents of the Soviet Union and undermining external leaders, institutions, and values (Bureau of Public Affairs, 1981, p. 1). The active measures were carried out in a subversive/covert manner and used techniques such as:

- Manipulation of written news agencies in the targeted countries by the insertion, by Soviet agencies, of false information;
- Use of falsehoods and disinformation through production and dissemination of false or partially true documents (black and gray propaganda) and by spreading rumours, insinuations and distortions of facts/events;
- Control of local and international communist organisations;
- Dissemination of information through clandestine stations;
- Using economic manipulation by influencing prices (where possible) and disseminating real and false information to local

businessmen and policymakers in an attempt to direct their investment plans to the interests of the Soviet Union;

- Conducting political influence operations by exploiting contacts in the political, economic and media environments of targeted states. A particular attention was paid to politicians, where that type of operation was trying to build their loyalty toward the USSR, and then use them as private channels with foreign government officials. Once influenced, the Soviet Union falsely gave them the impression of special relevance by inviting them to meet with high-ranking Soviet officials. In reality, through loyal local politicians, the Soviet Union was transmitting mixtures of false, real, and distorted information that favoured the Soviet agenda;
- The use of academics and journalists, so that the recruited academics submitted to Soviet orders, and the recruited journalists indirectly represented the Soviet Union and disseminated communist propaganda (Ib., pp. 2-3).

In this light, *active measures* were a type of actions that we would currently include in the field of psychological operations, information operations and HUMINT. However, within the Soviet/Russian military theory, *active measures* – also called *active operations* – take many forms. In general, they aim to use influence on the domestic and foreign policy issues of the targeted state; implementation of solutions in international issues; misleading, undermining and weakening the opponent; disruption of the opponent’s hostile activity; and fulfilling other purposes (Mitrokhin, 2002, 2004, p. 13). When carried out by external intelligence services, in particular, *active measures* extend their scope to the military, economic and ideological aspects of the adversary. The methods used include misinformation, exposure, discrediting, compromising, persuasion, or coercion – exerting psychological pressure on individuals to persuade or persuade them to behave in a certain way – special positive action/pressure — exercising influence over governments, parties or political and public figures using various forms and materials through agents and contacts recruited/cultivated –, clandestine actions etc. (Ib., pp. 13, 67-68). Also, *active measures* play a role in the context of counter-intelligence actions, being different from protection measures, where the goal is to penetrate the logic of the opponent, prevent opportunities

The active measures were carried out in a subversive/covert manner and used techniques such as: manipulation of written news agencies in the targeted countries by the insertion, by Soviet agencies, of false information; control of local and international communist organisations; dissemination of information through clandestine stations.

for the opponent, increase ambiguity, expose and interrupt hostile activities from the earliest stages, to block the opponent's possibilities of initiative, to frustrate him and to make him act in unfavourable conditions (Ib., p. 251).

From the experience of recent years, we see that there are few differences between past and present *active measures*. The notable differences consist in the experience the Russians have capitalised on, which has led to the professionalisation of *active measures*, a wider use of technology and the use of the permissive information environment of Western states generated by the inadequacy of their own protection systems to current *active measures*. In this regard, summarising the technological element, we will refer to some aspects.

The generalisation of the virtual space and the widespread use of digital platforms that generate content, distribute information and are forums for discussion, all led to the emergence of an alternative/parallel information environment to the classic one. In addition to the obvious advantages of computer and information interconnection, there have been acute disadvantages, such as: dissemination, between users, of content and information based on emotions; digital enclaving of users based on common representations and beliefs; promoting ignorance towards scientific domain; accentuation of the story to the detriment of real events; glorification of utopian life patterns, dramatization and alteration of objective reality etc. (Wardle & Derakhshan, 2017, pp. 12, 13, 15). These trends are a favourable environment for *active measures* (including for the recruitment/cultivation of agents), with the virtual space representing both the channel and the meeting place. Due to this subjectivisation, people prefer to form virtual groups, called *echo chambers,* through which they can express their common beliefs and ideas, without the phenomenon of debate and where they can express their unfettered, radical and uncensored views about life and the world. (Ib., pp. 49-50).

In addition to the obvious advantages of computer and information interconnection, there have been acute disadvantages, such as: dissemination, between users, of content and information based on emotions; digital enclaving of users based on common representations and beliefs; promoting ignorance towards scientific domain; accentuation of the story to the detriment of real events; glorification of utopian life patterns, dramatization and alteration of objective reality.

With the subjectivisation of the individual's perception of reality, the role of psychological component has increased as part of *active measures*, and has led to an efficiency in identifying and valuing individuals. Although we cannot indicate exactly the stages used by the Russians, we can state that before launching *active measures*, the organising institutions carry out extensive research on the targeted state, which establishes the civilisational particularities determined by geography, historical evolution, composition and ethnic origins, religion, economic status and the structure of society (Gordon, 1996, p. 205). However, it should be noted that, at a deductive level, pre-analysis is not carried out before the action plan, objectives and targets that will underpin the conduct of active operations *(active measures)* have been established. Then, information is collected, which is analysed, taking into account the latent attitudes of certain groups or the population on issues related to the political, economic, military and social fields, and then another analysis is performed that tries to identify possible vulnerabilities, having a specific target in sight as the analysis determines the level of dissent, fear and dissatisfaction that will be exploited (Ib.). Depending on the information obtained, a decision is made regarding the methods and techniques to be used, the favourable means of communication, the contents and messages disseminated, the spaces where the *active measures* take place (virtual and/or real), the staff involved (own, clandestine and/or recruited from the targeted state) etc., all the activity to be monitored, evaluated and adjusted (Ib., p. 206). Even with an impressive amount of knowledge about the adversary, the success of active operations is not guaranteed due to the protectionist activities of the security structures in the target state and the linguistic and cultural peculiarities of its population.

Even with an impressive amount of knowledge about the adversary, the success of active operations is not guaranteed due to the protectionist activities of the security structures in the target state and the linguistic and cultural peculiarities of its population.

Active measures continue to be an instrument of influence of the Russian Federation, which is constantly being improved and which produces effects, generally, in the medium and long term. Although we have only presented theoretical aspects, we cannot attribute to chance some concordances between this theoretical framework and certain events (outbreak of protests, contradictions of statements/decisions of government officials within the same state, exacerbation of false information flows at sensitive moments etc.). Thus, we can see that the intensity of their manifestation is no different from the Cold War period, which obliges us to make greater efforts to defend ourselves.

Maskirovka is a concept with a long evolution in Russian military thinking and theory that has an extended applicability and adaptability. As Barton Whaley (1969, 2007) points out, the Orientals were the ones who discovered the potential of manipulating information during a war through information blockades, misleading operations, overloading communications with confusing information, until the adversary went mad. Over time, techniques and forms of military deception have been taken over mainly from Sun Tzu (and not only) and adapted to Western wars (by Antoine Henri Jomini, Carl von Clausewitz, B. H. Liddell Hart).

Maskirovka is a concept with a long evolution in Russian military thinking and theory that has an extended applicability and adaptability. As Barton Whaley points out, the Orientals were the ones who discovered the potential of manipulating information during a war through information blockades, misleading operations, overloading communications with confusing information, until the adversary went mad.

Turning to the Russian military deception, this is not very different from the Western one, but it has a wide applicability. For example, in intelligence work, *maskirovka* refers to the use of natural conditions, the creation of artificial situations and the use of devices to conceal and camouflage the activity of one's own agents and intelligence officers (Mitrokhin, p. 64). *Maskirovka* is also used in counterintelligence, where it is a set of special measures designed to hide or mislead the opponent as to the true nature of the measures taken by the security structures along with the forces involved and the resources used (Ib., p. 247). In this respect, we note a slight resemblance to what OPSEC (Operations Security) measures would represent.

In the military sphere, *maskirovka* is an umbrella concept that is composed of three other concepts such as *camouflage, concealment* and *military deception* (which includes the use of truth, falsehood, deception and misleading), and its applicability extends to strategic, operational and tactical levels (Hamilton, p. 65). At the strategic level, *maskirovka* ensures the disorientation of the opponent by hiding the preparations for conducting operations, the strategy that is used, intentions and weapons involved; at the operational level the goals of *maskirovka* are diminished in size and focus on simulations, disinformation, feints and coverage of the preparations for the operations to be carried out; and at the tactical level *maskirovka* focuses on coverage and demonstrations (creation of false fighting positions, camouflage of troops and equipment etc.) (Maier, 2016, pp. 16-17).

We can also add that there are perspectives that consider that a more consistent applicability of *maskirovka* is encountered at the operational level because, usually, the tasks consist in: masking the movements of troops or when they are withdrawn after they have been spotted by the opponent; altering the opponent's perception and/or deny it the possibility of being able to identify one's own weaponry; distracting the opponent; overloading the opponent's intelligence structures with data and information; diverting the opponent's attention from real threats and simulating the use/lack of force to cover one's own vulnerabilities or to give the opponent a false impression of security; conditioning the opponent with a certain routine/behaviour that would cause him misconceptions; and misleading the adversary into not understanding its ongoing actions and not being able to respond promptly to an incident/event (Dick, 2013, p. 190).

Maskirovka, like any military operation, is based on a planning that generally takes into account: initiative, plausibility, consistency, and synchronisation and diversity.

Maskirovka, like any military operation, is based on a planning that generally takes into account:

- Initiative – the preference to penetrate and influence the decision-making process of the target in an attempt to generate confusion, indecision and mistakes;
- Plausibility – plans must be plausible, as a construction, from the perspective of the target;
- Consistency and synchronisation;
- Diversity – in order to prevent standardisation or stereotyping in planning, it is recommended to carry out multiple, credible and related military deception measures so that each can confirm the other and cumulatively contribute to the story of deception (Hamilton, pp. 66-67).

Moreover, within the same plan, according to the Soviet/Russian perspective, it is important to use the optimal category of *maskirovka*, which consists of: camouflage measures, which are classic measures to hide the equipment by using colours, natural vegetation, terrain etc.; imitation, which starts from the use of baits (in misleading) to the use of the electromagnetic spectrum to imitate the radio signals of the opponent; demonstrations of forces, which have a dual-role given by the intention of increasing or diminishing ambiguity about one's capabilities and intentions of simulating the intention to attack the opponent in order to monitor his reaction or make him take an unwise decision; and disinformation, which aims to provide the adversary, through various channels and forms, with erroneous, partially real, false information flows (Ib., pp. 68-69).

Based on the theoretical framework of *maskirovka*, the initiator tries to present a representation of reality, false and credible enough, to attract the attention of the target in dead spots, but also to generate favourable conditions for their own intentions. *Maskirovka* uses mainly strategic surprise and influence – which ensures the preservation of the fighting force, reduces risks and acts as a force multiplier – is a strongly centralised and coordinated process, and the limitations do not exist, regardless if the target is a military, governmental or civilian one, the process is constrained only by the cost-benefit relationship and the related risks (Maier, pp. 6-7). In Russian military thinking, *maskirovka* is the best way to achieve strategic surprise, generating openings in the defence of the opponent that would traditionally have been obtained at much too high costs; *maskirovka* is the best way to alter the perception of the reality of adverse decision-makers so as to entice them to make inappropriate or wrong decisions; and in the tactical field, *maskirovka* is used to protect one's own forces by masking forces and disseminating false or misleading information to direct the effects of opposing weapons in directions irrelevant to the combat action (Ib., pp. 8-9).

In Russian military thinking, maskirovka is the best way to achieve strategic surprise, generating openings in the defence of the opponent that would traditionally have been obtained at much too high costs; maskirovka is the best way to alter the perception of the reality of adverse decision-makers so as to entice them to make inappropriate or wrong decisions.

As we can see, this term is used more in military matters, as opposed to active measures. However, given its purpose of altering reality and the fact that Russian intelligence operations are designed and executed by a mix of civilian-military personnel, we can assume that *maskirovka* is also used outside the theatre of operations. Its use, as a form of information warfare in the virtual space against civilian targets and decision-makers, reminds us of the ideas expressed by Russian military theorists regarding the use of the indirect approach or the prospect of regime change by non-military/asymmetric means.

Reflexive control (this name is found more often in Western literature) or perception management is a complementary concept of *maskirovka*, developed since the ’60s, and, in general, *maskirovka* and *reflexive control* are carried out together. Unlike the components discussed, *reflexive control* focuses on the intellectual confrontation of opponents, where officers examine the given situation objectively and, based on experience and training, they look for ways to manipulate the tactical field in their favour by analysing the opponent’s patterns and tendencies corroborating the information obtained with their own possible action forecasts (Thomas, 2019, pp. 41-42). According to Russian military thought, *reflexive control/perception management* is carried out in the information environment and aims to obtain informational and psychological effects against decision-makers in an attempt to persuade them, through various channels, to abandon the initial plans and act to the detriment of their own interests or objectives (Ib., pp. 4-2). Basically, *reflexive control* seeks to generate the optimal conditions for Russian actions, using *maskirovka* and *active measures*, so that the aim is not to outperform the opponent’s military, but to project/simulate a certain image or state of affairs that would distort the objective reality and affect the opponent’s ability to predict, anticipate and act by disordering the decision- maker.

Reflexive control focuses on the intellectual confrontation of opponents, where officers examine the given situation objectively and, based on experience and training, they look for ways to manipulate the tactical field in their favour by analysing the opponent’s patterns and tendencies corroborating the information obtained with their own possible action forecasts.

However, due to social, political and technological developments, in the Russian conception, *reflexive control* can extend beyond military art, to actions such as misleading or deceiving foreign experts, corruption of computer networks and manipulation of social media and/or public opinion of a state, having applicability in:

- Negotiations – the use of a mix of marketing techniques and reflexive control;
- Deception and military doctrine – the publication of official programmatic and doctrinal documents that project a certain image regarding the intentions and directions of action of the Russian Federation;
- Deterrence – in the context of nuclear arsenals, the parties are trying to convince themselves of the futility of blackmail with the use of force and military pressure;

- Military exercises – the organisation of military actions that convey messages different from the real intentions and that take place simultaneously in different areas;
- Stratagems – the implementation of sets of measures, interconnected by characteristics such as purpose, place and time, to thwart the opponent's plans using hiding, masking, misleading, deception etc.;
- C4 – parasitising command and control, computer and communication systems with distorted or false data and information that would lead to the execution, by the opponent, of actions that would compromise military and/or political leaders in front of subordinates and convince civil society of their anti-national intentions;
- Psychological-information warfare – modelling the opponent's behaviour by using complex military, political and diplomatic measures;
- Analysis and reflexive approach – the analysis reveals the probable objectives of the opponent and the means by which he wants to obtain them, and the reflexive approach tries to obtain the intellectual superiority over the opponent based on the analysis;
- Internet – manipulating social trends or emotions by determining target groups/ individuals to act in a certain direction. (Ib., pp. 43-46):

In the Russian view, reflexive control is a process by which the initiator tries to exploit vulnerabilities in the value system of the opponent, which is composed of "filters", where filters consist of concepts, knowledge, ideas and experience of the opponent. Thus, after identifying a point of minimum resistance, an information weapon (composed of methods and techniques of information distortion) is used, which would have the ability to generate changes in adverse information processes and systems (civilian and military).

The subject of *reflexive control* is widely discussed in both Western and Russian literature, and the definitions, methods and applicability of this concept are more extensive than the details presented. However, we are particularly interested in the relevance that Russian military theorists attach to *reflexive control* in the context of psychological-informational war (or information warfare). In this regard, *reflexive control* has the role of causing the opponent to disillusion himself and to make those decisions that will determine deficiencies in the management of his own systems. In the Russian view, *reflexive control* is a process by which the initiator tries to exploit vulnerabilities in the value system of the opponent, which is composed of *"filters"*, where filters consist of concepts, knowledge, ideas and experience of the opponent (Pynnöniemi, 2019, p. 219). Thus, after identifying a point of minimum resistance, an information weapon (composed of methods and techniques of information distortion) is used, which would have the ability to generate changes in adverse information processes and systems (civilian and military) (Ib.). It is important to note that when deploying the information weapon, the target is attacked by several attackers/from several directions simultaneously and in this way the victim fails to distinguish between ally and opponent, which ultimately leads to the loss of the notion of threat (Ib., p. 220). In this way, the action of *reflexive control* torments the target as it produces effects in two possible directions: latency in the ability to react to objective and direct threats or subjectivise threats, causing exacerbated reactions and distracting from immediate dangerous events.

The action of reflexive control torments the target as it produces effects in two possible directions: latency in the ability to react to objective and direct threats or subjectivise threats, causing exacerbated reactions and distracting from immediate dangerous events.

Comparing *reflexive control* with *active measures*, we notice that there are similarities in terms of shapes and techniques, both of which concern the cognitive dimension of the target. The most visible difference is the purpose and focus of the actions, so that *reflexive control* is intended exclusively for external targets, while *active measures* have a more general applicability, internal and external. However, there is a nuance that we need to keep in mind: *active measures, maskirovka* and *reflexive control* are concepts with a long evolution, so they are designed to be jointly deployed, to complement each other and to adapt to new operational concepts, technologies and needs.

ORIENTATION MODEL

Given the concepts, notions and ideas presented, we further propose an orientation model to highlight the mode of action of the Russian Federation, emphasising the idea of regime change through corrupting/affecting the information environment of the targeted state. We believe that this model can contribute to a clearer understanding of the Russian course of action on the states of the European Union and NATO, given that the use of military force against these states is still a risky move.

As we mentioned, before initiating actions against a state/states, pre-analyses and analyses are performed to identify their minimum resistance points, subsequently exploiting them in particular. Even if we are talking about EU and NATO states, there are some general vulnerabilities in their democratic systems that facilitate the application of non-military forms and measures, information warfare or the idea of regime change.

In democratic systems, there is a distinction between individual and state, where the two entities have different needs and objectives, and security is perceived in various forms. For example, the state may be interested in ensuring international security, territorial security and some visibility and relevance in the international bodies of which it is a part, but the individual may be more interested in his economic prosperity and in his professional, sentimental or ideological fulfilment. However, the existence of this distinction is the foundation that can lead to the erosion of the power and legitimacy of the state as it can determine: the enclavisation of society, in which individuals feel an increased fidelity to the elements closer to their lives such as family, clan, religious community, region etc.; and the enclavisation of the state, along with its institutions, where its role is limited only to the administrative component (Buzan, 2017, p. 90). Thus, in order to reduce this gap between state and individual/society, the political system plays the role of mediator in the conflict of social relations, political actions being social acts, especially by the fact that there are no clear boundaries that limit the politicisation of social life (Denni & Lecomte, 2004, pp. 21, 25). From this point appear the vulnerabilities that can be exploited by the Russian Federation, especially at the information level.

In democratic systems, there is a distinction between individual and state, where the two entities have different needs and objectives, and security is perceived in various forms. For example, the state may be interested in ensuring international security, territorial security and some visibility and relevance in the international bodies of which it is a part, but the individual may be more interested in his economic prosperity and in his professional, sentimental or ideological fulfilment.

Political parties contribute to the political education of the individual and thus have the ability to structure public opinion by analysing, for electoral purposes, the situation of the state, proposing topics for political debate and coming up with solutions, but disseminate political battle at all levels of society through any channels (Bréchon, 2004, pp. 119-120). Naturally, society is not a homogeneous and harmonious system, being marked by conflicts generated by the existence of social stratification and the divergent interests of different social groups (Denni & Lecomte, p. 73). But the more violent the political conflict is expressed in society (in addition to the pre-existing tensions), the higher the chances of extremist parties to appear, and if there are infused, in the middle of the conflict, elements of information distortion, the fears that will arise inside the society or social groups will generate embryonic ideological forms (ultra-nationalism, anti-globalism, religious fanaticism, anarchism etc.) with escalation potential (Bréchon, pp. 80, 110). However, two other problems are generated here: a) political parties are conditioned, in the political offer, by the mood and preferences of public opinion/society, so that the political agenda cannot be too far from these preferences (Ib., p. 92); b) the state may face a long period of disorder in political life, but for the individual, the escalation of a violent political struggle becomes a source of insecurity (Buzan, pp. 83-84) that radicalises it and subsequently changes its value system.

These aspects, in practice, are the basis of Russian ideas regarding the influence of the opponent in the political (decision-making) sphere and of the population. As a first step, they must gain supremacy over the opposing information environment by taking the initiative to determine the information shock. In this regard, the Russian Federation may conduct a series of operations, including *active measures*, *maskirovka* and *reflexive control*, oriented, in the first instance, to the individual and society, and later to the political environment. In this first stage, the operations would aim to block the society's ability to organise ways to mediate social conflicts (Denni & Lecomte, p. 31), causing its fragmentation following the escalation of conflicts that multiply and could no longer resolve naturally.

The Russian Federation may conduct a series of operations, including active measures, maskirovka and reflexive control, oriented, in the first instance, to the individual and society, and later to the political environment. In this first stage, the operations would aim to block the society's ability to organise ways to mediate social conflicts, causing its fragmentation following the escalation of conflicts that multiply and could no longer resolve naturally.

These forms and measures can be so sudden that the security systems of the targeted state can be subject to strategic surprise and thus react late to Russian information attacks. Then, by exposing individuals to Russian information flows for a long time, this could lead to disruption of the information environment, so as to obtain the desired effects. However, conditioning is not sufficient because the Russian Federation acts simultaneously or in stages (depending on the specifics of the targeted state) in several directions. Specifically, in the first instance, it is quite likely to focus its effort on blocking the access of the population/groups to correct information in order to subjectivise their reality, subsequently penetrating the society with active and passive agents of influence (active – intelligence officers/recruited agents engaged in active measures; passive – influential people who have no direct links to external actions, but are part to them). After ensuring a favourable information environment, the Russian Federation can disseminate false information through various channels, especially social media echo chambers, and ensure that confusion, dissatisfaction, and ultimately radicalisation is established. In addition, the Russian Federation can also target the political environment of the state in order to make it vulnerable so that it can no longer assume its role as regulator and guardian of global social and value unity against destabilising elements (Ib., p. 35). According to the theoretical perspectives presented, the vulnerability of the political environment can be achieved through covert actions such as deception and misleading, blackmail, threat, corruption *(figure no. 1)*, but also through more direct actions such as infiltration of influence vectors that generate and maintain a degree of instability, subversion, sabotage and even assassination (wet operations). Russian information actions could pursue the following already mentioned actions: 1) discredit and delegitimise the state's institutions and its political environment; 2) induce chaos among the population; 3) mislead and distort reality; 4) monitor, assess the effects and adjust the forms and means if necessary.

The vulnerability of the political environment can be achieved through covert actions such as deception and misleading, blackmail, threat, corruption, but also through more direct actions such as infiltration of influence vectors that generate and maintain a degree of instability, subversion, sabotage and even assassination (wet operations).

Before the radicalisation of the individual, information attacks must ensure the destruction of the citizen's trust and respect for the pre-existing order within the state and motivate him to act to change/demolish it. The execution of these information operations can be carried out in the medium and long term to substantiate, at the cognitive level, the mystification of reality/deception. Over time, the first signs of changes in value systems in society and the political environment such as the emergence of extremist parties, ultranationalism, religious fundamentalism, anti-globalism, isolationism, anti-Europeanism, anti-Americanism etc. appear. Once the changes in attitude begin to become visible then individuals and society will determine changes in the political environment – which has also been subject to external influence – and this, in turn, will bring changes in the state apparatus from its structure to the fundamental and organic laws. Of course, in an operation that target a state, various techniques and means are analysed and used, and the details are consistent and consist of as many particularities as possible that can contribute to the successful completion of Russian *"hostile actions".*

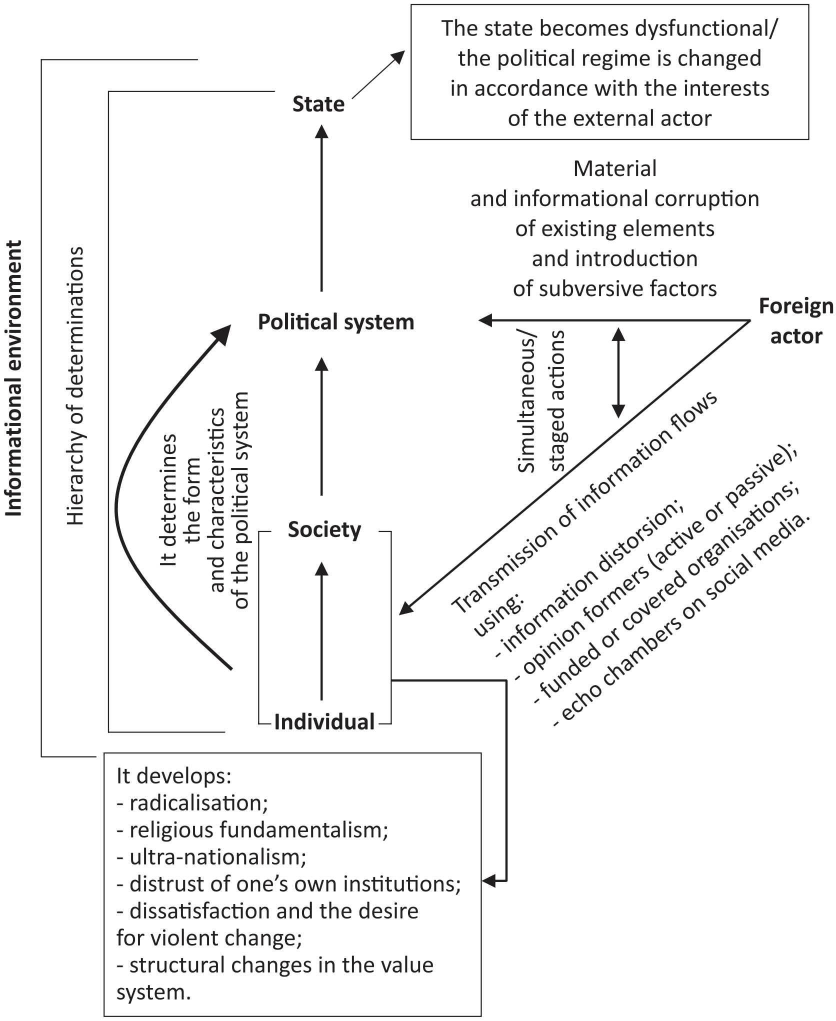
The state becomes dysfunctional/
the political regime is changed
in accordance with the interests
of the external actor
State
Material
and informational corruption
of existing elements
and introduction
of subversive factors
Foreign
actor
Political system
Simultaneous/
staged actions
Informational environment
Hierarchy of determinations
It determines
the form
and characteristics
of the political system
Transmission of information flows
Society
Transmission of information flows
using:
- information distorsion;
- opinion formers (active or passive);
- funded or covered organisations;
- echo chambers on social media.
Individual
It develops:
- radicalisation;
- religious fundamentalism;
- ultra-nationalism;
- distrust of one's own institutions;
- dissatisfaction and the desire
for violent change;
- structural changes in the value
system.

Figure no. 1: Orientation model of how the social-political structure of a state could be changed by the affected information environment
(Source: made in own conception)

In this section, we have tried to build an orientation model that is based on some essential, but general, aspects of democratic states. Based on the presented Russian military concepts and perspectives, we have constructed this hypothetical model to highlight how real are Russian actions to destabilise an internal state or to change its political regime in order to generate the optimal conditions for further interventions.

CONCLUSIONS

The definitions and interpretations presented have the purpose to build a synthesis on some fundamental concepts in the theoretical arsenal of the Russian Federation and to clarify (as much as possible) some ambiguities regarding Russian forms and practices. The paper attempts to draw attention to the conceptual complexity of the Russian military, especially in the context in which some analysts/researchers classify Russian actions as a zero-sum game. As we have presented, both the Russian military perspectives and their concepts are based on a complex planning that encompasses different forms and measures, coordinated or synchronised, where the goals are varied and target the military, civilians and decision-makers. In this logic, whether the Russian Federation launches asymmetric operations, non-military measures or a psychological-information warfare, using forms such as *active measures, maskirovka* and *reflexive control*, the actions will pursue the fulfilment of a line of operations to influence the target in desired/predicted directions. Hence, we can say that these actions, although slow in effect, aim to generate optimal conditions for action for the Russian Federation, which leads us to consider the fact that an operation to influence a target can be staged and can be carried out in the long term (referring to a duration of years).

Both the Russian military perspectives and their concepts are based on a complex planning that encompasses different forms and measures, coordinated or synchronised, where the goals are varied and target the military, civilians and decision-makers.

Whether or not they have the material, human and financial capabilities to conduct operations over the years, it must be acknowledged that, in theory, they have an advantage over NATO states because they develop and improve operational concepts based on the initiative, strategic surprise, flexibility and manoeuvrability, influence, misleading and exploitation of minimum strengths. In this regard, we find a very problematic aspect in the fact that *"hostile actions"* are framed between the state of peace and war, something that we do not find in the conception of NATO. The theorising of information warfare in its psychological-informational and technical-informational forms determines another conceptual disadvantage for NATO.

Given that most autocratic states use, to varying degrees, information operations to influence targets in various directions, we believe that the theoretical and conceptual resizing of military use of information is required at NATO level. Once general tools have been set up, the member states' security structures can use them, depending on their cultural specificity, to counter or cancel Russian indirect approaches, information attacks, asymmetric operations or non-military measures, but not only.

In the end, we can only estimate that the threats of a military and informational nature will not fade, but will be amplified, leading to even more complex forms that are difficult to counter. Time is an ally for those who know how to use it optimally, so NATO and the EU must use the remaining time to protect their information environment, defence systems, decision-makers and societies from Russian interference.

Given that most autocratic states use, to varying degrees, information operations to influence targets in various directions, we believe that the theoretical and conceptual resizing of military use of information is required at NATO level.

BIBLIOGRAPHY:

1. Andrew, C., Mitrokhin, V. (1999, 2000, 2018). *The Mitrokhin Archive: The KGB in Europe and the West*. Vol. I. Penguin Books.
2. Bréchon, P. (2004). *Partidele politice*. Trad. Marta Nora Țărnea, Adina Barvinshi. Cluj-Napoca: Editura Eikon.
3. Buzan, B. (2017). *Popoarele, statele și frica: O agenda pentru studii de Securitate internațională în epoca de după Războiul Rece*. Trad. Vivia Săndulescu. Chișinău: Editura Cartier.
4. Chiru, I. (2019). *Analiza în intelligence: de la artă la știință*. București: Editura Tritonic.
5. Clark, R.M., Mitchell, W.L. (2019). *Deception: Counter-deception and Counterintelligence*. Washington, D.C.: CQ Press.
6. Denni, B., Lecomte, P. (2004). *Sociologia politicului*. Vol. I. Trad. Marta Nora Țărnea. Cluj-Napoca: Editura Eikon.
7. Dick, C.J. (2013). *Catching NATO Unawares: Soviet Army Surprise and Deception Techniques*. In Barton Whaley (ed.), Hy Rothstein (ed.). *The Art and Science of Military Deception* (pp. 181-192). Boston, London: Artech House.
8. Duțu, P. (2013). *Ameninţări asimetrice sau ameninţări hibride: delimitări conceptuale pentru fundamentarea securităţii şi apărării naţionale*. București: Editura Universităţii Naţionale de Apărare *"Carol I"*.
9. Franke, U. (2015). *War by Non-military Means: Understanding Russian Information Warfare*. Swedish Defence Research Agency (FOI).
10. Fridman, O. (2019). *On 'Gerasimov Doctrine': Why the West Fails to Beat Russia to the Punch*. In *Prism*, 8(2), 101-112.
11. Giles, K., Seaboyer, A. (2019). *The Russian Information Warfare Construct*. Defence Research and Development Canada.

12. Giles, K. (2016). *Handbook of Russian Information Warfare*. Rome: NATO Defense College, Research Division.
13. Gordon, J.S. (1996). *Intelligence and Psychological Operations.* In Benjamin F. Findley (ed.). Frank L. Goldstein (ed.), *Psychological Operations: Principles and Case Studies* (pp. 203-211). Alabama: Air University Press. Maxwell Air Force Base.
14. Göransson, M. (2021). *Understanding Russian thinking on gibridnaya voyna*. In Mikael Weissmann (ed.), Niklas Nilson (ed.), Björn Palmertz (ed.), Per Thunholm (ed.). *Hybrid Warfare. Security and Asymmetric Conflict in International Relations* (pp. 83-94). London, New York, Dublin: I.B. TAURIS, Bloomsbury Publishing Plc.
15. Hamilton, D.L. (1986). *Deception in Soviet Military Doctrine and Operations*. Monterey, California: Naval Postgraduate School.
16. Kabernik, V. (2019). *The Russian Military Perspective*. In Ofer Fridman (ed.), Vitaly Kabernic (ed.), James C. Pearce (ed.). *Hybrid Conflicts and Information Warfare: New Labels, Old Politics* (pp. 43-65). Boulder, London: Lynne Rienner Publishers.
17. Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O., Oberholtzer, J. (2017). *Lessons from Russian's Operations in Crimea and Eastern Ukraine*. RAND Corporation.
18. Koribko, A. (2015). *Hybrid Wars: The Indirect Adaptive Approach to the Regime Chance*. Moscow: Peoples' Friendship University of Russia.
19. Liddell Hart, B.H. (1929, 2008). *Strategy*. BN Publishing.
20. Maier, M. (2016*). A Little Masquerade: Russia's Evolving Employment of Maskirovka*. Kansas: US Army School for Advanced Military Studies, Fort Leavenworth United States.
21. Mattsson, P.A. (2015). *Russian Military Thinking – A New Generation of Warfare*. In *Journal of Baltic Security 1(1)*, 61-70.
22. Mitrokhin, V. (ed.). (2002, 2004). *KGB Lexicon: The Soviet Intelligence Officer's Handbook*. London, New York: Frank Cass & Co. Ltd.
23. Pynnöniemi, K. (2019). *Information-Psychological Warfare in Russian Security Strategy*. In Roger E. Kanet (ed.), *Routledge Handbook of Russian Security* (pp. 214-226). London, New York: Routledge Taylor & Francis Group.
24. Renz, B., Smith, H., Bukkvoll, T., Echevarria, A.J., Giles, K., Scheipers, S., Strachan, H., Thornton, R. (2016). *Russia and Hybrid Warfare: Definitions, Capabilities, Scope and Possible Responses*. Kikimora Publications, Aleksanteri Institute, University of Helsinki.
25. Robinson, P. (2010). *Dicționar de securitate internațională*. Trad. Monica Neamț. Cluj-Napoca: CA Publishing.
26. Sinclair, N. (2020). *A Logic All Its Own. Russian Operational Art in the Syrian Campaign*. In *Military Review 100(1)*, 12-21.

27. Thomas, T.L. (2016). *Thinking like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War*. Foreign Military Studies Office.
28. Thomas, T.L. (2019). *Russian Military Thought: Concepts and Elements*. The MITRE Corporation.
29. Wardle, C., Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking*. Strasbourg: Council of Europe.
30. Whaley, B. (1969, 2007). *Stratagem. Deception and Surprise in War*. Norwood: Artech House.
31. Bureau of Public Affairs (1981). *Soviet "Active Measures". Forgery, Disinformation, Political Operations*. Washington D.C.: United States Department of State.
32. FM 3.-1. (2016). *Information Operations*. Headquarters, Department of the Army.