DOI 10.52781/cmm.e012

Russian reflexive control: military theory and applications

Control Reflexivo Ruso: teoría militar y aplicaciones

Abstract: The development of information security doctrine in the Russian Federation has been in the works since the first decade of this century. Currently, the doctrine is applied both at the governmental level and as an instrument for the application of military power. The present work presents how the Russian Federation is managing its actions based on the Reflective Control (CR) theory. As the theory involves the Russian understanding of information, technical data, cognitive contents and "information resources" are understood as technological and human, as well as being employed by the Strategic Communication system (Public Relations, Public Diplomacy and Security Systems of the Information), for a specific purpose. This work also describes the interaction of the CR with Doctrina Germazinov, the Information Warfare activities, with the use of non-military measures, the use of Cyber Warfare, social media and the "Controlled Chaos" measures, all with the objective to ensure success in Russian combat and development.

Keywords: Reflective Control; Strategic Communication; Cyber/ Information Warfare; Influence Operations and Controlled Chaos.

Resumen: El desarrollo de la doctrina de la seguridad de la información en la Federación de Rusia ha estado funcionando desde el primer decenio de este siglo. Actualmente, la doctrina se aplica tanto a nivel gubernamental como como instrumento de aplicación del poder militar. Este artículo presenta cómo la Federación Rusa está manejando sus acciones basadas en la Teoría del Control reflexivo (CR). Dado que la teoría implica la comprensión rusa de la información, los datos técnicos, el contenido cognitivo y los" recursos de información " se entienden como tecnológicos y humanos, así como, son empleados por el sistema de Comunicación Estratégica (Relaciones Públicas, Diplomacia Pública y Sistemas de Seguridad de la Información), para un propósito específico. En este trabajo también se describe la interacción de la CR con la doctrina Germazinov, las actividades de guerra de la información, con el uso de medidas no militares, el uso de la guerra cibernética, los medios sociales y las medidas de "caos controlado", todo con el objetivo de garantizar el éxito en el combate y el desarrollo ruso.

Palabras clave: Control Reflexivo;Comunicación Estratégica; Guerra Información /Cibernética; Operaciones de influencia y caos controlado

João Ricardo da Cunha Croce Lopes
Exército Brasileiro. Escola de Comando e Estado-Maior do Exército.
Rio de Janeiro, RJ, Brasil
ricardo@croce.ggf.br

Received: Sep. 19, 2021
Approved: Nov. 20, 2021

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 Introduction

One of the main goals of the commander in war is to interfere in the decision-making process of the enemy. This goal is often achieved through misinformation, camouflage, or other strategies. For Russia, one of these basic methods is the use of the Reflexive Control theory, which is defined as a way of transmitting specially prepared information to a partner or opponent in order to persuade them to make a predetermined decision, desirable for the initiator of the action (ЛЕФЕВР; СМОЛЯН, 2010). This method can be used against "decision-making processors", human or machine.

Despite the fact that the theory has long been developed in Russia, it still finds itself undergoing constant updates in the present day.

In this article, the military aspect of the Russian concept of Reflexive Control and its role as a weapon in the information war, in accordance with the military doctrine of Defense of the Russian Federation, will be presented.

The knowledge presented here was the result of studies done in Moscow, as well as its deepening carried out through the texts, doctrines, articles and lectures to which I gained access. Although there are several manuals and a vast material, many of these were not directly made available by my “comrades”. The translation of technical terms was also a complicating factor, even after more than 10 (years) of contact with the Russian language. For these reasons, this article took a long time to be submitted.

2 Development

The nature of Reflexive Control Theory (RC) exists for much longer than similar concepts of information warfare and information operations. In fact, it appeared in Soviet military literature 40 years ago. Vladimir A. Lefebvre defined Reflexive Control as "a process in which one of the opponents transmits the other reasons for decision-making" (ЛЕФЕВР, 1984, p. 14).

The development of the Theory of Reflexive Control went through four periods:

- Research (from the early 1960s to the late 1970s);
- Practice-oriented (from the late 1970s to the early 1990s);
- Psychological / pedagogical role (from the early to mid-1990s);
- Psychosocial role (since the late 1990s).

The Soviet and then, after 1991, Russian armed forces have long been exploring techniques of using the theory of Reflexive Control (*especially at tactical and operational levels*): as a disguise (*to deceive*), for the purpose of misinformation as well as to influence the decision-making processes of the enemy. For example, the Russian army already owned, in 1904, the military camouflage school. In 1929, this school laid the foundation for the concept of camouflage and created guidelines for future generations (*Maskarovka*).

Reflexive Control is also seen as a means of information warfare. For example, Major General N.I. Turko, a professor at the Academy of the General Staff of the Russian Federation, established a direct link between information wars, operations and the strategies of Reflexive Control. He noted that the most destructive manifestation, in the tendency to rely on military force, is due to the possible impact of Reflexive Control of the opposite party, through the proper development of the theory and practice of information warfare, which is more significant than the direct use of military force.

Turko believed that Reflexive Control is the most important information weapon for achieving military goals even more than traditional "firepower". This view was shaped largely by his belief that the American use of information weapons during the Cold War did much more to defeat the Soviet Union than any other weapon, as well as was the source that caused its collapse. Finally, Turko mentioned reflexive governance as a method of achieving geopolitical superiority and as a means of managing military negotiations, an area that should be more recognized by countries entering into such negotiations with the Russians.

By definition, Reflexive Control occurs when **the governing body conveys a controlled system of motives and principles that will serve as an excuse to come to a desirable solution, but the real intentions are kept in absolute secrecy** (ТУРКО; МОДЕСТОВ, 1996).

The "Reflection" encourages certain processes to simulate the reasoning of an enemy or to simulate a possible behavior of the enemy, forcing him to make an unfavorable decision for himself. In fact, the enemy comes to a solution based on the **representation of a situation he shaped**, including the location of detachments and structures on the opposite side, as well as the intentions known to him from opponents.

Initial ideas for decision-making are formed primarily on the basis of intelligence, data and other factors that are based on a sustainable set of concepts, knowledge, ideas and, finally, experience. This set is commonly referred to as a "filter" that helps the commander separate the necessary information from useless data, true data from false, and so on.

In military decision-making processes, the “human-machine-assisted” process is more prevalent. Currently, automated decision-making systems operated only by machines are not yet approved (SUTYAGIN, 2015). The adversary may try to influence the human being; and, by another process, the adversary may try to influence the machine.

In all decision-making processes, the importance of recurrent information collection and evaluation is emphasized, as well as a comprehensive approach in order to allow planners to create Lines of Action (LA) for their executions, as well as models for the LA of opponents. In this way, the Lines of Action are mostly based on intelligence and information provided by various Situational Awareness (SA) systems, weapons systems and the like. Thus, decision-making processes depend heavily on the collection of data that is real, correct and timely. Inaccurate and/or irrelevant information, as well as delays in submission, can seriously impair a decision-making process. In the context of machine-assisted decision-making, this means that false, irrelevant, or premature information can be introduced to the human, to the machine, or both. The Russian RC acts and both 02 (two) processes – Human and Machine-assisted Human.

The main task of Reflexive Control is also to explore, as a tool, morality, psychological factors and others, as well as personal characteristics of commanders. In the latter case, biographical data, habits and psychological differences can be used in deceptive acts. In a war where Reflexive Control is used, the party with the highest quality of "reflection" (*more able to imitate the thoughts of the other side or predict their behavior*) will have better chances to win.

The quality of "reflection" depends on a large number of factors, the most important of them – analytical skill, general erudition, the sphere of knowledge about the enemy and experience. The military author Colonel S. Leonenko (ЛЕОНЕНКО, 1995) added that in the past, strategy was the main tool of Reflexive Control, but today "tricks" and camouflage have replaced the method.

Although the formal terminology of Reflexive Control did not exist in the past, the opposing parties actually used it intuitively when trying to identify and collide with each other's thoughts, as well as plan and change their impressions of themselves, provoking a wrong (misleading) decision.

If successful, the RC on the enemy allows to influence military plans and awareness of the situation, as well as, their actions. Thus, Reflexive Control focuses more on the less tangible subjective element of "Military Art" than on the more objective "Military Science".

Achieving successful Reflexive Control requires a deep study of the "inner nature" of the enemy, his ideas and concepts; Leonenko described them as a "filter" through which all data about the outside world passes. A successful Reflexive Control represents the culmination of an information operation.

2.1 Reflexive Control Detailing

The history of the concept of Reflexive Control (RC) stems primarily from the work carried out by Vladimir Lefebvre from 1963 to 1967 in the Soviet Union. After the publication of two works Конфликтующие структуры (ЛЕФЕВР, 1967) – Conflicting Structures and Алгебра конфликта (ЛЕФЕВР; СМОЛЯН, 2010) – Conflict Algebra, Lefebvre's work became the subject of a classified report of the KGB in 1968. Lefebvre's main work (1984) is entitled *Reflexive Control: the Soviet concept of influencing the decision-making process of an opponent* (ЛЕФЕВР, 1984).

The processes of Reflexive Control are based on the Soviet (and now Russian) system, ethical legacies that are very different from those of the West (Christian), in which Russians have a particular understanding of what constitutes "truth".

According to Lefebvre, the concept of *vranyo* (вранио – lie/deception) refers to the "dissemination of untruths that have some basis in reality" (ЛЕФЕВР; СМОЛЯН, 2010) similar to *likelihood*.

Lefebvre defined the *Reflexive Control* as being "a process in which one of the opponents transfers to the other the foundations for decision-making" (ЛЕФЕВР, 1984, p. 81). In other words, there is a substitution of the motivating factors of the opponent to encourage him to make decisions that are unfavorable to him.

For the Armed Forces of Russia, **Reflexive Control** (RC) is the term used to describe **the practice of pre-determining the decision of an opponent in your favor, changing key factors in the perception of the opponent's world** (ЛЕФЕВР, 1984). The term is found mainly in the discussion of information warfare techniques. In this context, the practice represents a key asymmetric facilitator for obtaining critical advantages, neutralizing the opponent's strengths, causing him to choose harmful courses of action for himself.

Exploiting the moral stereotypes of behavior, psychological factors, personal information about the commander (biographical data, habits, etc.), the RC makes it possible to increase the chances of victory, however, it is noted that such tactics require information about the enemy with a high degree of detail and quality!

The manipulation of public opinion in the West through social networks, *troll* factories and networks of *bots*, while driving anti-US, anti-NATO and anti-elite narratives, are part of this policy.

The application of *Reflexive Control* to change the decision-making cycle of the control object (*target audience/decision-maker/public opinion*) acts through the influence of the idea of a situation of the object of control.

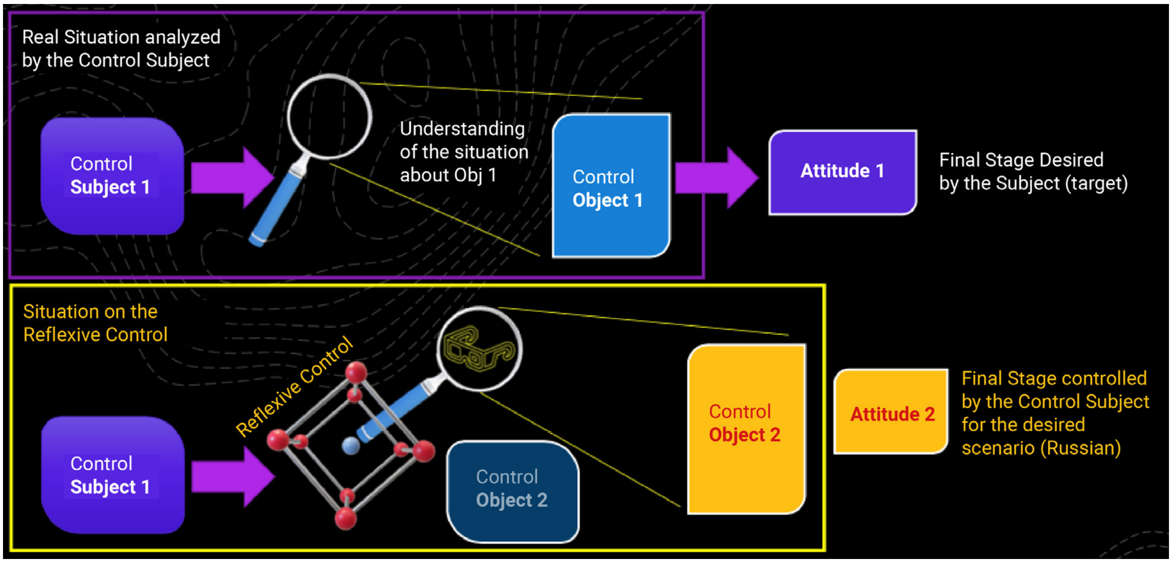
The control subject (*Russian*) takes measures to provide the control object with information that reflexively leads to action in the interests of the control subject (*Russian*).

Instead of denying information entirely, or providing false information, the intention of Reflexive Control is to manipulate the information available through information tools (capabilities relating to information warfare-systems, intelligence actions, espionage, other) to the object of control (*target*) so that they use this information to make a reflexive decision in the interests of the control subject.

Example: **Real Situation → Control Subject X Control Object = action 01**
Real situation + the idea of the controller directing to change
the decision cycle → influence messages for verisimilitude to the real situation.
(targeting the desirable scenario) =
Desired real situation → Control Subject + Control Object = action 02.

As mentioned earlier, decisions are made through a fair, objective, accurate approach based on information relevant to the situation, <u>influencing the approach</u>, the situation changes.

Figure 1– Scheme of Russian Reflexive Control


Real Situation analyzed by the Control Subject
Control Subject 1
Understanding of the situation about Obj 1
Control Object 1
Attitude 1
Final Stage Desired by the Subject (target)
Situation on the Reflexive Control
Reflexive Control
Control Subject 1
Control Object 2
Control Object 2
Attitude 2
Final Stage controlled by the Control Subject for the desired scenario (Russian)

Source: The Author (2021).

Attitudes, knowledge, and skills are analyzed to determine critical thinking skills, decision making, predictive (*and prospective*) judgment, problem solving, creativity, openness to experience, and other leadership behaviors.

According to the analyzed attitudes, the competencies of inference, Recognition of Assumptions, Deduction, Interpretation and Evaluation of Arguments are measured (indicators).

From the "score" of each leader and/or target (*public*), the persuasive action of Reflexive Control is shaped.

2.2 Opinions of military experts: Ionov, Komov and Chausov

Major M. D. **Ionov** wrote several articles on the subject of Reflexive Control (ИОНОВ, 1994, 1995). He was one of the first military theorists to assess the importance of Reflexive Control. The concept of "Reflexive Control" was not present in any Soviet military encyclopedia when he began to write in the 70s, so it simply could not exist! As a result, in his first articles, Ionov talked about "managing the enemy", and not about Reflexive Control.

At the same time, Ionov also understood the close relationship between advertising and reflexive Control and the need to combine the use of reflexive techniques to organize the management of Reflexive Control (ИОНОВ, 1994).

Ionov identified four main methods to help transmit information to the enemy in order to facilitate the organization of control over him.

1) Applying pressure by demonstration of force. Such a show of force can be exerted in various ways that span different aspects, from diplomatic or economic pressure, such as the threat of economic sanctions, threats of military action, such as increased combat readiness of the Armed Forces, or provocations close to declarations of war.

> The pressure of power, including the use of superior force, displays of force, psychological attacks, ultimatums, threats of sanctions, threats of risk (manifested through a focus on irrational leadership behavior, or delegation of authority to the irresponsible person), military intelligence, provocative maneuvers, weapons tests, restriction of enemy access or isolation of certain areas, increased combat readiness of the Armed Forces, formation of coalitions, an official declaration of war, support for the destabilizing situation of internal forces, disabling and publicizing victory, "pumping" and publicizing the victory, demonstrating relentless actions and showing mercy to an enemy ally who stopped resisting (ИОНОВ, 1994, p. 45, author's translation).

2) Providing false information. This approach suggests the use of camouflage, denial and deception "*Maskirovka*" (Doctrine of Dissimulation) at all levels in order to manipulate the announcement and reception of a situation. This includes showing great strength where.

> Methods of providing false information about the situation, including camouflage (showing weakness in a strong spot), creating false structures (showing "strength" in a weak spot), leaving one position to strengthen another, leaving dangerous objects in this position ("Trojan Horse"), hiding true relations between units or creating false ones, maintaining the secrecy of new weapons, bluffing about weapons, changing the methods of operation or the deliberate loss of documents (ИОНОВ, 1994, p. 46, author's translation).

3) Affecting the decision-making process of the opponent. Such an approach includes systematic modeling of processes, the publication of deliberately distorted doctrines, as well as the presentation of false information to the opponent's system and key figures.

> Provoking the enemy to find new directions of escalation or ending the conflict: a deliberate demonstration of a chain of Special Action, hitting the enemy's stronghold when he is not there, subversive activities and provocations, leaving open the route for the enemy to leave the siege, forcing the enemy to commit punitive actions that lead to the expenditure of its Armed Forces, resources and time (ИОНОВ, 1994, p. 46, author's translation).

4) Affecting the timing of the decision. Here, the element of surprise can be employed by the sudden start of a military operation or induce the opponent to focus on another area of conflict to slow the reaction.

> Impact on the enemy's decision-making algorithm, including the systematic conduct of games through which the dissemination of typical plans, publication of a deliberately distorted doctrine; Impact on controls and key figures transmitting false situation data; Backup form actions to act to neutralize the enemy's operational thinking; changing the timing of a decision that can be made through the sudden onset of hostilities; transmit information about the situation of a similar conflict - working in what appears to be feasible and predictable, the enemy makes an ill-considered decision that will change the path and nature of his operation (ИОНОВ, 1994, p. 47, author's translation).

According to **Ionov** (ИОНОВ, 1994), it is necessary to evaluate human goals for the Reflexive Control of a person or group, taking into account individual or group psychology, way of thinking and professional level of training.

Colonel S. A. Komov, a Russian military theorist, wrote about the informational impact of Reflexive Control and he was possibly the most prolific author on the topic of information wars in the 1990s. On the pages of the magazine "Military Thought", Komov supported the meaning given by Ionov to Reflexive Control, giving it another name, "intellectual" methods of information warfare. He listed the main elements of the "intellectual" approach to information warfare, which he described as:

- Distraction (deviation of attention) – creating a real or imaginary threat to one of the vital dislocations of the enemy (flanks, rear, etc.) during the preparatory phase of hostilities, forcing him to reconsider the common sense of his decisions);
- Overload (at the expense of large amounts of conflicting information often sent to the enemy);
- Paralysis (creation of perceptions of special threats to vital interests or weak spots);
- Exhaustion (forcing the enemy to perform useless actions and thereby exhausting the Armed Forces);
- Deception (provoking the enemy to redeploy his forces to the threatened region during the preparatory stages of hostilities);
- Division (convincing the enemy that he must act against the interests of the coalition);
- Calm (forcing the enemy to believe that pre-planned operations are being trained instead of preparing for offensive actions - and thus reduce their vigilance);
- Intimidation (creating an irresistible perception of superiority);
- Appeasement (by decreasing vigilance and creating the illusion of conducting planned training, and not preparing for offensive actions);
- Provocation (impose on the enemy data so that he performs beneficial actions on your side);

- Proposal (to offer information that touches the enemy legally, morally, ideologically or in other spheres);
- Pressure (to offer information that discredits the government in the eyes of the population) (КОМОВ, 1997, p.18-22, our highlights, author's translation).

Finally, the article of the Captain of the first rank **F. Chausov** (ЧАУСОВ, 1999), continues to discuss Reflexive Control, which is defined as the process of intentional transfer of certain information to the opposing party, which will have an impact on the decision-making by that party corresponding to the information transmitted. Chausov formulated the following principles of Reflexive Control:

- **the principle of purpose** – the process should be goal-oriented, using the full range of measures of Reflexive Control required;
- **the principle of updating** – planning should be "updated", providing a fairly complete picture of the intellectual potential of the command and personnel, especially in situations related to the global information space;
- **the principle of correspondence** – the mutual consistency of goals, place, time and methods of Reflexive Control must be observed;
- **the principle of modeling** – we must not forget to predict and model the actions and states of the opposite side during the execution of Reflexive Control;
- **the principle of anticipation** – current events must be anticipated and anticipated (ЧАУСОВ, 1999, p. 12, our highlights, author's translation).

It also includes **risk assessment**, the essence of which boils down to the danger of being mistaken in case of an incorrect assessment of the consequences. With this approach, the maximum risk will be if the enemy unravels the plan on its own.

2.3 The RC in the Russian Military Doctrine – Gerasimov Doctrine

In the first two decades of this century, Russia conducted operations in several former Soviet states, aimed at establishing a sphere of influence in these countries, and preventing NATO and the EU from expanding their areas of influence, as well as to protect Russian interests and ethnic minorities abroad (Russian ENS, 2021).

In this same period, Western analyses of the conflicts in which Russia took part focused on the different forces that Russia used to achieve its objectives: cyber forces in Estonia, conventional forces in Georgia and Special Operations Forces (FOpEsp) in Crimea area of Ukraine (BERZINS, 2014).

Western military specialists were especially interested in the operational teachings of the Armed Forces of the Russian Federation and how they supplemented their conventional military means with FOpEsp, transport, naval infantry and with rapid reaction forces. Others also speculated how Russia would use cyber resources in future conflicts. However, most of these studies it has a limited scope with only a focus on military *hard power*. In addition, most of them are based on Western assumptions about the Russian war mode, using military means within traditional domains air, sea and land, expanded with the new cybernetic domain. In reality, the Armed Forces of the Russian Federation (AFRF) changed its doctrine of war in an **operational concept** to achieve the goals of its foreign policy (ПОДБЕРЕЗКИ, 2014; ДОКТРИНА..., 2016; РОССИЯ, 2021; RUSSIAN, 2014).

In 2003, Russia launched a "*white paper*" in support of this new policy, which described a change in military thinking and defined a new operational concept based on the integration of strategic, operational and tactical elements. The concept was updated with the lessons of the Estonian and Georgian conflicts. It is characterized by the use of non-military means and non-traditional domains, such as youth groups Partisans, cyber-attacks, civilian media and forces "*proxy*". Vital to the new operational concept is the rapid destruction, disruption or control of communications, economy, infrastructure and political institutions to disrupt the command and control of the enemy, as well as total cyber dominance.

In this section this New Doctrine (NTG) is detailed, as well as, it is described the Russian operational framework and its links with information warfare activities, military concepts and strategic positions, followed by a brief exemplification of the application of the new doctrine in the conflict of Ukraine (Crimea), of 2014.

The main goal is to reveal tactical and operational level actions (*Strategic Communication and Reflexive Control activities*) of the new doctrine (NTG) and the cumulative effects and goals that these actions need to achieve in order to gain a better understanding of the new Russian operational concept (DEFENSE INTELLIGENCE AGENCY, 2017).

2.4 The Russian approach to a conflict

In February 2014, the chief of the General Staff of the AFRF, general Valery Gerasimov, described in his article "*The Value of Science in Foresight*" (ВАЛЕРИЙ, 2013), the new operational concept based on the lessons of the Estonian and Georgian conflicts.

Gen Gerasimov explained that AFRF has developed unique situational planning models for applying military and non-military means, such as FOpEsp, forces "*proxy*", civil media and cyber capabilities to influence all actors, disrupt communication and destabilize regions in order to achieve their goals.

During the conflicts of Estonia, Georgia (BARABANOV, 2014), Ukraine (ANALYSIS..., 2014) (HAINES, 2015) and Syria (SUTYAGIN, 2015), Russia has established civilian capabilities such as youth groups and state media and mobilized Russian ethnic minorities abroad, appealing to feelings of marginalization, a sense of self-esteem and belonging, and a perception that "Mother Russia" has more to offer than the home country. Then Russia provoked international reactions and created a general perception of despair of the military and political leadership of the target countries, after which these countries were willing or forced to accept the new situation created by Russia (FRIDMAN; 2019; GALEOTTI, 2019; LANKINA; WATANABE, 2017; SZOSTEK, 2017).

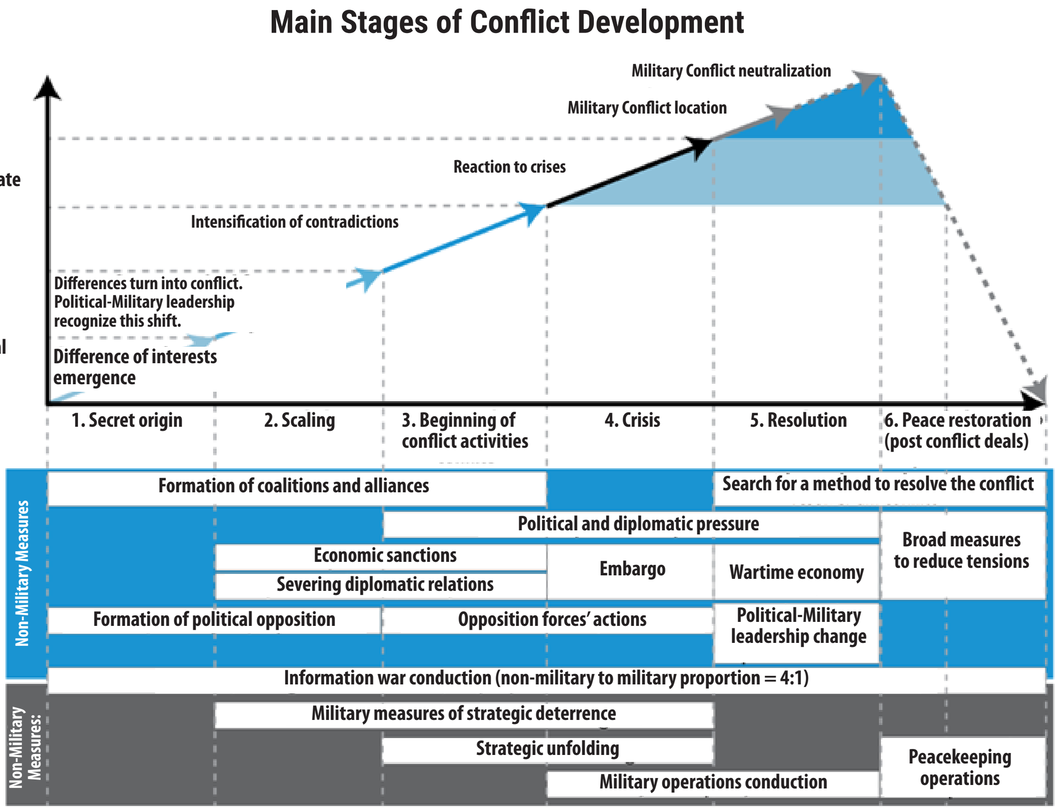
The so-called "Gerasimov Doctrine" is an approach of society that causes a change of means and domains and poses a challenge to the Western mode of war due to unfamiliarity with its ways, means, effects and goals.

Gen Gerasimov described the current framework of the Russian operational concept as the use of "*all non-military methods in resolving interstate conflicts*" [1].

It incorporates six phases as shown in Figure 01: secret origin, escalation, the outbreak of conflict activity, crisis, resolution and ending with the restoration of peace.

This operational concept is a set of systems, methods and tasks for influencing the perception (RC) and behavior of the enemy, the population and the international community at all levels. He uses a systems approach based on "Reflexive Control" (perception management) to target the enemy leadership and change their guidance in such a way that they make decisions favorable to Russia and take actions that lead to a sense of despair within their leadership and establish a basis for negotiation on Russian terms. According to Ionov, in this case, Reflexive Control "considers psychological characters of human beings and involves intentional influence on their decision-making models" (BARTLES, 2016, p. 31, author's translation).

Figure 2 – The role of non-military methods in resolving interstate conflicts.


Main Stages of Conflict Development
Military Conflict
Immediate Military Threat
Direct Military Threat
Potential Military Threat
Military Conflict neutralization
Military Conflict location
Reaction to crises
Intensification of contradictions
Differences turn into conflict. Political-Military leadership recognize this shift.
Difference of interests emergence
1. Secret origin
2. Scaling
3. Beginning of conflict activities
4. Crisis
5. Resolution
6. Peace restoration (post conflict deals)
Non-Military Measures
Formation of coalitions and alliances
Search for a method to resolve the conflict
Political and diplomatic pressure
Broad measures to reduce tensions
Economic sanctions
Severing diplomatic relations
Embargo
Wartime economy
Formation of political opposition
Opposition forces' actions
Political-Military leadership change
Information war conduction (non-military to military proportion = 4:1)
Non-Military Measures:
Military measures of strategic deterrence
Strategic unfolding
Military operations conduction
Peacekeeping operations

Source: Adapted from Герасимов, 2014.

The New Doctrine (NTG) has not evolved in a vacuum over the past decade, but it is a double reaction to the events that unfolded after the collapse of the Soviet Union.

[1] Ivanovich, Mironov Sergey. Lecture at the Diplomatic Academy of the Ministry of Foreign Affairs of Russia. The topic of the lecture: "Security and the role of military force in ensuring international security" Course: "Military-Political Aspects in international relations and arms control", 2017. Author's source.

First of all, the evolution is a reaction of the Russian leadership under President Vladimir Putin, to combat the cognitive model that reflects the internal structure of a decision-making system. This model offers an approach of interrelated mechanisms based on history, social conditions and linguistics, to deceive, tempt, intimidate or misinform the enemy. Reflexive Control mechanisms can cause psychological effects ranging from disappointment to suggestion. If one of these mechanisms fails, the overall Reflexive Control approach needs to engage another mechanism, or its original effects can degrade rapidly.

Finally, Russian operational art relies on concealment, also a technique of Reflexive Control, divided into two levels. Concealment of the operational level concerns the measures of "way to achieve operational surprise and is designed to disorient the enemy in relation to the nature, concept, scale and time of impending combat operations". (ГЕРАСИМОВ, 2014, p.19) and strategic-level concealment are "activities that surreptitiously prepare a strategic operation or campaign to disorient the enemy in relation to the true intentions of actions". (ГЕРАСИМОВ, 2014, p. 19)

Gen Gerasimov explained the new operational concept with some of the same principles as Georgi Isserson, one of the leading Soviet military thinkers before World War II. Isserson defined the operational art as the ability of direction and organization, in which operations are a chain of efforts throughout the depth of the operation area, with principles of shock, speed, efficiency, mobility, simultaneity, technological support and a decisive moment in the final phase. Gerasimov added to the notion of Isserson the application of asymmetric and indirect actions by civilian/military components, Special Operations forces and technical weapons (ISSERSON, 2013) to weaken the economy and destroy key infrastructure in a potential area of operations. The new operational concept is therefore a mere continuation of the existing Russian operational art with different means, not only in the physical domain but also in the information domain.

Russia uses "*extraterritorial forces*", both paramilitary and cyber, supported by institutions and companies (media or not), Spetsnaz fighters and *Cossack* to conduct different types of operations, such as unconventional, information, psychological and cyber operations, as well as assistance to security forces and **strategic communication**. Russia manages these military and non-military means through state-controlled enterprises and organizations under a centralized political command structure. This structure, coupled with the fact that the forces employed consist of a mixture of ethnic Russians and Russians abroad, make Russia not only explore social conditions, but also cultural and linguistic factors in the former Soviet states and at home to create "*extraterritorial forces*". Studies the behavior, ethnic composition and demography of all potential opponents to reveal advantages that can exploit to achieve their goals[2] (АННЕНКОВ et al, 2006, 2011, 2015).

[2] Ivanovich, Mironov Sergey. Lecture at the Diplomatic Academy of the Ministry of Foreign Affairs of Russia. The topic of the lecture: "Security and the role of military force in ensuring international security" Course: "Military-Political Aspects in international relations and arms control", 2017. Author's source.

2.5 Detailing the use of the Gerasimov Doctrine (ASYMMETRIC WARFARE GROUP, 2016; BARTLES, 2016; DEFENSE INTELLIGENCE AGENCY, 2017;) (NTG) (GORENBURG, 2017), with emphasis on information warfare and Reflexive Control

For the complete understanding of the Doctrine, I will approach the Operational Art in 07 (seven) phases, that is, 01 (one) more than presented by Gen. Gerasimov (ГЕРАСИМОВ, 2014), aiming to present the total actions of the information doctrine (ДОКТРИНА, 2016), with Strategy / Reflexive Control of NTG.

The details must be accompanied with the assistance of the document contained in **Appendix n. 01**.

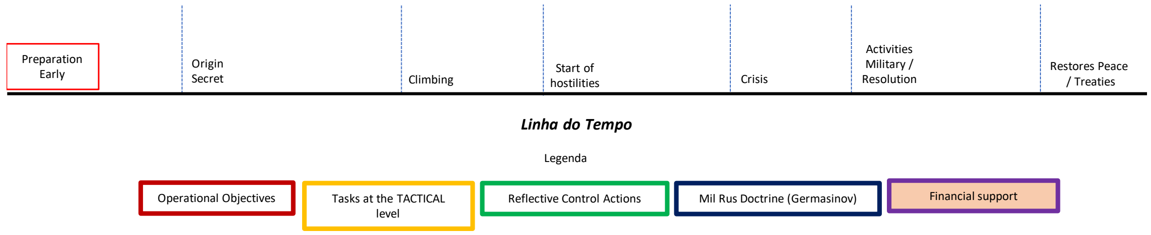
On the baseline, it lies from the development of time, from left to right.

Vertically, 03 (three) fields of action are delimited: military measures (at the base), non-military measures (at the center) and information warfare (at the top).

In the evolution of time, within each field, the actions of: Operational Objectives, Tasks at the Tactical Level, Reflexive Control Actions, the actions of the Gerasimov Doctrine and the necessary Financial Support / Diplomatic Effort are identified.

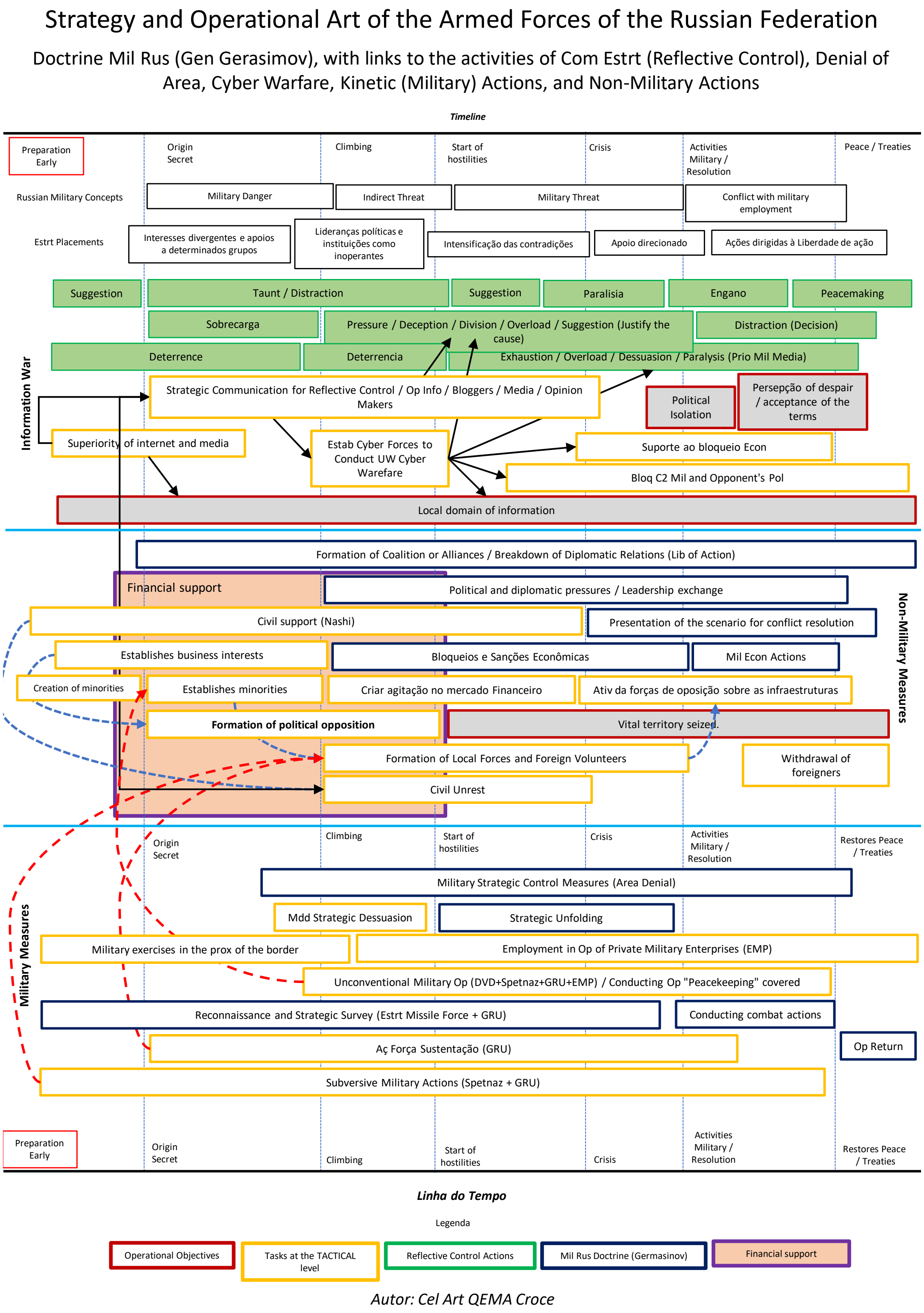
The description of the detail is approached, within the temporal phase, from the base to the top, presenting the triggering of the actions within each field.

Figure 3 – Frame of the base of the detail Appendix 1.


Preparation Early
Origin Secret
Climbing
Start of hostilities
Crisis
Activities Military / Resolution
Restores Peace / Treaties
Linha do Tempo
Legenda
Operational Objectives
Tasks at the TACTICAL level
Reflective Control Actions
Mil Rus Doctrine (Germasinov)
Financial support

Source: The Author (2021)

Figure 4 – Strategy and Operational Art of the Armed Forces of the Russian Federation



Strategy and Operational Art of the Armed Forces of the Russian Federation

Doctrine Mil Rus (Gen Gerasimov), with links to the activities of Com Estrt (Reflective Control), Denial of Area, Cyber Warfare, Kinetic (Military) Actions, and Non-Military Actions

Timeline

Preparation Early | Origin Secret | Climbing | Start of hostilities | Crisis | Activities Military / Resolution | Peace / Treaties

Russian Military Concepts: Military Danger | Indirect Threat | Military Threat | Conflict with military employment

Estrt Placements: Interesses divergentes e apoios a determinados grupos | Lideranças políticas e instituições como inoperantes | Intensificação das contradições | Apoio direcionado | Ações dirigidas à Liberdade de ação

Information War

Suggestion | Taunt / Distraction | Suggestion | Paralisia | Engano | Peacemaking

Sobrecarga | Pressure / Deception / Division / Overload / Suggestion (Justify the cause) | Distraction (Decision)

Deterrence | Deterrencia | Exhaustion / Overload / Dessuasion / Paralysis (Prio Mil Media)

Strategic Communication for Reflective Control / Op Info / Bloggers / Media / Opinion Makers

Political Isolation

Persepção of despair / acceptance of the terms

Superiority of internet and media

Estab Cyber Forces to Conduct UW Cyber Warefare

Suporte ao bloqueio Econ

Bloq C2 Mil and Opponent's Pol

Local domain of information

Non-Military Measures

Formation of Coalition or Alliances / Breakdown of Diplomatic Relations (Lib of Action)

Financial support

Political and diplomatic pressures / Leadership exchange

Civil support (Nashi)

Presentation of the scenario for conflict resolution

Establishes business interests | Bloqueios e Sanções Econômicas | Mil Econ Actions

Creation of minorities | Establishes minorities | Criar agitação no mercado Financeiro | Ativ da forças de oposição sobre as infraestruturas

Formation of political opposition

Vital territory seized.

Formation of Local Forces and Foreign Volunteers

Withdrawal of foreigners

Civil Unrest

Military Measures

Origin Secret | Climbing | Start of hostilities | Crisis | Activities Military / Resolution | Restores Peace / Treaties

Military Strategic Control Measures (Area Denial)

Mdd Strategic Dessuasion | Strategic Unfolding

Military exercises in the prox of the border | Employment in Op of Private Military Enterprises (EMP)

Unconventional Military Op (DVD+Spetnaz+GRU+EMP) / Conducting Op "Peacekeeping" covered

Reconnaissance and Strategic Survey (Estrt Missile Force + GRU) | Conducting combat actions

Aç Força Sustentação (GRU) | Op Return

Subversive Military Actions (Spetnaz + GRU)

Preparation Early | Origin Secret | Climbing | Start of hostilities | Crisis | Activities Military / Resolution | Restores Peace / Treaties

Linha do Tempo

Legenda

🟥 Operational Objectives | 🟨 Tasks at the TACTICAL level | 🟩 Reflective Control Actions | 🟦 Mil Rus Doctrine (Germasinov) | 🟪 Financial support

Autor: Cel Art QEMA Croce

Source: The Author (2021)

a) Phase 0 – Preparation in Advance

Military Measures – Small infiltrations of FOpEsp and GRU are triggered in order to carry out subversive actions (support) and recognition. The means of the Strategic Missile Force and the GRU carry out a weekly update of Geoint data and detailed strategic reconnaissance. Military commands conduct military exercises within their area, but in the vicinity of the borders (Rec GE).

Non-Military Measures – Minorities are "triggered" or created, there is also the triggering of the "Nashi forces" (DENNING, 2015), Partisans or Cossacks, as well as the EMP aiming at future support. Economically, contracts are carried out between companies interested in the area, mainly infrastructure companies, as well as, the co-opting of elite elements in the target area, through financial corruption.

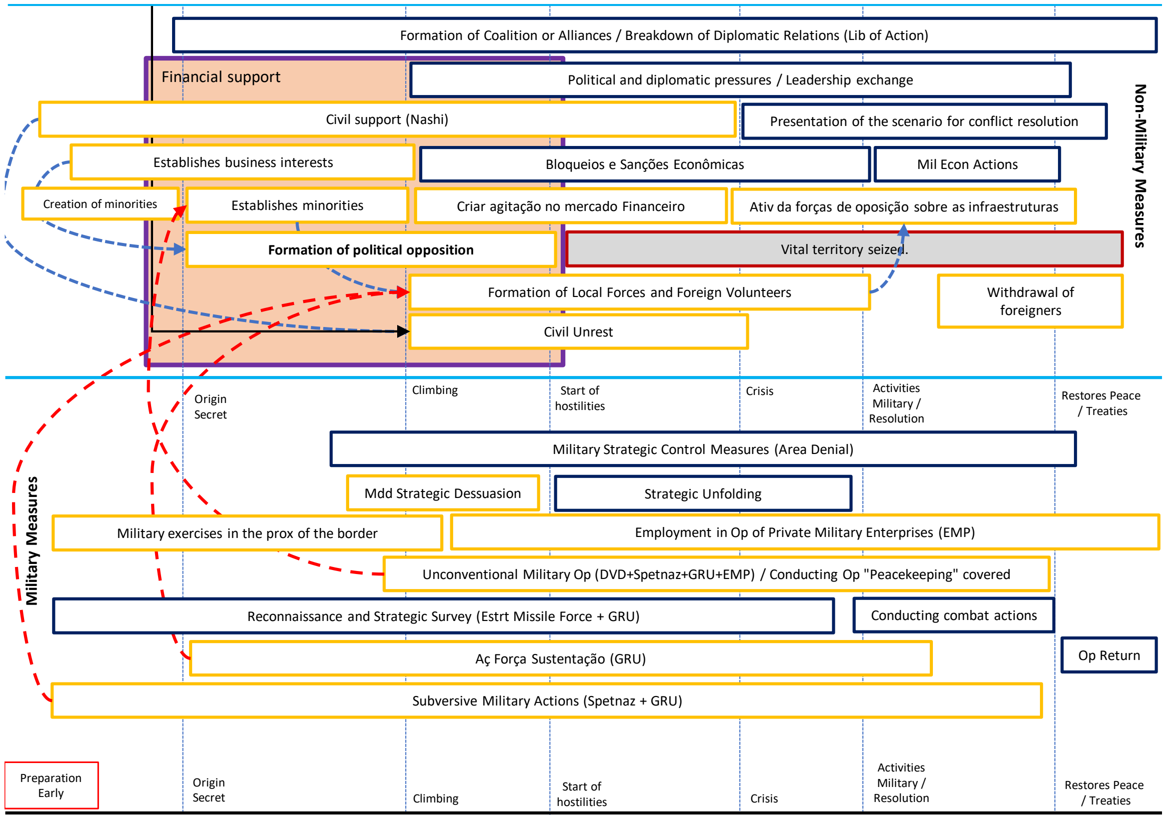
Information War – The networks, "backbones" and cyberinfrastructure are updated, initiating actions to enable the superiority of the internet and media. The operational goal is the local domain of information. The actions of Com Strategy/RC triggered are aimed at Suggestion and Dissuasion. The suggestion is directed at minorities and errors of local government (generation of enmities). Deterrence is aimed at hiding the strategic displacement, as well as, passing on the idea of "Lost Cause".

By way of example, the phase of early preparation for the conflicts of Georgia, Ukraine and Estonia began in 1991, when they all became independent and separate states from the Soviet Union, focusing on two separatist regions: South Ossetia and Abkhazia. Both regions did not have large ethnic Russian populations, but the inhabitants had a distinctly different culture and language from the Georgian population, more related to the areas on the north, inside Russia. Tensions in Ukraine soon followed, largely because of an ethnic Russian minority in Crimea who wished to join Russia. At the same time, the Estonian government passed a law that rejected Russian as an official language, forcing the Estonian language over ethnic Russians as a requirement to gain Estonian nationality. Russia saw these developments as a marginalization of the rights of ethnic Russians. In the following years, Moscow issued passports to ethnic Russians in all three countries, creating a Russian minority, which it promised to protect. Tensions escalated when Estonia joined the EU and NATO in 2004 and subsequently refused to build an oil pipeline together with Russia. In most cases, Russia infused the situation by granting citizenship to ethnic Russians or other inhabitants with complaints, creating Russian citizens in neighboring states. It is one of Russia's main strategic objectives to protect ethnic Russians wherever they are.

b) Phase 1 – Secret Origin

Military Measures – In this phase the support forces are structured, with the support of the GRU, aiming at the formation of local forces, EMP and foreign volunteers (Force Proxy) for the escalation phase. The activities of reconnaissance and monitoring of situational awareness remain, as well as, strategic displacement and military exercises in the border strip are intensified. At the tactical level, the movement of strategic deterrents (Def Aae, GE and Missiles) is already observed.

Figure 5 – Frame of military and non-military measures and their connections during the Secret Origin (check the complete diagram on the appendix).


Formation of Coalition or Alliances / Breakdown of Diplomatic Relations (Lib of Action)
Financial support
Political and diplomatic pressures / Leadership exchange
Civil support (Nashi)
Presentation of the scenario for conflict resolution
Establishes business interests
Bloqueios e Sanções Econômicas
Mil Econ Actions
Creation of minorities
Establishes minorities
Criar agitação no mercado Financeiro
Ativ da forças de oposição sobre as infraestruturas
Formation of political opposition
Vital territory seized.
Formation of Local Forces and Foreign Volunteers
Withdrawal of foreigners
Civil Unrest
Non-Military Measures
Origin Secret
Climbing
Start of hostilities
Crisis
Activities Military / Resolution
Restores Peace / Treaties
Military Strategic Control Measures (Area Denial)
Mdd Strategic Dessuasion
Strategic Unfolding
Military exercises in the prox of the border
Employment in Op of Private Military Enterprises (EMP)
Unconventional Military Op (DVD+Spetnaz+GRU+EMP) / Conducting Op "Peacekeeping" covered
Reconnaissance and Strategic Survey (Estrt Missile Force + GRU)
Conducting combat actions
Aç Força Sustentação (GRU)
Op Return
Subversive Military Actions (Spetnaz + GRU)
Military Measures
Preparation Early
Origin Secret
Climbing
Start of hostilities
Crisis
Activities Military / Resolution
Restores Peace / Treaties

Source: The Author (2021)

Non-Military Measures – Increased financial support for co-opting activities of partners "loyal to the cause". From the formation of minorities (with ethnic descendants or not) are triggered training action and establishment of areas of operations (includes the study and validation of key areas for “area denial”). The actions of Nashi (civil support in all fields) and business interests are also intensified. Intense work on the formation of political opposition is carried out. The operational objective is the formation of alliances and/or a coalition, as well as the gradual “weakening” of diplomatic relations.

Information warfare – At this stage, the Russian operational concept, for external media, is that of “military danger”. That is, that the actions of other stakeholders can militarily affect the target area, aimed at giving freedom of action for Russian military employment. The political strategic positioning is dissemination in traditional media. The activities of Com Strategy/RC are intensified with the objectives of provocation, distraction, information overload in the internal systems of the target area, and increase the degree of Deterrence.

c) Phase 2 – Escalation

Military Measures – Efforts remain in subversive measures, support to the sustentation forces in the target area, monitoring of situational awareness (prioritizing Intel, GE, AAe, Cyber) and the means of strategic deterrence are already positioned. In this phase, the first EMPs appear on the ground, mainly of logistics and support to civil activities (health and covered Peacekeeping). The most identified differential is the provision of military means in DTAs near the border, carrying out maintenance activities of military exercises. The Train Force of the Ministry of Defence is widely employed for logistics.

Non-Military Measures – At this stage, the first manifestations and actions of civil unrest are identified. The training of local non-military forces and volunteer foreigners is already in conditions of employment. In the financial market, capital flight and various cyber actions in the financial system are identified. The formation of political opposition is felt with the increase in the amounts of (planned) protests. The force support Nashi is fundamental, along with diplomatic actions, aimed at ensuring the strategic-operational objectives of Blockade and Economic Sanctions, along with political / diplomatic pressures aimed at the change of leaderships in the target area.

Information warfare – The Russian concept of "Indirect Threat" is worked out to exhaustion. That is, that the actions of the civilian population must be supported and any movement of military means is considered a threat. In the face of the international community, the strategic position adopted is to publicize the image that political leaders and institutions are inoperative in the target area, needing “help” to control the “chaos”. In this phase, cyber forces are already structured and begin activities across the spectrum of C2, critical infrastructure and decision-making. The actions of Com Strategy/RC are mainly directed at Pressure, Deception, Division, Overload and Justification, aimed at increasing freedom of action and increasing controlled chaos in the target area. With the aim of isolating the decision-making process of the leadership in the target area, Deterrence actions (isolation of decisions and civil unrest) are undertaken.

Activities in the conflict of Ukraine

The escalating phase of the crisis began after President Yanukovych of Ukraine fled the country in February 2014 and a pro-Western government took power. According to Russia, the new government acted against the security of Russians inside Ukraine. Russia used the discourse of international humanitarian intervention for its protection and of Russians abroad to justify an intervention, again in reference to Western arguments for validating NATO involvement in the Kosovo crisis.

The next step of the Russian operation was the media campaign to gain support in Crimea and Russia and isolate the Government of Ukraine, as depicted in the center of phases one and two: strategic communication. The television and Internet were the dominant media in Ukraine. In Crimea, in total, 95% of the population gathered their news from television channels, which were almost all Russian state-owned. About 50% of the population of Crimea gathered their news from the Internet, and 70% of Crimean internet users rely on their news collection on the two main available Russian social networking sites. Russians and Ukrainians analyzed information about feelings collected from the Internet, finding a score of 76% for pro-Russian feelings in the region. Independent news providers are rated with a reliable score of 30%, and foreign news providers only have 5% reliability. In short, it is reasonable to state that Russia established the domain of information in the first phase of the new doctrine (NTG) – hidden origin – and that it used extra means during the next phase to maintain this domain described as the goal of "local information domain".

The Russian information campaign began with the comparison of the Ukrainian government and its Western allies with Nazis, gays, Jews and other groups of people that Russia claimed to be part of the government's comparison with Nazi Germany. This theme remained throughout the conflict. Russia also accused the Western media of oversimplifying demographic maps, signifying Eastern and southern Ukraine as the predominant ethnic Russians. Meanwhile, diplomatic channels and the Russian leadership began to emphasize the same issues of marginalized Russian minorities seeking reunification with Russia.

On February 14, a cyberattack emerged, targeting one of Ukraine's largest banks, attacked by malware, aimed at supporting unrest in the country and portrayed as one of the non-military means in Appendix 1.

d) Phase 3 – beginning of hostilities

Military Measures – Measures of area denial (dispersion of means) and strategic deployment within the operational range are established. The activities of the escalation phase are maintained, but with the aim of triggering the opposing side in order for it to mistakenly react to a predetermined action (argument for self-defense). We highlight the control actions of the electromagnetic spectrum and the use of "drones".

Non-Military Measures – Pressure actions in the political, economic, psychosocial and civil unrest fields are maintained. Some locations in the target area are now controlled by Proxy Forces and designated as Vital Territory. These are infrastructure, media facilities, neighborhoods located in the main DTAs, etc. The "*green men*" can be observed, usually Security EMP for NGOs partisans of humanitarian aid.

Information warfare – The Russian concept of "military threat" is worked with the focus on the military means of the target area (*The Defense Forces attack their own people*). Military actions on the civilian population, humanitarian support or on some Russian military means is considered a threat. In the face of the international community, the adopted strategic position of disseminating the image that political leaders and institutions are inoperative remains, but contradictions are intensified, mainly by diplomatic means. Antagonisms, disagreements and internal enmities of the target area are exacerbated. The actions of Com Strategy/RC in this phase are directed to two strands: the first, with Pressure, Deception, Division, Overload and Suggestion are directed to the political and economic fields; and the second, with exhaustion, informational overload, deterrence and paralysis are directed to the military and science and technology fields. Measures aimed at blocking military and political C2 (isolating the source of power) are initiated.

Note – at home and abroad, the Com Strategy/RC system often operates in a public-private partnership with Russian oligarchs or businessmen, as well as through the co-opting of "independent" hackers by intelligence agencies. The strategy is **feeding existing resentments, stereotypes and vulnerabilities**. Every actor who weakens the dominant systems and helps to undermine confidence in the democracies of the target area is received as a partner.

Activities in the conflict of Ukraine

Local paramilitary forces and Cossacks stormed the parliament and replaced it with pro-Russians, led by Sergei Aksyonov. While pro-Russian sympathizers seized more key facilities in Crimea, volunteers from Russia came to their aid and a strong Russian army of 40,000 soldiers began exercises on the Ukraine-Russia border. In the days after the seizure, the Cossacks remained to protect the Parliament Buildings against the Ukrainian army or pro-Ukraine sympathizers. From February 28, the militants occupied military facilities, airfields, the regional media and telecommunications centers. They turned off telephone and internet communication in Crimea as more planes with new troops landed at the seized airfields. It is this combination of unconventional warfare by Special Operations forces and Proxy Forces, coupled with an overwhelming conventional force conducting exercises on the border, that either leads to a desired provocation for a reaction or deterrence/pacification to prevent one, as depicted in Appendix 08.

For provocation or deterrence/pacification to work, the government needs to be more or less isolated, burdened with misinformation as depicted in the center of Appendix 1. Therefore, the militants blocked radio and cellular traffic to further isolate Crimea from Ukraine. The cyberattacks coordinated by Russia began in early March and hit the Ukrainian government, as well as NATO websites. Cyber Berkut, a Ukrainian group, which may have ties to Russian intelligence services, organized the attacks. These attacks hampered the leadership of NATO and Ukraine, but did not lead to isolation or overload. The United States convened a UN mission in the region in March; Russia refused. Instead, prime minister Aksyonov of the Autonomous Republic of Crimea, together with former Ukrainian President Yanukovych, called for Russian intervention on March 1 and an independence referendum on March 30.

e) Phase 4 – Crisis

Military Measures – The same measures are maintained as in the stage of the beginning of hostilities. However, logistics for military means are increased, according to the time planning of operations. The strategic deployment is practically completed and reconnaissance actions "at the limit of the area of responsibility" are triggered. Such actions can lead to small combats on the border (self-defense action and reaction).

Non-Military Measures – Proxy forces begin their most notorious activities with successive attempts to dominate areas of interest aiming at the operational goal of control of the target area. Subversive actions can be triggered in certain places (radio antennas, etc.), but always recognized as "acts of sabotage" by partisans (КРЕЦУЛ, 2015). In the political area, scenarios for negotiation are presented. However, with targeted EFD.

Information warfare – At the beginning of this phase actions are triggered for the economic isolation of the opponent. The measures of Com Strategy/RC of the previous phase are maintained, but the focus is directed to the political paralysis of the opponent, aiming at the operational goal that should be felt until the phase of armed conflict.

Activities in the conflict of Ukraine

With the Crimean government virtually removed, the effects of Reflexive Control such as distraction, pressure, suggestion and isolation (*local)* were successful. Russia was never able to completely isolate the Ukrainian government, however, as Western support for this government decreased during the conflict and the EFD was achieved.

f) Phase 5 – Military activities (armed conflict)

Military Measures – The doctrine of Russian military employment is applied, with area denial and massive employment of armored means. Actions are carried out with maximum speed and dispersion.

Non-Military Measures – Actions on the opponent's infrastructures are intensified by Proxy Forces. The pursued operational goal is the control of the vital territory. Actions of Military Economy (blockade of imports, breach of contracts, etc.) are triggered aimed at the replacement isolation of the opponent's MEM. In the diplomatic area, the pressures for validation of the intended scenario remain. Reports of corruption, image breakdown, discrediting, etc. are some of the activities developed with diplomatic objectives. Some companies are already present in "combat-free " areas providing infrastructure and logistical support. Contracts of contractors for reconstruction are signed.

Information Warfare – The strategic positioning sought is aimed at increasing any and all freedom of action. The operational goals of political isolation, perception of despair and acceptance of terms are sought endlessly. In the Com Strategy/RC the military side is maintained and the political side is directed towards the deception and distraction of the decision-making process. Before the public opinion is presented the proposed scenario and its acceptance is strongly worked. The message of restructuring the area with the employment of companies and support to the local population is the focus. Topics such as environmental protection and protection of local cultural heritage assets are raised. The help of entrepreneurs in the communication area is requested. However, in combat areas, all physical or informational access, of any media, is controlled. The monitoring of the theme on social media is strongly executed. As well as, the control of public opinion is accompanied.

Activities in the conflict of Ukraine

Then in the Russian approach were the tasks that would lead to provocations (a second time as a last resort) or exhaustion and paralysis of the Ukrainian government in Kyiv. Although the Ukrainian government decided not to be provoked strategically, the result at the operational level was devastating. The combined actions led to the breakdown of the morale of the Ukrainian forces in Crimea, through a combination of the Reflexive Control mechanisms of exhaustion and suggestion, as they handed over their bases, in many cases to join the Russian forces. The "Little Green Men" isolated the Ukrainian forces at their bases and then used the local Internet and media to start military information support operations, media campaigns and intimidation in combination with bribery.

By March 2, the militants had already cut the power lines at the headquarters of the Ukrainian Navy in Sevastopol, followed by the seizure of the communication facilities of the Ukrainian Naval Forces and the sabotage of all communication lines. A cyberattack in Crimean area did not occur. One reason for the absence may be that Crimea is a small area with only one internet hub, which was already in the hands of the "unknown" troops.

The Kyiv government admitted that the local police and armed forces in Crimea were corrupt, sympathized with the uprising or had low morale. Then Russian agents of influence penetrated the local intelligence and security forces. Together, the lack of communications and base support led to the tactical and eventually operational isolation of Ukrainian forces in Crimea and their perception of despair.

g) Phase 6 – Restoration of peace and signing of treaties

Military Measures – The withdrawal of part of the forces employed begins, leaving in the target area EMP for the formation of self-defense forces. The following stand out: Military Police troops, DQBRN, GRU, FOpEsp, FSB and Def AAe. Subsequently, in the event of annexation, AFRF troops will be deployed.

Non-Military Measures – Actions of withdrawals of foreigners and cataloging of the population are done. Civil-military partnerships for reconstruction begin their activities. Political organization and essential services are worked out and routine activities are supported.

Information Warfare – The strategic positioning sought is to maintain any and all freedom of action for acceptance of the terms. The operational goals of political isolation and acceptance of the terms is pursued incessantly. Themes of pacification of hostilities and return of economic activities are worked. The Com Strategy/RC is aimed at pacifying the target area, with the opening of places for visitation, inauguration of real estate projects and the encouragement of cultural tourism.

Activities in the conflict of Ukraine

In April 2014, Russia admitted that the "Little Green Men" were, in fact, AFRF Spetznaz and airborne troops. On March 16, Crimea held the referendum for independence ahead of schedule, and 96.77% voted for reunification with Russia (turnout was 83.1%). The Russian Duma (parliament) signed a treaty on March 18 formally incorporating Crimea into Russia, initiating the sixth phase, the restoration of peace. The conflict remains frozen (ØSTENSEN, Å.; BUKKVOLL, Ø. 2018).

3 Conclusion

The current Russian operational concept uses military and non-military means simultaneously and quickly in all physical and informational domains, through the application of asymmetric and indirect actions. Russia mitigates the capabilities of opponents, creates chaos, takes vital terrain and isolates the enemy leadership. Although Russia uses a conventional force in its superior operational concept and with which victory is almost certain, it does not want to employ military forces as such for its foreign policy.

The big fight is an unwanted escalation, as Russia seeks a psychological, not physical victory. Instead of military action, Russia wants to let the Strategic Communication System spread Reflexive Control. The culminating psychological effects of the Reflexive Control approach such as disorientation, suggestion, and concealment need to overcome provocation. In the end, it will cause exhaustion, paralysis and perception of despair among the political and military leadership of opponents. These plausible perceptions and misperceptions create the leadership for the final phase of the New Doctrine (NTG): **non-combat resolution**.

The evolution of the New Doctrine (NTG) and its framework is not over, since the Russian operational framework is anything but a fixed set of means and strategies. The Russian leadership can develop and employ new types of asymmetric means, depending on the situation in question.

In the opinion of General Gerasimov, each conflict has its own set of rules and therefore requires unique ways and means. On the other hand, the effects to be achieved must be related to phases and goals. Therefore, the lesson for possible future conflicts is not merely to fixate on the physical means of Russia, but, more importantly, to recognize the phases discussed and predict the effects desired by the opponent.

We found that the "Gerasimov Doctrine" tested its structure during the conflicts of Estonia, Georgia and Ukraine, and in all of them the desired final state was achieved.

Studies on the use of Strategic Communication combined with Reflective Control must be developed so that we can identify its effects, that is, us as a target, so that protective measures can be taken in a timely manner. In view of the latest activities of the companies Cambridge Analytica, SCL Group (defensa) and Psy-Group in the democracies of Australia, India, Philippines, Kenya, Malta, Malaysia, Romania, Trinidad and Tobago, Nigeria, United States and the UK – case Leave.EU (BORSHCHEVSKAYA, 2019; National Defense University, 2020. CSIS, 2020 and Congressional Research Service, 2021), which have modern features of the use of Reflexive Control, but not by the Russians.

References

АННЕНКОВ, В. И. etal. **Международная безопасность**: геополитические и военно-политические аспекты современности. Под общей редакцией проф. Анненкова В.И. Москва: РУСАВИА, 2015. 512 с.

АННЕНКОВ, В.И. etal. **Военная сила в международных отношениях**. Наставнический. Москва: КНОРУС, 2011. 496 с.

АННЕНКОВ, В.И. etal. **Безопасность России:** геополитические и военно-политические аспекты. Москва, 2006.

ANALYSIS: Russian military manpower – strengths, weaknesses, Ukraine standoff. **Caversham BBC Monitoring**, [London], May 15, 2014.

ASYMMETRIC WARFARE GROUP. **Russian new generation warfare handbook**. [S. l.]: AsymmetricWarfareGroup, Dec 2016. p. 68. Available in: https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf. Access in: 18 nov. 2021.

ВАЛЕРИЙ, Г. Ценность науки в ожидании: Новые вызовы требуют переосмыслить формы и способы ведения боевых действий. **Военно-промышленный курьер**, 26 февраля 2013. Disponívelem: http://www.vpk-news.ru/articles/14632. Access in: 26 jul. 2017.

BARABANOV, M. Hard Lessons Learned: Russian Military Reform up to the Georgian Conflict. In: HOWARD, C.; PUKHNOV, R. **Brothers armed**: military aspects of the crisis in Ukraine. Minneapolis: East View Press, 2014. p. 80-81.

BARTLES, C. K. Getting Gerasimov Right. **Military Review**, Fort Leavenworth, Kansas, v. 96, n. 1, p. 30-38, Jan/Feb 2016. Available in: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf. Access in: 19 nov. 2021.

BERZINS, J. **Russia's new generation warfare in Ukraine**: implications for Latvian Defense Policy. Latvia: Narional Defence Academy of Latvia, Apr 2014.p. 3-6. (Policy Paper, n. 2). Available in: https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf. Access in: 19 nov. 2021.

BIKKENIN, R. Questions of theory: information conflict in the military sphere: basic elements and concepts. **Information Conflict in Military Sphere**, [s. l.], p. 38-40, Sep. 18, 2003.

BOLDYREVA, Elena, Cambridge Analytica: Ethics And Online Manipulation With Decision-Making Process. 2018/12/31 pg. 102. DO - 10.15405/epsbs.2018.12.02.10 Available in: https://www.researchgate.net/publication/330032180_Cambridge_Analytica_Ethics_And_Online_Manipulation_With_Decision-Making_Process. Acessado em 19 Nov 21.

BORSHCHEVSKAYA, Anna. **Russian Private Military Companies: Continuity and Evolution of the Model.** Russia Foreign Policy Papers, Dec 2019. p. 21. Available in: https://www.fpri.org/wp-content/uploads/2019/12/rfp4-borshchevskaya-final.pdf. Acessado em 19 Nov 21.

CENTER FOR STRATEGIC & INTERNATIONAL STUDIES. **Not so private military and security companies**: Wagner Group and Russian Prosecution of Great Power Politics. Washington, D.C.: CSIS, Sept25, 2020. Available in: https://www.csis.org/blogs/post-soviet-post/not-so-private-military-and-security-companies. Access in: 1oct. 2020.

CENTER FOR STRATEGIC & INTERNATIONAL STUDIES. **Moscow's Mercenary Wars.** Washington, D.C.: CSIS, Sept 2020. Available in: https://russianpmcs.csis.org/. Acessado em 19 Nov 21.

CONGRESSIONAL RESEARCH SERVICE. Sept 16, 2020. **Russian Private Military Companies (PMCs)** Available in: https://crsreports.congress.gov/product/pdf/IF/IF11650. Acessado em 19 Nov 21.

ЧАУСОВ, Ф. Основы рефлексивного управления противником. **Морской сборник**, [s. l.], n.1, 1999.

DENNING, D. The rise of hacktivism. **Georgetown Journal of International Affairs**, Washington, D.C, Sep 8, 2015. Available in: https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism. Access in: 19 nov. 2021.

DEFENSE INTELLIGENCE AGENCY (United States). **Russia military power**: building a military to support great power aspirations. [Washington, D.C.]: DIA, 2017. p. 116.

ПОДБЕРЕЗКИН, А.**Анализ, стратегический прогноз и планирование в военно-политической области**. 2014. Центр военно-политических исследований, Московский государственный институт международных отношений, Университет МИД России, Московский, 2014. Available in: https://docplayer.com/64510400-Analiz-strategicheskiy-prognoz-i-planirovanie-v-voenno-politicheskoy-oblasti.html. Access in: 22 nov. 2021.

ДОКТРИНА информационной безопасности Российской Федерации.УтвержденаУказом Президента Российской Федерации от.n. 646, 5 декабря 2016 г. Available in: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html. Access in: 22 nov. 2021.

ГЕРАСИМОВ,В. В. Доклад начальника штаба Вооруженных Сил Российской Федерации: роль государства оборонной организации страны в соответствии с новым положением о штабе, утвержденным Президентом Российской Федерации. **ВестникАкадемиивоенныхнаук,**[s. l.], tom 1, n. 46, c. 14-22, 2014. Available in: http://www.avnrf.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhiv-nomerov/639-vestnik-avn-1-2014 . Access in: 5 apr. 2018.

FRIDMAN, O. On the "Gerasimov Doctrine": why the West Fails to beat Russia to the punch. **PRISM**, [Washington, D.C], v. 8, n. 2, p. 100-113, 2019. Available in: https://www.jstor.org/stable/26803233?seq=1#metadata_info_tab_contents. Access in: 18 nov. 2021.

GALEOTTI, M. **Moscow's mercenaries reveal the privatisation of Russian geopolitics**. In: OPENDEMOCRACY. London: open Democracy, Aug 29, 2017. Available in: https://www.opendemocracy.net/en/odr/chvk-wagner-and-privatisation-of-russian-geopolitics/. Access in: 29 ago. 2017.

GALEOTTI, M. The mythical 'Gerasimov Doctrine' and the language of threat. **Critical Studies on Security**, London, v. 7, n. 2, p. 157-161, 2019. Available in: https://www.tandfonline.com/doi/abs/10.1080/21624887.2018.1441623?journalCode=rcss20. Access in: 18 nov. 2021.

GORENBURG, D. **Russia's military modernization plans**: 2018-2027. In: GORENBURG, D. Russian Military Reform. Cambridge, Nov 27, 2017. Available in: https://russiamil.wordpress.com/2017/11/27/russias-military-modernization-plans-2018-2027/. Access in: 27 nov. 2017.

HAINES, J. R. Russia's use of disinformation in the Ukraine Conflict - analysis. **EurasiaReview**, [s. l.], 18 Feb 2015. Available in: http://www.eurasiareview.com/18022015-russias-use-of-disinformation-in-the-ukraine-conflict-analysis/. Access in: 30 may 2021.

IBS Center for Management Research. Facebook–Cambridge Analytica Data Scandal. Available in: https://www.icmrindia.org/casestudies/catalogue/Business%20Ethics/BECG160.htm. Acessado em 19 Nov 21.

Institute For National Strategic Studies (NATIONAL DEFENCE UNIVERSITY), Nov 24, 2020. **Russia's Escalating use of Private Military Companies in Africa**. Available in: https://inss.ndu.edu/Media/News/Article/2425797/russias-escalating-use-of-private-military-companies-in-africa/ . Acessado em 19 Nov 21.

ИОНОВ, М. Д. Психологические аспекты управления противником в антагонистических конфликтах (рефлексивное управление). **Прикладная эргономика**,[s. l.], Специальный выпуск. n. 1, 1994.

ИОНОВ, М. Д. Управление противником. **Морскойсборник**, n. 7, 1995.

ISSERSON, G. S. **The evolution of operational.** Translated by Bruce W. Menning. Fort Leavenworth, Kansas: U.S. Army Combined Arms Center's, 2013. Available in: https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/OperationalArt.pdf. Access in: 19 nov. 2017.

ЛЕФЕВР, В. А. Конфликтующие структуры. Москва: Высшая школа, 1967.

ЛЕФЕВР,В. А. Рефлексивный контроль: советская концепция влияния на процесс принятия решений противником. Москва: Научные приложения, 1984.

ЛЕФЕВР, В. А.; СМОЛЯН, Г. Л. **Алгебра конфликта**. 4 е. изд. Москва: Книжный дом, Либроком, 2010.

ЛЕОНЕНКО, С. Рефлексивное управление противником. **Армейский сборник**, [s. l.], n. 8, 1995.

КОМОВ, С. А. Оспособахведенияинформационнойборьбы. Военнаямысль, tom 4, n. 7-8, c. 18-22, 1997.

КОНОНОВ Д.А., Кульба В.В., Шубин А.Н. **Информационное управление: принципы моделирования и области использования** //Труды ИПУ РАН. Т. XXIII. - М.: ИПУ РАН. 2005. С. 5-29.Kononov D.A., Kulba V.V., Shubin A.N. Gestão da informação: princípios de modelagem e áreas de uso // Procedimentos de IPU RAS. T. XXSH. - M.: IPU RAN. 2005.S. 5-29.

КРЕЦУЛ, Р. Россия закрывает «черную дыру» на границе с Украиной.**ВЗГЛЯД.РУ,** Москва,1 июня 2015. Available in: https://vz.ru/society/2015/6/1/748541.html. Acessoem: 30 may 2021.

LANKINA, T.; WATANABE, K. 'Russian Spring' or 'Spring Betrayal'? The media as a mirror of Putin's evolving strategy in Ukraine. **Europe-AsiaStudies**, [London], v. 69, n. 10, p. 1526-1556, Dec 2017. Available in: https://www.tandfonline.com/doi/full/10.1080/09668136.2017.1397603. Access in: 18 nov. 2021.

ØSTENSEN, Å.; BUKKVOLL, Ø. **Russian use of private military and security companies - the implications for European and Norwegian Security**. Oslo: Chr. MichelsensInstitutt, 2018. (FFI-RAPPORT, n. 18/01300). Available in: https://www.cmi.no/publications/6637-russian-use-of-private-military-and-security. Access in: 23 nov. 2021.

РОССИЯ. Президента. Стратегия национальной безопасности Российской Федерации, Москва, n. 400, 2 июля 2021 года. Available in: http://static.kremlin.ru/media/events/files/ru/QZw6hSk5z9gWq0plD1ZzmR5cER0g5tZC.pdf. Access in: 22 nov. 2021.

RUSSIAN. President of the Russian Federation. Military Doctrine of the Russian Federation, approved by Russian Federation President V. Putin. In: RUSSIAN FEDERATION PRESIDENT. [Moscow], Dec 31, 2014. Available in: http://www.kremlin.ru. Access in: 30 may 2021.

RUSSIA'S new maritime doctrine. **Jane's Defense Weekly**, [s. l.], p. 4, Aug 14, 2015.

SUTYAGIN, I. Detailing Russian Forces in Syria. In: THE ROYAL UNITED SERVICES INSTITUTE. **Defense Systems**. London: RUSI, Nov 13, 2015. Available in: https://rusi.org/explore-our-research/publications/rusi-defence-systems/detailing-russian-forces-in-syria. Access in: 30 may 2021.

ТУРКО, Н.И.; МОДЕСТОВ,С.А. **Рефлексивное управление развитием стратегических сил как механизм современной геополитики**: Системный анализ на пороге 21 века‖: теория и практика» Москва, февраль 1996 г. с. 366.

SZOSTEK, J. The power and limits of Russia's strategic narrative in Ukraine: the role of linkage. **Perspectives on Politics**, Cambridge, v. 15, n. 2, p. 379-395, 2017. Available in: https://eprints.gla.ac.uk/167897/. Access in: 18 nov. 2021.

ECEME