Communications
2025, Vol. 12, No. 1, pp. 11-23
https://doi.org/10.11648/j.com.20251201.12

Research Article

The Russian Reflective Control: Theory and Military Applications

Joao Ricardo da Cunha Croce Lopes*

Brazilian Army, Army Command and General Staff School, Rio de Janeiro, Brazil

Abstract

The development of the information security doctrine in the Russian Federation has been underway since the first decade of this century. Currently, the doctrine is applied both at the governmental level and as an instrument for applying military power. From the National Security Doctrine, through the Military Doctrine and analyzing the applications carried out, the article presents how the Russian Federation governs its actions based on the theory of Reflexive Control (RC). Since the theory involves the Russian understanding of information, technical data, cognitive content and "information resources" are understood as technological and human. In this context, Strategic Communication (Public Relations, Public Diplomacy and Information Security Systems) has been the tool for applying the doctrine for a specific purpose. Here we describe the interaction of the RC with the Gerasimov Doctrine, the activities of Information Warfare, with the use of non-military measures, the use of Cyber Warfare, social media and contrasting it with "Controlled Chaos", all with the aim of ensuring Russian development and the social well-being of its population.

Keywords

Strategic Communication, Reflexive Control, Information Warfare, Influence Operations and Controlled Chaos

1. Introduction

One of the main objectives of the commander in war is to interfere with the enemy's decision-making process. This goal is often achieved through disinformation, camouflage, or another strategy. For Russia, one of these basic methods is the use of Reflective Control theory. This method can be used against human or machine "decision-making processors."

Reflective Control is defined as a way of conveying specially prepared information to a partner or adversary to persuade them to make a predetermined decision, desirable to the initiator of the action. [1].

Although the theory was developed a long time ago in Russia, it is still undergoing constant updates in the present day.

In this article, the military aspect of the Russian concept of Reflective Control and its role as a weapon in information warfare according to the Military Defense Doctrine of the Russian Federation will be presented.

2. Development

The nature of Reflective Control Theory (RC) exists much more than similar concepts of information warfare and information operations. In fact, it appeared in Soviet military literature 40 years ago. V. A. Lefebvre defined Reflective

*Corresponding author: ricardo@croce.ggf.br (Joao Ricardo da Cunha Croce Lopes)

Received: 15 May 2025; **Accepted:** 3 June 2025; **Published:** 25 September 2025

Control as "a process in which one of the opponents conveys the other reasons for decision-making" [1].

The development of the theory of Reflective Control went through four periods:

1. Research (from the early 1960s to the end of the 1970s).
2. Guided practice (from the late 1970s to the early 1990s).
3. Psychological/pedagogical performance (from the beginning in the mid-1990s).
4. Psychosocial Action (since the end of the 1990s).

The Soviet and Russian armed forces have long been exploring techniques of using reflective control theory (especially at tactical and operational levels) as disguise (deception) for disinformation purposes, as well as to manage the enemy's decision-making processes. For example, the Russian army already had in 1904, the military camouflage school. In 1929, this School of Disguise laid the foundation for the concept of camouflage and created guides for future generations (Maskarovka).

Reflective Control is also seen as a means of information warfare. For example, Major General N. I. Turko, a professor at the General Staff Academy of the Russian Federation has established a direct link between information warfare, operations and RC.

He noted that the most destructive manifestation, in the tendency to rely on military force, is due to the possible impact of the opposing party's Reflective Control, through the proper development of the theory and practice of information warfare, which is more significant than the direct use of military warfare.

Turko believed that Reflective Control is the most important information weapon for achieving military objectives than traditional "firepower". This view was shaped in large part by his belief that the American use of information weapons during the Cold War did far more to defeat the Soviet Union than any other weapon, as well as being the source that caused the collapse. Finally, Turko mentioned reflective governance as a method to achieve geopolitical superiority and as a means of managing military negotiations, an area that should be more recognized by countries entering such negotiations with the Russians.

By definition, Reflective Control occurs when the governing body transmits a controlled system of motives and grounds that will serve as an excuse to arrive at a desirable solution, but the real intentions are kept in absolute secrecy [2].

The "Reflection" Encourages certain processes to simulate the reasoning of an enemy or to simulate a possible behavior of the enemy, forcing him to decide unfavorable to him. In fact, the enemy arrives at a solution based on the representation of the situation he shaped, including the location of detachments and structures on the opposing side, as well as the known intentions of the opponents.

The initial ideas for decision-making are formed primarily based on intelligence, other data, and factors that are based on a sustainable set of concepts, knowledge, ideas, and ultimately 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 data, and so on.

In military decision-making processes, the "human-machine-assisted" process is more prevalent. Currently, automated decision-making systems only by machines are still approved (Kott 2015). The adversary may try to influence the human being; and, by another process, the opponent tries to influence the machine.

In all decision processes, the importance of recurrent information collection and evaluation is emphasized, as well as a comprehensive approach, to allow planners to create Lines of Action (LoA) for their executions, as well as models for the LoA of adversaries. In this way, the Lines of Action are mostly based on intelligence and information provided by various Situational Awareness (CS) systems, weapons systems and the like. Thus, decision-making processes rely 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 hinder 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, the machine, or both. The Russian RC acts in both 02 (two) processes – Human and Human assisted by machine.

The main task of Reflective Control is also to explore the morality, psychological and other factors, 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 reflective control is used, the party with the highest quality of "reflection" (better able to mimic the other side's thoughts or predict their behavior) will have better chances of winning.

The quality of "reflection" depends on many factors, the most important of which – analytical skill, general erudition, the sphere of knowledge about the enemy and experience. The military author Colonel S. Leonenko [3]. He added that in the past, strategy was the main tool for reflective control, but today "tricks" and camouflage have replaced the method.

While formal or official Reflective Control terminology did not exist in the past, opposing parties actually used it intuitively when they tried to identify and collide with each other's thoughts, as well as plan and change their impressions of themselves, provoking a wrong decision.

If successful, the RC on the enemy allows it to influence military plans and situational awareness, as well as its actions. Thus, Reflexive Control focuses more on the less tangible subjective element of "military art" than on the more objective "military science."

Achieve Successful Reflective Control It requires a deep study of the enemy's "inner nature," ideas, and concepts; Leonenko described them as a "filter" through which all data

about the outside world passes. A successful Reflective Control represents the culmination of an information operation.

2.1. Reflective Control Breakdown

The history of the concept of reflective control (CR) stems mainly from the work done by Vladimir Lefebvre from 1963 to 1967 in the Soviet Union. After the publication of two works Конфликтующие структуры [4] – Conflicting structures e Алгебра конфликта [5] – Algebra of Conflict, Lefebvre's work became the subject of a classified KGB report in 1968. Lefebvre's main work (1984) is entitled Reflexive control: the Soviet concept of influencing an adversary's decision-making process [6].

Successful reflective control processes are based on the Soviet (and now Russia's) system, ethical legacies that are very different from those of the "Christian" West, in that Russians have a particular understanding of what constitutes "truth."

According to Lefebvre, the concept of vranyo (вранио) refers to the "dissemination of untruths that have some basis in reality" (Similar to verisimilitude).

Lefebvre defined the Reflective control as being "a process in which one of the opponents transfers to the other the grounds for decision-making" (Lefebvre 1984). In other words, there is a substitution of the opponent's motivation factors to encourage him to make decisions that are unfavorable to him.

To the Armed Forces of Russia, Reflective control (RC) is the term used to describe the practice of pre-determining an opponent's decision in your favor, Changing key factors in the opponent's perception of the world [7]. The term is mainly found in the discussion of information warfare techniques. In this context, the practice represents a key asymmetric enabler for gaining critical advantages by neutralizing the adversary's strengths, causing him to choose harmful courses of action and other Russian objectives.

With the exploration of 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 media, troll factories, and bot networks, while pushing anti-US, anti-NATO, and anti-elite narratives, are part of this policy.

The application of the Reflective 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 Control object.

Or Control Subject (Russian) takes steps to provide the Control object information that reflexively leads to action in the interest of the Control Subject (Russian).

Rather than denying information entirely, or providing false information, the intent of reflective control is to manipulate the information available to the public. Control object (target) so that they use this information to make a reflective decision in the interest of the Control Subject.

Example: Actual Situation --> Control Subject X Control Object = Attitude 01

Real situation + the idea of the controller directing to change the decision cycle --> influence messages by verisimilitude to the real situation. (targeting the desirable scenario) = Desired Actual Situation --> Control Subject + Control Object = Attitude 02.

(vide Appendix Nr 1).

As mentioned earlier, decisions are made through a fair, objective, accurate approach based on information relevant to the situation, Influencing the Approach, the situation changes.

Healthy Analyzed attitudes, knowledge, and skills in order to determine critical thinking, decision-making, predictive judgment (and prospective), problem-solving, creativity, openness to experience, and other leadership behaviors.

According to the attitudes analyzed, the competencies of Inference, Recognition of assumptions, Deduction, Interpretation and Evaluation of arguments are measured.

From the score of each leader and/or target (public), is shaped to the persuasive action of reflective control.

2.2. Opinions of Military Experts: Ionov, Komov and Chausov

2.2.1. Major M D Ionov

He wrote several articles on the topic of Reflective Control. He was one of the first military theorists to assess the importance of Reflective Control. The concept of "Reflective Control" wasn't in any Soviet military encyclopedia when he started writing in the '70s, so it just couldn't exist! As a result, in his early articles, Ionov talked about "managing the enemy" and not about Reflective Control.

At the same time, Ionov also understood the close relationship between advertising and Reflective Control and the need to combine the use of reflective techniques to organize Reflective Management [8].

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

1) Applying Pressure by Show of Force. Such a show of force can be exercised in various ways that extend across different aspects, from diplomatic or economic pressure, such as the threat of economic sanctions, to threats of military action, such as increasing the combat readiness of the armed forces or provoking declarations of war.

Translated from Russian: Power pressure, including the use of superior force, show 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 intelli-

gence, provocative maneuvers, weapons testing, restriction of enemy access or isolation of certain areas, increased combat readiness of the armed forces, coalition building, official declaration of war, support for the destabilizing situation of the internal forces, disabling individual armed forces, "pumping" and publicizing victory, demonstrating ruthless actions, and showing mercy to an enemy ally who has stopped resisting.

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 there is, in fact, a weakness and vice versa, as well as the use of Trojan horse techniques.

Translated from Russian: Methods of providing false information about the situation, including camouflage (showing weakness in a strong place), creating false structures (showing "strength" in a weak spot), leaving one position to strengthen another, leaving dangerous objects in that position ("Trojan Horse"), concealing true relationships between units or creating false ones, keeping the secrecy of new weapons, bluffing about weapons, change the methods of operation or the deliberate loss of documents.

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

Translated from Russian: Provoking the enemy to find new directions of escalation or ending the conflict: a deliberate demonstration of a special chain of 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 encirclement, forcing the enemy to commit punitive actions leading to the expenditure of the armed forces, resources and time.

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 adversary to focus on another area of conflict to slow down the reaction.

Translated from Russian: Impact on the algorithm of the enemy's decision-making, 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; Actions in a backup manner to act to neutralize the enemy's operational thinking; change the timing of a decision that may be made through the sudden outbreak of hostilities; Convey information about the situation of a similar conflict - Working on what appears to be feasible and predictable, the enemy makes an ill-considered decision that will change the path and nature of his operation.

By Ionov, it is necessary to evaluate the human goals for the Reflective Control of a person or group, taking into account individual or group psychology, way of thinking and professional level of training.

2.2.2. Colonel S. A. Komov [9]

A Russian military theorist wrote about the informational impact of Reflective Control, and he was possibly the most prolific author on the subject of information warfare in the 1990s. In the pages of the magazine "Military Thought" Komov supported the meaning given by Ionov to Reflective 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:

1. Distraction (Attention Deviation) – creating a real or imagined threat to one of the enemy's vital dislocations (flanks, rear, etc.) During the preparatory phase of hostilities, forcing him to reconsider the common sense of his decisions).
2. Overload (at the expense of large amounts of conflicting information often sent to the enemy).
3. Paralysis (creation of perceptions of special threats to vital interests or to the weakest points).
4. Exhaustion (forcing the enemy to perform useless actions and thus depleting the armed forces).
5. Deception (provoking the enemy to redeploy his forces to the threatened region during the preparatory stages of hostilities).
6. Division (convincing the enemy that he must act against the interests of the coalition).
7. Calm (forcing the enemy to believe that pre-planned operations are being trained instead of preparing for offensive actions – and thus reducing their vigilance).
8. Intimidation (creating an irresistible perception of superiority).
9. Appeasement (through decreased vigilance and the creation of the illusion of conducting planned training and not preparing for offensive actions).
10. Provocation (imposing data on the enemy so that he performs beneficial actions by your side).
11. Proposal (offering information that touches the enemy legally, morally, ideologically or in other spheres) and;
12. Pressure (offering information that discredits the government in the eyes of the population).

2.2.3. Captain of the First Rank F. Chaucov

Finally, the article of the captain of the first rank F. Chausov continues to discuss Reflective 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 of that party corresponding to the information transmitted [10].

Chausov formulated the following principles of Reflective Control:

1) the principle of finality – the process must be goal-oriented, using the full range of necessary reflective control measures.
2) 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.

3) the principle of correspondence – the mutual consistency of objectives, place, time and methods of reflective control must be observed.
4) the principle of modeling – we must not forget to predict and model the actions and states of the opposite side during the execution of reflective control procedures.
5) The principle of anticipation – current events must be anticipated and anticipated.

And (+) Plus risk assessment → the essence of which boils down to the danger of making a mistake in the event of an incorrect assessment of the consequences. With this approach, the maximum risk will be if the enemy unravels the plan by himself.

2.3. The RC on 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 those countries, preventing NATO and the EU from expanding, as well as to protect Russian interests and ethnic minorities abroad.

In the same period, Western analyses of Russia's conflicts focused on the different forces Russia used to achieve its objectives: cyber forces in Estonia, conventional forces in Georgia, and special operations forces (SOF) in the Crimea area of Ukraine.

Western military experts were especially interested in the operational teachings of the Armed Forces of the Russian Federation and how they complemented their conventional military assets with SOF, transport, naval infantry and with rapid reaction forces. Others have also speculated how Russia would use cyber assets in future conflicts. However, most of these studies has a limited scope with only a focus on the Hard power military. Also, most of them are based on Western assumptions about the Russian mode of war, using military means within traditional domains of air, sea and land, expanded with the new cybernetic domain. In reality, the FAFR changed its war doctrine in an Operating Concept to achieve the objectives of its policy abroad.

In 2003, Russia launched a "White Paper" in support of this new policy that described a shift in military thinking and defined a new operational concept based on the integration of strategic, operational and tactical elements. The concept has been updated with lessons from the Estonian and Georgian conflicts. It is characterized by the use of non-military means and non-traditional domains such as youth groups Partizans, cyberattacks, 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 enemy's command and control, in addition to total cyber dominance.

This section details this New Doctrine (NDG), as well as describes the Russian operational framework and its links with Information Warfare activities, military concepts, and strategic positions, followed by a brief example of the application of the new doctrine in the 2014 Ukraine (Crimea) conflict.

The main objective is revealing tactical and operational level actions (Reflective Control and Strat Com Activities) of the New Doctrine (NDG) and the cumulative effects and goals that these actions need to achieve to gain a better understanding of the new Russian operational concept.

2.4. The Russian Approach to a Conflict

In February 2014, the Chief of Staff of the FAFR, General Valery Gerasimov, described in his article "*The value of science in foresight*" [11], the new operational concept based on the lessons of the Estonian and Georgian conflicts (Figure 1).

Brig. Gen. Gerasimov explained that the FAFR developed unique situational planning models to apply military and non-military means, such as SOF, forces "*proxy*", civilian media and cyber capabilities to influence all actors, disrupt communication, and destabilize regions in order to achieve their goals. Although the article describes Gerasimov's thoughts on means, phases, and broad actions (forms) used in the new operational concept, it does not depict the effects and objectives that the FAFR want to achieve with these actions, nor does it portray how the FAFR uses social conditions to support them, which will be described here.

During the Estonian, Georgian and Ukrainian conflicts, Russia established civilian capacities such as youth groups and state media and mobilized ethnic Russian minorities abroad, appealing to feelings of marginalization, a sense of self-worth 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 desperation from the military and political leadership of the targeted countries, after which these countries were willing or forced to accept the new situation created by Russia.

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

The Gen Gerasimov described the current framework of the Russian operational concept as the use of "All Non-Military Methods in Interstate Conflict Resolution".

It incorporates six phases as shown in figure 1: covert origin, escalation, outbreak of conflict activity, crisis, resolution, and ending with the restoration of peace.

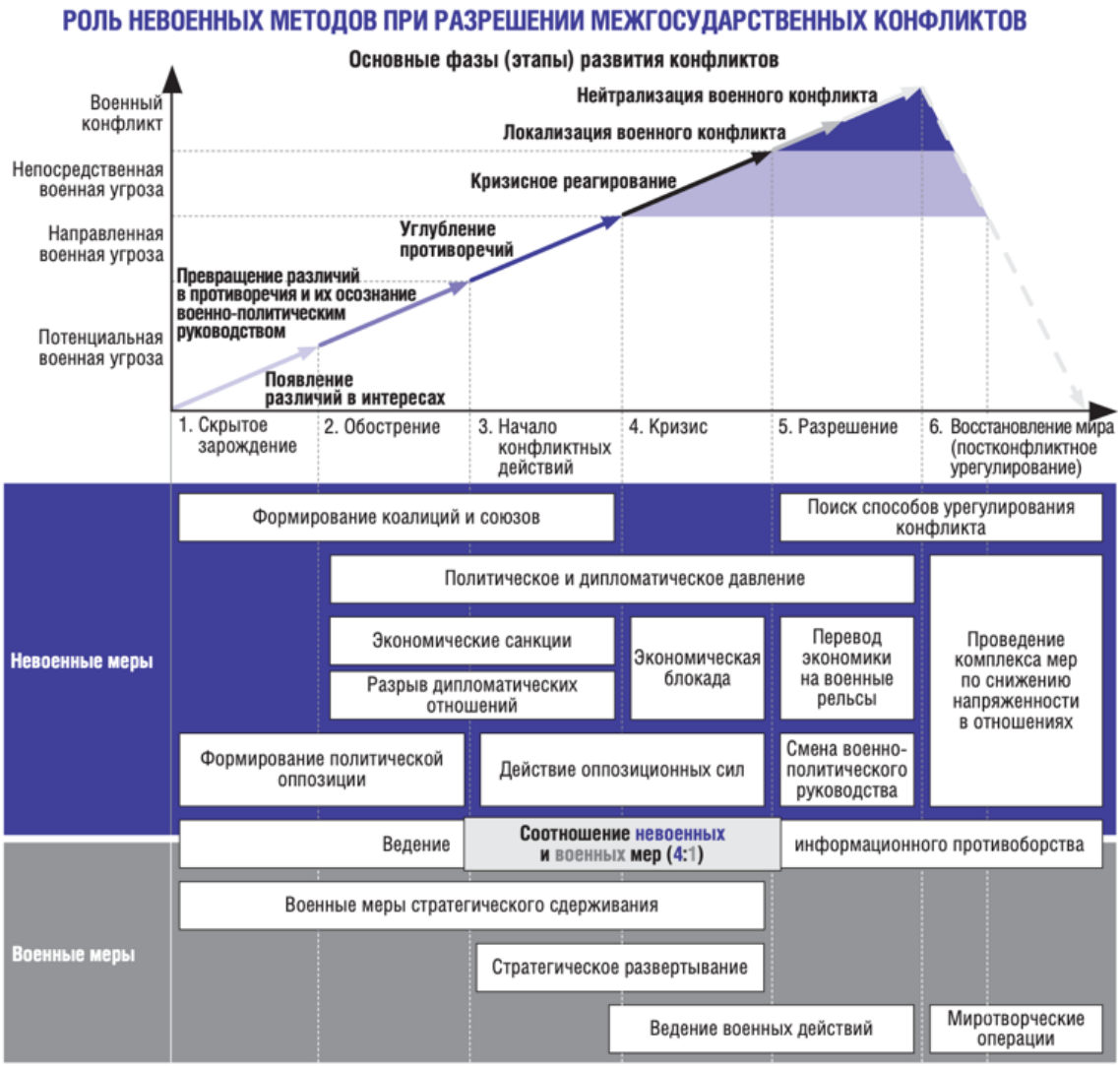

Figure 1. *The role of non-military methods in the resolution of interstate conflicts.*

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

The New Doctrine (NDG) has not evolved in a vacuum during the last decade, but it is a twofold reaction to the events that unfolded after the collapse of the Soviet Union.

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

Finally, the Russian operational art relies on the occultation, also a reflective control technique, divided into two levels. The concealment of the operational level concerns the measures of "manner to achieve operational surprise and was designed to disorient the enemy regarding the nature, concept, scale, and timing of impending combat operations." And the strategic-level concealment is "activities that surreptitiously prepare a strategic operation or campaign to disorient the enemy from the true intentions of the actions."

The 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 to direct and organize in which operations are a chain of efforts throughout the depth of the area of operation, with principles of shock,

speed, efficiency, mobility, simultaneity, technological support and a decisive moment in the final phase. Gerasimov added to Isserson's notion the Implementation of asymmetric and indirect actions by civilian/military components, Special Operations Forces and Technical Weapons 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 otherwise), Spetsnaz fighters and Cossacks to conduct different types of operations, such as unconventional, intelligence, psychological and cyber operations, as well as assistance to security forces and Strategic Communication. Russia manages these military and non-military assets through state-controlled companies and organizations under a centralized political command structure. This structure, coupled with the fact that the forces employed consist of a mix of ethnic Russians and Russians abroad, cause Russia to not only exploit social conditions but also cultural and linguistic factors in the former Soviet states and at home to create “Extraterritorial forces”. Studies behavior and demographics of all potential opponents to reveal advantages that you can exploit to achieve your goals.

2.5. Detailing the Use of the Gerasimov Doctrine

For a complete understanding of the Doctrine, we will address the Operational Art in 07 (seven) phases, that is, 01 (one) more than the one presented by Gen. Gerasimov, aiming to present the total of the actions of Estrt Com / Reflexive Control of the NDG.

The detailing must be accompanied by the support with the figure contained in the Appendix Nr 02.

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

Three (3) fields of action are delimited: Military Measures (at the base), Non-Military Measures (in the center) and Information Warfare (at the top).

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

The description of the detailing is addressed, within the temporal phase, from the bottom to the top, presenting the triggering of actions within each field. (Main Text Paragraphs).

2.5.1. Phase 0 – Early Preparation

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

Non-Military Measures – Minorities are "activated" or created, there is also the activation of the "Nashi Forces", partisans or Cossacks, as well as the PMCs aiming at future support. Economically, contracts are made between companies interested in the area, mainly infrastructure companies, as well as the co-optation of elements of the Elite in the target area, through financial corruption.

Information war – The networks, backbones and cyber infrastructure are updated, initiating actions to enable the superiority of the internet and media. The operational objective is the local domain of information. The actions of Estrt Com/RC triggered vision the Suggestion and the Deterrence. The suggestion is directed to minorities and mistakes of the local government (generation of enmities). Deterrence aims to hide strategic displacement, as well as to convey the idea of "lost cause".

By way of example, the early preparation phase for the conflicts in Georgia, Ukraine and Estonia began in 1991, when they all became independent and separate states of the Soviet Union. In Georgia, tensions began immediately in 1991 over 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 closely related to the areas north of them, within 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 on 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 the 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 a pipeline alongside Russia. In most cases, Russia has 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.

2.5.2. Phase 1 – Secret Origin

Military Measures – In this phase, the sustaining forces are structured, with support from the GRU, aiming at the formation of Local Forces, EMP and foreign volunteers (Proxy Forces) for the Escalation phase. Situational awareness reconnaissance and monitoring activities continue, as well as strategic deployment and military exercises in the border area. At the tactical level, the movement of strategic deterrent means (Def Air Def, GE and Missiles) is already observed.

Non-Military Measures – Financial support for co-optation activities of "loyal to the cause" is increased. From the formation of minorities (with or without ethnic descendants), training actions and the establishment of areas of operations are triggered (including the study and validation of key areas for "area denial"). The actions of the Nashi (civil support in all fields) and business interests. Strong work in the formation of political opposition is executed. The operational objective is the formation of alliances and/or a coalition, as well as to gradually "weaken" diplomatic relations.

Information War – At this stage, the Russian operational concept, for external media, is that of "Military Danger". That is, that the actions of other interested parties can militarily affect the target area, aiming to give freedom of action to Russian military use. The strategic political positioning is the dissemination in traditional media. Wither/RC activities are intensified with the objectives of Provocation, Distraction, Information overload in the internal systems of the target area and increase the degree of Deterrent.

2.5.3. Phase 2 – Escalation

Military Measures – Efforts remain in subversive measures, support the sustaining forces in the target area, monitoring situational awareness (with Prio for Intel, EW, Air Def, Ciber) and the means of strategic deterrence are already in place. In this phase, the first PMCs appeared on the ground, mainly for logistics and support for civilian activities (health and peacekeeping covered). The most identified differential is the disposition of military resources in DTAs in the vicinity of the border, carrying out maintenance activities for military exercises. The Min Def Train Force is widely employed for logistics.

Non-Military Measures – In this phase, the first manifestations and actions of civil unrest are identified. The training of local non-military forces and foreign volunteers is already in a position to be employed. 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 number of (planned) demonstrations. The support of force Nashi it 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 leadership in the target area.

Information War – The Russian concept of "Indirect Threat" is worked to exhaustion. That is, that the actions of the civilian population must be supported, and any movement of military means is considered a threat. Before the international community, the strategic position adopted is to disseminate the image that political leaders and institutions are inoperative in the target area, needing "help" to control the "chaos". At this stage, cyber forces are already structured and begin activities across the C2 spectrum, critical infrastructure, and decision-making process. Estrt Com/RC actions are mainly directed to Pressure, Deception, Division, Overload and Justification, aiming to increase freedom of action and increase controlled chaos in the target area. With the objective 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 Ukraine conflict

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. Russia argued that it was an illegal act, as Ukrainians had not followed the impeachment process as described in Ukrainian law. 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 from Russians abroad to justify an intervention, again in reference to Western arguments to validate NATO's 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 at the heart of phase one and two: strategic communication. Television and the 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 Crimea's population gathered their news from the Internet, and 70% of Crimea's Internet users rely on their newsgathering on the top two available Russian social networking sites. Russians and Ukrainians analyzed sentiment information collected from the Internet, finding a score of 76% for pro-Russian sentiments in the region. In Russia, these numbers were comparable; More than 75% of the population trusts their state-run media. 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 claim that Russia established the information domain in the first phase of the New Doctrine (NDG) – 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 were part of the government's comparison with Nazi Germany. This theme remained throughout the conflict. Russia has also accused Western media of oversimplifying demographic maps, signifying eastern and southern Ukraine as predominant ethnic Russians. Meanwhile, diplomatic channels and Russian leadership have begun to emphasize the same issues of marginalized Russian minorities seeking reunification with Russia.

To prevent NATO and the EU from helping Ukraine, Russia has intensified its information campaign. Russian media have used past events for conspiracy aimed at shaping the EU's perception of Ukraine as an unreliable partner. To this end, Russia has made many public statements about Ukrainian violations of the Russian-Ukrainian agreement on energy

revenues and rights related to the gas pipeline transiting through Ukraine. The messages further softened the EU's already divided response, resulting in a temporary isolation of Ukraine. On February 12, leaders of pro-Russian organizations in Crimea met to discuss the future of Crimea and decided to support Russia. The Russian Consulate in Crimea began issuing Russian passports to all Crimean inhabitants in the same week to create a Russian majority on the peninsula. Finally, on February 14, a cyberattack emerged, targeting one of the largest banks in Ukraine, attacked by malware, aimed at supporting the unrest in the country and portrayed as one of the non-military means in Appendix 02.

2.5.4. Phase 3 – Beginning of Hostilities

Military Measures – Area denial measures (dispersion of means) and strategic deployment within operational range are established. The activities of the escalation phase are maintained, but with the objective of triggering the opposing side so that it reacts wrongly to a predetermined action (argument for self-defense). Actions to control the electromagnetic spectrum and the use of drones stand out.

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 the Proxy Forces, being called Vital Territory. These are infrastructure facilities, media facilities, neighborhoods located in the main DTAs, etc. The "Green Men" can be observed, usually EMP security for NGOs partizans humanitarian aid.

Information War – The Russian concept of "Military Threat" is worked with a focus on the military assets of the target area (The defense forces attack their own people). Military actions on the civilian population, humanitarian aid or on some Russian military means is considered a threat. Before the international community, the strategic position adopted to disseminate the image that political leaders and institutions are inoperative is maintained, but the contradictions are intensified, especially by diplomatic means. The antagonisms, dissent, and internal enmities of the target area are exacerbated. The actions of Estrt Com/RC in this phase are directed to two aspects: 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 Estrt Com/RC system often operates in a public-private partnership with Russian oligarchs or businessmen, as well as through the co-optation of "independent" hackers by intelligence agencies. The strategy is feeding existing resentments, stereotypes and vulnerabilities. Any actor that weakens dominant systems and helps undermine trust in the democracies of the target area is welcomed as a partner.

Activities in the Ukraine conflict

Local paramilitary forces and Cossacks stormed the parliament and replaced it with pro-Russian ones, led by Sergei Aksyonov. While pro-Russian sympathizers have seized more key installations in Crimea, volunteers from Russia have come to their aid and a strong Russian army of 40,000 troops has begun 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-Ukrainian sympathizers. From 28 February, the militants occupied military installations, airfields, regional media and telecommunications centers. They shut down telephone and internet communication in Crimea as more planes with new troops landed at seized airfields. It is this combination of unconventional warfare by special operations forces and proxy forces, along 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.

For provocation or deterrence/pacification to work, the government needs to be more or less isolated, burdened with disinformation as depicted in the center of Appendix 01. Therefore, the militants blocked radio and mobile phone traffic to further isolate Crimea from Ukraine. The Russian-coordinated cyberattacks 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 have hampered the leadership of NATO and Ukraine, but they have not led to isolation or overwhelm. The United States convened a U. N. mission to the region in March; Russia refused. Instead, Prime Minister Aksyonov of the autonomous Republic of Crimea, along with former Ukrainian President Yanukovych, called for a Russian intervention on March 1 and an independence referendum on March 30.

2.5.5. Phase 4 – Crisis

Military Measures – The same measures are maintained as in the phase of the beginning of hostilities. However, the logistics for military means are increased, according to the time planning of the 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 in the border strip (self-defense action and reaction).

Non-Military Measures – The Proxy Forces begin their most notorious activities with successive attempts to dominate areas of interest with the operational objective of controlling the target area. Subversive actions can be unleashed in certain places (radio antennas, etc.), but always recognized as "acts of sabotage" by partisans. In the political area, negotiation scenarios are presented. However, with targeted EFD.

Information War – At the beginning of this phase, actions are triggered for the economic isolation of the opponent. The Estrt Com/RC measures of the previous phase are maintained, but the focus is directed to the political paralysis of the op-

ponent, aiming at the operational objective that should be felt until the phase of armed conflict.

Activities in the Ukraine conflict

The crisis began when paramilitary and Cossack forces attacked Ukrainian military bases. In some cases, Ukrainian forces surrendered, while in others paramilitary and Cossack forces had to use more force, supported by the so-called "Little Green Men". These "Little Green Men" were well armed, well trained, wore uniforms and masks, and had no military emblems on their uniforms. They would not speak to the media or reveal their identity. While Russian officials commented on many events in the conflict, they were consistently silent on sensitive issues, namely the presence of Russian soldiers in Crimea.

With the Crimean government all but removed, the effects of reflexive control such as distraction, pressure, suggestion, and isolation (local) were successful. Russia has never been able to isolate the Ukrainian government, however, as the Western support for this government Decreased during the conflict and the EFD was achieved.

2.5.6. Phase 5 – Military Activities (Armed Conflict)

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

Non-Military Measures – Actions on the opponent's infrastructure by the Proxy Forces are intensified. The operational objective sought is the control of the vital territory. Military economy actions (blocking imports, breach of contracts, etc.) are triggered aiming at the isolation of the replacement of the opposing MATE. In the diplomatic area, the pressures for validation of the intended scenario remain. Accusations of corruption, loss of image, discredit, 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 from contractors for reconstruction are signed.

Information War – The strategic positioning sought is aimed at increasing any and all freedom of action. The operational objectives of political isolation, perception of despair and acceptance of terms are incessantly pursued. In Estrt Com/RC the military aspect is maintained, and the political aspect is directed towards the Deception and Distraction of the decision-making process. Before public opinion, the proposed scenario is presented and worked hard to accept it. The message of restructuring the area with the employment of companies and support for the local population is the focus. Themes such as the protection of the environment and the protection of local cultural heritage assets are raised. The performance of entrepreneurs in the communication area is requested. However, in combat areas, all physical or informational access, from any media, is controlled. The monitoring of the theme on social media is heavily executed. As well as the control of public opinion is monitored.

Activities in the Ukraine conflict

Next 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 Kiev. 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 surrendered their bases, in many cases to join the Russian forces. The "Little Green Men" isolated Ukrainian forces in their bases and then used the internet and local media to initiate military operations in support of information, media campaigns, and intimidation in combination with bribery.

Fighting was identified in the eastern region of Ukraine, more precisely near the "Oblast" of "Donbass".

On 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 on the Crimean area did not take place. 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 Kiev government admitted that the local police and armed forces in Crimea were corrupt, sympathetic to the uprising or had low morale. Then Russian agents of influence penetrated local intelligence and security forces. Together, the lack of communications and support to the bases led to the tactical and eventually operational isolation of Ukrainian forces in Crimea and their perception of despair. On the other side, the "Little Green Men" remained disciplined. They did not reveal their identity and dealt with the skirmishes, not escalating them into a conventional war.

2.5.7. Phase 6 – Peacemaking and Signing of Treaties

Military Measures – The withdrawal of part of the forces employed begins, leaving them in the target area EMP for the formation of self-defense forces. Troops from the Military Police, CBRN, GRU, SOF, FSB and Air Def stand out. Subsequently, if there is an annexation, FAFR troops will be deployed.

Non-Military Measures – Actions to remove foreigners and catalog the population are undertaken. Civil-military partnerships for reconstruction begin activities. Political organization and essential services are worked on, and routine activities are supported.

Information War – The strategic positioning sought is to maintain any and all freedom of action to accept the terms. The operational objectives of political isolation and acceptance of terms are incessantly pursued. Themes of pacification of hostilities and return of economic activities are worked on. Estrt Com/RC is aimed at the pacification of the target area, with the opening of places for visitation, inaugu-

ration of furniture enterprises and the encouragement of cultural tourism.

Activities in the Ukraine conflict

In April 2014, Russia admitted that the "Little Green Men" were actually FAFR Spetsnaz and Airborne troops. On March 16, Crimea held the referendum for independence ahead of schedule and 96.77% voted for a reunification with Russia (the turnout was 83.1%). The Duma the Russian parliament (parliament) signed a treaty on March 18 formally incorporating Crimea into Russia, beginning the sixth phase, the restoration of peace. The conflict remains frozen.

3. Conclusions

The current Russian operational concept uses military, and non-military means that engage simultaneously and rapidly in all physical and information domains, through the application of asymmetric and indirect actions. Russia mitigates the capabilities of adversaries, creates chaos, seizes 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 the 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 disseminate reflexive control. The culminating psychological effects of the reflective control approach, such as disorientation, suggestion, and concealment, need to outweigh provocation. In the end, it will cause exhaustion, paralysis and a perception of despair among the political and military leadership. These credible perceptions and misperceptions create the lead for the final phase of the New Doctrine (NDG): Non-combat resolution.

The evolution of the New Doctrine (NDG) and its framework is not over, as the Russian operational framework is anything but a fixed set of means and strategies. The Russian leadership may develop and employ new types of asymmetric means, depending on the situation at hand.

In General Gerasimov's opinion, each conflict has its 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 Russia's physical means, but, more importantly, to recognize the phases discussed and predict the desired effects of the opponent.

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

Studies on the use of Strategic Communication combined with Reflective Control should 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 (*Defense*) and Psy-Group in the democracies of Australia, India, the Philippines, Kenya, Malta, Malaysia, Romania, Trinidad and Tobago, Nigeria, the United States, and the United Kingdom (case Leave. EU), which have modern features of the use of reflexive control (maybe not by the Russians).

Abbreviations

Air Def	Air Defense
CBRN	Chemical, Biological, Radiological and Nuclear
DTA	Tactical Direction of Action
EW Recon	Electronic Warfare Reconnaissance
FAFR	Armed Forces of the Russian Federation
FSB	Федеральная Служба Безопасности Российской Федерации - ФСБ / Federal Security Service of the Russian Federation
GRU	Гла́вное разве́дывательное управле́ние - Main Intelligence Department DoD RU
LoA	Lines of Action
NDG	New Doctrine - Gerasimov
PMC	Private Military Company
RC	Reflective Control
SA	Situational Awareness
SOF	Special Operation Force
Strat Com	Strategic Communication

Acknowledgments

For this article there is no acknowledgement of contributions or thanks.

Author Contributions

Joao Ricardo da Cunha Croce Lopes is the sole author. The author read and approved the final manuscript.

We kindly recommend referring to *CRediT Taxonomy* (https://credit.niso.org/) for the detailed term explanation.

Funding

This work is not supported by any external funding.

Conflicts of Interest

The author declares no conflicts of interest.

Appendix

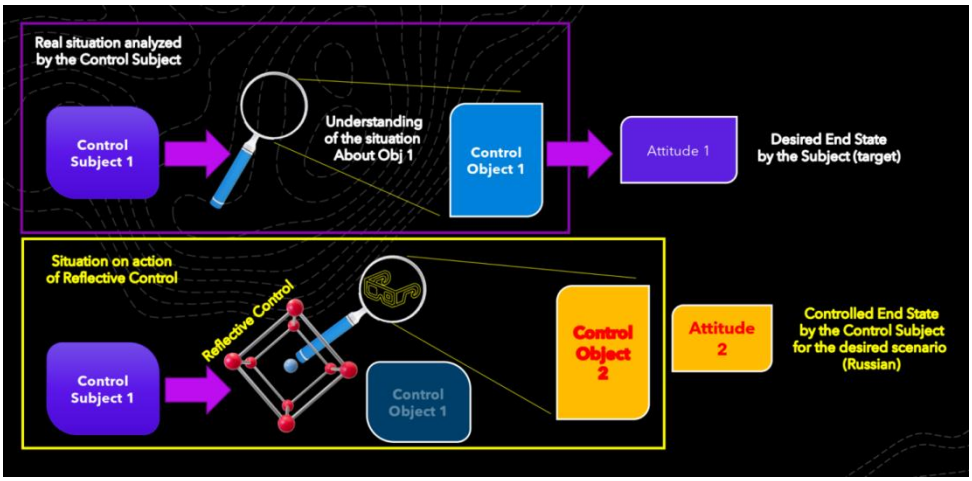

Figure A1. *Reflexive control image.*

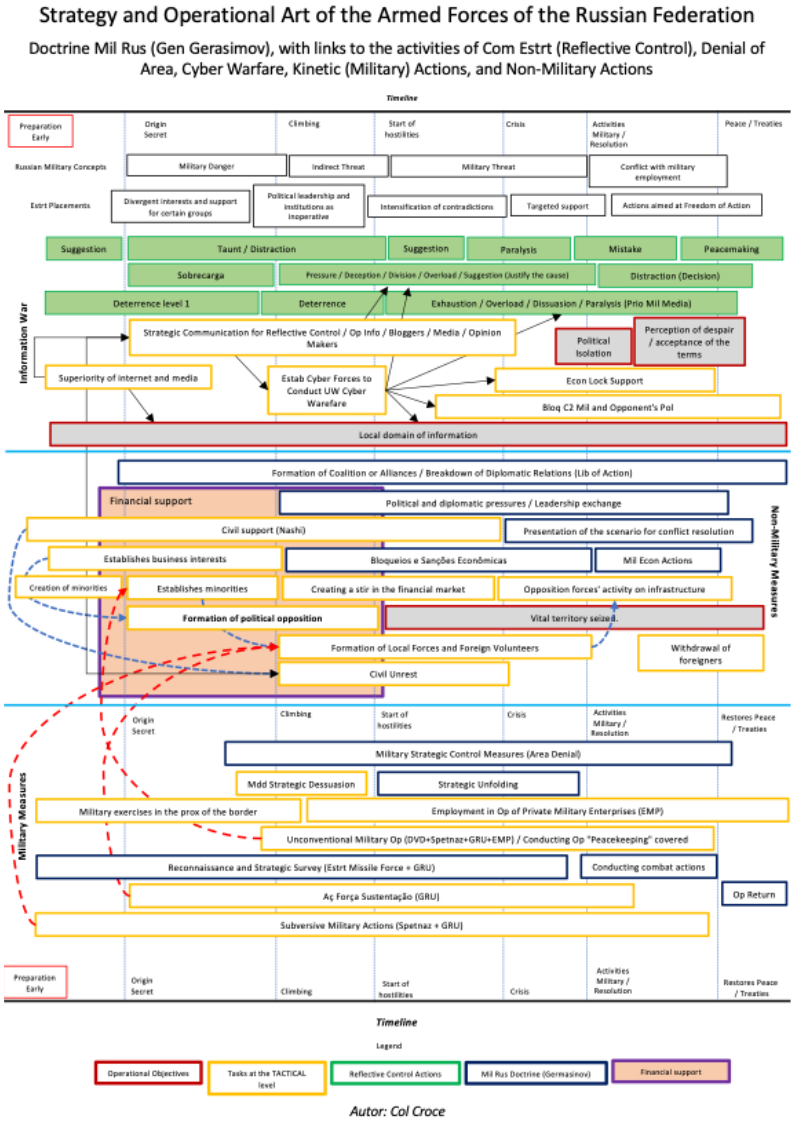

Figure A2. *Strat and Op Art AF RF.*

References

[1] Владимир А. Лефевр, "Рефлексивный контроль: советская концепция влияния на процесс принятия решений противником", (Москва: Научные приложения, 1984). Vladimir A. Lefebvre, "Reflexive Control: The Soviet Concept of Influence on Enemy Decision-Making" (Moscow: Scientific Applications, 1984).

[2] Turko N. I., Modestov S. A. Reflective Management of the Development of Strategic Forces as a Mechanism of Contemporary Geopolitics / Systems Analysis on the Threshold of the 21st Century: Theory and Practice" Moscow, February 1996, p. 366.

[3] Леоненко С. Рефлексивное управление противником // Армейский сборник. No 8. 1995. Leonenko S. Reflexive control of the enemy/Army collection. No. 8. 1995.

[4] Лефевр В. А. Конфликтующие структуры. М.: Высшая школа, 1967. Lefebvre V. A. Conflicting structures. Moscow: Higher school, 1967.

[5] Лефевр В. А., Г. Л. Смолян. Алгебра конфликта. 4" е. изд. М.: Книжный дом «Либроком», 2010. Lefebvre V. A., G. L. Smolyan. Algebra of Conflict. 4" e. ed. M.: Book House "Librokom", 2010.

[6] Лефевр В. А., Г. Л. Смолян. Алгебра конфликта. 4" е. изд. М.: Книжный дом «Либроком», 2010. Lefebvre V. A., G. L. Smolyan. Algebra of Conflict. 4" e. ed. M.: Book House "Librokom", 2010.

[7] Владимир А. Лефевр, "Рефлексивный контроль: советская концепция влияния на процесс принятия решений противником", (Москва: Научные приложения, 1984). Vladimir A. Lefebvre, "Reflexive Control: The Soviet Concept of Influence on Enemy Decision-Making" (Moscow: Scientific Applications, 1984).

[8] Ионов М. Д. Психологические аспекты управления противником в антагонистических конфликтах (рефлексивное управление) // Прикладная эргономика. Специальный выпуск. 1. 1994. Ianonov, M. D. Psychological aspects of enemy management in antagonistic conflicts (reflective management) / Applied ergonomics. Special edition. 1. 1994.

[9] Комов С. А. О способах ведения информационной борьбы // Военная мысль. No. 4(7-8). 1997. С. 18-22. Komov S. A. On the Ways of Information Warfare / Military Thought. No. 4(7-8). 1997. p. 18-22.

[10] Чаусов Ф. Основы рефлексивного управления противником // Морской сборник. No 1. 1999. Chausov F. Basics of Reflective Control of the Enemy Collection. Navy. N1. 1999.

[11] Валерий Герасимов, 'Ценность науки в ожидании. Valery Gerasimov, 'The Value of Science in Anticipation'. VPK news, 27 February 2014. Accessed July 26, 2017, http://www.vpk-news.ru/articles/14632

Biography

Joao Ricardo da Cunha Croce Lopes is a Colonel in the Brazilian Army. He holds a Master's degree in Military Sciences (2011) and Military Operations (2003). Expert in intelligence, GEOINT and information warfare, he has worked on the development of systems and the training of Brazilian and friendly nation officers. In the Army General Staff, he was the Brazilian representative in the MCDC (multinational Capability Development Campaign) and in the National Committee for the Security of Critical Infrastructures. Qualified in the Russian language, he was an instructor at the Military University of the Ministry of Defense of the Russian Federation in Moscow (2017). He currently works as a government and business consultant.

Research Field

Joao Ricardo da Cunha Croce Lopes: Decision support systems, Intelligence systems, Artificial intelligence development, Information operations, Information governance and security.