NOBODY: THE NAME BEHIND INFORMATIONAL BLINDNESS. THE RUSSIAN INFORMATION WARFARE IN UKRAINE

Adrian LESENCIUC*, Iasmina-Georgiana SAUCIUC*, Agata JAGIEŁŁO-TONDERA**

*Department of Fundamental Sciences, Faculty of Air Security Systems, 'Henri Coandă' Air Force Academy, Brașov, Romania , **Military University of Technology, Warsaw, Poland

Abstract: *Under the guise of the name of Nobody that the cunning Odysseus chooses in his confrontation with the Cyclops Polyphemus, the current Russian information war in Ukraine has all the characteristics of disinformation by doctrinal dissimulation. The very concept of information warfare, borrowed from Western doctrines, covers a wider field of action, being operationally in line with the reflexive control theory inherited from the Soviet period. The tools, techniques and methods of Western information operations are no match for those engaged in Russian information warfare, because the Russian Federation is raising the stakes of this conflict from the hard power level to the springs of all forms of power, soft and hard: political, economic, symbolic and military, under a misleading name. This article aims to further investigate the forms of Russian doctrinal dissimulation by using concepts such as hybrid warfare (Lesenciuc, 2023) and to analyze the objectives, activities, targets and effects of Russian information warfare in the invasion of Ukraine.*

Keywords*: information operations; information confrontation; reflexive control; Russian invasion in Ukraine; doctrinal dissimulation*

1. INTRODUCTION. THE SEARCH FOR *NOBODY*

Ulysses, the king of the small island of Ithaca in the Ionian Sea, was called "Odysseus" by the Greeks – a name that can be translated as "the ugly one." He took part in the Trojan War as one of Helen's suitors and played a significant role in the conflict: acting, on one hand, as a mediator between Agamemnon and Achilles; on the other hand, bringing Iphigenia to Aulis to be sacrificed; infiltrating the city as a spy and negotiating Helen's betrayal of the Trojans; and, most famously, devising the wooden horse – the poisoned gift that would alter the course of the war. We shall not focus on these feats of war, most of which would now be classified as soft power actions in contemporary terminology, but rather on the moment, after his wanderings at sea, when – upon reaching the land of the Cyclopes – he managed to deceive Polyphemus, blinded his single eye, and left him lost in the fog, searching for a culprit who had given his name as *Nobody*. (Οὖτις, in old Greek)

The search for *Nobody* has become symptomatic of confrontations in which the soft dimension – particularly the symbolic dimension of power – prevails, and in which deception, psychological operations aimed at influencing the adversary's will, and the informational exploitation of other domains – such as the cyber domain, for instance – are typical courses of action. The Machiavellian pattern of action, blending cynical practices of political influence (ugly practices, possible to associate them with pre-Machiavellian, Odyssean political cunning – implying trickery, deceit, lack of scruples, corruption, betrayal, etc.) with symbolic, economic, and above all military actions, necessarily involves dissimulation, starting with the simple act of naming. On the topic of doctrinal dissimulation in the use of the concept *gibridnaya voina*, seemingly similar to *hybrid warfare,* we elaborated in the study *Hybrid War or the Return to Absolute War through Doctrinal Dissimulation* (Lesenciuc, 2023). However, the distinction between the two terms became evident not long after the publication of the Gerasimov Doctrine (Gerasimov, 2013), through the works of Andrew Monaghan (2015), Mark Galeotti (2016; 2018; 2019), Ofer Fridman (2018), among others. Even though the concept of "doctrinal dissimulation" – which involves disinformation through the use of identical military terminology in differing doctrines, concealing divergent actions under the same label in order to achieve surprise – has not yet opened a distinct line of academic inquiry, numerous subsequent studies have noted the operational divergence projected within a

seemingly unified semantic field, including those of Anastasiya Filina (2023) and Lance Bokinskie (2024).

In *Hybrid War...* (Lesenciuc, 2019), we attempted to highlight what may lie hidden within a name – more precisely, the strategic potential embedded in the act of naming within doctrinal frameworks:

> As long as the symbolic forms through which disinformation-altered messages can be packaged require constant diversification – and such diversification is usually met with appropriate countermeasures on the battlefield, ultimately shaping a certain horizon of expectations – the Russian school of military thought has devised a solution aligned with the need expressed in the Gerasimov Doctrine: to maintain initiative in the confrontation with the American doctrine.
> However, this position at the forefront of global military thinking was not achieved through the concepts of information warfare, network-centric warfare, or even hybrid warfare.
> Its strategic priority lies in the appropriation and operational use of the doctrines of adversaries or potential adversaries (in any case, competitors in the field of *soft power*), with the aim of deception and disinformation (Lesenciuc, 2023:32).

Yet, although the effects of disinformation through doctrinal dissimulation are more pronounced in the case of the hybrid warfare concept than in that of information warfare, such an analysis of the information operations design remains worth considering.

Evidently, behind these acts of "informational blindness" stands *Nobody* – an entity without identity and, more importantly, without a name – who can thus appear under its true name on the stage of international relations without facing any consequences.

2. RUSSIAN INFORMATION WARFARE

2.1 Information warfare. The major transformations of recent years in the information environment, combined with battlefield experience and the lessons learned from recent conflicts, have elevated the concept of information operations to increasing importance within most doctrinal frameworks, particularly in NATO member states.

Throughout history, information has been a crucial and decisive pillar in the conduct of conflicts, representing a fundamental requirement in shaping the conditions for victory. As conflicts have evolved – driven by advances in military capabilities, technologies, procedures, and combat tactics – the communicational/ informational architecture of the battlefield has gained prominence, eventually becoming central.

Beginning with Operation Iraqi Freedom (2003), when "air supremacy became a means to achieve and maintain information supremacy" (Lesenciuc, 2014:135), the informational architecture of the battlefield could no longer be overlooked. This led, on the one hand, to the transformation of the battlefield into a networked environment and, on the other, to the increasing hybridization of military actions. In the context of contemporary warfare, many military actions have shifted focus from destruction to information and influence. Taking into account the diversification of conflict participants, the hybrid nature of military actions has become increasingly evident, reflected in the growing role of "soft," non-lethal, or non-kinetic military actions—among which information operations stand out as the most significant. Today, information operations are recognized as a force multiplier across all dimensions of military engagement. Enabled by technology, they can initiate strategic actions aimed at influencing political decision-making, public opinion, and the course of events at the strategic level.

In an era marked by the hybridization of power forms, increasingly blurred boundaries between soft and hard power, rapid technological innovation, and significant socio-political transformations, contemporary conflict is no longer defined solely by conventional military actions but also by an intensified struggle within the informational sphere. Within this context, information operations have become fundamental to strategic planning. These operations go beyond merely acquiring and transmitting information; they also involve manipulating and shaping perceptions in order to influence public opinion, political decisions, and even the course of conflicts (Jagiełło-Tondera, 2019).

Nowadays, the evolution of conflicts has undergone significant transformations, requiring not only military force, but also informational manipulation and influence over public opinion. The new paradigm of conflict is marked by contradictory trends, involving both the alternation and overlap between heightened interest in battlefield architecture and the mass deployment of troops, as well as between the effects of constructivist thinking in international relations and the resurgence of political realism, re-branded through illiberal regimes.

The very use of the term "information war" represents a victory in the imposition of Russian terminology, as the reference term in Western doctrines – including those of NATO – is "information operations."

In the Russian context, however, the use of the term "information war" naturally reflects an extension beyond the scope defined in Western doctrines – namely, beyond the boundaries of military power, where such concepts would traditionally be expected to apply.

In the Western sense, Information Operations are, according to NATO specific Doctrine,

> A staff function to analyze, plan, assess and integrate information activities to create desired effects on the will, understanding. and capability of adversaries, potential adversaries and audiences in support of mission objectives. (AJP 10.1, 2023:14-15)

The information environment,

> the principal environment of decision-making; where humans and automated systems observe, conceive, process, process, orient, decide and act on data, information and knowledge. (AJP 10.1, 2023:10),

has become the true confrontational space in contemporary conflict, characterized by the hybrid pattern of associated actions, from physical destruction per se to psychological operations or presence, profile and posture (see the full spectrum of key coordinated domains in the information operations chariot in relation to the predominant types of information activities, Lesenciuc, 2016:70). In spite of these transformations, rigorous military planning characterizes information operations, and this planning cannot neglect the consideration of objectives, activities, targets and effects, an analytical scheme that we will apply in the following to highlight the implementation of the Russian information warfare concept.

2.2 Theoretical and doctrinal foundations of Russian information warfare. The use of information for manipulation is a fact of warfare everywhere and at all times. Therefore, the component elements of information operations: psychological operations, misleading, cyber operations, electronic warfare and others are of considerable antiquity and have been used in various forms in different conflicts. In the case of the Russian Federation, however, there is a strong Soviet tradition - a radiography of this period of the field's development was made by Allen & Moore (2018:61-62), later materialized by a significant post-Soviet academic interest, starting from the concept of "reflexive control" (*reflexivnoe upravlenie*), atypical of Western military thinking, whose roots can be traced back to the 1960s and which was later tested at the tactical and operational level along with *maskirovka* (deception) and disinformation (Thomas, 2004:239). From the perspective of this theory which is still producing effects today and which is focused on the moral and psychological exploitation of the adversary, starting with the commanders of enemy structures, imitating the behavior of the adversary is a useful strategy:

> In a war in which reflexive control is being employed, the side with the highest degree of reflex (the side best able to imitate the other side's thoughts or predict its behavior) will have the best chances of winning. The degree of reflex depends on many factors, the most important of which are analytical capability, general erudition and experience, and the scope of knowledge about the enemy. (Thomas, 2004: 242)

The theory of reflexive control involves actions that fit into what is the Western concept of information operations, such as influencing the enemy's decision-making algorithm or altering the decision-making time, to which are added actions on the soft, political and symbolic power levels, such as measures to present false information about the situation and, above all, power pressure, including effects on both soft and hard levels, in the perspective of :

> the use of superior force, force demonstrations, psychological attacks, ultimatums, threats of sanctions, threats of risk (developed by focusing attention on irrational behavior or conduct, or delegating powers to an irresponsible person), combat reconnaissance, provocative maneuvers, weapons tests, denying enemy access to or isolating certain areas, increasing the alert status of forces, forming coalitions, officially declaring war, support for internal forces destabilizing the situation in the enemy rear, limited strikes to put some forces out of action, exploiting and playing up victory, demonstrating ruthless actions, and showing mercy toward an enemy ally that has stopped fighting. (Ionov, 1994:47, *apud* Thomas, 2004:244-245)

From the perspective of Russian military theorist S.A. Komov (1997:18-22, *apud* Thomas, 2004:248-249), in the meantime "refexive control"

was called “intellectual control”, it was assimilated to information warfare and involves the following actions: distraction, overload, paralysis, exhaustion, deception, division, pacification, deterrence, provocation, overload, suggestion and pressure. The concept is very important to the Russian Federation and is now widely used, based on the belief that the United States and the European West won the Cold War thanks to reflexive control initiatives.

As in the case of hybrid warfare, for using the concept of information warfare – although a similar term pre-exists in Russian scholarship, proposed in 2006 by Russian professor and political scientist Igor Panarin - General Valery Gerasimov, Russian Armed Forces Chief of Staff blamed Western states, involved in hybrid actions in the colored revolutions in Ukraine, Kyrgyzstan, Georgia and in the Arab Spring phenomenon, invoking the need for defense, and the response to the hybrid threat carried out on the soft and hard power levels could only come through an action tool that would involve both simultaneously. In this sense, two years before the Gerasimov Doctrine, the Ministry of Defense of the Russian Federation had already defined information warfare on the skeleton of the "reflexive control" theory, as follows:

> as the ability to . . . undermine political, economic, and social systems; carry out mass psychological campaigns against the population of a state in order to destabilize society and the government; and force a state to make decisions in the interest of their opponents. (*Conceptual Views regarding the Activities of the Armed Forces of the Russian Federation in Information Space*, 2011, *apud* Thomas, 2015:12, *apud* Allen & Moore, 2018:60))

at a time when a more westernized concept of information operations, *information confrontation*, was operational in the Moscow scientific environment:

> Russian military doctrine also describes a broader concept of information confrontation (информационное противоборство) that incorporates military/technical battlefield effects and informational/psychosocial effects “designed to shape perceptions and manipulate the behavior of target audiences (Allen & Moor, 2018:60).

The reference element in the operation of the three concepts: reflexive control at the theoretical level, information war at the political, economic, symbolic and military level and information confrontation predominantly at the military level is that they are continuously applicable, before, during and after the actual military actions, under the conditions of the declaration or non-declaration of war. The three levels (theoretical, and applied: strategic and operational) ensure the construction of an altered, convenient reality, in line with the main narratives and carrying content aligned with these narratives, capable of producing distrust, disorder and dissent.

2.3 Russian Information Warfare. The implementation of the concept of information warfare, in its classical sense, has never been confined to the Western projective framework of information operations. Possessing exceptional informational capabilities, the Russian Federation has developed a distinct approach to conducting information activities both on the battlefield and beyond its spatial and temporal boundaries, based on the notion of ensuring individual and societal information security (Thomas, 2007:40). Timothy L. Thomas attributes this difference in approach to the broader context, noting that the Russian Federation has been undergoing a process of transition marked by institutional and philosophical instability, as well as vulnerabilities generated by various internal factors, in contrast to the United States.

The concept of information warfare, in this terminological formulation, is attributed to Igor Panarin (2006:146) and constitutes one of the pillars of hybrid warfare, alongside Evgheni Messner’s insurgency warfare and Aleksandr Dugin’s network-centric warfare, as we highlighted in my analysis of this concept (Leenciuc, 2023:31-32), exceeding the purely military scope and engaging in disinformation through doctrinal dissimulation.

> From a content perspective, the differences are significant. Each of the concepts analyzed, starting with that of hybrid warfare, exceeds the boundaries of the theater of operations. For instance, the “network” in Dugin’s concept of net-centric war represents a "flexible weapon" that requires engagement at the political, social, economic, and cultural levels. The information in Panarin’s *information warfare*, in turn, constitutes a flexible weapon and exceeds the American military concept, targeting informational confrontation in the political, diplomatic, economic, and military arenas. Dugin’s and Panarin’s concepts are ideologically fueled in a similar way and define, at different levels, similar phenomena. In short, the Russian theory of *hybrid warfare* is based on American concepts used within the scope of military

> operations, extending them – under the guise of American nonlinear actions condemned by Gerasimov – into a broader confrontation, across all levels: *soft* (political, economic, cultural) and *hard* (military). In fact, Russian policy relies on this misdirection through terminological confusion and the use of propaganda at various levels, exceeding military boundaries.

Panarin's information warfare concept involves informational confrontation on issues that include, among other things, propaganda (at all levels) and intelligence activities – exceeding the American doctrinal framework that includes this component, military intelligence on the battlefield: information operations intelligence integration (IOII) (Lesenciuc, 2016:54) – and assumes, based on a thought process rooted in the realist paradigm, the continuous and constant informational confrontation between state actors. After being grounded in the theoretical foundations of "reflexive control" and the doctrinal principles of information warfare, the concept was first applied during the 2008 conflict in Georgia, where the informational confrontation during peacetime was initially won by the Georgians, then by the Russians. This led to a series of post-conflict reforms within the military. The informational confrontation occurred on two levels: information-technical (focused on cyber confrontation, or cybernetic operations, see Vevera & Ciupercă, 2019:33-34) and information-psychological (focused on psychological confrontation in the Western sense, supplemented by extensive propaganda actions), with effects on international relations (Iasiello, 52-53). The effects of this propaganda included the imposition of a standardized image in international political relations.

The same did not occur during the Crimean conflict. Although there were a number of similar premises, such as the fact that in both annexed regions, South Ossetia and Crimea, a high percentage of the population was of Russian origin or pro-Russian orientation, the lessons of the Georgian war did not serve to impose an image that would lead, at the political level (since Russian information warfare also covers this layer), to the international recognition of the peninsula's annexation. On the information-technical level, the Russian Federation extended attacks not only on the Ukrainian state but also on officials and institutions in NATO and EU member states. On the information-psychological level, the Russians could not justify a direct threat, which is why propaganda, disinformation, and deception were extended especially in new media and produced effects mainly at the political and social levels, with only subsidiary military arguments. The Russian information warfare during the Crimea annexation period involved dissimulation on multiple layers, including the application of democratic exercises in the peninsula.

> Perhaps the most telling aspect of success, Russia kept its biggest adversaries—the United States and NATO—from intervening thereby enabling a referendum in which the Crimean parliament voted to join Russia. While the West refuses to acknowledge Crimea's secession, Russia attests full compliance with democratic procedures, a fact difficult to argue against on an international stage (Iasiello, 2017:58)

The Russian information warfare is an asymmetric weapon in the confrontation with the states against which it was applied, Georgia and Ukraine, reinforcing the idea that this concept, as generally understood by Western states within the framework of information operations, can produce major geopolitical effects with limited resources and minimal military involvement. However, all of this unfolded under the imprint of disinformation through doctrinal dissimulation, meaning deceiving important adversaries regarding the content of a term extended in its application at the level of soft powers: information warfare. The concept was later included in what is technically referred to as the "new generation war," as emphasized by Emilio J. Iasiello (2017:60), or, keeping the projective framework from which we started, as an independent dimension of *gibridnaya voina.*

3. THE INFORMATION WAR IN UKRAINE STARTING FROM 2022

In the period leading up to Russia's invasion of Ukraine and throughout the ongoing conflict, social media served as a battleground for both state and non-state actors, as well as individual or corporate entities that spread various war scenarios influenced by dominant narratives or counter-narratives. As the war prolonged, digital platforms were flooded with disinformation produced as part of the Russian information war strategy. Analyzing these operations from the perspective of objectives, activities carried out, targets, and intended/achieved effects, the conflict in Ukraine constitutes a comprehensive framework for examining Russian information warfare.

The objectives of Russian information warfare derive directly from the goals of the invasion and are primarily focused on the political dimension, which exceeds the classical understanding of information operations. As early as 2014, Jolanta Darczewska (2014:3) highlighted this aspect:

> Russia's occupation and annexation of Crimea, its aggressive behaviour against eastern Ukraine (the conflict over "Novorossiya") and its destabilisation of the Ukrainian state have become yet another field of Russia's experimentation with information operations.

She also noted that these strategic objectives have remained unchanged for many years. The difference between 2014 – the year of Crimea's annexation and the opening of the conflict in Donetsk and Luhansk – and the beginning of the conflict in 2022 lies in the fact that the initially concealed military commitment is now covered by the phrase "special military operation," with the observation that two of the identified features have remained the same: "the information space is the main battlefield" and "large groups of the public are being involved in the fight" (Darczewska, 2014:8).

In the context in which both state actors involved in the conflict – the Russian Federation and Ukraine – widely use social media to promote their own versions of unfolding events and to amplify contrasting narratives about the war, including its causes, consequences, and progression, the information operations conducted by the Russian Federation, unlike previous actions, have involved, in the case of the war in Ukraine, both a focus on new mass communication tools and the achievement of a third level of action – the formation of the so-called information system. This involves collecting, analyzing, and complementing digital data, as well as discrediting media outlets and other sources of information, according to the analysis by Cherniavska *et al.* (2023:920). Moreover, this level surpasses the earlier stages: information campaign (which entails the formation of social and political thought and the influence on social, economic, and political sentiment) and information attack (carried out through the discrediting of national attributes and the use of propaganda rhetoric).

The response of the Ukrainian administration was at the same level. Government officials, citizens, and state agencies turned to a variety of platforms, including Facebook, Twitter, TikTok, YouTube, and Telegram, to disseminate information. For example, in the early days of the war, Kyiv issued appeals on Facebook for donations to purchase UAVs or even campaigns to join associations of personnel who own or operate drones. Informal donation pages were created to support online efforts aimed at acquiring civilian drones. The Russian administration made similar attempts, but their efforts were not as successful as those of the Ukrainians. Nevertheless, drone donations supported both actors in generating and sustaining concentrated military power. The objectives achieved with the help of this technology included conducting reconnaissance and aerial surveillance missions, as well as assessing target effects and optimizing the use of ground-based assets.

The activities associated with the creation of the information system as a result of the information war triggered reactions from the international community. Due to the sanctions imposed on the Russian Federation, states that had previously maintained strategic partnerships with the aggressor state chose not to intervene or express any reaction regarding the conflict. The effects of the information war initially turned into a significant victory for Ukraine, which succeeded in gaining international support through political instruments, complementing these actions with efforts on the informational front.

Ukraine's success in gaining international sympathy was reinforced by results on the battlefield, while psychological actions to boost confidence in its own troops were carried out through targeted *new media* messaging, including memes featuring the "Saint Javelin" and farmers towing Russian tanks. The outcome, alongside political efforts to mobilize military and humanitarian donations, led to significant fundraising for the war, with substantial donations primarily from NATO member states. The Russian Federation responded to this unexpected support by trying to maintain the functionality of what is referred to as the "information system" (Cherniavska *et al.*, 2023) at a level of informational aggression that Iryna Vekhovtseva (2023:27) called "information violence" — a form of non-kinetic, aggressive influence that contradicts the natural course of events, manifests imperceptibly and over time, and involves imposing the beliefs of the Russian Federation or distorted information about Ukraine while establishing asymmetric relations.

Indeed, since the beginning of 2014, Russia has launched informational operations, promoting disinformation regarding a false Ukrainian

chemical and biological weapons program in order to justify the invasion and discourage sympathy and support for Ukraine. Among the false claims circulated by the Russian Ministry of Defense are accusations that Ukraine carried out a "chemical drone attack" against Russian forces, and that it launched a new anti-drone laser – all promoted with the aim of deterring Western support.

The activities associated with Russian information warfare go far beyond the conceptual framework of information operations as understood by Western NATO and EU member states. In its operations, the Russian Federation has included actions within the social media sector – where they attempted bombardment with stimuli in a deployment aligned with the principles of network warfare developed by ideologue Aleksandr Dugin (2009), through non-state entities associated with the Eurasian movement: "These agitation-propaganda and intelligence-organisation activities are carried out by non-state actors" (Krawczyk & Wiśnicki, 2022:279). They also used deepfake elements powered by AI to reinforce ideologically altered information and fake news, mainly through Telegram, the most important social media platform in both Russia and Ukraine. Grouping these actions under the umbrella of information war, projected at the level of soft power, was done in accordance with the principles of reflexive control:

> "Thanks to numerous network connections, it intoxicates the information environment by reinforcing Russian narrative lines according to the principles of Russian reflexive management theory." (Krawczyk & Wiśnicki, 2022:284)

The targets of Russian information warfare have become increasingly diverse, both in terms of the wide range of operations it encompasses – from psychological to cyber operations – and especially due to the testing and adaptation of new technologies to the realities of the battlefield. As a result, the targets are primarily concentrated outside military structures: administrative institutions, critical infrastructures, websites, networks, and individuals. The tools through which these targets are reached in information warfare include, primarily, propaganda, dis- and misinformation, Distributed Denial of Service (DDoS), website defacement, malware etc.

The effects of the informational operations intentionally carried out by the Russians can be grouped into a series of action themes that, as can be observed, target not only the Ukrainian army, but the entire population of the country, as well as targets outside it:

a) Demoralization of Ukrainians through disinformation actions aimed at undermining the morale of the population and institutions in Ukraine; creating and spreading internal unrest in Ukraine, starting from the dissemination of fake news, such as those about the surrender of the government or the Ukrainian army; lowering the morale of the troops and the trust of the Ukrainian population in their own army by launching accusations of corruption and incompetence against the country's leadership;

b) Creating a rift between Ukraine and its allies through disinformation campaigns that include false narratives about relations with neighbors, particularly with Poland, regarding intentions to annex territories; amplifying such information through networks and spreading false informational materials, including maps and documents with an impact on an unprepared public; disinformation about the erosion of Ukraine's relations with Western Europe due to internal issues and the high costs associated with the war; spreading false information about the involvement of Ukrainian refugees in criminal activities outside the country's borders; spreading materials about the disproportionate social benefits that Ukrainian refugees receive in host countries, which can provoke social and political tensions within these countries;

c) Strengthening the positive public perception of the Russian Federation (Most of these targeted at the Russian domestic audience, emphasizing the need for Russia to "sell" a certain image of the war to its own population), based on scenarios aimed at reinforcing the perception of the Russian state's reasons for launching military operations, relying on the denial and distortion of information, including dismissing as false information regarding war crimes; creating false news spread across networks about the inhumane and unjust actions of the Ukrainian army; creating fake social media accounts promoting Russian narratives; denying the effects of sanctions against Russia and supporting the claim that these measures have harmed the West far more than the sanctioned state.

Essentially, the narratives presented by Russia and Ukraine are diametrically opposed. Russia frames the war in Ukraine, which President Vladimir Putin insists is a "special military operation," as a necessary defensive measure in response to NATO's expansion into Eastern Europe. Additionally, the Russian president frames

the military campaign as essential for "denazifying" Ukraine and ending an alleged genocide being carried out by the Ukrainian government against Russian-speaking citizens.

The scale of information uploaded on social media and the speed at which it proliferates create new and complex challenges in combating disinformation campaigns, complemented by other tools involved in informational warfare. The aim of Russian informational actions is not to make Ukrainians or allies believe something, but to spread distrust, confusion, and disinterest in the actual situation on the battlefield. The most widespread narrative of the Russian Federation, which portrays Ukraine as a "failed state," is disseminated through a series of messages, which Dzhus (2023:85) summarizes as follows: "The messages that fill this narrative are about history, corruption, culture, economics, and more. That is anything that can be used to support the narrative." The narratives and informational actions aimed at influencing the will to fight and the trust in one's own forces are contradictory and easy to counter with rational arguments, but the creation of a climate of distrust in information sources is, in fact, the most acute problem in this context.

4. CONCLUSIONS. IDENTITY OF *NOBODY*

A few days before the beginning of the war in Ukraine, US President Joe Biden, visibly tired but firm in his statements, spoke about the identity of *Nobody*, the one willing to produce information blindness through information war. From President Biden's speech, various analysts have drawn attention to various aspects of the speech, insisting on the firmness of the statements, the readiness for diplomatic dialogue, the unity of the West, the distrust of the Russian side in the absence of any written understandings. I would like to emphasize the last firm response by the American President on Russia's possible courses of action, when the diplomatic option was still open:

> And if Russia attacks the United States or our Allies through asymmetric means, like disruptive cyberattacks against our companies or critical infrastructure, we are prepared to respond. (Biden, 2022, *apud* Meyer & Johnson, 2022).

Therefore, Joe Biden, in a speech of an overtly informative character, addressing first American citizens, then Russian citizens and then citizens of NATO member countries, considered the possibility of Russian military attack on Ukraine, i.e. invasion of Ukrainian territory, but concluded by emphasizing the likelihood of asymmetric attacks. During the Cold War, neither Stalin, Khrushchev nor any of the other Soviet presidents committed the folly of direct confrontation. Wars were fought through third parties (proxy wars) in Korea, Vietnam, the Middle East. The entry of one of the two superpowers into the war: the US in Korea and Vietnam, the USSR in Afghanistan, has entailed a direct non-involvement of the other side. The war in Ukraine is perhaps the biggest challenge since the Cuban Missile Crisis, which is why the American president has cautiously considered all possibilities.

Probably the most important statement is the one about Russia's asymmetric attacks, especially cyber attacks. It could be inferred from the discursive organization that the US is preparing for a false de-escalation of the military situation on the border with Ukraine, coupled with massive cyber-attacks and various other forms of asymmetric informational manifestations, not to be claimed at the state level, but to be blamed on *Nobody*.

In fact, Putin's policy has been to build asymmetric instruments with which to counter the action capabilities of his adversaries. For example, in the Russo-Georgian war of 2008, Russia, which in 2008 was led by Medvedev but had Putin as prime minister (we are not debating the Kremlin leader's thirst for power here), did not impose its will solely through the 200 000 troops deployed in South Ossetia and Abkhazia. The military confrontation was coupled with cyber-attacks, which involved taking control of the Georgian presidential website as well as important institutions, including the Parliament, the National Bank, the Foreign Ministry. The result of the war was the imposition of the Kremlin's own will, forcing the Georgians to accept Russia's conditions. President Bush's lack of reaction and the appointment of Sarkozy as EU mediator reinforced Putin's conviction that he can do anything. The annexation of Crimea happened under similar conditions. Russia, concerned about the fate of Russians in Crimea, has begun a series of military intimidation operations in the area. Propaganda has been used to fuel the secessionist current within the population of the region. The clashes between the pro-Russian separatists and the Ukrainians and Tatars who demanded that the *status quo* be maintained were arbitrated, this time too, by Russian military, at the very time of the referendum. The Russian military seized control of local government bodies, blocked airports, acted on local critical infrastructure, and through their

intimidation and propaganda imposed a result reminiscent of the Soviet period: more than 95% of the population of Crimea voted for annexation to Russia. Russian military maneuvers on the border with Ukraine and, subsequently, cyber-attacks against Ukraine, against the background of the Gerasimov doctrine, have once again led to the imposition of the will of the Kremlin, and more specifically the will of President Vladimir Putin.

All of this was possible because disinformation through doctrinal dissimulation worked. NATO member states expected information operations as they projected in their own doctrines, while the Russian Federation had built the much larger infrastructure of information warfare that went beyond the military dimension of the conflict. NATO member states expected hybrid actions as their own theorists were trying to define them, while *gibridnaya voina* was already a monster oversized to the scale of Putin's ambitions. Putin's Russia did not refrain from using asymmetric means, including cyber-attacks, against Ukraine and other countries, under the protection of a doctrine fed from the Western doctrinal corpus. The Gerasimov Doctrine had already achieved, through doctrinal dissimulation, the transfer of American concepts from the strictly military application to the societal level (it generalized war, transformed it from a space of eminently military actions into a space of interference of forms of power). Hybrid warfare, based on the concepts of insurgency warfare, information warfare and cyber warfare, has made it possible to use these concepts – which are to be found in NATO and US doctrinal apparatus – but has deliberately mixed up the offensive and defensive dimensions of information operations. While in NATO doctrine, for example, defensive psychological, cyber and electronic actions can be carried out to protect its own information, information systems and troops, offensive actions and the exploitation of an adversary's infrastructure require the approval of targets by the North Atlantic Council, Russia carries out offensive actions against its adversaries or potential adversaries without any moral restrictions. Moral asymmetry primarily characterizes Russia's actions. Long-term, an international agreement regarding the morality of using offensive informational means is needed, while short-term, a response with the same measure from the targeted countries is required. The first measure will reduce the informational fog of the contemporary battlefield and will prohibit hiding behind the name *Nobody*, while the second will force the clarification of identity and intentions, in a chivalrous spirit.

Note on naming: One of Putin's major territorial targets remains the city of Odessa, built by Empress Catherine II on the ruins of the Turkish fortress Hacıbey after the Russo-Turkish war of 1787-1792. At that time, the empress chose the feminine version of the name Odysseus. The current war, fought under the mask of the name *Nobody*, under which Odysseus hid on the shores of the Cyclops, can only lead to the emergence of a *No Man's Land* of uncertainty.

BIBLIOGRAPHY

1. Allen, T.S. & Moore, A.J. (2018). Victory without Casualties: Russia's Information Operations. *The U.S. Army War College Quarterly: Parameters.* Vol.48, no.1. 59-71. doi:10.55540/0031-1723.2851
2. Bokinskie, L. (2024). Russian Political Warfare: What It Is, What It's Not, and Why It Isn't Working. *Global Insight. A Journal of Critical Human Science and Culture*. Vol.4. https://doi.org/10.32855/globalinsight.2024.003.
3. Cherniavska, B.; Shevchenko, S.; Kaletnik, V.; Dzhahupov, H. & Madryha, T. (2023). Information Warfare in the World and Information Security Issues in the Context of the Russian-Ukrainian War. *Review of Economics and Finance*. 21. 916-922.
4. Darczewska, J. (2014). The Information War on Ukraine. New Challenges. *Cicero Foundation Great Debate Paper*. No.14/08.
5. Dugin, Aleksandr. (2009). *The Eurasian Idea.* San Francisco, CA: Counter-Current Publishing.
6. Dzhus, O.A. (2023). Key indicators of Informationa Warfare Russia against Ukraine. *Political life.* No.2. 83-88, https://doi.org/10.31558/2519-2949.2023.2.10
7. Filina, A. (2023). *Gibridnaya Voyna in Light of the War in Ukraine: Analysing Changes in Russian Interpretations and the Use of Hybrid Warfare Concept* (Master's Thesis). Prague: Charles University.
8. Fridman, O. (2018). *Russian Hybrid Warfare. Resurgence and husPoliticisation*. London: Hurst & Company.
9. Galeotti, M. (2016). *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right.* Morrisville, NC: Lulu Press.

10. Galeotti, M. (2018). (Mis)Understanding Russia's Two 'Hybrid Wars'. *Critique & Humanism.* 49. 17-27.
11. Galeotti, M. (2019). *Russian Political War. Moving Beyond the Hybrid*. London: Routledge.
12. Gherasimov, Valerii [Герасимов Валерий]. (2013, 27 februarie). Ценность науки в предвидении Новые вызовы требуют переосмыслить формы и способы ведения боевых действий (Ţennosti nauki v predvidenii). Военно-Промышленный Курьер*/ Voenno-Promîşlennîi Kurier*. 8 (476).
13. Jagiełło-Tondera, A. (2019). Niebezpieczne metafory. Język jako narzędzie kreowania rzeczywistości. In K. Śmiałek & W. Śmiałek (eds.), *Ewolucja wojen. Wielość uwarunkowań.* Warszawa: Wydawnictwo Wojskowej Akademii Technicznej.
14. Iasiello, E.J. (2017). Russia's Improved Information Operations: From Georgia to Crimea. *The US Army War College Quarterly: Parameters.* Vol. 47, no.2. 51-63. doi:10.55540/0031-1723.2931
15. Krawczyk, P. & Wiśnicki, J. (2022). Information warfare tools and techniques in the context of information operations conducted by the Russian Federation during the 2022 war in Ukraine. *Cybersecurity and Law*. 8(2). 278-286.
16. Lesenciuc, A. (2014). *Introducere în arta militară.* Brașov: Editura Academiei Forțelor Aeriene „Henri Coandă.
17. Lesenciuc, A. (2014). *Războiul informațional.* Brașov: Editura Academiei Forțelor Aeriene „Henri Coandă.
18. Lesenciuc, A. (2023). *Războiul hibrid sau Întoarcerea prin disimulare doctrinară la războiul absolut.* Editată de Statul Major al Apărării, Colecția revistei *Gândirea Militară Românească*. București : CTEA.
19. Meyer, J. & Johnson, K. (2022, February 16). A Russian invasion could reach farther than Ukraine. How a cyberattack could affect you. *USA Today* [online]. URL: https://eu.usatoday.com/story/news/politics/2022/02/16/ukraine-russia-cyberattack-fears/6803170001/ [Accessed on April, 2025].
20. Monaghan, A. (2015). The 'War' in Russia's 'Hybrid Warfare'. *The US Army War College Qaurterly: Parameters.* Vol. 45, no.4. 65-74.
21. NATO. (2023, 7 January). *Allied Joint Doctrine for Information Operations.* AJP-10.1. Brussels: NATO Standardization Office (NSO).
22. Panarin, Igor. (2006). *Informatsionnaya voyna i geopolitika.* Moscova: Pokolenie.
23. Thomas, T.L. (2004). Russia's Reflexive Control Theory and the Military, *Journal of Slavic Military Studies.* 17. 237-256.
24. Thomas, T.L. (2007). Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations. *The Journal of Slavic Military Studies.* 11(1). 40-62. https://doi.org/10.1080/13518049808430328
25. Verkhovtseva, I. (2023). Російська інформаційна війна проти україни 2014–2024 рр. Як предмет наукових студій:концепт «інформаційне насильство». *Obraz*, 2024. Vol.2 (45). 26-35. https://doi.org/10.21272/Obraz.2024.2(45)-26-35.
26. Vevera, A.V. & Ciupercă, E.M. (2019). The dimensions of Cyber Warfare in th Sino-Russian Space. *Romanian Cyber-Security Journal.* Vol.1, no.2. 31-36.