Information Environment Analysis and Its Role in Combating Influence Operations: The Example of the Russian Invasion of Ukraine

JL. Albert Martínez; A.A. García Juan; C. Martínez Bernalt;
JM. Valdés de Olives and S. Fernández Juin
Joint Chiefs of Staff of the Spanish Armed Forces
SPAIN

Lajaula.in.7@gmail.com

ABSTRACT

The advent of social media has given state and civil actors the capacity to affect and influence society at a worldwide scale. Geographical and demographic boundaries have long been dissolved in favour of instant connectivity and globalisation. Collaterally this has given foreign actors the capacity to strongly influence consolidated democratic societies, bombarding them with narratives that are in complete discordance with the values and characteristics that shape them. Influence operations in its traditional definition could only target generic population groups through their long-term exposure to conventional media - this means of distortion have proven in the past to be extremely expensive, often having had to employ considerable resources and requiring meticulous coordination only to reap minimal rewards. With the appearance of the internet and the rise of social networks, short term exposure to negative narratives and ideas can now be attained with a minimal amount of time and few assets, assuring much more effective results than influence operations targeted at conventional media. Russia has developed wide-ranging disinformation campaigns both on social and conventional media to confuse and undermine information environments. These tactics have evolved and adapted to modern times but are not unfamiliar to Western security services. Post-Soviet influence operation tactics are built on the same theoretical framework established during the Cold War. Russian disinformation applies that same theoretical background and adapts it to contemporary societies and new methods of communication. In the case of modern influence operations, long-term public exposure to hostile narratives continues to be achieved by the Russian media establishment, often adapted to meet the cultural and linguistic requirements of foreign countries, while short term exposure is achieved through online trolls, bots and local influencers on social media. This ends up translating into influence operations masquerading under the false premise of journalism and sporadic and spontaneous trains of thought arising from social media users. The weaponization of Lysenkoism against foreign actors and the use of influencers and trolls on social media has been leveraged during both the invasion of Crimea in 2014 and that of Ukraine in 2022. In both examples Russian propaganda and disinformation have been used for psychological warfare (mainly to demoralise Ukrainian combatants) and to influence Western's public opinion about the conflicts. The example of the Russian invasion of Ukraine holds a great importance in the context of modern warfare - the war on Ukraine is the most widely covered conflict in modern history, and the mobilisation of users on social networks and mass media has for the first time begun to have a direct impact on the battlefield. Pro-Ukrainian narratives have proven an ability to bolster the morale of the population and draw foreign attention to the conflict, which has materialised in two different ways: 1) By affecting the political determination of a foreign third parties in the conflict and 2) by mobilising civilian support for Ukrainian war effort (in this regard we must mention the monetary support driven by social media movements such as the North Atlantic Fellas Organisation to the Ukrainian army). On the other side of the conflict, the proliferation of Russian narratives on foreign information environments have tended to materialise in a positive public attitude towards the invasion of Ukraine. This means that certain individuals bombarded with Russian narratives will begin to see the conflict not only as legitimate, but as a war of aggression on Russia. Other examples of such positivity towards the war include the denial of war crimes committed by Russian occupation forces under the pretext that such crimes are 'false flag' operations deployed by Ukrainian forces or even by Western operatives. This type of cognitive dissonance might not be

perceived at first glance as a threat to Western democracies but if permitted to exist uncontested or to flourish in an information environment (as a result of Russian influence operations) the effects could be destructive in both a political and sociological sense. The information environment analysis is a tool designed to combat disinformation and hostile narratives as well as to provide decision-and policymakers with early warning signs of harmful hybrid actions on national information environments. The objective of this research is to (in the context of the Ukrainian War) analyse Russian influence operations and their effect on Western information environments whilst highlighting the importance of an effective methodology to apply information environment analysis at a Strategic Communication level.

1.0 INTRODUCTION

Although the historical roots of the Russian-Ukrainian conflict date back more than 300 years [1], given the focus of this article, it is unavoidable to mention the historical event that laid the foundations for what is known as the Ukrainian War (2022): the annexation of Crimea (2014). Motivated by the rise of Ukrainian ties with the EU, Russia seized the territory of Crimea, acquiring a geostrategic enclave that would allow it to extend its power in the Mediterranean, the Middle East, and North Africa. [2].

Eight years after the conflict that represented a turning point for European security, Moscow decided to invade Ukraine in February 2022. Before the invasion, Russian propaganda machinery began to elaborate pro-Russian narratives and disinformation to undermine Ukraine's morale. The Kremlin's prewar narratives were mainly focused on justifying the military intervention in Ukraine while attempting to deny any possible Russian responsibility for the upcoming invasion [3]. The main justification for the war was built upon the idea that Ukraine is a "Nazi state", that represents a threat not only to the Russian security architecture but to Western values as a whole. This narrative vinculating Russia's role in the world and Judeo-Christian values has been a recurring narrative since the 2014 Crimea invasion. The vinculation of both narratives has the sole purpose of legitimizing the invasion on Western audiences; the appeal to judeo-christian values and the threat of a "Nazi state" in the heart of Europe was thought by Moscow to be sufficient to win the coming information war [2].

Although Russia attempted to mask its movements under the disguise of "Peacekeeping forces in Lugansk and Donetsk" US intelligence was able to determine with exact precision the dates for the upcoming invasion. The Kremlin's propaganda machinery wasn't enough to conceal Russia's real intentions from Western intelligence agencies but still quite effective when analyzing Western audiences and their reaction to the invasion [4].

After the failed attempt to take Kyiv, Russia was forced to switch from an offensive informational perspective to a purely reactive one. The massacres of Bucha marked a changing point in Russia's information warfare on the war of Ukraine; prewar narratives would no longer be effective, and Russia would be forced to modify its strategy and begin reacting to Ukraine's and NATO's actions. Russian state media immediately switched from narratives and disinformation that legitimized/concealed the invasion to messages that portrayed Russia and its allies as the main victims of the war. With the arrival of the winter, the war entered into a stale-mate. Large troop movements were stopped while Russia's information warfare intensified. The new narratives were focused on undermining NATO's support to Ukraine as well as portraying it as the main responsible for escalating the conflict into a "World War". These allegations of "escalation" were often accompanied by messages loaded with nuclear rhetoric that often showed Russia as a peaceful nuclear state that would be forced to employ nuclear weapons in Ukraine [5].

The strategic changes regarding Russia's information warfare can be interpreted as an indicator of lack of preparation but equally as dangerous if we take into consideration the enormous machinery and resources that the Kremlin possesses to influence Western audiences. The "Wagner Coup" and the multiple failed offensives of the Russian army are indicators that Russia's internal propaganda campaigns (specifically,

those designed to boost the morale of its troops in Ukraine) may not be providing the expected results [6]. Regardless of the effectiveness of internal propaganda, Russia's external propaganda is still a threat to Western governments, their stability, and democracy [7].

The War of Ukraine is the best example so far of the integration of conventional war with hybrid warfare. For this article, we will only focus on the cognitive aspect of the conflict, specifically on a methodological approach to the analysis of Information Environments and how to protect them from Russian narratives and Disinformation [8].

2.0 CONCEPTUAL APPROACH

To elaborate an effective methodology that allows the study of an information environment, it is necessary to establish a conceptual framework. NATO's doctrinal documentation (AJP-10) does provide a preliminary approach toward establishing that particular framework. For this article, we will only focus on the following concepts.

NATO's doctrine defines an Information Environment as "An environment comprised of the information itself, the individuals, organizations, and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs". The concept originally provided in the Allied Joint Doctrine for Strategic Communications is broad as it involves practically any system that transfers and processes information both physical and digital. This may prove difficult to apply when analyzing an environment as it requires massive amounts of resources only to merely establish a framework of study from which to operate. The concept is way too theoretical to be used in a practical and daily-based scenario.

The Information Environment Analysis is (as defined in NATO doctrine) a process to understand and respond to threats in an information environment. It also includes the evaluation of NATO's strategic communications effectiveness when applied to a specific audience or environment. The Allied Joint Doctrine for Strategic Communications establishes that the analysis of an audience should be an integral part of an Information Environment Analysis. This may generate future problems, as to understand the intricacies of human groups and the flow of information within them, audiences must be investigated and categorized before the Information Environment Analysis; specifically when establishing our framework of study.

The flow of information within an Information Environment needs to be categorized to be the subject of further analysis. NATO doctrine proposes the concept of Narratives to categorize and group large quantities of information. The AJP-10 defines a narrative as "A spoken or written account of events and information arranged in a logical sequence to influence the behavior of a target audience". The definition of this concept doesn't take into account the cognitive aspect of a message; this is, the superior idea behind a message that is retained by individuals when exposed to a narrative. In vernacular, this would be when an individual or a group of individuals' moral, ethical, and cultural values have been rewired after being exposed to certain narratives.

To complete NATO's definition of a narrative we propose the inclusion of the concept of force-idea. A force idea is the ultimate consequence of a narrative. It is the mental representation of an idea that is retained by the individual and included as an intrinsic part of himself as a result of consistent exposure to messages. A group of narratives in an information environment may have different messages but they can still all be targeted at divulging or reinforcing a specific force-idea, that forms part or could form part (with sufficient exposure to those narratives) of the collective conscience of an audience. When we refer to the collective conscience of an audience we need to specify that this includes the cultural, political, ethical, and moral aspects of a group of individuals.

Narratives can be employed tortiously to manipulate an audience. Disinformation, ultimately, is the employment of a narrative to mislead or influence a particular audience. According to NATO, Disinformation can be defined as "Information which is intended to mislead".

3.0 RUSSIAN TACTICS, TECHNIQUES, AND PROCEDURES ON INFORMATION WARFARE

After the conceptual approach, it is necessary to understand how Russia interprets information warfare. The concept of "Active Measures" made its first appearance in the 1960s during the Cold War. It can be simply defined as a facade aimed at concealing and influencing foreign governments. The influence was achieved through the employment of several psychological and information warfare techniques such as disinformation, propaganda, sabotage, extortion, etc. These measures constitute an integral part of Russia's cultural warfare strategy. One of the noteworthy transformations of contemporary active measures, as compared to those of past decades, is the shift from rigid centralization to diversified, and even somewhat universalized, responsibilities. This has resulted in competition among various stakeholders who are expected to develop their semi-autonomous plans while aligning them with overarching objectives [9].

Despite these organizational advancements, the techniques employed as active measures have undergone no substantial changes over the years. The primary transformation occurred in the 1990s with the inclusion of cyberspace as a new operational domain. This expansion broadened the array of tools available and ushered in an unparalleled enhancement in dissemination capabilities [10].

Nonetheless, it is vital to note that, while this particular perspective appears to have established itself within public opinion, information warfare, and operations are neither a new phenomenon nor confined to the virtual realm, nor limited solely to propaganda, disinformation, manipulation, false news, or cyberattacks [10].

Western sources highlight Moscow's perception of information warfare as an asymmetrical instrument situated within the ambiguous boundaries of the conflict's grey zone. The Russian understanding of information warfare encompasses not only military actions but also a wide array of non-military activities that span the physical, logical, and cognitive domains. These include molding public opinion to garner support for military endeavors without the direct application of armed force [11].

The application of Russian information warfare is adaptable to varying contexts, ranging from peacetime to escalations and open conflicts, spanning strategic, operational, and tactical dimensions. It encompasses offensive and defensive facets, aiming to achieve information superiority over adversaries while safeguarding the nation's information infrastructure for the sake of strategic stability [11].

In this context, "the information landscape is an all-encompassing domain, wherein any medium, channel, or physical, radio-electronic, digital, or cognitive vector can be manipulated, modified, or corrupted, thereby transforming them into instruments of information warfare (informatsionnoe oruzhie)" [11].

Consequently, an assortment of strategies is utilized within the realm of information warfare, including the disruption of air defense systems, suppression of communication facilities, manipulation of GPS signals, online censorship, the dissemination of disinformation, image tampering, and the removal of journalistic content. When employed in concert, these tactics are designed to achieve both technical impacts on adversary infrastructure and psychological effects on their perceptions [12]. It is posited that Russia employs a wide array of active measures encompassing the use of multilingual online media and platforms, such as TASS, Sputnik, and RT, to project Russia's image internationally while undermining the influence of Western media. These channels serve as conduits for official propaganda and act as sounding boards for supplementary activities occurring within the blogosphere and social networks. Additionally, Russia leverages clandestine media to propagate unofficial disinformation, often denoted as "grey" or "black"

propaganda. Moreover, modern agents of influence and collaborators who espouse pro-Russian narratives are more numerous and prominent, traversing the entire political spectrum. They harness media outlets and social platforms to disseminate ostensibly objective propaganda while actively engaging with their followers. Finally, active measures harness a gamut of digital tools to maximize their efficacy and minimize traceability, including the deployment of trolls, hackers, and bots [12].

4.0 THE INFORMATION ENVIRONMENT ANALYSIS AND ITS INTEGRATION WITHIN A STRATEGIC COMMUNICATIONS PLAN

Before attempting to analyze the flow of information within a particular audience the need to establish a framework of study must be addressed. An information environment in its simplest form comprises traditional media (written press, radio, and television) and digital media. When applying NATO doctrine to the concept, an information environment can be defined as the main decision-making environment where individuals and organizations receive, process, and transmit messages, information, and knowledge. This is the cognitive domain.

The cognitive domain can be defined as the dimension in which all these activities take place either through action or inaction (Weaton et al. 2022). Individuals or groups of individuals can be influenced by the flow of information in the cognitive dimension; their behavior, values, and morals can be affected and modified. The cognitive domain is composed of two layers: 1) the cognitive layer and 2) the social layer. The cognitive layer involves the interpretation of information but excludes its transmission while the social layer focuses on the behavior of individuals prompted by their socio-cultural context.

With the advent of the digital age, the flow of information is much faster. Individuals are constantly exposed to rapidly changing narratives meaning that their behaviour can be easily conditioned by the constant exposure to messages both through digital and traditional media. In this context, a comprehensive understanding of the information environment is vital mainly because although the cognitive field has always been at stake, today it has gained even more relevance.

A considerable part of the data flow is propaganda and disinformation; both cannot be considered ‘information’ as both elements are naturally targeted at influencing and penetrating groups of individuals to modify their behavior and their way of thinking [13]. Occasionally a disinformation narrative can be more successful at influencing an audience than a rather plain or positive narrative. Both propaganda and disinformation can affect the decision-making process by influencing a society or segmented groups especially when applying tailor-made narratives to groups of individuals.

As previously mentioned, the proposed methodology for an Information Environment Analysis necessarily requires the establishment of a framework of study [14]. Our framework of study can be defined by a country, continent, region, etc... or any other form of political and geographical divisions that may be of interest to policymakers and decision-makers. Once this framework has been defined, a PMESII analysis must be performed to understand the context in which that particular geographical or political entity unfolds. Once this prior approximation has been successfully made, a mapping of the flow of information within our information environment must be done to understand the perception and behaviors of the public as well as to determine if these behaviors and perceptions are being influenced by third-party actors or state actors with nefarious motifs [15]. This step involves classifying the media outlets (both digital and physical), social network actors, etc. based on audiences, ideological tendencies, affinity with the government, political parties, religious groups, and in short power groups.

Audience analysis will allow us to identify leverage points that can change or reinforce audience attitudes or behaviors. A preliminary classification of an audience must fall into one of these three categories: friendly, neutral, and hostile. The level of classification may be increased on further investigations but must always be approached from the general feeling of the audiences towards us.

As defined by NATO, the information environment analysis attempts to evaluate the effectiveness of strategic communications or in other words, to understand and shape the information environment by informing and influencing the attitudes and behaviors of audiences. NATO doctrine on strategic communications consists of three main elements: understanding, integrated planning, and narrative-driven execution. The latter uses narratives as a global expression of a strategy to inform and influence all audiences and give context to the campaign, operation, or situation [16]. The integration of an information environment analysis into a strategic communications plan is necessary not only to determine the main narratives and force ideas that affect the target audience but also to establish early warning indicators both to determine the effectiveness of our plan or to detect foreign threats and disinformation that may be affecting the behaviors of individuals within our target audience.

5.0 PROPOSED METHODOLOGY FOR AN INFORMATION ENVIRONMENT ANALYSIS AND ITS EFFECTIVENESS IN COMBATING RUSSIAN INFLUENCE OPERATIONS; THE THREE-PHASE APPROACH

The proposed methodology for an Information Environment Analysis is based on the recollection of large quantities of data with sufficient quality to determine the underlying narratives that affect the targeted Information Environment. This method involves several phases that must be followed rigorously to ensure its success.

The first phase involves determining an Information Environment through the careful examination of all the sociological, political, and economic elements of the target population. It is advisable to establish a simple framework such as a country, region, or continent. If wanting to analyze several audiences at the same time, it is recommendable to group those audiences by cultural, linguistic, or geopolitical similarities. For example, in the context of the war on Ukraine, EU countries could be grouped under the same information environment due to the political, cultural, and economic similarities between those countries. If our information environment comprises a large quantity of countries (or audiences) the level of information that will be gathered will have a considerably lower quality when compared to the singular analysis of an audience.

In the framework of the study, the principal actors, cultural groups, influencers, and media outlets and their scope must be defined to improve the quality of our data. Individuals must be grouped by the level of hostility they show towards the relevant actors that have been identified within the system. Hostility can be determined by the number and the content of the messages emitted by individuals. The more polarised an environment is, the easier it will be to propagate disinformation within that audience. Early warning indicators must be established in this phase to detect harmful messages that may flow inside our Information Environment.

The extraction of data must be focused on traditional and digital media, especially digital newspapers and social media. The main explanation for this is the rapid and constant nature of highly digitized Information Environments. When dealing with the war in Ukraine, digital media outlets can emit large quantities of publications in a matter of hours, especially during events such as the “Wagner Coup”. Social media has a similar nature, users will interact and exchange information with different grades of hostility. A narrative first seen on a digital media outlet can be replicated and viralised on social media, expanding the original audience of the outlet to millions of users. Another process that may occur is the spontaneous appearance of a narrative on social media that is replicated on a digital outlet. Once a media outlet replicates a narrative first seen on a social network, users or individuals will believe that narrative to be truthful, regardless of the disinformation found within that narrative or linked to it.

The purposeful relegation of social media when analyzing an Information Environment may impede decision-makers from detecting disinformation campaigns. Russia understands the importance of social

media; the US has dominated traditional media forcing Russia to further develop its capacities on social media to counteract US influence [17]. During the 2014 invasion of Crimea, one of the main narratives seen both on social media and traditional media was that "Ukraine is turning into a fascist state". This narrative was further employed by Russian state media outlets during the 2022 invasion of Ukraine. This narrative is a disinformation narrative designed to delegitimize Ukraine's existence and even though the EU managed to block the access to Russian media, there's still a considerable amount of Russian channels and users that continue to propagate this narrative on social media. If we decide to ignore social media in our analysis, our capacity to detect and counteract against the "denazification" narratives would be minimal and as previously mentioned if our audiences are continuously exposed to these narratives, their behavior or their way of perceiving Ukraine could rapidly change.

A second phase would imply the analysis of all the recovered data. This phase must be recurring meaning that it must be constantly repeated to inform decision-makers on what kind of messages are affecting our Information Environment. The period for our analysis will be determined by the quality level of the data we want to achieve. If the analysis is performed daily, it is quite probable that the data samples might not be enough to detect patterns, narratives, and force ideas. The analysis phase must once again be focused on the groups, actors, and individuals that have been identified during the first phase so that we can understand the changes that are occurring in those groups. A system of indicators should help to identify if our audience is being influenced by a Russian disinformation campaign (or other foreign actors). Indicators must be based on two different but complementary layers 1) hostility and 2) narratives and force-ideas. If our audience begins to swiftly vary their aggressiveness towards other actors in the system this might indicate that our audience might be the subject of a targeted campaign. The second layer focuses on the rapid change of narratives and force-ideas. If our audience begins to emit or transmit contradicting messages this might indicate that the 'conversation' is being manipulated for a nefarious purpose, such as destabilizing, demoralizing, or merely changing the perception of individuals.

Finally, the third phase should include a prospective analysis of how those particular groups and individuals might evolve in the near future when exposed to our Strategic Communications Plan or foreign harmful narratives. For the successful elaboration of a prospective analysis, all elements of both the first and second phases must be achieved. How the prospective analysis is done, will be highly influenced by the level of detail of our original framework of study. This third phase is the more complex one as it requires a considerable amount of data to support our prospective analysis.

6.0 CONCLUSIONS

Russian communications strategy during the war in Ukraine has proven to be extremely varying and adaptable, especially when taking into account the different events that have taken place during the conflict. Narratives have arisen and disappeared in a matter of days making it extremely difficult to analyze an ever-changing information environment.

To adapt to the Russian narrative bombardment and disinformation, the Information Environment Analysis appears as an essential tool not only for Strategic Communications but also to protect the general public opinion from hostile narratives and disinformation. NATO doctrine gives us a primary approach to the correct elaboration of an Information Environment Analysis but the concepts previously mentioned are difficult to apply daily and require tools too complex or costly to provide consistent results.

The proposed methodology in this article attempts to complete or further develop NATO doctrine on this matter through a simple but effective approach, based on the observation and compilation of messages. The proposed preliminary approach is based on the identification of digital media outlets (and their narratives and hostility towards the actors within our system) and the careful monitoring of social media. Social Networks are likely to show the general perception of the public to narratives and events as well as the identifying

users that might expand harmful narratives and disinformation. The three1phase approach should complete NATO's doctrine and allow users to develop a successful information environment analysis while understanding the intricacies and complexity of information environments, especially when analyzing those implicated in a conflict such as the War on Ukraine.

Hostility and the careful analysis of narratives and force ideas need to be mandatorily implemented as indicators of 'change'. Variations in our system of study need to be rapidly identified to support the decision-making process, not only when related to Strategic Communications but also when exposed to disinformation structures, such as Russian state media.

7.0 REFERENCES

[1] Fabián, F. O. (2022, 29 November). Panorama de la Guerra entre Rusia y Ucrania. Global Affairs and Strategic Studies. https://www.unav.edu/web/global-affairs/panoramade-la-guerra-entre-rusia-y-ucrania

[2] Masters, J. (2023, 14 February). Ukraine: Conflict at the Crossroads of Europe and Russia. Council on Foreign Relations. https://www.cfr.org/backgrounder/ukraine-conflict-crossroads-europe-and-russia

[3] J., & Matasick, C. (2022, 3 November). Disinformation and Russia's war of aggression against Ukraine. OECD. https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/

[4] Center for Preventive Action. (2023, 17 October). War in Ukraine | global conflict tracker. Council on Foreign Relations. https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine

[5] Messieh, N. (2023, 21 June). Undermining Ukraine. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine/

[6] Colom Piella, G.. Wagner and his "march for freedom": the two days that shook the Kremlin. IEEE Opinion Paper 70/2023. https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO70_2023_GUICOL_Wagner.pdf

[7] Colom, G.; & Vallejo , G. M. (2023, October). Segundas impresiones militares de la guerra de Ucrania. Revista Ejército, 986, 12–18.

[8] Littell, J., & Starck, N. (2023). Russian influence operations during the invasion of Ukraine. International Conference on Cyber Warfare and Security, 18(1), 209–217. https://doi.org/10.34190/iccws.18.1.971

[9] Zochowski, D. (2018, November 7). Active measures. Russia's Key Export. OSW Centre for Eastern Studies. https://www.osw.waw.pl/en/publikacje/point-view/2017-05-30/active-measures-russias-key-export

[10] Marín Gutiérrez, Francisco. ¿Comprendemos la desinformación?: Rusia y la evolución de las medidas activas. Documento de Opinión IEEE 26/2022. https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO26_2022_FRANMAR_Rusia.pdf

[11] Colom Piella, G. (2020). Anatomía de la desinformación rusa. Historia Y Comunicacion Social, 25(2), 473-480. https://doi.org/10.5209/hics.63373

[12] Colom Piella, G. 2019. Los enfoques estadounidense y ruso a la guerra informativa en M. R. Torres (Ed.), #Desinformación Poder y manipulación en la era digital (pp. 1–14). Comares, S.L.

[13] Baqués Quesada, J. (2021). De las guerras híbridas a la zona gris: la metamorfosis de los conflictos en el siglo XXI. UNED

[14] Blunt, R., Riley, & C., Ritcher, M. (2018). Using Data Analytics and Machine Learning to Asses NATO`s Information Environment. In NATO Science and Tecnology Organization. https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-160/MP-IST-160-S2-2.pdf

[15] Klonowska, K., & Bekkers, F. (2021). Behaviour-Oriented Operations Military Context. The Hague Centre for Strategic Studies. https://hcss.nl/wp-content/uploads/2021/03/Behavior-Oriented-Operations-March-8th.pdf

[16] Schwile, M., Welch, J., Fisher, S., Whittaker, T., & Paul, C. (2021). Handbook for Tactical Operationes in the Information Environment. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/tools/TLA700/TLA732-1/RAND_TLA732-1.pdf

[17] Treyger, E., Cheravitch J., & Cohen, R. (2022). Russian Disinformation Efforts on Social Media. Santa Monica, CA: RAND Corporation, https://www.rand.org/pubs/research_reports/RR4373z2.html.