Norwegian Institute of International Affairs

NEW STRATEGY CENTER

HOW TO DEAL WITH THE INFORMATION WARFARE CHALLENGE IN THE BLACK SEA REGION?

FLANKS Policy Brief

Alina BÂRGĂOANU

Jakub GODZIMIRSKI

Daniel IONIȚĂ

The research is a result of the implementation of the bilateral initiative "Enhance knowledge of Russia's behaviour in the Kola Peninsula and the Arctic region, as well as the Crimean Peninsula and the Black Sea region – and to compare in terms of similarities and differences", financed under the Fund for bilateral relations 2014-2021.

Project implemented by

Authors:

Alina BÂRGĂOANU

Jakub GODZIMIRSKI

Daniel IONIȚĂ

Graphics coordinator:

Izel SELIM

www.nupi.no

www.newstrategycenter.ro

Summary

In the aftermath of the conflict between Russia and Ukraine the situation in the Black Sea Region has attracted more attention. The scope of Russian intervention in Ukraine, the annexation of the territory of the neighbouring state and Russia's massive use of various active measures to promote what the ruling Russian elite understood as the country's national interests have forced regional actors to adopt various types of counter-measures. The aim of this policy brief is to examine how countries in the Black Sea Region (BSR) should deal with the new challenge posed by Russia's use of various information-related instruments and how the situation in the information sphere in the area should be dealt with by regional actors and other players with stakes in this region.[1]

The issue of Russian information warfare in the region and beyond it must be dealt with in a balanced manner. On the one hand it is important to understand what drives Russian policy in that area and what the role of information tools in Russian strategic designs is. On the other hand, it is also important to adopt a rational approach to this challenge and appropriate measures to deal with it at both national and regional levels.

Having in mind the institutional framework shaping situation in the region it is crucial to help countries in the region improve their national ability to deal with this challenge by increasing the level of national resilience. Important steps in this direction can be made by improving institutionalised cooperation and coordination among countries that belong to the same Western institutional clubs, by adopting a flexible and constructive approach to cooperation with other countries in the region that face similar problems and are interested in deepening their cooperation on these questions with Western institutions, and by

[1] This policy brief presents the most important findings and conclusions presented in more detail in the FLANKS Working Paper *Information Warfare and Information Operations in the Black Sea Area* prepared jointly by members of the FLANKS project and available at the projects website at https://www.newstrategycenter.ro/flanks-project/

adopting a realistic approach to cooperation with other actors in the region who are either unable or unwilling to work together on addressing these questions.

Understanding the challenge of information warfare

The unprecedented technological and societal changes and the more active use of information tools by many actors have put the issue of information warfare higher on national and international agendas. Information warfare in the broadest terms can be defined as the conflict or struggle between two or more groups in the information environment, but various actors have adopted various approaches to the use this tool in the political context. On the one hand there is a Russian broad approach where information operations can be launched not only during the open conflict, but also in peace time as an element in what is sometimes referred to as a full-spectrum approach to conflict, and on the other hand there is the Western approach treating information operations as limited, tactical tools carried out during open hostilities.

Using information and information manipulation as a policy instrument is not by any means a new phenomenon. What is however a new dimension is how the higher level of digitization of political and social space and the relatively recent emergence of social media have changed what could be described as 'framework conditions' for information operations. While only some decades ago the national information space was more homogenous and much easier to be controlled and shaped by national decisionmakers, today the information space is no longer subject to any national control and both producers and consumers of information can produce and consume information in an almost unlimited and uncontrolled and uncontrollable manner.

The higher level of political conflict between the West and the rest, including Russia and China, the more active use of information tools in what could be termed as the war of competitive narratives that aims at winning the hearts and minds of population in the

opposing camps as well as various approaches to the use of information operations adopted at national levels explain why the issue of information warfare deserves more attention and needs to be addressed by national and international policymakers.

Russian approaches to information warfare

Russia is one of the important and most active state agents employing information warfare to advance its strategic agenda. Its approach is driven by an all-encompassing strategic understanding of information warfare both for peace and wartime, by identifying and creating security gaps, by mounting offensive and defensive information operations, and by the integration of propaganda and disinformation for tactical purposes.

The Russian policymakers and experts treat questions related to information warfare as an important element of broadly understood security, both in defensive and offensive terms. Many Russian experts see Russia as the main victim of Western strategic information warfare aimed at weakening or even destroying Russia as an important and sovereign actor. However, there are also many examples of the offensive use of information operations by Russia, in areas close to Russia's borders and elsewhere.

These defensive and offensive aspects of information warfare are well understood by Russian policymakers who in 2016 "produced" the country's Doctrine for Information Security. The document approaches information in the broadest possible manner, defines threats to information security as "a combination of actions and factors creating a risk of damaging the national interests in the information sphere", and lists several national interests in the information sphere.

What seems to worry Russian officials the most in defensive terms is the question of how to protect the country against what they define as malign external influences. The most important defensive challenges are the questions of transboundary information circulation

that is used for geopolitical goals, goals of a military-political nature contravening international law or for terrorist, extremist, criminal and other unlawful ends detrimental for international security and strategic stability.

This dual defensive/offensive approach is also visible in how these questions are addressed in Russian strategic documents. The 2015 National Security Concept mentioned information-related questions 36 times, focusing on defensive aspects of information security, while the Foreign Policy Concept of the Russian Federation, approved in November 2016, pays more attention to the offensive utility of information measures for Russian foreign and security policy. It states, for instance that "the State's foreign policy activities shall be aimed at … bolster[ing] the standing of Russian mass media and communication tools in the global information space and convey[ing] Russia's perspectives on international process to a wider international community".

Examination of the role of information operations in Soviet/Russian policy towards the West has a long history and those questions should be therefore well understood by those who are responsible for policy towards Russia in the West. However, when the Ukraine crises unfolded in 2014, the West was not mentally or politically prepared to cope with Russia's massive information campaigns that combined traditional methods of Soviet-style propaganda with the use of new information channels in what is sometimes recognised as a key dimension in an ongoing Russian "hybrid war" on the European theatre. The Russian government has been accused of directly or indirectly sponsoring various more covert information efforts, such as "troll factories" that are to support Russian official efforts in the field of information or the production and circulation of false information that was to saw confusion and undermine cohesion of Western societies.

Russian information operations serve several strategic goals set by the current regime. The most important of these goals is Russia's interest in undermining the cohesion of the West and popular trust in Western institutions and elites that support European and trans-

Atlantic integration and cooperation. These efforts are launched not only in the countries that have already joined Western institutions but even more so in the countries that aspire to become a part of the broadly understood West. The information operations aim therefore at making the Western ideas less attractive to Russians and other post-Soviet citizens who could be inspired by Western values which could in turn undermine Russia's dominant position in the region, as was the case with Ukraine in 2014.

To achieve these objectives in the region Russian disinformation tactics rely on a set of commonly-shared narratives such as: (1) reinterpretation of history and emphasizing old communal fears and existential security dilemmas; (2) spreading of fake news and conspiracy theories with an anti-Western tinge; (3) using negative stories from one country to influence perception or emotions in another one; (4) amplifying anti-establishment and anti-European sentiments; and (5) scapegoating the foreigner, the immigrant, and the globalization process.

By undermining the Western cohesion and attractiveness Russia may be able to better promote its own interests in an international environment characterized by a higher level of compartmentalization, lack of Western unity and where known rules of the game are put under pressure, also from within the West, to mention only the case of the anti-liberal turn symbolized by Donald Trump or the developments in some of the EU and NATO member states described as democratic backsliding.

Russian information challenge in the Black Sea Region

The Black Sea Region is one of the areas where the questions related to information warfare have gained more traction in the policymaking circles, especially in the aftermath of the 2014 Russian aggression against Ukraine and the annexation of the Crimean peninsula that have resulted in growing tensions between Russia and the broadly understood West. The geographical proximity of the area of the hot conflict involving two greatest – in territorial

terms – European countries and the Russian hyperactive use of information space to promote its official vision of the conflict as well as its more aggressive policy towards its neighbours have forced regional actors to rethink their approaches to regional cooperation and adopt various measures to counter negative impacts of Russian actions.

Russia's has clear strategic interest in the Black Sea Region as this region represents a critical strategic intersection, where Russia meets various types of actors. This also explains why this region is among the main battlegrounds for Russia's information warfare where specific tactics and the distribution of narratives are used to undermine good neighbourly relations among the states in the region – Bulgaria, Georgia, Romania, Russia, Turkey and Ukraine, and the hinterland, including the South Caucasus and Moldova.

To understand what impacts Russian efforts in the information sphere can have in the region it is crucial to map what types of actors in the region Russia must deal with. The list of those actors includes:

- Western and non-Western institutions and organisations;
- States, like Romania, Bulgaria and Turkey that have already joined various Western institutions such as the EU and/or NATO;
- States, like Georgia or Ukraine that have expressed interest in joining Western institutions and/or deepening cooperation with the West;
- States, like Armenia, that for various reasons have sought a closer cooperation with Russia itself;
- Political units, like Abkhazia, South Ossetia, Transdniestria or the two units DNR and LNR established in Eastern Ukraine that have created some forms of statehood that are recognized either by only a small number of states, or not recognized at all.

Russian policy in general and towards the region is informed by the predominantly realist understanding of international relations where a zero-sum game is believed to be played. The main opponent of Russia in this realist game is a collective and united West

represented by its institutions (the EU and NATO). It is therefore of utmost importance from the Russian point of view to limit the West's ability to project its soft power to Russia and to areas that the current regime defines as Russia's exclusive zone of interests and influence. In addition, it is also crucial from the Russian official point of view to weaken the Western influence in the areas where the liberal West has already expanded or can be expected to expand.

Russian information operations serve often this strategic purpose and are tailored to be most effective in the given political, institutional, geographical, social and historical context. Taking into account the complexity of the institutional set up in the Black Sea Region and the variety of actors operating in this area we should therefore expect Russian information operations to be tailored to address specific regional issues and to be aimed at various types of actors.

We should also expect these operations to attempt to exploit various types of strategic vulnerabilities existing in the region, such as weak governance, underdeveloped civil society space, underfunded independent media or corruption. Russian objectives can also be attempted achieved by cultivating relationships with autocratic leaders and populist parties or by building political alliances with ideologically friendly political groups and individuals, or by establishing pro-Russian organizations in civil society to legitimate and diffuse Moscow's views.

The very same institutional set up existing in the BSR shapes also the space for the Western response to those Russian information-related attempts at influencing the situation in the region. As the states of the region belong to various institutional clubs and have chosen various political paths their ability to resist information pressure from Russia will depend not only on their national capabilities, that vary greatly, but also on how they can cooperate and coordinate their policies in the broader institutional context.

Both the EU and NATO have been paying increasing attention to the questions related to various aspects of information warfare and their institutional expertise on these questions should be shared with all regional actors who either are their members or seek closer cooperation with these institutions. However, when trying to coordinate their policies these institutional actors must have in mind national interests, conditions and vulnerabilities to actions in the information sphere undertaken by other actors.

For instance country reports for Bulgaria, Ukraine, Georgia, Moldova, and Armenia suggest that the overall resilience of these countries to Russian propaganda is rather low, showing variable levels of vulnerability to media manipulation, fake news, and the narratives prompted by Russian-controlled media. There are various explanations for why the situation has developed in that way but there is apparently a strong correlation between outlets employing Russian-based propaganda narratives and increased patterns of ownership, financial dependency, and informal political links between pro-Russia groups and media outlets. For example, in Bulgaria the impact is more constrained, in Romania more limited due to the linguistic barrier, in Ukraine the situation is mixed, because on the one hand the authorities have embarked on more active policy to limit the Russian influence in the information space, but the level of Russian media penetration is still relatively high, while in Georgia, Armenia, and Moldova, which rely heavily on Russian media, Russian influence is still more prominent.

Conclusions and policy recommendations

When addressing questions related to various aspects of information warfare and operations national and regional policymakers must focus on what is realistically possible to achieve and embark on policies that will help them address these issues at national levels. When planning policies and measures to be taken they need to consider not only national conditions, capabilities and vulnerabilities but also how the information-related challenges can be coped with by combining national capabilities and various forms for

institutional intergovernmental and expert coordination and cooperation. As mentioned earlier both the EU and NATO have embarked on more active policies when addressing the issue of various forms of external malign influence, including questions related to various forms and aspects of information warfare and operations.

In his recently published comments on the UK policy towards Russia Mark Galeotti shared his views on how to deal with the Russian information challenge in the current strategic context.[2] His opinions seem to hold value not only in the British context but also in more general terms and will be therefore used as a point of departure for policy recommendations presented in this policy brief.

In this recent text Galeotti argued that Information operations continue to be regarded as a serious threat, but at the same time there is still very little evidence that they actually have a major impact on people's attitudes in the areas that are targeted by Russia. His main conclusion was that policymakers should focus on addressing challenges on what he described as the demand side of the information operations. In his opinion the main problem faced by the West is what he refers to as a crisis of political legitimacy, making communities that feel alienated and unheard the natural constituency for information operations peddling alternative answers, conspiracy theories, and bile.

Policymakers that must deal with the challenge of the information warfare face therefore a double challenge. n the one hand it is crucial to address the issue on the supply side, or in other words get a good understanding of the role of information operations in strategic designs of the potential enemy and a realistic expectation of how our policies can – or cannot – influence the choices of our potential opponents in this field. To be better prepared to meet this challenge it is also important to map what kind of information operations can be launched to influence our societies by those potential opponents.

[2] Galeotti, Mark (2020) Ten Suggestions for A 'Russia Strategy' for the United Kingdom available at https://warontherocks.com/2020/07/ten-suggestions-for-a-russia-strategy-for-the-united-kingdom/

By getting a better understanding of what information operations can be launched by potential opponents those policymakers should also be better prepared to address the key problems on the demand side, which should be their main preoccupation. Their main task must therefore be to design and implement effective measures on the demand side, in their own societies that must be better prepared to meet the information challenge in an informed manner to make them less receptive to Russian arguments and less vulnerable to Russian projection of various types of soft power, including tailored information operations that are to influence opinions and perceptions in the targeted societies.

Galeotti argues that the most effective way of addressing the information challenge – not only from Russia but in more general terms – is to combine proper media and social media regulation with better media education at every level, from schoolchildren to seniors, to improve resilience to any malign efforts that could be met in the information sphere. In addition, it is also important to address what could be termed the root causes of distrust in societies they are to protect against external malign influence, which is a fundamental question that leaves the societies much more vulnerable to such information operations and manipulations.

Media and social regulation, mentioned above, should also combined with regulating the cyber, or digital environment. A botnet can be used for a DoS (DDoS) cyber attack as easy as for spreading fake news. In case of a cyber attack you can filter the traffic from the specific IP and get back the services. It could be useful to filter the news originating IP, as well. But for that, is necessary to control the cyber space without human rights violation, which is challenging. Operating a dynamic domain like cyber domain, require high level of knowledge and skills and for obtaining these, public policy should be rapidly developed and implemented in the area. For the EU countries, the EU COM support in legal framework elaboration and capacity building is continuously provided, but for the others States in the Black Sea region the Western partners support is vital.

The countries in the Black Sea Region face various types of challenges in this area and their responses should be therefore tailored to help them address the general political and specific, information-related challenges in the best possible manner. An important factor influencing their policies is also how they perceive the Russian information challenge in the region, which in turn is a function of their strategic perception of Russia either as an important partner or as a actual or potential source of strategic threat. The countries of the region that have become members of the Western clubs (the EU and NATO) and those seeking closer cooperation with Western institutions are perceived by Russia as potential enemies and should be expected, due to the logic of appropriateness, to embark on policies recommended and coordinated by those Western clubs. Countries of the region that have chosen to seek closer strategic cooperation with Russia will be on the other hand less prone to adopt Western-style policies towards this challenge, while the policies of the countries that still haven't made a clear strategic choice in favour of Russia or the West will be most probably characterized by a high level of vacillation.

Alina Bârgăoanu is a university professor; expert within the High Level Expert Group on Fake News and Online Disinformation, European Commission (2018); expert within the European Center of Excellence for Countering Hybrid Threats (since 2019); guest expert at Harvard University's Center for European Studies (2018-2019); domains of interest include: fake news and disinformation in the online environment, strategic communication, technological and digital literacy, online regulatory means, the Transatlantic relationship.

Jakub M. Godzimirski has been working on Russian foreign and security policy issues at NUPI for more than 20 years, paying special attention to the role of energy resources in Russian grand strategy. In addition he also has worked on European policy and its impact on developments in Central and Eastern Europe, including relations with Russia.

Daniel Ioniță is an expert in policies and strategies, with competencies in the field of cyber security acquired during the administrative and operational development of CERT-RO, from the position of director of the Analysis, Policy and Cooperation Department (January 2012 - March 2019). During the rotating Presidency of Romania at the EU Council, he coordinated, as president, the work of the European Group - Horizontal Working Party on Cyber Issues. He is a brigadier general in reserve.

The Norwegian Institute of International Affairs [NUPI] is a leading centre for research on international issues in areas of particular relevance to Norwegian foreign policy. NUPI has three main pillars of research and expertise: security and risk, growth and development, and international order and governance. The Security and Risk pillar covers traditional security and defence policy and peace operations, as well as other aspects of risk in Norwegian foreign policy related to greater investment, travel and presence abroad. Growth and development focuses on the emerging powers, international economics and developmental issues. Order and governance covers the multilateral system, regional organizations and how diplomacy as an institution works and evolves.

New Strategy Center is a Romanian think tank specialising in foreign, defence and security policy, a non-partisan, non-governmental organisation. New Strategy Center operates at three main levels: providing analytical inputs and expert advice to decision-makers; holding regular debates, both in-house and public, on subjects of topical interest; expanding external outreach through partnerships with similar institutions or organisations in Europe and the US, joint policy papers and international conferences. The Balkans and the Black Sea space are priority areas of interest for New Strategy Center.