Norwegian Institute of International Affairs

NEW STRATEGY CENTER

INFORMATION WARFARE AND INFORMATION OPERATIONS IN THE BLACK SEA AREA

FLANKS Working Paper

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.

Iceland Liechtenstein Norway grants

Norway grants

Project implemented by

NUPI Norwegian Institute of International Affairs

NEW STRATEGY CENTER

Authors:

Alina BÂRGĂOANU

Jakub GODZIMIRSKI

Daniel IONIȚĂ

Graphics coordinator:

Izel SELIM

www.nupi.no

www.newstrategycenter.ro

INFORMATION WARFARE AND INFORMATION OPERATIONS IN THE BLACK SEA AREA[1]

We live in an age that is driven by information.
Technological breakthroughs . . . are changing the face of war
and how we prepare for war.
William Perry, US Secretary of Defense (1994–1997)

Information warfare (IW) represents a continuously evolving preoccupation for defence planners, decision- and policy makers and researchers alike, prompted by the rapid evolution of communication infrastructures and technologies, such as cyberspace, microcomputers, and other information technologies (Molander et al., 1996).

Defining the concept starts with the realization that, in the 21st century, hard military aggressions based on inflicting physical damage to the opponent is only one possible form of attack. Conflict has taken new, immaterial forms, such as "launching non-lethal attacks against an enemy's information systems" (Stupples, 2015), or, in other words, information warfare. When potential adversaries attempt to damage infrastructures involving the control of electric power, money flow, air traffic, oil and gas, and other information-dependent items using ITC-related techniques, this form of IW inevitably takes on a strategic aspect (Molander et al., 1996).

Nowadays, the widespread use of mobile Internet-based technologies for all possible needs – starting from personal, basic needs to organizational, societal strategic ones – creates a totally new information environment which is platform, algorithm, big

[1] The FLANKS Policy Paper *Information Warfare and Information Operations in the Black Sea Area* was prepared by members of the FLANKS project and is available at the project's website at https://www.newstrategycenter.ro/flanks-project/

data driven, an environment that is inherently unstable and prone to cyber operations. The fact that, in such an environment, cyber operations target either the content (the information as such) or the information infrastructure to the point that the traditional distinctions content/ form, medium/ message no longer hold only adds to the complexity of the analysis dedicated to IF. Besides, more often than not, famous influence operations of recent times followed a two-step approach: targeting the information infrastructure (e-mail, databases), then using the extracted information to manipulate/ distort/ pollute/ inundate the whole information eco-system.

I. Defining information warfare

At the end of 1980s and the beginning of 1990s, the concept of IW was a cornerstone in the debate about the revolution of military practice, implying a redefinition of strategy to accommodate the unprecedented technological and societal changes (Ventre, 2016).

IW can be defined as the "conflict or struggle between two or more groups in the information environment" (Porche et al, 2013, xv). More nuanced definitions discriminate between two main understandings of how this new type of warfare is to be conducted: "The entry for "information war" (*informatsionnaya voyna*) in a glossary of key information security terms produced by the Military Academy of the General Staff makes a clear distinction between the Russian definition – broad, and not limited to wartime – and the Western one – which it describes as limited, tactical information operations carried out during hostilities." (Giles, 2016, 4).

The term is not without ambiguity, being used to refer to protecting or attacking the battlefield information, hacking, surveillance of one's information systems, and compromising the integrity of information (Hämäläinen, 2019).

In time, the term of IW has been replaced in the official vocabulary of the military operation with other formulations (e.g. information operations); however, its relevance for the analysis of modern conflicts remains, as proven by the pervasiveness of the term in recent scientific literature (Ventre, 2016).

Today, there is a significant overlap between the notion of IW and the notion of cyber warfare, suggesting that this particular type of conflict, using information and information systems as a weapon against the same targets owned by an opponent (Schwartau, 1996), is not limited to the military sphere, and can easily target civil infrastructures. Hence, the notion of hybrid warfare, a new type of conflict based on fluid distinctions between war and peace, between military and civilian spheres, between internal and external actors, where all sectors of a society of may be weaponised: economy, finance, natural resources, the judiciary, public information and public public sphere.

II. Current features and examples of the information warfare

As resulting from a systematisation of the numerous definitions provided in the literature (Ventre, 2016, 5-6), a number of features of the contemporary IW emerge: close link to our new technical and social structures, exploitation of our dependence on information technologies for social, economic, political, and cultural transactions, a fight to control the digital space in addition/ instead of the physical one, and use of information and the information digital infrastructure to attack the enemy.

Today, Western countries are investing important funds, efforts, and expertise to match the IW of China and Russia, especially in relation to attacking, defending and exploiting the vulnerabilities of Internet-based communications networks. What is becoming central to all warfare today is combining "electronic warfare, cyberwarfare and psy-ops (psychological operations) into a single fighting organisation." (Stupples, 2015).

One important manifestation of IW is instilling political turmoil and social divisions by taking advantage of the affordances of the digital age, with the contribution of individuals, plutocrats, and foreign states (Moore, 2018). In recent times, the acts of IW include attempts to compromising voting systems, vote suppressing to spreading propaganda and fake news, and direct attacks on public infrastructure via information systems, with satisfactory results in respect to the objectives (Desouza et al., 2020). Prominent examples in this regard are: Russia's 2007 Estonian and 2008 Georgian cyber campaigns (Guadagno & Guttieri, 2019), the Islamic State propaganda on social media

(Prier, 2020), Russia's use of IW in the conflict in Ukraine, 2014 (Giles, 2016), Russia's attempt at influencing the results of the Brexit referendum or of the US Presidential elections, 2016 (Desouza et al., 2020; Moore, 2018), and North Korea's cyber-attacks against South Korea, targeting banks, media companies, and national identification systems (Libicki, 2017).

For a proper understanding of the phenomenon, we must place the weaponisation of information and attention on social media at the heart of today's IW, taking into consideration its end goal of bending the information environment according to personal, organisational, or even national agendas (Singer, & Brooking, 2018). At the same time, attention must be given to anticipating future moves of those actors involved in IW, such as: kinetisation - "a greater overlap between the kinetic and non-kinetic dimensions of Russian operations"; personalization of attacks – customized attacks targeting high-level officials, military personnel, and prominent public figures; mainstreamization – by means of "crude disinformation, absurd fake news and infotainment websites"; proxyzation – identifying new fronts, particularly in Africa and Latin America, at the same time with intensifying polarizing, anti-system, anti-institutional narratives in Western countries (Vilmer et al, 2018, 159-62).

As we have already underlined, the current Internet-, platform-based information eco-system is such designed that it blurs the traditional distinctions between information (content) and information infrastructure. Being aware of the emerging features of the information eco-system, various actors involved in IW get more sophisticated and launch cheaper, and more deniable operations that seek to distort, sometimes even hack the information infrastructure by automated, aggressive techniques (bots, Artificial Intelligence, sock puppet accounts, clickbait, psychographics, micro-targeting, manipulation of algorithms) in order to distort/ amplify/ boost public visibility of a certain content. Hence, the new battlefields in IW: public attention, public opinion, public moods.

III. Information operations in the modern battlefield

A related concept to IW are information operations (IO), which include the collection of tactical information about an adversary together with the dissemination of propaganda

for competitive advantages over the opponent (RAND Corporation, n.d.). IO can be a "component of any type of military operation and can include efforts to exploit information as a commodity, in addition to technologically driven activities in such areas as cybersecurity, electronic warfare, and operations security" (Marcellino et al., 2017, 1). IO are playing a more significant role with the increase and development of new technologies.

IO are playing an increasingly important role in the national security, and are defined by some authors as attempts to "use and operationalize the power of information" by the government, while the target of IO is "the adversary decision-maker, and therefore the primacy of effort will be to coerce that person, or group of people, into doing or not doing a certain action" (Armistead, 2004, 16). Scholars examine how the power has changed over the last decades and put forward the idea that "information as an element of power is the most transferable and useful force at all political levels" (Armistead, 2004, p.9). Thus, in this "new battlespace of asymmetrical warfare that employed information technology and exploited the speed and reach of global connectivity to deliver content", information operations rely on the use of "many different capabilities such as deception, psychological operations, and electronic warfare to shape and influence the information environment" (Armistead, 2004, 9).

Some authors argue that the term is "employed by the U.S. intelligence community to describe actions taken to disrupt the information streams and information systems of a geopolitical adversary", and "unlike information warfare which is generally conducted during actual combat, information operations can be carried out in peacetime environments to influence civil affairs" (Arif, Stewart & Starbird, 2018, 3). IO are considered to be a key component of many contemporary countries' way of war. For example, recent studies emphasize that Russian IO encompasses the presence of a hybrid force, an emotional appeal, a platform control, a subverted reality and a manipulation of diaspora (Allen & Moore, 2018, 67).

In recent years, several studies attempted to emphasize the major relevance and occurrence of information operations in the modern battlefield. Multiple studies focus mainly on the Russian information operations, for instance, in the case of Crimea

annexation and the Donbass War (Pomerantsev & Weiss, 2014; Sazonov,et al, 2017). Some attempted to identify the Soviet origins of current Russian information operations (Treurniet, 2016), while others highlighted how hybrid regimes across the world are adopting similar tactics in their countries or that information operations are the key component of Russia's contemporary way of war (Pomerantsev, 2015; Allen & Moore, 2018).

Since the spread of the Internet and the social media networks explosion and reach, studies focused more on the way the international terrorists and insurgents use the internet and the information operations to present or advance their political agenda (Theohari & Rollins, 2011), on the strategic logic of Islamic State information operations (Ingram, 2015), on China's attempts to boost country's international approval rating (Brady, 2015) or on United States psychological actions and information operations in Afghanistan between 2001 and 2010 (Munoz, 2012).

Thus, an important IO strategy is to disseminate multiple contradictory narratives to create "information fatigue in which populations are overwhelmed with information and unable to determine what information is accurate - or more dangerously, no longer care" (Allen & Moore, 2018, 67). The ultimate goal is to undermine and destabilize "the economic and political foundations of the adversary" (Berzins, 2014, 48). In this hybrid landscape, "information operations have a great role to play" (Berzins, 2014, 49), as a "critical soft power tool", because they allow to shape perceptions of the targeted groups (Treurniet, 2016, 42). One of the goals of IO is not necessarily to "convince someone of something, but to strategically direct discourse in ways that kill the possibility of debate and a reality-based politics" (Pomerantsev & Weiss, 2014, 16). Information operations cover "all the uses of information and disinformation, by states or nonstate actors, as a tool of state power and includes military information support operations, cyberspace operations, electronic warfare, military deception, psychological operations, public affairs, and strategic communications" (Allen & Moore, 67). In terms of effects, they elicit confusion, division, disenchantment, and paranoia, and, consequently, "can potentially serve to silence political dissent, enable historical revisionism, and hinder collaboration" (Arif, Stewart & Starbird, 2018, 3).

Russia is one of the important state agents that employ information warfare (IW) to advance its agenda. Its approach is driven by a number of characteristics: an all-encompassing understanding of IW both for peace and wartime, creating security gaps, perpetually mounting offensive, and the integration of propaganda and disinformation as valuable IW tactics (Porotsky, 2019)

IV. Information warfare in Russian strategy

The Russian policymaking community treat questions related to information warfare as an important element of broadly understood security. In the current edition of the National Security Concept (President of the Russian Federation 2015) information-related questions are mentioned no less than 36 times. The document states that Russia is being put under "informational pressure" and recognises that "an entire spectrum of political, financial-economic, and informational instruments have been set in motion in the struggle for influence in the international arena". As a consequence, Russia must deal with the increasing level of confrontation in the global information arena that is caused by the aspirations of some countries to utilise informational and communication technologies to achieve their geopolitical objectives. To counter these threats the state is to develop an improved system for identifying and analysing threats in the information sphere, to protect society from the influence of destructive information from extremist and terrorist organisations, foreign special services, and propaganda structures.

Russian expert debate on the use of information instruments as a strategic tool is characterized by the dual, defensive and offensive, approach. On the one hand many Russian experts see Russia as the main victim of Western strategic information operations aimed at weakening or even destroying Russia as an important and sovereign actor (Bartosh 2014, 2015, 2017, Panarin 2017). On the other hand, there is also a good understanding of how to use information operations offensively as exemplified by the Russian aggressive use of strategic communication after the outbreak of the conflict in Ukraine (Darczewska 2014, Giles 2015, Herpen 2016).

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 (President of the Russian Federation 2016). This official document provides many insights into Russian thinking about the role of information in the broader political context. 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. In the context of strategic communication aimed at both the domestic and foreign audience especially the question of "providing the Russian and international community with reliable information on the State policy of the Russian Federation and its official position on socially significant events in Russia and in the world, and applying information technologies to ensure the national security of the Russian Federation in the sphere of culture" and the issue of "facilitating the development of an international information security system aimed at countering threats of the use of information technologies to compromise the strategic stability, at strengthening equal strategic partnership in the sphere of information security, as well as protecting the information sovereignty of the Russian Federation" seem to be most crucial.

What seems to worry Russian officials the most in defensive terms is the question of how to protect the country against 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. Also, the fact that several countries are building up their information technology capacities to influence the information infrastructure in pursuing military purposes, that intelligence services are using information and psychological tools to destabilize the internal political and social situation in various regions across the world, thus undermining sovereignty and violating the territorial integrity of other states, are viewed as serious challenges. This document states also that Russia needs to counter a trend among foreign media to publish an increasing number of materials containing biased assessments of State policy of the Russian Federation. In addition, the document claims that Russian mass media face blatant

discrimination abroad and the population in Russia is put under growing information pressure aiming at eroding Russian traditional and spiritual values.

While the National Security Concept focused on defensive aspects of information security, the Foreign Policy Concept of the Russian Federation, approved in November 2016, is very frank about 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" (The Ministry of Foreign Affairs of the Russian Federation 2016).

Examination of the role of information operations in Soviet/Russian policy towards the West has a long history (see Barghoorn 1962, Byrnes 1962, Pipes 1973, Shultz and Godson 1986, Van Oudenaren 1986, Bittman 1987, Thomas 1998, Thomas 2014). Nonetheless, 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 (Pomerantsev, Weiss and Institute of Modern Russia 2014, Herpen 2016, Malashenko 2016, Bergmann and Kenney 2017, Polyakova 2017). Some scholars hold that information operations should be recognised as a key dimension in an ongoing Russian "hybrid war" on the European theatre (Baev 2016). 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 (Soldatov and Borogan 2015, Aro 2016) or the production and circulation of false information.

Shekhovtsov (2018) observes that RT routinely uses radical right-wing European politicians and personalities as political commentators. This may legitimize RT points and appeal to some fringe groups in the Western societies that are used by official Russia to promote interests that are consistent with the interests of the current regime but not necessarily with the interests of the Western institutions and countries in question (Makarychev and Braghiroli 2016).

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, 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.

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. In the predominantly realist Russian understanding of international relations where a zero-sum game is believed to the played, a collective and united West represents the greatest challenge in both power and value terms. It is therefore of utmost importance, from this Russian realist perspective, 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. Undermining the cohesion, attractiveness and unity of the West and its partners may be therefore viewed as the best way of advancing Russia's strategic interests, including the interest in being recognized as a legitimate great power, which is the key Russian strategic concern. Russia aims therefore at weakening the trust between the ruling elites and population in the West and in the countries that may seek closer cooperation with the West and is therefore interested in "helping" political forces that represent more pro-Russian and anti-Western EU views to be put in charge of national policies (Gressel 2017, Gude 2017, Rogers and Tyushka 2017, Shekhovtsov 2018).

When launching information operations, Russian policymakers will often tailor their efforts so as to be most effective in the given political, geographical, social and historical context. For instance, in Central and Eastern Europe they seek to sway policies away from European integration and toward Russia by exploiting such strategic

vulnerabilities as weak governance, underdeveloped civil society space, and underfunded independent media, and by cultivating relationships with rising autocratic leaders and nationalist populist parties. Other areas subject to Russian information activities have different strategic vulnerabilities, so approaches must be more subtle: aimed at building political alliances with ideologically friendly political groups and individuals, and establishing pro-Russian organizations in civil society to legitimate and diffuse Moscow's views (Polyakova, et al. 2016). In the following section we examine therefore how Russian information efforts have been tailored when approaching actors in the Black Sea Region and what measures have been taken in the region to address information-related security challenges.

V. Russian Information Warfare in the Black Sea Region

The Black Sea region is among the main battlegrounds for Russia's IW, where specific tactics and the distribution of narratives are used to undermine good neighborly relations among the states in the region (involving six countries – Bulgaria, Georgia, Romania, Russia, Turkey and Ukraine, and the hinterland including the South Caucasus and Moldova) (Rebegea, 2017). Russia's has clear strategic interest in the region, as the Black Sea region represents a critical intersection: "Many experts believe that whoever controls or dominates the Black Sea can easily project power to the European continent, mainly in the Balkans and Central Europe, but also in the Eastern Mediterranean as well as the South Caucasus and the northern Middle East." (Anastasov, 2018). IW and IO in the region play an important part in Russian national security strategy for fragmentation and subversion, are presented as purely defensive measures and are to help recreate a buffer zone in areas where Russia meets the West (Schwartz, & Diamond, 2017).

Russia's interventions have been described as the employment of "soft-power tools of malign influence" (Flanagan & Chindea, 2019, 7), while taking advantage of democratic and governance shortcomings. Their playbook of techniques includes: "sensationalism rather than facts; binary black-and-white portrayal of Russia in positive terms and the West in negative terms; sarcasm; baseless historical parallels and generalizations; and heavy citation of Russian officials and news agencies" (Flanagan & Chindea, 2019, 7).

Although the domestic situation of the Black Sea states varies, Russian disinformation tactics rely on a set of commonly-shared narratives, as synthetized by Rebegea (2017): (1) Reinterpreting 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.

The considerable attention given to Russia's IW reflects acute concerns about the growing impact of nation-driven strategies to control the narratives surrounding their operations, while influencing the decisions and behavior of other actors, facilitated by the new technologies and habits of acquiring and using information on social media (Tashev et al., 2019).

The effects are variable according to the targeted states, with the question of media ownership being quintessential: "There is 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 in the five Black Sea countries." (Filipova, & Galev, 2019). For example, in Bulgaria the impact is more constrained, while in Georgia, Armenia, and Moldova, which rely heavily on Russian media, it is more prominent (Flanagan & Chindea, 2019, 7).

Country reports in Bulgaria, Ukraine, Georgia, Moldova, and Armenia (Filipova et al, 2018) suggest that the overall resilience of the Black Sea region to Russian propaganda is rather low, showing variable levels of vulnerability to media manipulation, fake news, and the narratives prompted by Russian-controlled media.

Some authors (Thomas, 2004; Snegovaya, 2015; Treurniet, 2016) argue that Russia's information warfare in not a novelty and "is fundamentally based on older, well-developed and documented Soviet techniques" (Snegovaya, 2015, 9). In Ukraine "disinformation serves the obvious purpose of concealing Russia's actual objectives. It confuses the enemy. It allows Russia to deny that its forces are present in Ukraine because its combat operations

are hidden under an active propaganda campaign" (Snegovaya, 2015, 9). Disinformation campaigns in Ukraine serve military and strategic objectives and encompasse "confusion, obfuscation and constraining U.S. decision-making" (Snegovaya, 2015, 17). For instance, "propaganda espoused by Russia's media, spin-doctors and political technologists is often promoted through various media outlets, such as RT, Sputnik or Perviy Kanal and believed by Russian leaders and public (Kuzio & D'Aniere, 2018, 8), while "Russian trolls on the Internet, Twitter, Facebook and fake websites promote pre-determined narratives and crowd out legitimate debate" (Tanchak, 2016, 261). These narratives revolve around the portrayal of the Ukrainian army "as murderers, criminals, and Nazi perpetrators (using fabricated stories of crucified children and raped women)", as well as "denying Moscow's involvement in the conflict", and "raising doubts and encouraging suspicions about NATO's posture and ability to defend its member states" (Makhashvili, 2017, 311).

Russian information warfare may be observed in the whole post-Soviet space, , from the Baltic states to Ukraine, Georgia or Republic of Moldova. Thus, Russian information warfare in Republic of Moldova is supported by several main factors: systemic and ubiquitous presence of Russian propaganda in the public space, Russian mass-media retransmitted in Moldova and other local based Russian media institutions, promotion of simple and accessible narratives based on the principle "good-evil/ truth-lie" (Chifu & Năntoi, 2016, 235). Studies show that numerous "media outlets are using various methods / techniques of propaganda to promote Russia's position in the Ukrainian conflict, Transnistrian conflict or pro-Russian view regarding European Integration of Moldova" (Saran, 2016, 750). The media landscape is dominated by Russian TV channels that keep and amplify "the existence of a set of stereotypes positively related to Russia's President Vladimir Putin, in particular" (Saran, 2015, 750).

In a similar way, Russian informational tactics in Georgia are "often built on emotional messages to create and strengthen negative stereotypes of ethnic, religious and sexual minorities, discrediting the Western political or cultural space and supporting homophobic and xenophobic opinions among the public" (European Initiative, 2016, 21). "By cultivating these myths, Russia presents itself as Georgia's only ally with a common

identity, religious faith, history and culture. Simultaneously, it portrays the West as a threat to all the above-mentioned values" (Makhashvili, 2017, 311; European Initiative, 2016, 21).

Authors consider that "media manipulation and psychological war in Ukraine and Republic of Moldova is a struggle to conquer the minds of the people through various psychological methods in order to subordinate the masses often under the guise of illusion of receiving freedom and control of information" (Saran, 2015, p. 751). As seen earlier, Russian information warfare "is blossoming in Georgia and Ukraine in parallel to and in order to hinder their accelerated European integration. Another dimension of this warfare is targeted against the EU member states and aims at splitting the societies, change governmental calculations and this way weaken their engagement (individually or via EU) with the Eastern Partnership countries" (Makhashvili, 2017, 312). The new generation war "allows the Kremlin to simultaneously back far-left and far-right movements, greens, anti-globalists and financial elites. The aim is to exacerbate divides and create an echo chamber of Kremlin support" (Pomerantsev & Weiss, 2014, 6).

VI. Information operations and the state of the cyber environment

Information warfare actions are easier to be carried out in an insecure cyber environment. As an example, fake news are easier spread and essential services are easier affected in an area where cyber security capabilities do not exist, or do not cooperate, or do not have necessary capacities, skills and abilities to perform their functions. At least for this reason, it is important to know and to understand the cyber environment where warfare actions can be carried out.

Existing cyber security capabilities in the Extended Black Sea area, public authorities' capabilities and capacities, as well as the features of the public or private cyber infrastructures should be analyzed in order to find out what kind of information operation could be carried out by a state actor in this area.

V.1. Common cyber security challenges in the extended Black Sea Area

Public authorities in the region are aware of the risks and challenges of the cyber field and of the interest of at least one actor from the BS extended area to exploit existing vulnerabilities. The prevalent stakeholders in the cyber-domains are the states, since most of them are involved in rather complex and challenging relations with their immediate neighbours.

At the same time, there is a lack of strategic approaches to provide for cyber security or counter cybercrime and make use of electronic evidence in criminal proceedings, as reflected in the absence of dedicated policy documents on cybercrime and electronic evidence as mainstream challenges of criminal justice systems. This runs against a fairly common understanding that the majority of critical information systems that such strategies and action plans need to address are owned and run by private business entities, who also become stakeholders in the process of ensuring security of cyberspace.

The difficulty of coming with a meaningful, coordinated response, has to do with the following factors:

a) there are overlaping responsibilities between the various actors involved ;
b) legislation is either lacking or there are different, conflicting intepretations of it; privacy experts in various EU member states have a wide range of interpretations of how personal information may be defined. For example, an IP address can qualify as personal information in one country, but not in another. Categorisation is another issue in terms of which types of personal data should receive the highest level of protection. Due to the fact that such privacy-related questions are so complex most of the times, extensive information sharing between different actors is often inhibited;
c) there is a gap between policy and operational requirements in various Member States;
d) there are technical challenges, meaning there is a gap of making available a platform for information exchange and sharing – MISP at technical level – due to the hard approach in cyber security which means a strict control of sharing and/or exchange of information; at the same time, on the operational side, with incidents that require

looking up for details on entities that are responsible for URLs and IP addresses under investigation, a European forum exists that has a database of all European IPs and their corresponding owners (the Regional Internet Registry27, or RIPE); however, the data in this registry is quite difficult to retrieve, and it can sometimes be impossible to find the entity responsible for an IP address;

e) there are different approaches to cyber security, based on different interests;
f) the level of actual mutual trust between actors is a challenge. Trust issues are among the most crucial obstacles to enhanced and effective communication between stakeholders, all over the world and in the area of our concern. In the particular community of cybersecurity experts, trust is the single most important feature of a successful cooperative relationship. Regarding the BS region, this issue is even more dramatic, given the fact that the public's trust in government and public authorities has been constantly eroding;
g) there is a need for public-private cooperation and awareness.

V. Cyber security challenges – country assessments[2]

Romania

According to the Romanian National CERT, CERT-RO, 2018 annual report (CERT, 2019), numerous servers are vulnerable, unpatched, poorly configured and not monitored by owners. At the same time, millions of devices (PCs, phones, tablets, IoT) were compromised due to operating unpatched/unlicensed software and having no security/anti-malware protection.

The end users' level of cybersecurity culture is reduced to low level, a primary challenge being the fact that educating people in this area is a long-term endeavor. The EU provisions for securing the essential services' implementation is delayed by financial and technical shortages, national authority for NIS Directive not being actually set up.

[2] Results of meetings, discussions and evaluation with the public authorities and private companies representatives during the Council of Europe different projects carried out in the Eastern Partnership Program and Balkans Area projects.

Republic of Moldova

Both the public and the private sector are fully aware of the threats and risks originating from cyberspace. While private sector entities and NGOs are more worried about cybercrime, the government sector, law enforcement agencies, intelligence services and the military are concerned more about the rising number of cyber incidents and cyber-attacks.

When talking about cybercrime, most often this refers to ransomware, online fraud, attacks against networks and critical infrastructure, cryptocurrencies-related fraud, fraud related to harvesting, accessing and manipulating data. Other offences include hate speech and social media abuse, online radicalisation, grooming and distribution of child abuse materials, espionage and money laundering.

The existing capacities in the cyber domain are as follows. The Moldavian Cyber Security Center (CERT-GOV-MD, n.d.) is located under the Special Telecommunication Center, the governmental entity in charge with providing cyber security for the government networks and systems. The CSC experts have access only to the government bodies and limited capabilities to act as a real national center in terms of incident response. The CERT-GOV-MD cooperates with law enforcement agency – Centre for Combating Cyber Crimes – in the following areas: fighting cybercrime (by reporting suspicious incidents), capacity building (by organizing joint cybersecurity workshops and trainings), awareness raising (by organizing cyber security conferences). Cooperation with state institutions is mainly based on internal regulation, bilateral agreements and voluntary commitments. The public-private cooperation needs serious improvement, as this could be the most crucial block in building security of the cyberspace.

Ukraine

Public awareness in Ukraine about cyber-related risks has increased a lot for the past years. One of the main reasons for this is the massive malware campaign against the Ukrainian public and private networks and computers, as well as cyber espionage and cyber-attacks against the public infrastructures that have taken place during recent years.

As a result of these incidents that impacted both public and private sector entities, including in economic terms, more and more attention has been paid to information security, cybersecurity and prevention of cybercrime.

The main threats include cybercrime offences such as fraud, illegal access to computer systems and networks, DDoS attacks, different malware, ransomware and wipe attacks. Attackers often aim at confidential information and personal information of government officials. Therefore, cyber espionage has been a frequent occurrence. In some cases, when data breach or data theft, including from government databases, occurred, the data was put on sale by the cyber-criminals.

Ukrainian authorities have witnessed advanced persistent threats and coordination and planning of the attacks. There have been cases of cooperation between the perpetrators and insiders. Often phishing and social engineering attacks have taken place earlier in order to obtain credentials or other information that can be used to launch an attack against the computer system or network. Attacks against computer systems and networks have repeatedly included attacks against critical infrastructure. In order to harm or paralyze computer systems and networks, including those belonging to the government or critical infrastructure, physical attacks against network infrastructure, including copper and fiber optic cables have occurred.

Ukraininan authorities, beside private sector representatives set up a cooperation frameworks, procedures to request and disclose data, information exchange channels including contact points and other technical details concerning everyday cooperation to fight cybercrime and ensure cyber security.

There is an obligation for critical infrastructure objects, identified in the recently adopted Law of Ukraine on basic principles of providing cyber security in Ukraine, to report on cyber incidents. However, technical and practical details for efficient cybercrime reporting still need to be developed.

Although most of the cybercrime is committed by criminals, there is still reason to believe that often **hacktivists, cyber fighters and terrorists** can be behind the attacks. Large-scale attacks that are sophisticated and require lots of resources and efforts to

prepare could have been state sponsored. Information operations and fake news campaigns have been detected on different social media sites and foreign media outlets with a primary purpose to cause distress and confusion among the population as well as to create a negative image of government and the country.

Georgia

Georgia is fairly advanced when it comes to cyber security and uniform perception of threats and challenges, as evidenced by recent international and European rankings.

As the current set of cybersecurity and cybercrime strategies draw near the end of their respective cycles, development of a cybercrime strategy as a component of the national cybersecurity strategy and on the basis of up-to-date perception of cybercrime threats and challenges would be beneficial.

The CERT.GOV.GE under the Data Exchange Agency is one of two dedicated governmental CSIRTs in Georgia: the CERT-GOV-GE and the Ministry of Defence CERT. The Law on Information Security defined that the government CERT is responsible for the handling of incidents, providing alerts, raising awareness and educating (e.g. penetration testing). The protection of the Georgian critical infrastructure is a priority task; there is no national CERT operating currently in Georgia, although the CERT-GOV-GE is currently performing these functions (CERT-GOV-GE, n.d.).

Bulgaria

The Council of Ministers, assisted by the Cyber Security Council and the National Cyber Security Coordinator, are responsible for the implementing of the National Cyber Security Strategy and National Network and Information Security Strategy. These bodies also manage and organise the national cyber security system on a strategic level.

On an operational level, Bulgaria's administrative bodies have special powers and competences. The “National Security” State Agency is mandated to protect strategic communication and information systems from potential cyber security incidents, and to create a Monitoring and Incident Reaction Centre. The General Directorate for Combating

Organised Crime is to establish a Center for investigation, and fight cyber security crimes on a national level.

The "Electronic Governance" State Agency (or the "E-Governance Agency") as a national competent authority is empowered to monitor, coordinate and facilitate the compliance of all administrative bodies to network and information security requirements.

Turkey

Turkey has a system for combating cybercrime that is consistent with its desire for good cybersecurity and the various threats the country faces. The training and competence of magistrates and police services is strongly supported by an appropriate level of technical means and a firm will to improve.

The Cybercrime Department is underway with a project that seems to make the system more effective and centralised, and has the ability to provide the (significant) analysis capability that is needed. More centralised and more structured reporting (as in: reporting resulting in structured data, rather than free-text options such as email) will likely free up capacity to make more advanced (and more useful) intelligence and analysis available.

The extended Black Sea Area

Armenia

Armenia currently has no dedicated strategy or action plan on cybercrime as such in place or in development. Educational programmes need to be developed. For this purpose, organizations that possess the necessary knowledge will need to (re-)shape the corresponding skill profile and combine capabilities to develop comprehensive education curricula.

The development of better cyber-defense capabilities requires a new combination of skills and knowledge. Policy needs to create proper conditions that will lead to better education in the area of cybersecurity and in particular in cyber threat intelligence.

Development of the existing national CERT seems to be the most pressing need and option for Armenia. At the same time, setting up clear responsibility to this structure, allotting necessary resources, and establishing terms and conditions to fulfil, it would be more than necessary and useful.

Azerbaijan

From the perspective of the law enforcement and governmental community, there is an understanding of the differences of challenges vs. actual threats: cyber threats can affect security of state, society and private sector, while challenges are more specific cases of lack of resources to tackle these threats.

The Ministry of Internal Affairs investigates the majority of cyber-attacks, but given the state interest affected, there are very common instances of joint investigative teams with State Security Service used to cooperate on these incidents.

For the private sector, specifically telecommunications companies, attribution for attacks and identification of perpetrators is very often a challenge. One particular area in which this is preavelnt are Internet cafes (without logging user Ids) as well as public wifi. Carrier-grade NAT (CGN) and resources of ISPs in this regard are mainly technical challenges.

VII. Policy recommendations

Based on our analysis, here is a set of broad policy recommendations for increasing the resilience of public and private cyber infrastructures, as well as the resilience of the digital communication and information eco-system in the face of information warfare and information operations.

a) Educational and training programmes need to be developed; for this purpose, organisations that have the necessary knowledge will have to upgrade the corresponding skills profile and combine capabilities in order to develop comprehensive education curricula.
b) The cybersecurity community needs to elaborate standard operational procedures based on technical solutions that will allow rapid interventions in cyberspace that

do not jeopardise privacy and security properties of user data (i.e. confidentiality, integrity and availability of information).

c) A regional mechanism of cooperation should be developed in order to have a coordinated response of all entities involved in the security of the cyber space (e.g. further defining the current focus of CERT on social media).
d) Public institutions should focus their investment in new equipment and technologies to provide safe e-government services to the entire population.
e) One specific area of most interest is the need for methodology to address the policy makers and legislators, in order to change their perception of cybercrime and cybersecurity threats.
f) Broad alliances, between government agencies, private sector, civil society (academia, journalists, NGOs) must be built in order to clarify the scope of information warfare and information operations, differentiate between various actions and build resilience and foresight.
g) Technology, cyber and data literacy programs should be designed to address politicians, decision-makers and mainstream journalists.
h) Awareness among decision-makers around the technological, economic, social, and geopolitical environment for information operations should be built.
i) General literacy and awareness programs about the new technological/ cyber environment (risks, challenges, scope, vulnerabilities, behavioural changes) should be designed to address the general public.
j) Vulnerabilities (internal vulnerabilities, including financial and economic challenges, weak media and information ecosystem, low trust in public authorities, external divisions, competing agendas, and lack of coordinated, trans-national responses) must be properly addressed, while temptation to explain these vulnerabilities solely or predominantly via information warfare and information operations must be resisted.

References

Advisory mission and workshop on online fraud and other cybercrime reporting mechanisms 15 - 16 March 2017, Ankara Turkey Provided under the iPROCEEDS project

Ahmer A., Stewart, L.G. & Starbird, K. (2018). Acting the Part: Examining Information Operations Within #BlackLivesMatter Discourse. *Proceedings of the ACM on Human-Computer Interaction,* Vol. 2, CSCW, Article 20, 27 pages. https://doi.org/10.1145/3274289

Allen, T.S. & Moore, A.J. (2018). Victory without Casualties: Russia's Information Operations. *Parameters,* No. 48(1), pp.59-71.

Anastasov, P. (2018, May 25). The Black Sea region: a critical intersection. *NATO Review.* https://www.nato.int/docu/review/articles/2018/05/25/the-black-sea-region-a-critical-intersection/index.html

Armistead*, L. (Ed.). (*2004*). Information operations: Warfare and the* hard *reality of soft power.* Potomac Books, Brassey's Inc.

Aro, J. (2016). "The Cyberspace War: Propaganda and Trolling as Warfare Tools." *European View* 15(1): 121-32.

Baev, P. (2016). "Russia and Central And Eastern Europe: Between Confrontation and Collusion." *National Security and Defence* (9-10): 87–97.

Barghoorn, F. C. (1962). "Propaganda: Tsarist and Soviet." In *Russian Foreign Policy. Essays in Historical Perspective*, ed. Ivo Lederer. London and New Haven, CT: Yale University Press. 279–309.

Bartosh, A. (2014). "Gibridnye vojny buduschego – prognozirovanie i planirovanie." *Nezavisimoye Voyennoye Obozreniye*, 19 December.

Bartosh, A. (2015). "Stupeni eskalatsii: tsvetnaya revolyutsiya, gibridnaya vojna… Chto dal'she? Dominirovanie na planete kak glavnyj trend v politike SSHA i NATO." *Nezavisimoye Voyennoye Obozreniye*, 27 February.

Bartosh, A. (2017). "Gibridnaya vojna stanovitsya novoj formoj mezhgosudarstvennogo protivoborstva." *Nezavisimoye Voyennoye Obozreniye*, 7 April.

Bergmann, M., and C. Kenney. (2017). "War by Other Means. Russian Active Measures and the Weaponization of Information." Washington DC: Center for American Progress.

Berzins, J. (2014). Russia's New Generation Warfare in Ukraine. *National Defense Academy of Latvia, Policy Paper No. 2,* available at: https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf

Bittman, L. (1987). *The new image makers : Soviet propaganda and disinformation under Gorbachev*. Boston: Boston University's Program for the Study of Disinformation.

Brady, A. (2015). Authoritarianism Goes Global (II): China's Foreign Propaganda Machine. *Journal of Democracy,* No. 26(4), pp. 51-59, doi:10.1353/jod.2015.0056.

Byrnes, R. F. (1962). "Attitudes towards the West." In *Russian Foreign Policy. Essays in Historical Perspective*, ed. Ivo Lederer. London and New Haven, CT: Yale University Press. 109–41.

Chifu, I., Năntoi, O. (2016). *Război informațional. Tipizarea modelului agresiunii.* București:Editura Institutului de Științe Politice și Relații Internaționale Ion I.C. Brătianu al Academiei Române

Darczewska, J. (2014). "The anatomy of Russian information warfare. The Crimean operation, a case study." , Warsaw: Centre for Eastern Studies.

Desouza, K. C., Ahmad, A., Naseer, H., & Sharma, M. (2020). Weaponizing information systems for political disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT). *Computers & Security*, *88*, 101606.

Filipova, R. et. al. (2018). *Russian Influence in the Media Sectors of the Black Sea Countries. Tools, Narratives and Policy Options for Building Resilience*. Center for the Study of Democracy. http://ipre.md/wp-content/uploads/2018/10/Russian_Influence_in_the_Media_Sectors.pdf#pdfjs.action=download

Filipova, R., & Galev, T. (2019, January 17). Russian Influence in the Media Sectors of the Black Sea Countries: Tools, Narratives and Policy Options for Building Resilience. *Disinfo Portal.* https://disinfoportal.org/russian-influence-in-the-media-sectors-of-the-black-sea-countries-tools-narratives-and-policy-options-for-building-resilience/

Flanagan, S.J. & Chindea, I. A. (2019). *Russia, NATO, and Black Sea Security Strategy. Regional Perspectives from a 2019 Workshop.* RAND Corporation. https://www.rand.org/pubs/conf_proceedings/CF405.html

Giles, K. (2015). "The Next Phase of Russian Information Warfare." Riga: NATO StratCom COE.

Giles, K. (2016). *Handbook of Russian information warfare.* NATO Defense College "NDC Fellowship Monograph Series". https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook%2C%20Russian%20Information%20Warfare.pdf

Gressel, G. (2017). "Fellow Travellers: Russia, Anti-Westernism, and Europe's Political Parties." London: ECFR.

Guadagno, R. E., & Guttieri, K. (2019). Fake News and Information Warfare: An Examination of the Political and Psychological Processes From the Digital Sphere to the Real World. In *Handbook of Research on Deception, Fake News, and Misinformation Online* (pp. 167-191). IGI Global.

Gude, K. (2017). "Russia's 5th Column." Washington DC: Center for American Progress.

Hämäläinen, H. (2019, December 4). Information Warfare. *Medium.* https://medium.com/social-media-writings/information-warfare-d4289484a241

Herpen, M. v. (2016). *Putin's Propaganda Machine : Soft Power and Russian Foreign Policy*. Lanham: Rowman & Littlefield.

Ingram, H. J. (2015). The strategic logic of Islamic State information operations, *Australian Journal of International Affairs*, No. 69 (6), pp. 729-752, DOI: 10.1080/10357718.2015.1059799

Kuzio, T. & D'Aniere, P. (2018). The Soviet Origins of Russian Hybrid Warfare. *E-International Relations,* pp.1-25, https://www.e-ir.info/2018/06/17/the-soviet-origins-of-russian-hybrid-warfare/

Libicki, M. C. (2017). The convergence of information warfare. *Strategic Studies Quarterly*, *11*(1), 49-65.

Makarychev, A., and S. Braghiroli. (2016) "Russia "Understanders" in Europe: Discourses, Communication, Consequences " In *PONARS Policy Memo*. Vol. 435.

Makhashvili , L. (2017). The Russian information war and propaganda narratives in the European Union and the EU's Eastern Partnership countries. *International Journal of Social Science and Humanity,* Vol. 7, No. 5, pp. 309-313 http://www.ijssh.org/vol7/840-HF0035.pdf

Malashenko, A. (2016) "Blesk i nishcheta rossiyskoy propagandy.Vrag perestal byt' klassovym. Propast' mezhdu nami i nimi opredelyayetsya tsennostnymi razlichiyami." *Nezavisimaya Gazeta*, 19 December.

Marcellino, W., Smith, M.L., Paul, C. & Skrabala, L. (2017). *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*. Santa Monica, CA: RAND Corporation, https://www.rand.org/pubs/research_reports/RR1742.html.

Ministry of Foreign Affairs of the Russian Federation. (2016). "Foreign Policy Concept of the Russian Federation."

Molander, R. C., Riddile, A., & Wilson P. A. (1996). *Strategic Information Warfare: A New Face of War.* RAND Corporation. https://www.rand.org/pubs/monograph_reports/MR661.html.

Moore, M. (2018). *Democracy Hacked. Political Turmoil and Information Warfare in the Digital Age*. Oneworld Publications

Munoz, A. (2012), *U.S. Military Information Operations in Afghanistan: Effectiveness of Psychological Operations 2001-2010*. Santa Monica, CA: RAND Corporation, https://www.rand.org/pubs/monographs/MG1060.html.

Our Democracies, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and

Panarin, I. (2017). *Gibridnaia voina protiv Rossii, 1816-2016 gg.* . Moscow: Goriachaia liniia--Telekom.

Perception of threats and challenges of cybercrime in the Eastern Partnership Results of the threat mapping exercise sessions in Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine, February-May 2018

Pipes, R. (1973) "Operational Principles of Soviet Foreign Policy." *Survey* 19(2): 40–61.

Polyakova, A. (2017). "Here's Why You Should Worry About Russian Propaganda?" The Atlantic Council of the United States, http://www.atlanticcouncil.org/blogs/new-atlanticist/here-s-why-you-should-worry-about-russian-propaganda.

Polyakova, A., M. Laruelle, S. Meister, and N. Barnett. (2016). *The Kremlin's Trojan Horses. Russian Influence in France, Germany, and the United Kingdom*. Washington DC: The Atlantic Council.

Pomerantsev, P&Weiss, M. (2014). The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money". *Institute of Modern Russia,* https://www.interpretermag.com/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/

Pomerantsev, P. (2015). The Kremlin's Information War. *Journal of Democracy*, No. 26, pp. 40-50, doi:10.1353/jod.2015.0074.

Porche, I., Paul, C., York, M., Serena, C. C., & Sollinger, J. M. (2013). *Redefining information warfare boundaries for an army in a wireless world*. Rand Corporation.

Porotsky, S. (2019, June 10). Analyzing Russian Information Warfare and Influence Operations. *Global Security Review.* https://globalsecurityreview.com/cold-war-2-0-russian-information-warfare/

President of the Russian Federation. (2015) "The Russian Federation's National Security Strategy." Moscow: President of the Russian Federation.

President of the Russian Federation. (2016) "Doctrine of Information Security of the Russian Federation." Approved 5 December 2016 by Decree nr. 646 ed. Moscow: President of the Russian Federation

Prier, J. (2017). Commanding the trend: Social media as information warfare. *Strategic Studies Quarterly*, *11*(4), 50-85.

Rebegea, C. (2017, March 23). *The Black Sea as a Battleground for Information Warfare: A View from Bucharest.* Foreign Policy Research Institutite. https://www.fpri.org/article/2017/03/black-sea-battleground-information-warfare-view-bucharest/

Regional workshop on criminal justice statistics on cybercrime and electronic evidence 14-15 May 2018, Bucharest, Romania Provided under iPROCEEDS project

Rogers, J., and A. Tyushka. (2017). "'Hacking' Into The West: Russia's 'Anti-Hegemonic' Drive And The Strategic Narrative Offensive." *Defence Strategic Communications* 235–60.

Saran, V. (2016). Media Manipulation and Psychological War in Ukraine and The Republic of Moldova. *CES Working Papers*. Centre for European Studies, Alexandru Ioan Cuza University, vol. 8(4), pp. 738-752.

Sazonov, V., Müür, K. & Kopõtin, I. (2017). Methods and tools of Russian information operations used against Ukranian armed forces: the assessments of Ukrainian experts. *ENDC Occasional Papers,* Volume 6, pp. 52–66.

Schwartau, W. (1996). *Information Warfare: Second Edition.* Thunder's Mouth Press

Schwartz, H.A., & Diamond, C. (2017, June 28). *Russia's Design in The Black Sea: Extending the Buffer Zone.* Center for Strategic & International Studies. https://www.csis.org/analysis/russias-design-black-sea-extending-buffer-zone

Shekhovtsov, A. (2018). *Russia and the Western Far Right - Tango Noir*. London, New York NY: Routledge.

Shultz, R. H., and R. Godson. (1986). *Dezinformatsia: Active Measures in Soviet Strategy*. New York: Pergamon Press.

Singer, P. W. , & Brooking, E. T. (2018). *Like War. The Weaponization of Social Media.* Houghton Mifflin Harcourt Publishing

Snegovaya, M. (2015). *Putin's information warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (ISW Russia Report 1). Washington, DC: Institute for the Study of War.

Soldatov, A., and I. Borogan. (2015). *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. New York: Public Affairs.

Stupples, D. (2015, December 3). What is information warfare? *World Economic Forum.* https://www.weforum.org/agenda/2015/12/what-is-information-warfare/

Tanchak, P.N. (2016). The Invisible Front: Russia, Trolls, and the Information War against Ukraine' in Olga Bertelsen ed., *Revolution and War in Contemporary Ukraine: The Challenge of Change:* Stuttgart.

Tashev, B., Purcell, M., & McLaughlin, B. (2019). Russia's Information Warfare. Exploring the Cognitive Dimension. *MCU Journal,* vol. 10, no. 2, 129-147.

Theohary, C. & Rollins, J. (2011). Terrorist Use of the Internet: Information Operations in Cyberspace. *Report for the Congressional Research Service*, https://fas.org/sgp/crs/terror/R41674.pdf

Thomas, T. (2014). "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?". *The Journal of Slavic Military Studies* 27(1): 101-30.

Thomas, T. L. (1998). "Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations." *The Journal of Slavic Military Studies* 11(1): 40-62.

Thomas, T., L. (2004). Russia's Reflexive Control Theory And The Military. *Journal of Slavic Military Studies*. No. 17, pp. 237–256, https://www.rit.edu/~w-cmmc/literature/ Thomas_2004.pdf.

Treurniet, R. (2017). *The Soviet Origins of Russian Information Warfare Manifestations of Reflexive Control in Ukraine.* Master Thesis. MSc. Crisis and Security Management Faculty of Governance and Global Affairs University of Leide, retrieved from https://openaccess.leidenuniv.nl/bitstream/handle/1887/83864/Treurniet_CSM_2017.pdf?sequence=1

Van Oudenaren, J. 1986. *Soviet Policy Toward Western Europe Objectives, Instruments, Results.* Santa Monica CA: Rand Corporation.

Ventre, D. (2016,). *Information warfare*. John Wiley & Sons.

Vilmer, J.B., Escorcia, A., Guillaume, M. Herrera, J. (2018). *Information Manipulation: A Challenge for Our Democracies* Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018, retrieved from https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

Web sources

European Initiative – Liberal Academy Tbilisi (2016). *Threats of Russian Hard and Soft Power in Georgia*. available at: www.ei-lat.ge/images/doc/policy%20document.pdf

RAND Corporation. (n.d.). *Information Operations.* https://www.rand.org/topics/information-operations.html

Bulgaria adopts new cyber security strategy. https://www.cms-lawnow.com/ealerts/2018/11/bulgaria-adopts-new-cyber-security-act

MD-CERT. (n.d.). *Despre noi.* https://cert.md/ro/about-us/

CERT-RO. (2019). *Evoluția amenințărilor în spațiul cibernetic românesc în anul 2018.* *https://cert.ro/vezi/document/raport-alerte-2018*

Forum of Incident Response and Security Teams. (n.d.). *CERT-GOV-GE Team Information.*

https://www.first.org/members/teams/cert-gov-ge

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.