POLITICKÉ VEDY / POLITICAL SCIENCES

Časopis pre politológiu, najnovšie dejiny, medzinárodné vzťahy, bezpečnostné štúdiá / Journal for Political Sciences, Modern History, International Relations, security studies

URL of the journal / **URL časopisu**: https://www.politickevedy.fpvmv.umb.sk

Author(s) / Autor(i): **Miroslava Pačková**
Article / Článok: Russian Active Measures in Cyberspace through the Lens of Security Sectors
Publisher / Vydavateľ: **Fakulta politických vied a medzinárodných vzťahov** – UMB Banská Bystrica / Faculty of Political Sciences and International Relations – UMB Banská Bystrica
DOI: https://doi.org/10.24040/politickevedy.2023.26.4.55-91

Recommended form **for quotation of the article / Odporúčaná forma citácie článku:**

PAČKOVÁ, M. 2023. Russian Active Measures in Cyberspace through the Lens of Security Sectors. In *Politické Vedy*. Vol. 26, no. 4, pp. 55-91. ISSN 1335 – 2741. Available at: https://doi.org/10.24040/politickevedy.2023.26.4.55-91

RUSSIAN ACTIVE MEASURES IN CYBERSPACE THROUGH THE LENS OF SECURITY SECTORS[1]

Miroslava Pačková*

ABSTRACT
This article examines Russian active measures in cyberspace, focusing on the implications for across security sectors. Initially, the study contextualizes the increasing reliance on cyberspace for conducting subversive activities that target military, political, societal, and economic structures, particularly after the Ukrainian Euromaidan in 2013. Utilizing a qualitative analysis of open-source data, the research identifies the diverse tactics employed by Russian actors, including sophisticated use of code and content to manipulate public perception and governmental processes. Key findings reveal that while activities in the military and political sectors are characterized by a high degree of technological sophistication, societal sectors predominantly face threats from disinformation campaigns. Notably, no significant cyber active measures were detected within the environmental sector. The study concludes that Russian cyber tactics are deeply embedded in their broader geopolitical strategy, necessitating robust countermeasures. Enhanced cybersecurity policies and international cooperation are recommended to bolster resilience against such foreign malign influences.

Key words: Intelligence Services, Russian Federation, Propaganda, Cyberspace, Security Sectors.

Introduction

The concept of active measures corresponds with the current Russian hostile information influence against post-communist countries as well as the West. Generally, the current state is characterised by using cyberspace and the significant role of intelligence services. Active measures are embedded in Russia's political and strategic culture, as well as in the tradition of the intelligence

* Mgr. Miroslava Pačková, Ph.D. is a Researcher at the Centre for Security and Military Strategic Studies, University of Defence, Kounicova 65, Brno, Czech Republic, e-mail: miroslava.packova@unob.cz.

DOI: https://doi.org/10.24040/politickevedy.2023.26.4.55-91

[1] This work was supported by the University of Defence under Grant DRZO OZKON 2022+[number 531733].

services. It can be positioned anywhere between open (white) propaganda and even terrorism. In between is a broad grey area that is now the main stage for Russia's confrontation with the West to undermine its administrative, political, social, economic and cultural foundations. The most common actors of active measures are the media, politicians or parties, cultural or religious organisations, the military, the business sector, and especially the intelligence services. Technological developments play an important role in the form of active measures, currently mainly through the transfer of measures into cyberspace.

The need for researching Russian cyber active measures increased with the events of the Ukrainian Euromaidan in 2013 and the subsequent Russian occupation of the eastern parts of the country and the Crimean Peninsula. At that time, Russia transferred part of the fighting to cyberspace. In the years that followed, malicious cyber operations, both technical and social, were used in the Baltics, Central Europe, the so-called West including the US and finally during the Russian occupation of Ukraine.

1. Literature review and aims of the study

Research of Russian cyber active measures follows the geographic proximity to the aggressor; it is mainly the domain of post-communist countries (Central Europe and the Baltics) (e.g. Gregor and Mlejnková et al., 2021; Galeotti, 2016-2019; Spruds et al., 2016). However, European and American organisations (e.g. Atlantic Council, EUvsDisinfo, NATO Stratcom CoE, Stopfake) or European institutions in cooperation with academia (e.g. the Computational Propaganda Project of Oxford University funded by the European Commission) take up a substantial part of it with their expert studies. US provenience conducts research towards Russian interference in the US electoral process and the geopolitical significance of Russian operations (Lindwill and Warren, 2020), or towards election influence and countermeasures (Brattberg and Maurer, 2018).

In the modern scientific debate, active measures are discussed by **Jolanta Darczewska** (2018), who summarizes the historical conception, especially in the framework of Dennis Kux´s ideas (1985). In the Journal of Strategic Studies, **Kragh and Åsberg** (2017) study the narratives used by Russian active measures in Sweden. Finally, the author of this paper and **Jan Hanzelka** (2019), writing in the Slovak journal Political Science, focus on three European Union countries with different political, cultural, historical, and economic realities and compare the Russian approach to the application of active measures against these countries.

In the same journal, we can also find a text by **Martin Slávik** (2019) that analyses the functioning of the Czechoslovak StB in the framework of active measures. Other contemporary authors are **Olga Bertelsen** (2021) and **Thomas Rid** (2020), who also direct their books to non-academic readers. **Thomas Rid's** 2020 book, which describes the history of Soviet and, more recently, Russian active measures, partly presents current cases of active measures with use in cyberspace. However, the book is aimed at a wider audience than the professional sphere and describes individual cases in a sometimes fiction-like manner. We conclude that the deficit in expert studies using the concept of active measures needs to be alleviated. Compared to the non-expert and popular science texts, there is a dearth of expert studies, especially in the context of society's need for scientific understanding of Russian malicious influence in cyberspace.

Current research on Russian cyber active measures can also be characterized as the study of actors and the tools they use, whether with the aim of simple empirical studies or more ambitious countermeasure design (e.g., Reichborn-Kjennerud and Cullen, 2017). For example, the phenomenon of Kremlin trolling has been addressed, especially after the Russian meddling in the US presidential election in 2016 (e.g. Howard, Ganesh and Liotsiu, 2018; The Computational Propaganda Project, 2016; NATO Stratcom Centre of Excellence: publications 2017-2021; Pavlíková, Šenkýřová and Drmola, 2020). Also, a broad group of authors focused on tools such as fake news or disinformation (e.g. Molina, Sundar, and Lee, 2019; Gregor and Mlejnkova et. al., 2021). Fewer researchers have conducted their research through the lens of threatened values. A small number of authors focus their studies exclusively on the threatened values (also called targets or vulnerabilities by various authors). **Bízik et al**. (2020) and **Divišová et. al.** (2021), for example, focus on the dimensions of resilience to hybrid threats considering psychological, social, institutional and national vulnerabilities. **Damarad and Yeliseyeu** (2018) work with the resilience of entities threatened by disinformation. However, taking threatened values into account is no less important for the overall picture than focusing on the actors and their tools.

The presented study seeks to fill the research gap with a focus on values threatened by Russian cyber active measures. The issue of threatened values will be placed within one of the core concepts of security and strategic studies, namely the Copenhagen School's security sectors (Buzan and Weaver, 1998). The authors, within the framework of the so-called extended security concept,

operate with security dynamics in five sectors: military, political, social, economic and environmental. Sectors are based on the so-called referent objects and the threatened values attached to them. As **Mareš and Mlejnková** (2021, p. 77) note, in terms of security analysis, research on propaganda and disinformation (and thus a substantial part of active measures) was studied from the perspective of the military and regime dimensions towards the end of the 20th century. The Copenhagen School, with its five sectors, expanded the field of research. It included the threatened values of the social, economic and environmental sectors.

Therefore, the author derives the following research question: *How do current Russian cyber active measures manifest themselves in the sector of security?*

2. Methodology

To be designated as active measures in cyberspace, operations should meet the following conditions.

- Operations take the form of political or military warfare. They are manipulative, create political or social pressure, and influence political decision-making.
- Operations pursue Russian foreign policy interests.
- Operations take place in cyberspace.

The following are several optional conditions that can be used as indicators of active measures.

- An operation has multiple stages; it starts with the extraction of sensitive data by a cyber-attack, which is then used for operations using hostile content.
- Operations are directed or supported by the intelligence services of the Russian Federation.
- The operations are conducted in such a way that accountability can be denied.

The author also considers it necessary to further define the political (and thus military) and social sectors through the lens of referent objects for analysis, as there could be overlap. For hostile content operations, the end goal of active measures might be unclear. The author will therefore proceed as follows:

For the political sector, the author operates with goals closer to real-world

politics and the execution of political power. The targets are states, governments and political leaders as power holders. In the analysis, the author will only work with citizens as targets associated with referent objects in the political sector when active measures directly affect political decision-making, especially in the context of immediate elections.

Citizens will be perceived as part of the societal sector if they are targeted for their general social mindset and identity. Again, there may be overlaps, especially if it is impossible to distinguish where efforts to influence elections begin and end. If such actors are identified, this will be pointed out during the analysis.

2.1 Research logic

This qualitative research uses an inductive method. It builds on data observation at the beginning of the research process. Then, regularities and their meanings are sought in the data, which is followed by the formulation of tentative conclusions (Disman 2002, p. 287). The sequence of steps in the article can also be related to the logic of research, which **Drulák** (2008, p. 235) refers to as the internal process of a qualitative study. According to **Drulák**, the simplest representation of research logic is the hermeneutic circle; however, each research will create its pattern. The logic of research in a qualitative study jumps from one end to the other and occasionally closes into loops. Research activities, such as literature study and data collection, usually run in parallel or the researcher moves from one activity to another. In the present study, this is relevant for the categories of actors of cyber active measures, the individual cases of actors, and the specification of objectives, which are continuously added to as the research progresses. The sequence of steps from the initial data collection to the final discussion of the outputs is as follows: Data collection → categorisation → selection of representative cases → inclusion in the framework for analysis → characterisation and analysis of cases → answering the research question and final discussion.

The basic units of data that have been collected are actors or incidents in cyberspace that use either hostile code or content and meet the conditions for inclusion in Russian cyber-active measures. Data on each actor was collected through a systematic search of Internet sources. At the outset, the author formulated the requirements for the subjects of the search, i.e., the exact areas and topics; in the case of this study, actors and incidents associated with the Russian Federation using tools of warfare in cyberspace. The author then defined the types of documents to be searched (expert articles, analyses and reports by

governmental and non-governmental organisations, analyses by cybersecurity companies, media articles and leaked documents). In the next step, the author defined keywords/phases, which she then entered through an internet search using Google. The basic phrases were: 'Russia cyber-attack; 'Russia disinformation'; 'Russia propaganda', 'Russia cyber espionage' 'Russia ransomware'; 'pro-Russian influencers'; 'Russia microtargeting' etc. After entering the search query into the search engine and searching, the relevance of the results was assessed, followed by debugging and editing. The tuning of keywords and phrases as well as the formulation of new ones took place throughout the whole analysis. The collected data was then categorized into the most general categories of actors of active measures in cyberspace while it was conceptually consistent with the actors presented in the chapter threats in cyberspace. Examples of the constructed categories are the cyber groups CyberBerkut and Anonymous Ukraine, from which a category of patriotic hackers was created. If it was not possible to create a category from certain cases linked to the concepts from the theoretical chapter, such a category was created by the author. For the sake of clarity, the author works exclusively with the optics of actors in the creation of categories in the analysis.

The work focuses territorially on countries in the Euro-Atlantic area with a deeper focus on EU member states, due to similar political situations and shared values. However, the author also includes in the analysis some cases from the US that are relevant to the context and tied to actors operating in the EU. This approach is a response to the rapidly evolving threat and risk-creation environment that cyberspace presents.

The same logic applies to the timeframe of the analysis. In particular, the article focuses on the period from the Russian occupation of eastern Ukraine in 2013 until early 2022. 2013 marks the beginning of the Ukrainian crisis, when more talk of Russian hybrid or information warfare is beginning to emerge (e.g. Giles, 2016). Given the severity of the simultaneous Russian invasion of the entire territory of Ukraine (from 2022 onwards), key findings affecting the outcomes of the article will also be included.

2.2 Representativeness

To ensure maximum representativeness, two actor cases in each category were singled out for analysis in the baseline. The number two was chosen as the average of the actor types identified. However, if more actors were identified in a category with specific characteristics, they were also listed or analysed in more

depth.

If only one case of an actor was identified in a category, or if others identified were of very marginal importance, only this one actor was elaborated. However, the author approached the elaboration of the single actor in a category only if it was a significant actor using sophisticated tools. In other cases, the primary approach has always been to merge possible categories into more general ones that include multiple actors.

3. Theoretical background

3.1 Active Measures

Active measures (Bittman 1972, 1985; Darczewska, 2018; Kux, 1985; Rid, 2020; Schoen and Lamb, 2012; Schultz and Godson, 1984; Sulc, 1985; United States Information Agency, 1988; United States Information Agency, 1992) represent (if restricted to the realm of cyberspace) a relatively comprehensive model for malicious information influence analysis. The concept of active measures links the history and present which **Gärtner** (2020, p. 40) describes by the evolutionary not revolutionary character of Russian warfare doctrine. The characteristic variables do not change over time, they adapt to recent technological development.

Active measures combine overt and covert methods which cover a complex system of Russian approaches to achieving political and foreign policy goals through informational influence. The tools for achieving these goals target the fundamental weaknesses of Western democracies - freedom of expression and open society while also targeting the West's preeminent instrument of defence, namely Article 5 of the Washington Treaty (Galeotti, 2019).

The most comprehensive definition of active measures (Darczewska, 2018, p. 252) first appeared in the counterintelligence dictionary of the KGB (Komitet Gosudarstvennoy Bezopasnosti, in English Committee for State Security,) (Nikitchenko, 1972). If we abbreviate it, it describes active measures purely in terms of the activities of the KGB, namely as procedures to predict the opponent's actions and avert his subversive actions offensively. These activities exploit the positions of agents within the opponent's inner circle, they use disinformation and obfuscation. The definition according to former KGB agent **Vasily Mitrokhin** (2018a, b) is more general and characterizes active measures as activities aimed at influencing aspects of the political life of the opponent, his foreign policy as well as deceiving him, weakening his position or disrupting his plans. Also, the

testimony of **Ladislav Bittman**, a former Czechoslovak State Security agent with a practical focus on active measures is a valuable source of information. **Bittman** defines active measures as political, military and economic disinformation and covert actions designed to manipulate public opinion, government and influential private organisations and personalities (2000, p. 51).

3.2 History of active measures

According to **Holzer** and **Kuchyňková** (2005), the political system of the Soviet Union realistically fulfilled the model of a totalitarian state described by **Hannah Arendt**. The emergence of active measures replicates the establishment of a totalitarian state with its roots in the October Revolution of 1917, which was accompanied by the accumulation of power in the hands of a small group of revolutionaries (Sakwa, 1998, p. 292). However, the evolving modus operandi has its roots before the October Revolution (Darczewska, 2018, p. 254). The term active measures first appeared between 1919 and 1920 during the founding of the Comintern and Cheka (Styrna, 2011). As Bertelsen (2021, p. 14) mentions, KGB-led measures had two dimensions, domestic and foreign. Further inspiration can be found within the Andropov Institute (the Soviet intelligence academy) where active measures were taught.

Active measures gained importance in 1960 (Schultz and Godson, 1984, p. 12). One of the most notable operations, codenamed STORM, took place in 1967 when the KGB succeeded in using a false war plan to damage the reputation of the US on the international stage (Rid, 202, p. 267 and p. 364-365; Hughes, 1985).

After the collapse of the Soviet Union, there has been a shift towards authoritarian use of power (Holzer and Kuchyňková 2005). Since the beginning of the 21st century and the rise of Vladimir Putin, there are already several reasons to label Russia as an authoritarian regime, mainly due to the decline of political pluralism, the development of democracy and personal freedoms (Mochtak and Holzer 2017). In parallel with these trends, a renaissance of active measures has begun, especially with the person of **Vladimir Putin**. The reuse of old techniques is hidden under the so-called 'defensive strategy against the West's information war' (Darczewska and Zhokhovski 2017, 38), which, according to the Russian interpretation, seeks to attack the Russian regime mainly through organising unrest in society.

3.3 Tools of active measures

Active measures can oscillate between classic official diplomacy and illegal intelligence operations. The following list presents the main tools of active measures that link history and the present. The author has compiled the categories according to the basic literature on active measures and examples from practice related to their relevance and frequency. These are:

- allied political parties,
- agents of influence,
- cultural, religious and educational organisations,
- military operations,
- press and media,
- forgeries,
- economic warfare,
- and secret services operations.

The most typical tool is influencing the political parties and individuals with access to power (so-called agents of influence). Soviets manipulated foreign political parties through financial flows or personnel (Bittman 1985, p. 38; Sulc 1985, pp. 14-15). According to the Latvian Security Service (2016), Russian intelligence currently aims to recruit or influence the middle management of political parties.

Soviets also use tools within the social or socio-political sphere. The aim of the establishment and functioning of various organisations (so-called fronts) was to promote Soviet ideology and policies.

Besides political warfare, military operations have their place in Russian active measures too. Soviet active measures included military and paramilitary operations, the use of proxies, support for terrorism and insurgency (Schultz and Godson 1980; Sulc 1985, 20; United States Information Agency 1992), but also infiltration into the military structures of opponents (e.g. NATO structures, as described by Bittman 1985, p. 133). Today's military measures typically use proxies in the aggressive operations in Ukraine, Syria or the Central African Republic, thus in areas with ongoing military conflicts (Stronski 2020).

The Soviet active measure was often neglecting foreign media manipulation. It rather created its media content, as retired General **Keith B. Alexander** points out (Global Security 2020; cf. Kux 1985). An important tool was forgeries (Bittman 1972, p. 30) with the media as a leading facilitator (Bittman, 1985, p. 38). Former as well as current media manipulation is usually linked to disinformation.

Economic active measures were another part of the complex system of influence which targeted especially Soviet republics and satellites (CIA 1986; US Department of State 1981; Bittman, 1985, p. 212). Current economic active measures are strongly linked to specific national political or economic structures.

Given the privileged position of the intelligence services in active measures, we consider the involvement or management of all mentioned actors. However, some operations are exclusively conducted by the secret services. At the time of the bipolar confrontation, these included espionage, sabotage, provocation, wet affairs or assassination under the command of the KGB (e.g. Bittman 1985; Kuzio 2021, pp. 138-141). After the collapse of the Soviet Union, the legacy of the KGB was spread over three secret services, namely the FSB, the SVR and the GRU. We find a similar pattern of operations now as in the past, but with the addition of the latest technologies available for espionage and sabotage.

3.4 Threats in the Cyberspace

This work understands cyberspace as the realm of computer networks and the users behind them, where information is stored, shared and communicated online (Singer and Friedman, 2014, p. 47). Threats in cyberspace can be categorized according to several criteria: most commonly by motivations of the attackers or the sophistication of the attacks. Andress and Winterfeld (2012, p. 33) define several basic types of motivations: economic gain, seeking lucrative employment, popularity/high status in cyberspace, entertainment, hacktivism, terrorism and war. In terms of sophistication, web defacements are usually placed at the tail. Distributed denial of service, phishing attacks and spear phishing follow. Advanced persistent threat (APT), which is most associated with cyber espionage (Jensen et al., 2019, p. 216), is seen as the most sophisticated. It can operate in multiple vectors, such as by attacking media and supply chains or social engineering (ENISA, 2021).

In recent years, attention has also been paid to attacks by cyber saboteurs using ransomware, i.e. extortion malware that, in addition to primarily economic motivations, also pursues political ones (NATO, 2021a). Ransomware particularly threatens critical infrastructure, the disruption of which can be devastating for society (Molina, 2022; Bochman and Freedman, 2021, pp. 13-15).

Active measures can also be related to political activism, which, in the context of cyberspace, is linked to hacktivism (Singer and Friedman 2014, pp. 77-79; Andress and Winterfeld 2012, pp. 197). However, since the label is associated with citizens' struggles for democratic values, Russian active measures do not fit

the concept. A more appropriate label for these actors is patriotic hackers (Singer and Friedman 2014, pp. 270).

However, as authors (Ibid., p. 48) add, cyberspace is primarily an information environment made up of digitized data that are shared. Therefore, besides hostile code operations discussed above, it is a domain of hostile content as well. Hostile code operations use of malicious software (malware) (Jirásek, Novák and Požár, 2015, p. 115), which includes computer viruses (more ibid. p. 125), worms (more ibid. p. 37), Trojan horses (more ibid. 119), ransomware and spyware. Hostile content operations consist of sharing disinformation, fake news (e.g. Pamment et al., 2019), radical, extremist (Winter et. al., 2020) and various harmful content. Harmful content can evolve into weaponization or falsification of history (Jurvee et. al., 2020).

Current actors using hostile content operations in cyberspace include online journalists, hybrid trolls (Al-Rawi and Rahman, 2020; Spruds et al. 2016, pp. 10-11), bots (Computational Propaganda Project, 2016; Gorwa and Guilbeault, 2018; Nimmo, 2019), disinformation news media, politicians and political parties, bloggers and influencers. Disinformation is the core tool of most of these actors. NATO (2021) considers disinformation as the deliberate creation and dissemination of false or manipulated information to deceive or mislead. It may be disseminated through the sources, primary disinformation channels, secondary channels (e.g. non-serious media) and the target audience that disseminates the content (Mareš and Mlejnková, 2021, p. 83; Gregor and Mlejnkova, 2021, p. 9).

Nowadays, hostile content operations using artificial intelligence (Langguth et al 2021; Pavlíková, Burešová, and Drmola, 2021, pp. 61-65) and deep learning are broadly discussed. Chessen (2017) defines the combination of artificial intelligence and tools such as bots, machine learning and deep learning as MADCOM (machine-driven communication tools). When combined, it becomes a powerful tool for online manipulation with highly personalized campaigns. The high personalisation of campaigns relates to the term microtargeting (Zuiderveen, 2018). Cambridge Analytica, which created a highly personalised campaign in 2016 using data on up to 50 million social media users which aimed to convince Britons to vote for Brexit, is a practical example.

3.5 Security Sectors

Active measures are implemented in various environments with various actors. **Bittman** (2000, p. 51) mentions political, military and economic active

measures, while **Radin**, **Demus** and **Marcinek** (2020, p. 9) operate with political, military, economic, social and cyber entities. The analysis uses the sectoral division according to the Copenhagen School of Security represented by the work of **Barry Buzan**, **Jaap de Wild** and **Ole Waever** (1998), one of the essential concepts of security and strategic studies (Waisová, 2004). The authors work with five sectors - military, political, social, economic and environmental. For the military and political sectors, which belong to the classical non-extended sectoral concept, the research focuses exclusively on states as reference objects and their associated threatened values such as territorial integrity and sovereignty. The expanded concept of security, which runs on a horizontal axis, adds the social, economic and environmental sectors.

3.6 Referent objects

Western values such as pluralism and openness are seen as weaknesses that can be exploited (Global Security, 2020; Pynnöniemi, 2018, p. 7). Thus, active measures target the society's fundaments, namely citizens and their mindsets. **Olga Bertelsen** (2021, 27) notes that the evolution of Russian active measures has also pointed to other targets besides the minds of citizens, namely the technology or governmental infrastructures of states. Targeting people's minds and societies can still be seen as the primary goal of active measures, but multiple paths can lead to this goal. These can be identified through sectoral divisions and reference objects.

The new expanded paradigm of security sectors (Buzan and Weaver, 1998) expands from the state as the traditional referent object. The referent objects in the five security sectors are entities that are existentially threatened and can legitimately claim the right to survive. The school rejects a focus on the state alone, adding firms, humanity, the environment, the world economy or democracy.

The following paragraphs introduce the Copenhagen School's sectors and the associated key referent objects and values at risk that complement them. The reference objects and values will also be complemented by aggressor targets relevant to cyberspace, based on traceable information from open sources. These may be supplemented by additional targets that emerge in the analysis section.

For the military sector, the primary referent object is the state. The Copenhagen School also lists the constituent parts of the state, the government or the nation (here conceived as the Westphalian) state, in the case of a military

threat. Furthermore, tribes, nations, and even religions can be included if they cannot be separated from the state. The values at stake are sovereignty and territorial integrity.

Through the optics of active measures, the author considers targets such as military structures, especially NATO, or lower-level military intelligence agents, as described by **Bittman** (1985, pp. 44, 67 and 133). If these active measures are transferred to cyberspace, they can be camouflage, deception, proxy actor attacks (Alexander, 2017, p 2; Bagge, 2019) or, more generally, attacks using malicious code or content. These target both military structures and units or individuals.

The basic reference object of the political sector is the state as a political organisation and so-called quasi-superstates (for example the European Union). **Buzan**, **de Wilde** and **Weaver** (2005) further include transnational movements, tribes, ethnic minorities and clans in the political sector if they have established strong political institutions. The radicalisation of public discourse, coupled with undermined trust in political institutions and political representatives, can lead to a search for alternatives represented by the far right and left and a diminishing of the credibility of mainstream political parties (Mareš and Mlejnková, 2021, p. 88). Thus, attacker threatens the state as a political institution and democratic system. Through the lens of threatened values, these are the founding principles of the state - sovereignty, territorial integrity, international regimes and state ideologies. Specifically, the political ecosystem, diplomacy, and decision-makers, but also e.g. upcoming elections, election campaigns or their members are threatened by malicious code and content attacks in cyberspace. Typical targets have always been European political parties with the aggressor's financial funding. However, as **Bertelsen** (2021, p. 52) notes, the funding of political parties has had only a limited impact with uncertain reciprocity in the future. The Kremlin has adopted a new strategy that orientates directly on elections. The direct subversion of the electoral process becomes an easier target in the context of the use of cyberspace.

In the social sector, the referent objects are social groups, tribes, clans, nations, civilizations, religious systems and races. Security threats are directed against state-forming groups of society or the security of social groups themselves (Waisova 2004, p. 75). The associated threatened values are identities, or as the authors describe "we" and national unity. When applied to cyberspace and active measures, values can be threatened through the targeting of voters, minorities and society. According to EUvsDisinfo (2021b), the most

effective disinformation operations target specific countries and regions by exploiting social tensions and bilateral disputes. The promotion of hate narratives heightens tensions between different groups of the population, whether political, social, ethnic or religious. Pre-existing conflicts in society can be artificially promoted to destabilize society (Mares and Mlejnkova, 2021, p. 88), The members of society (especially groups of citizens) then become instruments that create or amplify social conflict (Palomo, 2021).

In the economic sector, **Buzan** et al. include individuals, social classes, the world market and companies as reference objects. Companies can be included in the sector if they have an important position in the industrial base of the country. If they are local, they must have an immediate impact on communities and/or individuals. Threatened values at risk are economic development, basic human needs or existence itself. The term economic information warfare can be applied to the economic sector and active measures together. It refers to strategies, tactics, and operations that threaten a state's critical economic systems. **Libicki** (1995, p. 68) distinguishes two types of economic warfare; the first involves traditional blockade or bombing of industrial facilities to degrade the economy and national economic capacity (Niekerk and Ramluckan, 2019, p. 33). The second variant views economic information warfare as an aspect of information warfare, strongly linked to cyber operations. Economic information warfare is thus understood as activities to control, protect and potentially disrupt economic activity through information and information systems. Targets are critical national infrastructures (Deakin, 2003) which include energy, banking and finance, transportation and telecommunications. It is more amenable for aggressors to focus on economic disruption rather than directly attacking military and government targets. **Deakin** (Ibid.) also adds that degrading, disrupting, and destroying an opponent's infrastructure can complement diplomatic and military activities.

According to the Copenhagen School, the environmental sector is characterised by two categories of referent objects, namely the environment as such and civilisation about the environment. The second option is relevant to this study. It deals with threats caused by human activity affecting natural systems or planetary structures. The threatened values are human existence, quality of life and sustainability. **Buzan** himself was sceptical about the environmental sector, especially about the intrinsic nature of environmental threats and thus the impossibility of relating them to competition between states (Walach, 2016, p. 20).

However, if we relate the environmental sector to active measures, and

especially to cyberspace, the targets are mainly industrial systems, whose disruption in connection with political goals rejects **Buzan's** scepticism. Almost every industry with an environmental impact today faces a high risk of a cyber-attack with potentially fatal environmental consequences. Almost every industrial facility that stores or processes large quantities of, for example, chemicals, uses information and communication technology-dependent industrial control systems (Pačka, 2017). Examples include attacks on oil or gas pipelines, refineries (e.g., Bhopal, India 1984), chemical plants, marine systems (Eastern Venezuela 2002), water and electrical facilities (Massachusetts 2007), and transportation systems. The increasing digitisation of control systems and the potential for cyber-attacks also pose a threat to nuclear facilities. Real-world examples include the attack on the David-Besse nuclear power plant in Ohio in 2003, the Brown Ferry nuclear power plant in Alabama in 2006, and finally the Iranian nuclear facility in 2010. The Stuxnet worm (for more see Zetter, 2015) destroyed Iran's uranium enrichment facility and drew attention to the fact that nuclear power plants can also have accidents with leaks of radioactive material. The sophisticated Stuxnet can be referred to as APT according to the above terminology. It became the prototype of next-generation cyber-attacks. In the context of reference objects in the environmental sector, its potential to threaten the environment through the disruption of industrial control systems is significant.

4. Analysis and Results

The following part focuses on the actors and tools of active measures as they are manifested in the security sectors. First, a variety of actors were brought together based on open sources to cover the entire ecosystem of Russian cyber active measures. Subsequently, general categories have been created. If the type of the category did not fit into any of the classical types of actors known in the literature, or if they were their specific offshoots, they were placed in a category created by the author.

The following categories of actors were created (in alphabetical order) from the collected data:

- cyber spies and hackers with links to the secret services
- cyber saboteurs
- disinformation media[2]

[2] Disinformation media, for the purpose of the analysis, refer to wide scale of media actors with various links to Russian state, which use disinformation, fake news, malicious narratives or conspiracy

- embassies and diplomats
- hybrid trolls
- online journalists, bloggers and influencers[3]
- local governments
- organisations working on a specific topic
- organised crime
- patriotic hackers
- pseudo-experts
- political parties and its members
- paramilitary groups
- state media[4]
- state armed forces
- secret services involved in coordinated campaigns
- and umbrella organisations[5].

Linking the sectoral division according to the Copenhagen school of security with current Russian operations in cyberspace categorizes Russian cyber active measures. Based on the categories, the real actors are then analysed in more depth stressing targets of identified cyber active measures, which can be linked to reference objects and values threatened values.

Military sector

Table 1: Identified categories and actors in the military sector

category	**actor**
state armed forces	*Russian armed forces, Vojennyj obozrevatel'*
paramilitary groups	*Hungarian National Front, Czechoslovak reserve soldiers for peace, Slovak Conscripts*
patriotic hackers	*Anonymous Ukraine, Cyber Berkut*
cyber spies and hackers with links to the secret services	*Fancy Bear, Unnamed secret services unit*

theories. We also work with category of „state media" (see below), which is strictly linked to official Russian media under governmental supervision.

[3] Among the individuals participating in Russia's active measures, we include the category of journalists and bloggers disseminating hostile content. Journalists refer to persons working under particular media platforms, while bloggers are more individual and not linked to any official media subject.

[4] Category of state media refer to subjects clearly and officially linked to Russian state.

[5] Umbrella organisations refer to official state cultural, religious or social subjects, which cover various smaller, usually worldwide, organisations.

We identify state armed forces, patriotic hackers, paramilitary groups and cyber spies with links to military intelligence as actors of active measures in the military sector. The main referent object is the state with sovereignty and territorial integrity as threatened values. The stability of the Euro-Atlantic area, the credibility of states as security providers, the credibility of NATO, the armed forces and the trust between the allies themselves can be identified as specific threatened values. Cyber active measures target Western governments, states as providers of defence and security, NATO, armed forces, state cyber capabilities and military capabilities. Actors use hostile code as well as hostile content tools. In the case of code, attacks of less sophistication such as web defacements, DDoS attacks and phishing are taking place. This is especially true for the category of patriotic hackers. European governments, armed forces and cyber capabilities are targets. Operations can serve as reinforcements to conventional military operations that are specifically directed against the state or armed forces. Anonymous Ukraine, for example, has attacked official websites, mostly of Western defence organisations and authorities, mainly through DDoS attacks. The NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence) website was attacked in November 2013, as well as the Estonian Ministry of Defence website. The CCDCOE site was down for two hours, and the group called the entire operation a retaliation for alleged cyberattacks by NATO itself (Pavlíková, 2016).

For state armed forces as well as paramilitary groups, active measures are most often implemented through hostile content operations; most notably disinformation using fake news, extremist content sharing, online recruitment of members with their subsequent radicalisation, and commanding and engaging in their military activities (Forró, 2019; Kandrik, 2020, p. 4; Ježek, 2021; Československí vojáci v záloze za mír, 2020). State armed forces alone, represented by the online journal Vojennyj obozrevatel' and Russian armed forces during military exercise Zapad 2017 and 2021 are using mostly official communication strategy with the elements of disinformation.

States as providers of safety and security, in particular the armed forces, can be identified as targets through which referent objects are influenced. **Mareš** and **Mlejnková** (2021, p. 90) speak of paramilitary actors who undermine trust in the state as a provider of security and want to take power into their own hands to ensure public order. Given the focus on paramilitary groups' hostile content operations, the question of inclusion in the social sector also arises, as hostile and manipulative content can threaten social groups or nations themselves.

However, the author concludes, based on the available data, that the primary goal of paramilitary groups is to substitute the state as a security and defence provider, therefore classification in the military sector is more relevant.

In the category of cyber spies and hackers with links to the secret services, we identify a group practising cyber espionage with the following usage of fake news (thus, a combination of hostile code and content) with links to Russian military intelligence. Fancy Bear targeted especially armed forces and military capabilities. The attack on the Android app used by the Ukrainian artillery during the early years of the Ukrainian crisis could have facilitated the reconnaissance of separatists against Ukrainian soldiers. The malware's ability to extract communications and location data from an infected device made it an attractive way to determine the general location of Ukrainian artillery forces and strike against them (CrowdStrike, 2017). Another identified actor, the unnamed cyber group linked to Russian secret services, used fake news with web defacement. Group threatened NATO's trustworthiness during 2018-2019 (EUvsDisinfo, 2019; Tucker, 2019; Vandiver, 2019).

Political sector

Table 2: Identified categories and actors in the political sector

category	actor
embassies and diplomats	*Russian Embassy in the Czech Republic* *Russian Embassy in Denmark*
hybrid trolls	*Reconquista Germanica, Internet Research Agency*
patriotic hackers	*Cyber Berkut, Killnet*
political parties	*5 Star Movement, Bulgarian Socialist Party*
local governments	*Viktor Orban's government*
cyber spies with links to the secret services	*Cozy Bear, Fancy Bear, Ghostwriter*

In the political sector, we find several active measures actors linked to politics or service for the state. Members of diplomacy, political parties and local governments use only hostile content operations which include predominantly the sharing of disinformation and extremist content. States as political organisations and quasi-superstates were the most relevant referent objects for the analysis. Therefore, the founding principles of the state, especially the state ideology are threatened values. Elections, electoral campaigns, the political ecosystems, European governments, non-EU structures, decision-makers and diplomacy are

targets through which the referent objects are influenced.

Hybrid trolls, such as Reconquista Germanica and Internet Research Agency (hereafter IRA) target political parties, elections and citizens' decision-making, and the overall political ecosystem of given countries with the founding principles of the state as a threatened value. Reconquista Germanica used hostile content operations to promote alt-right ideology in connection with the Alternative for Germany (AfD) party during the German parliamentary elections in the 2017 campaign. The IRA has focused on states as political organisations by targeting citizens and their political decision-making in elections. However, it has manipulated social groups too (Robert S. Muller Report against Internet Research Agency 2018: 6; US Department of State, 2020). Therefore, the IRA will also be classified in the societal sector.

Furthermore, we identify patriotic hackers using hostile code as well as hostile content. Targets in this category represent a disruption of the electoral process and the political ecosystem. The state as a political organisation and democracy are threatened values. Cyber Berkut's operations against the Ukrainian electronic electoral infrastructure posed threats to these reference objects during the hot phase of the Ukrainian conflict (Greenberg, 2017; Pavlíková, 2016). In 2014, the group attacked the website of the Ukrainian Central Election Commission and changed the election results in favour of the far-right candidate **Dmytro Yarosh**. Russian state media coordinated with the hackers to publish the fake results (Greenberg, 2017). In addition to the attack against Ukraine's electoral infrastructure, the group also targeted the websites of the Polish and German governments (Stone, 2015). Otherwise, a more recent group Killnet focused on European governments and attacked them by DDoS with a change of their website contents (Antoniuk, 2022; CSIS, 2022; Roussi, 2022).

In the case of cyber spies with links to intelligence services, Cozy Bear (or APT 29 or The Dukes) who is working under the FSB or SVR is the best-known group. The group is responsible for espionage operations in Europe and the US, for which it is referred to as APT. Cozy Bear was also involved in hacking into the systems of the Dutch police investigating the downing of the MH17 plane over Ukraine (NL Times, 2021), in an influence campaign during the 2016 US presidential election and in an attempt to steal data for the development of vaccines against the Covid-19 disease (National Cyber Security Centre, 2020). The massive cyber-attack on SolarWinds systems also matches Russian active measures in its characteristics. Although the primary attack may have given the impression of sabotage, the real motivation was probably to gain sensitive

government information (Warrell, 2020b).

Cyber spies with ties to intelligence services such as Fancy Bear and Ghostwriter are mostly using phishing and subsequent content sharing, DDoS, web defacements as well as more sophisticated sabotage attacks on electoral infrastructure (e.g. 116th Congress Senate Report n.d.; Bertelsen, 2021, 53; Ringstrom and Balmforth, 2021; Foster et al., 2020).

Societal sector

Table 3: Identified categories and actors in the societal sector

category	**actor**
state media	*RT, Sputnik News*
umbrella organisations	*Russian World, Rossotrudnichevstvo*
hybrid trolls	*Internet Research Agency* *Reconquista Germanica*
organisations working on a specific topic	*Russian Institute for Strategic Studies* *Essence of Time*
disinformation media	*Geopolitica.ru, Redfish, InfoVojna, Aeronet* *Baltnews, Unnamed group*
cyber spies with links to the secret services	*Cozy Bea, Fancy Bear, Ghostwriter*
pseudo-experts	*Alexandr Dugin,Alexandr Dyukov*
journalists, bloggers and influencers	*Ricardo Fernandes Cabral,* *Graham Philips* *Russian Influencers on TikTok* *micro-influencers and nano-influencers*
secret services involved in coordinated campaigns	*Fancy Bear*

The societal sector is the most diverse in the number of categories of actors, but most uniform in the format of operations. With one exception, societal sector operations are built exclusively on operations of hostile content. This suggests that referent objects are most easily targeted by disinformation, harmful narratives, falsification of history and astroturfing. For a large part of actors, secondary disinformation channels or target audiences further disseminate hostile content (see Mareš and Mlejnková 2021, 83).

The umbrella organisations such as the Russian World (Russkiy Mir) and Rossotrudnichestvo are official activities (Kudors and Orttung, 2010) disseminating disinformation and harmful narratives. The Russian diaspora, as well as various population groups or the European community itself, can be seen

as targets; the reference objects are social groups and nations (possibly of a transnational nature). Russian state media as RT and Sputnik news have a similar position. RT mainly serves as a platform for further dissemination of distorted information through cyberspace, as it is usually the primary source for many non-state and marginal media outlets or individuals on social media.

RT is generally focused on the European community, whose citizens are targeted by the broadcasts. **Crilley** et al. (2022) summarise that according to current academic debates, the target audience may be citizens opposed to the establishment, corporatism and the West. However, they also target non-Western audiences, potential activists and local media that can further disseminate their content. Thus, social groups are referent objects and collective identity is threatened value.

Other categories using exclusively hostile content operations are organisations working on a specific topic. In Russian Institute for Strategic Studies, unlike genuinely scientific texts, there is a distortion of the facts. It targets groups with specific interests, and consequently the academic community. The Essence of Time is working similarly. However, its content sharing was used to recruit individuals for the Russia-Ukraine conflict engaging, either physically, through hostile content or fundraising.

As in the political sector, the same groups of hybrid trolls were identified. For the IRA, we can conclude that it did not only target the specific US presidential election in 2016 but also, through its long-term manipulative influence, trolls targeted referent objects of the societal sector, namely social groups in the US. Reconquista Germanica threatened German social groups outside the immediate electoral decision-making process.

Another category using exclusively hostile content operations covers disinformation media. The author divided this category into sub-categories because of its width and complexity. These are (a) websites and platforms with a specific ideological belief, (b) local language-specific media, (c) disinformation news media, and (d) fake media and accounts. The main referent objects for all categories and actors are the social groups. They are threatened dominantly through actors' targeting of groups with specific interests, Anti-Western and anti-establishment European citizens, anti-establishment activists, EU citizens, Baltic states citizens, grassroots movements, minorities and the Russian diaspora. The most used hostile content tools are disinformation, fake news, falsification of history and harmful narratives.

The category of pseudo-experts refers to persons or groups that present themselves with science or expert capital. They disseminate preferred ideological narratives and therefore threaten social groups as referent objects. However, academics or the scientific community are not targets. Pseudo-experts focus on easily manipulable social groups and local European populations. For example, **Alexandr Dugin** like **Alexandr Duykov** used disinformation, falsification of history, harmful narratives and radicalism against these targets (Tharoor 2022; Weidinger, Schmid and Krekó, 2017; Makonkalns, 2020; Naylor, 2020; The Baltic Times, 2007).

Journalists, bloggers and influencers participate in cyber active measures through hostile content on social media, blog platforms, or through manipulative videos. They use their popularity to amplify Russian state propaganda as well as harmful narratives. Micro-influencers and nano-influencers, who have a smaller number of subscribers (25,000 or less) are usually used in groups in a coordinated way for specific campaigns, for example sharing activist content focused on the Ukrainian conflict (Helmus et al., 2021). **Wooley** (2022) characterizes them by their ability to engage ordinary social media users (see Maheshwari, 2018). These actors also exploit EMAs - private communication apps (e.g. Telegram and WhatsApp) to target individuals in private communication format. Manipulative content is thus disseminated through establishing a closer relationship with the user (Wooley, 2022; Kraus, 2022).

One actor using hostile code as well as content operations was identified. As already mentioned in other sectors, Fancy Bear operated this way, especially during the 2016 US presidential election. The format of the operations can be described as "hack and leak", where the data extracted by hostile code are subsequently published, either in its original form or modified. The targets were various social groups in the US based on age, gender, race, religion or socio-economic status.

Economic sector

Table 4: Identified categories and actors in the economic sector

cyber spies with links to the secret services	*Sandworm Team*
cyber saboteurs	*Sandworm Team*
organised crime	REvil DarkSide/Blackcat

Even in the economic sector, an active measures actor category of cyber spies with links to secret services can be identified. The referent objects are the

state, institutions, companies and individuals. National warfare capabilities of the state, which are stolen and subsequently misused by cyber espionage, are targets. Furthermore, the critical infrastructure of the state whose disruption can cause economic damage to the state, its institutions or companies are also targeted. The development of the very existence of economic entities can be understood as a threatened value. In the case of more serious attacks on critical infrastructure, basic human needs are at risk.

A real-life example is the theft and misuse of exploit EternalBlue, which was stolen by the Sandworm Team for espionage (Greenberg, 2020). National warfare capabilities of the state and critical infrastructure were targeted. The Sandworm Team group is also known in cyberspace by other operations and names, with Black Energy, Quedagh and Electrum being among the best-known. Originally, the unit is thought to be the GRU Main Centre for Special Technologies (GTsST) (Marino, 2020) and was spying for governments, using zero-days, malware and spearphishing for years. Of its recent exploit of EternalBlue, businesses, government facilities, airports, and banks in Ukraine, Britain, and Spain were hit (Rothwell, Titcomb, and McGoogan, 2017).

Another category of actors is cyber-saboteurs. They target the nation-state's economic systems and critical infrastructure. Unlike cyber espionage, this involves primarily sabotaging networks, operations or systems to prevent or coerce an adversary to take a particular action or to compensate financially. Nevertheless, the referent objects and threatened values are the same as in the case of cyber espionage. Basic human needs may be compromised in the case of serious attacks on critical infrastructure, which are currently associated mainly with ransomware used by cyber saboteurs. The cyber-attacks on energy infrastructure in Ukraine in 2015, which were carried out by the Sandworm Team, have already become a significant form of sabotage in terms of scale and impact. The Sandworm Team operation using the NotPetya malware that affected critical infrastructure (including medical facilities) and global trade globally in 2017 can also be identified as cyber sabotage. The financial losses amounted to US$1 billion (US Department of Justice, 2019). The same attacker also disrupted an operation of the Kyiv metro, the Odesa airport, the Russian Central Bank, as well as two Russian media outlets with ransomware called BadRabbit in 2017 (National Cyber Security Centre, 2018).

The last category in the economic sector is characterised by organised crime groups operating in cyberspace; typically, in conjunction with intelligence services, which provide a channel for the implementation of active measures. The

targets are the economic systems of the nation-state, private companies and critical infrastructure. A real-world example of such an actor is REvil, which is a shortened version of the name Ransomware evil, referring to the type of attack. The group is responsible for a cyberattack using ransomware that hit thousands of private companies around the world in the spring of 2021 (Sanger, 2021). REvil was operating at the same time as the Russian civilian intelligence-linked group Cozy Bear. This may indicate coordination of attacks and thus inclusion in active measures. A fresh example from 2022 is the sophisticated ransomware attacks attributed to the DarkSide (now also BlackCat) group. The group presents itself as a modern-day virtual Robin Hood to take from wealthy companies and redistribute to charities (Kerner, 2022; Gallagher, 2022). The group gained attention with a cyberattack on the Colonial Pipeline, one of the largest and busiest oil pipelines in the United States. The pipeline runs from the Gulf of Mexico to states on the East Coast. According to **Kerner** (2022), this was the most extensive attack on critical infrastructure in the US. The attack affected several systems, such as accounting. Although the targets may give the impression of hitting the environmental sector, the attackers were probably not concerned with disrupting the functionality of systems leading to environmental destruction. On the contrary, the targets are precisely focused on the economic sector.

Environmental sector

Table 4: Identified categories and actors in the environmental sector

Political parties and its members	Bulgarian Socialist Party, Robert Huliak

If we think about potential actors where active measures in the environmental sector can be implemented, cyber-saboteurs and cyber-spies would correspond to them.

The referent objects in the environmental sector, according to the Copenhagen School, are civilisation linked to the environment, the state, the ecosystem and the human species. The threatened values are human existence, quality of life and sustainability. The targets that could be affected by cyber active measures are like those of the economic sector. However, the systems attacked would have an impact on the environment instead of economic indicators. Targets could be industrial warfare or other state systems, nuclear facilities, and any control systems that can cause an environmental disaster. Considering the

events till 2023, the attack of this scope did not take place (till 2022).

Besides this hypothetical threatening of environmental sector by hostile code, ongoing hostile content operation are taking place. Since the Russian invasion on Ukraine, "*the European Green Deal has taken on a new significance with respect to ending the EU's overreliance on Russian energy and exposure to the Kremlin's authoritarian influence*" (Center for the Study of Democracy, 2023). In the context of Russian active measures, we identify political parties or its particular members using disinformation and negative pro-Kremlin narratives on Green Deal politics. In Bulgaria, political actors (for example from *Bulgarian Socialist Party*) „*amplify and normalize disinformation narratives opposing the Green Deal both domestically and internationally*" (Ibid.). Another recent example refers to newest Slovak Environment Ministry nominee Rudolf **Huliak**, who does not believe in climate change, uses narratives as "Brussels eco-terrorists" and often shares pro-Russian disinformation on social media. Slovak president Zuzana **Čaputová** lately refused **Huliak** as a minister (Dennik N, 2023; Zmušková, 2023).

5. Discussion and conclusion

The outputs confirm the possibility of Russian cyber active measures research through the lens of threatened values. The analysis enabled drawing a comprehensive picture of the issue with the specification of the aggressor's tactics and targets. The application of the Copenhagen School's sectoral division using referent objects and threatened values contributes to the complexity. The expanded concept of security, which considers the social, economic and environmental sectors besides the military and political sectors, has proven relevant to the study of emerging threats using new technologies. Although it can be stated that the state is the main referent object affected by active measures, the analysis points to a much broader range of threatened values that almost replicate those defined by the authors of the extended sectoral concept.

The resulting manifestations of Russian cyber active measures are observed in military and political sectors while using hostile code and content tools across a whole range of sophistication. In the societal sector hostile content is prevalent, particularly through disinformation, fake news and malicious narratives. In the economic sector, actors involved in sophisticated operations using hostile code tools were identified. Finally, manifestations of hostile content operations were found in the environmental sector.

The analysis also specified the threatened values by the cyber active measures in the sectors. Besides those given by Copenhagen School (sovereignty and territorial integrity) it can be complemented by the stability of the Euro-Atlantic space, the credibility of states as security providers, the credibility of NATO, the armed forces and the trust between the allies themselves in the military sector. In the political sector, state ideology as European and hence American democracy is threatened. In the economic sector, critical infrastructure associated with basic human needs as threatened value was stressed.

As the research also showed, no Russian cyber active measures have been identified in the environmental sector. However, it certainly cannot be argued that the environmental sector has no relevance for active measures in cyberspace. Results from the economic sector point to the fine line that exists between the use and non-use of cyber tools which can have an environmental impact. While **Buzan** (2005) missed the intentionality in the case of environmental threats (see Walach 2016, 20), the transfer of threats into cyberspace radically changes the format.

It can also be stated that Russia is not using all available technology that can be used to cyber active measures. For the political and societal sectors, the use of MADCOM, microtargeting tools and artificial intelligence as deep fakes have not received many real contours. Actors using this type of tools can be states, governments or even individuals.

So far, the only significant use of micro-targeting by Russia is related to the 2016 US presidential election, which also involved the IRA and Fancy Bear actors identified in the analysis. Since then, the tool has not been applied in any significant way, although Russia continues to operate hostile content operations to large extent, especially on the European continent. Microtargeting and MADCOM can also be combined with other new technologies, e.g. deep fakes, facial recognition or biometrics. Sophisticated cyber sabotage that disrupts systems has the potential to threaten the economic sector's critical infrastructure. It can cause widespread economic damage, for example, blackout of national power grids. Also, with the help of deep fakes, disinformation or fake news attackers can jeopardise the credibility of economic actors or causes panic in the financial market (e.g. by informing about bankruptcy) (Pavlíková, Burešová and Drmola 2021, 64).

Although no cases of actors using hostile content operation in the environmental sector have been found, cyber actors mentioned in the theoretical section can became real in the future. Environmental threats focus on states'

industrial systems, their command-and-control systems and especially nuclear facilities. The closest attacks on these facilities took place in the summer 2022 when the Russian hacker group People's Cyber Army used web defacements which targeted the website of Ukraine's state-owned Energoatom, a company specialising in nuclear energy. Apart from a three-hour website outage, there was no compromise of functionality (Al-Jazeera, 2022).

The resulting research challenges are formulations of countermeasures that respond to the latest aggressor tactics as well as the needs of the threatened values. The author notes that research on targets within each sector itself requires a separate in-depth study to better link them to the countermeasures formulation. Another research challenge is to transfer the framework for analysis to other countries outside Russia. Although active measures are unwaveringly associated with Russia, there is no reason why the research-derived model could not be applied to other states using malign influence in cyberspace to achieve political goals.

References:

BITTMAN, Ladislav. 1972. The Deception Game: Czechoslovak intelligence in Soviet political warfare. Syracuse: Syracuse University Research Corp.

BITTMAN, Ladislav. 1985. The KGB and Soviet disinformation: an insider's view. Washington: Pergamon-Brassey's.

BITTMAN, Ladislav. 2000. Mezinárodní dezinformace. Praha: Mladá fronta.

BRATTBERG, Erik, Tim Maurer. 2018. "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks." Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

BÍZIK, Vladimír, Dominika Kosárová, Adam Potočňák, Richard Stojar. 2022. "Hybrid Interference: from the Particular to a Continuum: Empirical Test of the Multi-Dimensional Concept of "Hybrid"." Obrana a strategie 22 (1): 75-88. Available at: 10.3849/1802-7199.22.2022.01.75-88.https://doi.org/10.3849/1802-7199.22.2022.01.075-088

BUZAN, Barry, Ole Waever, Jaap de Wilde. 1998. Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers.https://doi.org/10.1515/9781685853808

BUZAN, Barry, Ole Waever, Jaap de Wilde. 2005. Bezpečnost - Nový rámec pro

analýzu. Praha: Centrum strategických studií.
CENTRAL INTELLIGENCE AGENCY. 1986. Speech on Soviet Active Measures. Office of Soviet Analysis. Washington, D.C.
CENTRE FOR THE STUDY OF DEMOCRACY. 2023. Countering Green Deal Disinformation Narratives in Bulgaria. Available at: https://csd.bg/publications/publication/countering-green-deal-disinformation-narratives-in-bulgaria/
CSIS. 2022. "Significant Cyber Incidents | Center for Strategic and International Studies." Www.csis.org. 2022. Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
ČESKOSLOVENŠTÍ VOJÁCI V ZÁLOZE ZA MÍR | Facebook. n.d. Www.facebook.com. Accessed March 2, 2023. Available at: https://www.facebook.com/groups/867025166711756.
CHESSEN, Matt. 2017. The MADCOM Future. Atlantic Council.
https://doi.org/10.1201/9781351251389-10
COMPUTATIONAL PROPAGANDA - Oxford Internet Institute. 2016. Ox.ac.uk. 2016. Available at: https://www.oii.ox.ac.uk/research/projects/computational-propaganda/.
CROWDSTRIKE. 2017. "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units." CrowdStrike Global Intelligence Team, March 23, 2017. Available at: https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf.
DAMARAD, Volha, Andrei Yeliseyeu. 2018. Disinformation resilience in Central and Eastern Europe. Desinformation Resilience Index. Kyiv.
DARCZEWSKA, Jolanta. 2018. "Active measures as the Russian hybrid aggression in a retrospect. Chosen aspects". Przegląd Bezpieczeństwa Wewnętrznego, 18 (10): 244-265.
DARCZEWSKA, Jolanta, Piotr Žochovski. 2017. Active Measures: Russia's Key Export. Warsaw: Center for Eastern Studies.
DEAKIN, Robert Luke. 2003. "Economic information warfare: analysis of the relationship between the protection of financial information infrastructure and Australia's national security." Diploma thesis, Queensland University of Technology.
DENNIK N. 2023. "Prezidentka nevymenuje Rudolfa Huliaka za ministra životného prostredia." Dennik N, October, 19, 2023. Available at: https://dennikn.sk/minuta/3634350

DISMAN, Miroslav. 2002. Jak se vyrábí sociologická znalost. Praha: Karolinum.
DIVIŠOVÁ, Vendula, Libor Frank, Jan Hanzelka, Antonín Novotný, Jan Břeň. 2021. "The Whole is Greater than the Sum of the Parts". Towards Developing a Multidimensional Concept of Armed Forces' Resilience Towards Hybrid Interference. Obrana a strategie, 21(2): 3-20. Available at: 10.3849/1802-7199.21.2021.02.003-020. https://doi.org/10.3849/1802-7199.21.2021.02
DRULÁK, Petr. 2008. Jak zkoumat politiku: kvalitativní metodologie v politologii a mezinárodních vztazích. Praha: Portál.
ENISA. 2021. "ENISA threat landscape for supply chain attacks". Available at: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
EUVSDISINFO. 2021. "Hungary: A Case Study on Targeted Pro-Kremlin Disinformation". EUvsDiSiNFO, June 7, 2021. Available at: https://euvsdisinfo.eu/exploiting-the-trauma-of-trianon/#
EUVSDISINFO. 2019. "Disinfo: German tank desecrated Jewish cemetery in Kaunas." Available at: https://euvsdisinfo.eu/report/german-tank-desecrated-jewish-cemetery-in-kaunas
FORRÓ, Tomáš. 2019. "Šesťdesiatnička z Prahy velí dobrovoľníkom, posiela ich bojovať za Putina na Donbas". DenníkN.sk, June 28, 2019. Available at: https://dennikn.sk/1510498/sestdesiatnicka-z-prahy-veli-dobrovolnikom-posiela-ich-bojovat-za-putina-na-donbas/?fbclid=IwAR3tdihZbe8_x7wihrMegHtKxNu6KbVIEzFP135G2NPJcEzl-FZtCmPF-rY.
FOSTER, Lee, Sam Riddell, David Mainor, Gabby Roncone. 2020. "Ghostwriter' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned withRussian Security Interests. Report". FireEye, July 29, 2020. Available at: https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html
GALEOTTI, Mark. 2016. "Heavy Metal Diplomacy: Russia's Political Use of its Military In Europe Since 2014". European Council on Foreign Relations. Available at: http://www.ecfr.eu/page/-/Heavy_Metal_Diplomacy_Final_2.pdf.
GALEOTTI, Mark. 2017. "Controlling Chaos: How Russia manages its political war in Europe". European Council on Foreign Relations, September 1, 2017. Available at: https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/.
GALEOTTI, Mark. 2018. "I'm Sorry for Creating the 'Gerasimov Doctrine'". Foreing Policy, March 5, 2018. Available at: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

GALEOTTI, Mark. 2019. "Active Measures: Russia's Covert Geopolitical Operations". George C. Marshall European Center For Security Studies, no. 31. Available at: https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0.

GÄRTNER. Lars. 2020. "Maskirovka 2.0 - Nydaning & kontinutet i rysk krigforing." Diploma thesis, Swedish Defence University.

GILES, Kier. 2016. The Next Phase of the Russian Information Warfare. Riga: NATO Strategic Communication Centre of Excellence.

GORWA, Robert, Douglas Guilbeault. 2018. "Unpacking the Social Media Bot: A Typology to Guide Research and Policy". Policy & Internet, 12(2): 225-248.
https://doi.org/10.1002/poi3.184

GREENBERG, Andy. 2017. "Everything We Know About Russia's Election-Hacking Playbook: A brief history of Russia's digital meddling in foreign elections shows disturbing progress". Wired, September 6, 2017. Available at: https://www.wired.com/story/russia-election-hacking-playbook/

GREENBERG, Andy. 2020. "Sandworm details the group behind the worst cyberattacks in history". TheVerge, July 28, 2020. Available at: https://www.theverge.com/21344961/andy-greenberg-interview-book-sandworm-cyber-war-wired-vergecast.

GREGOR, Miloš, Petra Mlejnková eds. 2021. Challenging Online Propaganda and Disinformation in the 21st Century. Cham: Palgrave Macmillan.https://doi.org/10.1007/978-3-030-58624-9

HELMUS, Todd C., Krystyna Marcinek, Julia Nething, Danielle Schlang, Ryan Andrew Brown. 2021. "Tweeting Out Surveys to Pro-Ukraine Influencers: Exploring the Potential for Enlisting Support in the Information Fight Against Russia". RAND. https://www.rand.org/pubs/research_reports/RR4429.html.

HOLZER, Jan, Petra Kuchyňková. 2005. Jelzinovo Rusko. Případová studie nejistého režimu. Brno: Mezinárodní politologický ústav Masarykovy univerzity v Brně.

HOWARD, Philip N., Ganesh Bharath, Dimitra Liotsiou. 2018. The IRA, Social Media and Political Polarization in the United States, 2012-2018. Computational Propaganda Research Project. University of Oxford. Available at: https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf.

HUGHES, John. 1985. Active Measures. Christian Science Monitor.

JEŽEK, Jakub. 2021. "Českoslovenští vojáci v záloze za mír jsou jen mašíblovský výhonek slepence ruského vlivu". A2larm.cz, May 4, 2021. Available at:

https://a2larm.cz/2021/05/ceskoslovensti-vojaci-v-zaloze-za-mir-jsou-jen-masiblovsky-vyhonek-slepence-ruskeho-vlivu/

JIRÁSEK, Petr, Luděk Novák, Josef Požár. 2015. Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie ČR v Praze. Česká pobočka AFCEA.

JUURVEE Ivo, Vladimir Sazonov, Kati Parppei, Edgars Engizers, Ieva Pałasz, Małgorzata Zawadzka. 2020. Falsification of History as a Tool Of Influence. Riga: NATO Strategic Communications Centre of Excellence. Available at: https://stratcomcoe.org/cuploads/pfiles/abuse_of_history_report_27-01-2020_reduced_file_size.pdf

KANDRÍK, Matej. 2020. "The Challenge of Paramilitarism in Central and Eastern Europe". German Marshall Fund of the United States. Policy paper no. 15. Available at: https://www.jstor.org/stable/pdf/resrep26757.pdf

KERNER, Michael Sean. 2022. "Colonial Pipeline hack explained: Everything you need to know". Techtarget, April 16, 2022. Available at: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

KRAGHM, Martin, Sebastian Åsberg. 2017. "Russia's strategy for influence through public diplomacy and active measures: the Swedish case. Journal of Strategic Studies, 40(6): 773-816. Available at: 10.1080/01402390.2016.1273830

https://doi.org/10.1080/01402390.2016.1273830

KRAUS, Rachel. 2022. "In the Russia-Ukraine information war, encrypted messaging apps provide opportunity and risk". Mashable, March 2, 2022. Available at: https://mashable.com/article/whatsapp-telegram-russia-ukraine-disinformation

KUDORS Andis, Robert Orttung. 2010. "Russian Public Relations Activities and Soft Power". Russian Analytical Digest, 81(2010). Available at: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/26212/eth-2215-01.pdf.

KUZIO, Taras. 2021. "Disinformation: Soviet Origins of Contemporary Russian Ukrainophobia." In: Russian Active Measures - Yesterday, Today, Tomorrow edited by Olga Bertelsen. ibidem Press.

KUX, Dennis. 1985. "Soviet and Disinformation: Overview and Assessment". The US Army War College Quarterly, 15(1). Available at: https://press.armywarcollege.edu/parameters/vol15/iss1/17/. https://doi.org/10.55540/0031-1723.1388

LAURELLE, Martin C. 1995. What is Information Warfare? Center for Advanced

Concepts and Technology Institute for National Strategic Studies. National Defence University, Washington D.C.

LINVILL, L. Darren, Patrick L. Warren. 2020. Engaging with Others: How the IRA Coordinated Information Operation Made Friends, The Harvard Kennedy School (HKS) Misinformation Review, 1(2). Available at: 10.37016/mr-2020-011.https://doi.org/10.37016/mr-2020-011

MAKONKALNS, Janis. 2020. "The Kremlin's "Historical War" against Latvia". Promote Ukraine, August 18, 2020. Available at: https://www.promoteukraine.org/the-kremlins-historical-war-against-latvia/

MARINO, Andrew. 2020. "Sandworm details the group behind the worst cyberattacks in history: An interview with author Andy Greenberg". The Verge, July 28, 2020. Available at: https://www.theverge.com/21344961/andy-greenberg-interview-book-sandworm-cyber-war-wired-vergecast.

MAREŠ, Miroslav, Petra Mlejnková. 2021. "Propaganda and Disinformation as a Security Threat." In Challenging Propaganda and Disinformation in 21st Century, edited by Miloš Gregor and Petra Mlejnková, 75-103. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-58624-9_3

MARINE, Robert Luke. 2003. "Economic information warfare: analysis of the relationship between the protection of financial information infrastructure and Australia's national security." Diploma thesis, Queensland University of Technology.

MITROKHIN, Vasili, Andrew Christopher. 2018a. Mitrokhin Archive: The KGB in Europe and the West. London: Penguin Books Ltd.

MITROKHIN, Vasili, Andrew Christopher. 2018b. Mitrokhin Archive II. London: Penguin Books Ltd.

MOCHTAK, Michal, Jan Holzer. 2017. Electoral violence in Putin's Russia: Modern authoritarianism in practice. Studies of Transition States and Societies, 9(1): 35-52. https://doi.org/10.4324/9781315225319-2

MOLINA, M.D., S.S. Sundar, Le T. D. Lee. 2021 "Fake News" Is Not Simply False Information: A Concept Explication and Taxonomy of Online Content." American Behavioral Scientist, 65(2): 180-212. Available at: 10.1177/0002764219878224. https://doi.org/10.1177/0002764219878224

MOLINA, Jesus. 2022. "Real time flames: Welcome to the Age of Cyber-sabotage. Waterfall, July 28, 2022. Available at: https://waterfall-security.com/welcome-to-the-age-of-cyber-sabotage/

NATO. 2021. "Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange

Server compromise". July 16, 2021. Available at: https://www.nato.int/cps/en/natohq/news_185863.htm

NATO Stratcom Center of Excellence. 2022. Publications 2017-2021. Available at: https://stratcomcoe.org/publications?tid[]=8

NATIONAL CYBER SECURITY CENTER. 2018. "Reckless campaign of cyber attacks by Russian military intelligence service exposed". National Cyber Security Centre, October 3, 2018. Available at: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

NATIONAL CYBER SECURITY CENTER. 2020. "Advisory: APT29 targets COVID-19 vaccine development". National Cyber Security Center, July 16, 2020. Available at: https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development

NAYLOR, Aliide. 2020. "How Russian Disinformation Targets the Former Soviet Bloc Around WWII Anniversaries". The Centre for Historical Analysis and Conflict Research, July 6, 2020. Available at: https://chacr.org.uk/2020/07/06/6-july-2020-how-russian-disinformation-targets-the-former-soviet-bloc-around-wwii-anniversaries/

NIEKERK, B. van, T. Ramluckan. 2019. Economic Information Warfare. Journal of Information Warfare, 18(2):31-48. Peregrine Technical Solutions.

NIKITCHENKO, V. F. et al., eds. Kontrrazvedyvatelnyjj slovar KGB. 1972. Moskva, SSSR.

NIMMO, Ben. 2019. Measuring Traffic Manipulation on Twitter. Computational Propaganda Research Project: University of Oxford. Available at: https://comprop.oii.ox.ac.uk/research/working-papers/twitter-traffic-manipulation/

NL Times. 2021. "Russia hacked Dutch police systems in 2017: Report". NL Times, June 8, 2021. Available at: https://nltimes.nl/2021/06/08/russia-hacked-dutch-police-systems-2017-report

PAČKA, Roman. 2017. "Role národních Computer Emergency Response Teams (CERT) v zajišťování kybernetické bezpečnosti státem." Rigorous thesis, Brno: Masaryk University.

PALOMO, Miguel. 2021. How disinformation kills: philosophical challenges in the post- Covid society. History and Philosophy of the Life Sciences, 43(2): 51. Available at: 10.1007/s40656-021-00408-4

https://doi.org/10.1007/s40656-021-00408-4

PAMMENT James, Vladimir Sazonov, Francesca Granelli, Sean Aday, Una

Bērziņa- Čerenkova, John-Paul Gravelines, Mils Hills et al. 2019. Hybrid Threats: Disinformation in Sweden. NATO Stratcom Centre of Excellence, Riga, Latvia.

PAVLÍKOVÁ, Miroslava. 2016. "Kybernetický boj mezi Ruskem a Ukrajinou v rámci ukrajinského konfliktu". Obrana a strategie, 16(1): 79-98. Available at: 10.3849/1802-7199.16.2016.1.077-094.

https://doi.org/10.3849/1802-7199.16.2016.1.077-094

PAVLÍKOVÁ, Miroslava, Jan Hanzelka. 2019 "Nástroje ruských aktivních opatření ve vybraných zemích EU". Politické vedy. 22(1): 108-131. Banská Bystrica: Fakulta politických vied a medzinárodných vzťahov UMB Banská Bystrica.

PAVLÍKOVÁ, Miroslava, Burešová Barbora, Jakub Drmola. 2021. "Propaganda and Disinformation Go Online". In Challenging Propaganda and Disinformation in 21st Century, edited by Miloš Gregor and Petra Mlejnková, 43-74. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-58624-9_2

PYNNÖNIEMI, Katri. 2019. "The Asymmetric Approach in Russian Security Strategy: Implications for the Nordic Countries". Terrorism and Political Violence, 31(1): 154- 167. Available at: 10.1080/09546553.2018.1555995.

https://doi.org/10.1080/09546553.2018.1555995

RADIN, Andrew, Alyssa Demus, Krystyna Marcinek. 2020. Understanding Russian Subversion Patterns, Threats, and Responses. RAND Corporation.

https://doi.org/10.7249/PE331

RID, Thomas. 2020. Active Measures: The Secret History of Disinformation and Political Warfare. London: Farrar, Straus and Giroux.

RINGSTROM, Anna, Tom Balmforth. 2021. "Swedish prosecutor says Russia's GRU hacked Sweden's sports body." Reuters, April 13, 2021. Available at: https://www.reuters.com/article/us-sweden-russia-hacking-idUSKBN2C01V5

REICHBORN-KJENNERUD, Erik, Patrik Cullen. 2017. Understanding hybrid warfare. MCDC Countering hybrid warfare project. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/717539/MCDC_CHW_Information_Note-Understanding_Hybrid_Warfare-Jan_2018.pdf

ROBERT S. MULLER Indictment against IRA. 2018. Available at: https://www.justice.gov/opa/press-release/file/1035562/download

ROTHWELL, James, James Titcomb, Cara McGoogan. 2017. "Petya cyber attack: Ransomware spreads across Europe with firms in Ukraine, Britain and Spain shut down". The Telegraph, June 27, 2017. Available at: https://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-

attack1/
ROUSSI, Antaneta. 2022. "Meet Killnet, Russia's hacking patriots plaguing Europe". Politico, September 9, 2022. Available at: https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/
SCHOEN, Fletcher, Christopher J. Lamb 2012. Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference. Center for Strategic Research. Institute for National Strategic Studies. National Defense University. https://doi.org/10.21236/ADA577586
SAKWA, Richard. 1989. Soviet politics in perspective. London: Routledge. https://doi.org/10.4324/9780203312438
SANGER, David E. 2021. "Russia's most aggressive ransomware group disappeared. It's unclear who made that happen." The New York Times, July 14, 2021. Available at: https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html
SHULTZ, Richard H., Roy Godson. 1984. Dezinformatsia: Active Measures in Soviet Strategy. Virginia: Pergamon-Brasseys International Defense Publishers.
SINGER, P. W., Allan Friedman. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001
SLÁVIK, Martin. 2009. "Spolupráce rozvědky StB a KGB v oblasti aktivních opatření". In: Aktivity NKVD/KGB a její spolupráce s tajnými službami střední a východní Evropy 1945-1989. II Sborník s medzinárodné konference. ÚSTR, Praha.
SPRUDS, Andris, Anda Rožukalne, Klavs Sedlenieks, Marns Daugulis, Diana Potjomkina, Beatrix Tölgyesi, Ilvija Bruge. 2016. Internet Trolling as Tool of Hybrid Warfare: the Case of Latvia. Riga: NATO Stratcom Centre of Excellence.
STRONSKI, Paul. 2020. "Implausible Deniability: Russia's Private Military Companies". Carnegie Endowment for Peace, June 2, 2020. Available at: https://carnegieendowment.org/2020/06/02/implausible-deniability-russia-s-private-military-%20companies-pub-81954
STONE, Jeff. 2015. "Meet CyberBerkut, The Pro-Russian Hackers Waging Anonymous - Style Cyberwarfare Against Ukraine". International Business Times, December 17, 2015. Available at: https://www.ibtimes.com/meet-cyberberkut-pro-russian-hackers-waging-anonymous-style-cyberwarfare-against-2228902

STYRNA, Paweł Piotr. 2011. The Post-Soviet Zone Twenty Years Later: An Empire Under Reconstruction. SFPPR Issue Brief.

SULC, Lawrence B. 1985. Active Measures, Quiet War; And, Two Socialist Revolutions. Washington, DC: Nathan Hale Institute.

THAROOR, Ishaan. 2022. "The global politics of Russia's notorious nationalist ideologue". The Washington Post, August 23, 2022. Available at: https://www.washingtonpost.com/world/2022/08/23/ideology-alexander-dugin-global-far-right/

TUCKER, Patrick. 2019. "Russian Trolls Are Hammering Away at NATO's Presence in Lithuania". Defence One, December 3, 2019. Available at: https://www.defenseone.com/technology/2019/12/russian-trolls-are-hammering-away-natos-presence-lithuania/161654/

U.S. DEPARTMENT OF JUSTICE. 2019. "Report On The Investigation Into Russian Interference in The 2016 Presidential Election". Available at: https://www.justice.gov/storage/report.pdf

U.S. DEPARTMENT OF STATE. 1981. Forgery, Disinformation, Political Operations. Special Report no. 88.

U.S. DEPARTMENT OF STATE. 2020. GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem. Available at: https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

U.S. INFORMATION AGENCY. 1988. Soviet Active Measures in the Era of Glasnost. A Report to Congress.

U.S. INFORMATION AGENCY. 1992. Soviet Active Measures in the "Post-Cold War" Era 1988-1991. A Report Prepared at the Request of the United States House of Representatives Committee on Appropriations by the United States Information Agency.

VANDIVER, John. 2019. "Lithuania says statement about accepting US nuclear weapons is fake". Stars and Stripes, October 18, 2019. Available at: https://www.stripes.com/news/lithuania-says-statement-about-accepting-us-nuclear-weapons-is-fake-1.603616

WAISOVÁ, Šárka. 2004. Od národní bezpečnosti k mezinárodní bezpečnosti: Kodánská škola na křižovatce strukturálního realismu, anglické školy a sociálního konstruktivismu. Mezinárodní vztahy, 39(3): 66-86.

WALACH, Václav. 2016. Význam bezpečnosti v sociálně vyloučené lokalitě. Dissertation thesis, Brno: Masaryk University.

WARRELL, Helen. 2020. "SolarWinds cyber attack linked to tools used by Russian hacking group". The Financial Times, January 11, 2021. Available at: https://www.ft.com/content/e1b247d5-ef53-4e82-afc3-9e3c2d7c5e2c

WEIDINGER, Bernhard, Fabian Schmid, Péter Kréko, Győry Lóránt, eds. 2017. Russian Connections of the Austrian Far-right. Budapest: Political Capital.

WINTER, C., P. Neumann, A. Meleagrou-Hitchens, M. Ranstorp, L. Vidino, J. Fürst. 2020. Online Extremism: Research trends in internet activism, radicalization, and internet strategies. International Journal of Conflict and Violence, 14(2): 1-20. Available at: 10.4119/ijcv-3809

WOOLEY, Samuel C. 2022. "Digital Propaganda: The Power of Influencers". Journal of Democracy, 33(3): 115-129. Johns Hopkins University Press. https://doi.org/10.1353/jod.2022.0027

ZETTER, Kim. 2015. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown.

ZMUŠKOVÁ, Barbara. 2023. "Slovakia's nominee for envi-chief does not believe in climate change." Euraktiv.sk, October, 18, 2023. Available at: https://www.euractiv.com/section/politics/news/slovakias-nominee-for-envi-chief-does-not-believe-in-climate-change/

ZUIDERVEEN BORGESIUS, Frederik J., Judith Möller, Sanne Kruikemeier, Ronan ÓFathaigh et al. 2018. "Online Political Microtargeting: Promises and Threats for Democracy". Utrecht Law Review, 14(1): 82-96. Available at: 10.18352/ulr.420. https://doi.org/10.18352/ulr.420