INFORMATION WARFARE/OPERATIONS OF THE RUSSIAN FEDERATION IN THE CONTEXT OF *SARS-COV-2*

Major Petre SCÎRLET
"Carol I" National Defense University, Bucharest

Lecturer Cristian ICHIMESCU, PhD
"Carol I" National Defense University, Bucharest

High-impact global events, such as the Covid-19 pandemic, occur very rarely – probably several times over a century – and produce, among other things, major geopolitical changes, targeting alliances, political blocs, regions, states and areas of influence.

The Covid-19 pandemic quickly affected the entire world, and the personal freedom of billions of people was restricted in an unprecedented way. However, the pandemic has not frozen the conflicts between various states of the world.

Although a global response to the SARS-CoV-2 coronavirus crisis is needed, the Russian Federation does not consider it in its best interest to contribute – and, in fact, the Kremlin is using the crisis to further destabilise the world.

Thus, simultaneously with the virus, an enormous amount of data and information is spreading all over the world, many of them being part of a large campaign to influence public opinion through warfare/information operations planned and executed by the Russian authorities.

The global framework created by the expansion of the pandemic represented the operational moment identified by the Kremlin to implement, once again, the complex machinery represented by information warfare/operations, which have thus become the most complex form of modern confrontation.

Keywords: information activities, Covid-19, disinformation, infodemia, cyber operations

WHAT IS/ARE CONTEMPORARY INFORMATION WARFARE/OPERATIONS?

The Romanian Doctrine from 2017, SMG-66, named the *Doctrine for Information Operations*, defines the notion of information operations as representing "*a staff function intended for the analysis, planning, evaluation and integration of all information activities in order to obtain the desired effects on the will, understanding, perception and capabilities of adversaries, potential adversaries and target audiences, approved by the CSAT* [Supreme Council of National Defence – editor's note]*, in support of the achievement of military objectives*"[1].

In 2009, NATO, within the doctrine AJP-3.10, *Allied Joint Doctrine for Information Operations*, defined *information operations* as being "*a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives"*[2].

NATO, within the doctrine AJP-3.10, Allied Joint Doctrine for Information Operations, defined information operations as being "a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives".

Analysing the definitions presented above, we can notice a series of similarities. According to the two doctrines, information operations are identified by the *effects* produced on three distinct categories: will; understanding and perception; capabilities. In addition to studying the doctrines mentioned above[3], information operations are put into practice by performing certain types of activities, namely influencing activities, activities against control and command capabilities, and activities of information protection.

According to some authors, for the Russian Federation, the concept of information warfare implies "*computer network operations alongside disciplines such as psychological operations, strategic*

[1] S.M.G.-66, *Doctrina operațiilor informaționale,* București, 2017, p. 15.
[2] AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009, pp. 1-3.
[3] AJP-3.10, *op. cit.*, p. 1-7, and S.M.G.-66, *op. cit.*, p. 21.

communications, influence"[4] and "*intelligence, counterintelligence, maskirovka, disinformation, electronic warfare*"[5].

We can thus notice the difference between the two meanings (NATO/Romania vs. the Russian Federation) in the sense of the complexity of the concept approached by the Kremlin, which is an extended concept and covers a wide and diverse range of activities. Thus, we notice that, for the Russian Federation, all areas form a unit under the concept of *information warfare* while NATO approaches the concept of *information operations*. Throughout this article, we will use the concept of information warfare/operations to characterise the information actions of the Russian Federation.

Throughout the Cold War, the Soviet strategy resorted to a series of so-called "active measures", which describe actions and strategies designed to influence the decisions of a state, its population and important political, military and social events in that state.

A characteristic of the information warfare/operations carried out by the Russian Federation is the offensive character, which has been found in all the information campaigns carried out by this state over time against various state actors. We will further present a short history of information warfare/operations implemented by the Russian Federation through the use of important areas, such as disinformation and active measures.

RUSSIAN HISTORY OF INFORMATION WARFARE/OPERATIONS

The basic ideas on which some of the forms of information warfare/operations carried out by the Russian Federation is/are based are not new, their origins dating as early as the Cold War. Throughout the Cold War, the Soviet strategy resorted to a series of so-called "*active measures*", which describe actions and strategies designed to influence the decisions of a state, its population and important political, military and social events in that state.

Allegations that the United States carried out biological weapons attacks were common accusations by opponents such as the USSR or Cuba, which sought to accredit to the international community the idea that the United States had violated the Biological Weapons Convention.

---

[4] Keir Giles, *Handbook of Russian Information Warfare*, NATO Defence College, 2016, p. 7.

[5] Khatuna Mshvidobadze, *The Battlefield On Your Laptop*, Radio Free Europe/Radio Liberty, 21 March 2011, http://www.rferl.org/articleprintview/2345202.html apud Keir Giles, *op. cit.*, p. 7.

While many allegations of biological weapons originated in the Kremlin, those were often amplified by media sources in the USSR's allied states. The Cuban media consistently claimed that the United States spread a variety of diseases in the period 1970-1980. At the same time, Russian authorities accused the United States of involvement in the development of particularly dangerous mosquito species in Pakistan, to be used for the rapid spread of biological weapons[6].

The accusations against the United States regarding the use of biological weapons were a practice often used by opponents during the Cold War, but the two most insidious campaigns were those related to the Korean War[7] and the AIDS disinformation campaign[8].

It can be seen that, during the Cold War, taking the NATO definition of information operations as a theoretical basis, the USSR mainly used *information activities to create the desired effects on the understanding and capabilities of different audiences*. We also observe the planning and execution, in particular, of influencing activities and information protection activities.

During the Cold War, taking the NATO definition of information operations as a theoretical basis, the USSR mainly used information activities to create the desired effects on the understanding and capabilities of different audiences.

Accusations of biological weapons surrounding the current SARS-CoV-2 pandemic continue the specific line of information warfare/operations conducted by the Soviet Union during the Cold War, but the confrontational capabilities and objectives pursued are much more complex.

The Russian Federation is currently leading perhaps one of the largest and most complex information warfare in recent years, integrating sequences of media operations, manipulation, disinformation, propaganda – white, black and gray, social media operations, cyber operations and involving the whole arsenal of tools specific to the information warfare, among which we would mention

---

[6] Jeffrey A. Lockwood, *Insects as Weapons of War, Terror, and Torture*, Annual Review of Entomology, Vol. 57:205-227 (Volume publication date January 2012), https://www.annualreviews.org/doi/full/10.1146/annurev-ento-120710-100618 retrieved on 11 April 2020.

[7] For further information, Sarah Jacobs Gamberini, Amanda Moodie, *The Virus of Disinformation: Echoes Of Past Bioweapons Accusations in Today's Covid-19 Conspiracy Theories*, 6 April 2020, https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/

[8] For further information, Douglas Selvage, Christopher Nehring, *Operation "Denver": KGB and Stasi Disinformation regarding AIDS*, 22 July 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids and Filippa Lentzos, *The Russian Disinformation Attack that Poses a Biological Danger*, 19 November 2018, https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/

the accusation of the opponent for committing atrocities, propaganda or discrediting the opponent's propaganda, exaggerated amplification of certain stakes, invoking protection etc.

All the confrontation capabilities listed above are used, but the dimension of disinformation along with the cybernetic one stands out from the other forms.

THE CORONAVIRUS OF DISINFORMATION – THE NEW RUSSIAN INFORMATION WARFARE –

During this period, a large number of people are locked in their houses and spend a lot of time on social media. According to the data, at the end of March, there were more than 3 billion posts and over 100 billion interactions on *#covid19*, *#coronavirus* and the like[9].

As early as 2 February this year, the World Health Organization (WHO) warned that the world was facing two epidemics[10] in parallel: one caused by the new coronavirus SARS CoV-2 and a second referring to a so-called "*infodemia*", describing this phenomenon as an overabundance of more or less accurate news.

The narrative proposed by the vectors of the Russian Federation mainly aims at altering the public space of the targeted audiences by injecting disinformation and propaganda. At the same time, another pillar is that of the lobby, which aims to influence the target audience through ideas conveyed in the public space by legitimate and credible message bearers.

Last but not least, elaborate psychological operations are used where the information disseminated but especially its effect on the target audience, namely the birth and creation or accentuation of fears, collective emotions, the preparation of the public to react to future events in a directed formula.

The narratives of the Russian Federation

Russian narratives can be divided into three categories: a so-called basic disinformation; complex disinformation and elaborate propaganda.

---

[9] Faruk Zorlu, *Covid-19: Infodemic Spreads Faster than Pandemic*, 31.03.2020, https://www.aa.com.tr/en/latest-on-coronavirus-outbreak/covid-19-infodemic-spreads-faster-than-pandemic/1786381 retrieved on 13 April 2020.

[10] The WHO raised the level of the Covid-19 epidemic to the level of a pandemic on 11.03.2020.

Basic disinformation consists of the least sophisticated types of disinformation. These approaches target the least informed public of the Russian masses and beyond, among whom the anti-American sentiment is historically strong and easily inflamed. The tools used include disinformation platforms, bloggers, as well as accounts used by Russians living in the US, Canada and the EU. For this target audience, Russian propagandists deliberately use unsophisticated language and primitive but convincing, simple arguments[11].

Complex disinformation promulgates similar ideas, but dressed differently. This approach is based on elaborate conspiracy theories that aim to create the so-called alternative reality and try to promote mistrust among the foreign public. Russian news platforms use pseudo-scientific "*evidence*" that the virus was created in an American laboratory to stop China's economic growth[12].

Complex disinformation promulgates similar ideas, but dressed differently. This approach is based on elaborate conspiracy theories that aim to create the so-called alternative reality and try to promote mistrust among the foreign public.

The third category presents an example of *elaborate propaganda*, designed for very narrow circles outside the Russian Federation. In this case, the Russian state relies on its own prominent scientists and sometimes uses foreign sources (mainly Chinese). According to their theories, "*Coronavirus ...has become the end of the modern world"*[13]. It is claimed that the world order established after the Cold War is now collapsing and giving way to a new period in which new leaders will emerge.

"*Disinformation plays with people's lives. Disinformation can kill*" said Josep Borrell, director of the European External Action Service, at a news conference in the second decade of March. This dangerous game started at the beginning of this year and has developed gradually.

The first disinformation on Covid-19 appeared in *Sputnik News* on 22 January[14], when an article was published stating that the virus was man-made, being a weapon created by NATO[15].

---

[11] *NATO Uses COVID-19 to Mobilise Western Military Forces against Russia*, 19.03.2020, interview with Alexander Artamonov for Novorossia News Agency, https://novorosinform.org/808651 retrieved on 13 April 2020.

[12] Vicky Peláez, *Scientists: Coronavirus Would Be a Weapon of Biological Warfare*, 13.02.2020, https://mundo.sputniknews.com/firmas/202002131090460452-cientificos-el-coronavirus-seria-un-arma-de-guerra-biologica/ retrieved on 14 April 2020.

[13] Alexander Dugin, *Pandemic and the Politics of Survival: the Horizons of a New Type of Dictatorship*, 05.04.2020, https://www.geopolitica.ru/en/article/pandemic-and-politics-survival-horizons-new-type-dictatorship retrieved on 14 April 2020.

[14] *Disinformation Can Kill,* 26.03.2020, https://euvsdisinfo.eu/disinformation-can-kill/ retrieved on 14 April 2020.

[15] *A New Chinese Coronavirus Was Likely Elaborated in NATO Biolabs*, https://euvsdisinfo.eu/report/a-new-chinese-coronavirus-was-likely-elaborated-in-nato-biolabs/, retrieved on 14 April 2020.

According to a study conducted by EUvsDisinf[16], analysing articles published in foreign media between 22 January and 25 March on the topic of Covid-19, the favourite target remains the USA, with 39 articles, articles in which it is claimed that the USA created the SARS-CoV-2 virus. The second most common narrative, with 26 published articles, is that the EU is failing to cope with the crisis and is disintegrating as a result, along with the Schengen area. In particular, this narrative of the EU's failure and lack of solidarity is on trend following the delivery of Russian aid to Italy. The narrative that the virus is used as a weapon against China and its economy comes third with 24 articles. The narrative that the entire coronavirus crisis is a secret plan of the global elite lies fourth, with 17 articles[17].

In the military, the disinformation targeted the multinational exercise Defender Europe 2020. The Russian leadership criticised the exercise as an offensive "anti-Russian scenario", but then used propaganda to spread the theory that executing the exercise could facilitate the spread of the SARS-CoV-2 virus in Europe due to the arrival and movement of a large number of troops.

In the military, the disinformation targeted the multinational exercise *Defender Europe 2020*. The Russian leadership criticised the exercise as an offensive[18] "*anti-Russian scenario*", but then used propaganda to spread the theory that executing the exercise could facilitate the spread of the SARS-CoV-2 virus in Europe due to the arrival and movement of a large number of troops.

Channels used

To achieve its goals, Moscow has a number of message propagation vectors that can be divided as follows:

1. Traditional media (*Russia Today* trust, which also owns Russia Today television station and *Sputnik* project*, Pervy Kanal*);
2. The virtual environment (the Kremlin's troll army) – structures specialising in activities on blogging platforms, news production, creating images and denigrating content to undermine a certain target, producing video content and writing pro-Kremlin comments posted in virtual environments. According to a report prepared for the Global Engagement

[16] *EUvsDisinfo* within the East StratCom Task Force is the project of the European External Action Service. It was set up in 2015 to respond to the Russian Federation's disinformation campaigns affecting the European Union. For more information https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en

[17] *Ibid.*

[18] *The US Defender 2020 Military Manoeuvre Is Explicitly Directed against Russia,* https://euvsdisinfo.eu/report/the-us-defender-2020-military-manoeuvre-is-explicitly-directed-against-russia after Alexander Rahr, *Defender 2020 ist ein Fehler, man muss auf Russland zugehen*, https://www.youtube.com/watch?v=5WCCwneR-DU&feature=emb_title retrieved on 14 April 2020.

Center[19] within the US State Department, the use of accounts controlled by the Russian state was noticed, initially used to influence the specific events of the conflict in Syria and the extensive strikes in France, to post messages related to the coronavirus pandemic.

According to the Department of State, when the Russian media began broadcasting anti-Western articles and interviews about the origins of the SARS-CoV-2 virus, Russian accounts started to promote them worldwide, covering more than 20 languages – from English to Russian and from Serbian to Arabic.

3. Involvement of influential figures from the Russian Federation, opinion formers enslaved to the Kremlin. Obviously, this picture could not miss one of the most influential geopolitical thinkers of the Russian Federation, Alexander Dughin, a Russian nationalist and a very public supporter of the Orthodox Church, who claimed that when the virus ends its march of victory across the planet, the existing world order will be destroyed. It is well known that its messages are part of the Russian agenda, intensely promoted in recent years, being one of the main tools through which Russian propaganda builds, promotes and develops the constituent elements of a brand image of the Russian Federation.
4. NGOs, think tanks and other discussion platforms whose purpose is to disseminate Russian propaganda.
5. And last but not least, we mentioned the involvement of Russian intelligence services in promoting messages in support of Russian foreign policy at EU level. They use freelance journalists, journalists, NGOs and research institutes.

According to a report prepared for the Global Engagement Center within the US State Department, the use of accounts controlled by the Russian state was noticed, initially used to influence the specific events of the conflict in Syria and the extensive strikes in France, to post messages related to the coronavirus pandemic.

If over the US the information warfare of the Russian Federation are aimed at destabilising and discrediting the US at the European level, taking advantage of the United States' inability to help its allies, the agenda for the European Union is more complex, aiming to undermine cohesion by cultivating a concentration of information activities on some EU member states.

[19] Lea Gabrielle, *Briefing on Disinformation and Propaganda Related to COVID-19*, https://www.state.gov/briefing-with-special-envoy-lea-gabrielle-global-engagement-center-on-disinformation-and-propaganda-related-to-covid-19 retrieved on 14 April 2020.

In this context, Moscow emulated China's movements to send aid to Italy and Spain and acted to claim all publicity and benefits.

From Russia, with love...

Moscow's aid to Italy in connection with the coronavirus has been widely covered in both the international[20] and Russian press. Italy gratefully welcomed the arrival of a Chinese plane – in the presence of the Italian president and the Chinese ambassador – carrying doctors and equipment.

The Russian state media presented the situation in Italy in the context of the country's struggle to limit the spread of coronavirus in different ways.

On Radio Vesti FM, controlled by the Kremlin, the public was told that the coronavirus epidemic would force Italy to leave the EU. Earlier, the Kremlin-controlled Sputnik promoted the conspiracy theory that the coronavirus could have been created to limit the economic burden of retired citizens on Italy's budget.

On *Radio Vesti FM*, controlled by the Kremlin, the public was told that the coronavirus epidemic would force Italy to leave the EU[21].

Earlier, the Kremlin-controlled *Sputnik* promoted the conspiracy theory that the coronavirus could have been created to limit the economic burden of retired citizens on Italy's budget[22].

Sputnik also accused members of the European Parliament of wanting to launch a campaign against Russian aid to Italy, when in reality they asked to analyse disinformation campaigns and the geopolitical use of aid.

At the same time, a video was intensely promoted in the Russian media in which an Italian citizen replaced the flag of the European Union with that of Russia, falsely conveying the idea that this current is a widespread one. A BBC television reporter contacted the Italian citizen to request a point of view stating that he had decided to raise several Russian Federation flags outside the store he owns to express his gratitude to Russia.

Another video that was distributed in the pro-Kremlin press shows the anthem of the Russian Federation being sung in Italy. Among the Russian publications that broadcast the video were the state-controlled network *Rossiya 1* and the pro-Kremlin television channel *REN TV*,

[20] According to an analysis by the Italian daily La Stampa, about 80% of the supplies sent by Russia are "*useless*" according to Jacopo Iacoboni, La Stampa, 25.03.2020, *Coronavirus, la telefonata Conte-Putin agita il governo: "Più che aiuti arrivano militari russi in Italia",* https://www.lastampa.it/topnews/primo-piano/2020/03/25/news/coronavirus-la-telefonata-conte-putin-agita-il-governo-piu-che-aiuti-arrivano-militari-russi-in-italia-1.38633327 retrieved on 15 April 2020.

[21] *Coronavirus: BBC Challenges Pro-Kremlin Reporting from Italy,* 01.04.2020, https://euvsdisinfo.eu/coronavirus-bbc-challenges-pro-kremlin-reporting-from-italy/ retrieved on 15 April 2020.

[22] *Ibid*.

whose story was presented online under the headline: "*Russia's anthem sounded in the streets of Italy*"[23].

The Russian media did not explain that the music in the video appears from inside the office of an organisation that the BBC article describes as "*neo-fascist*" and that the person behind the video is an activist with ties to Russia.

In its article, the BBC showed that two different videos with the Russian anthem, which circulated in the Russian media, are, in fact, recordings of the same event, but from different angles.

At the same time, with the help provided, Italy was also the target of cyber-attacks, as well as the whole of Europe.

Russian cyber operations

Cyber operations are one of the most important areas in the information warfare that the Russian Federation is waging against the background of the SARS-CoV-2 virus pandemic.

European Commission President Ursula von der Leyen warned on 24 March about a significant increase in cybercrime in the EU in the context of the Covid-19 pandemic[24].

Cybercriminals are taking advantage of the growing time people spend online because of the new measures taken by member states to stop the spread of the virus.

Cybercriminals are taking advantage of the growing time people spend online because of the new measures taken by member states to stop the spread of the virus.

The first group of hackers sponsored by the Kremlin to be employed on this front was the Hades group[25], which is rumoured to operate outside the Russian Federation, and with a link to the APT28 group, one of the most famous cyber espionage groups in the Russian Federation. According to Chinese cybersecurity company QiAnXin, Hades hackers launched a campaign in mid-February, when they hid a Trojan virus in documents containing the latest news about Covid-19. The documents were sent to targets in Ukraine, disguised in e-mails from the Public Health Centre of the Ministry of Health of Ukraine[26].

---

[23] *На улицах итальянских городов прозвучал гимн России*, 26.03.2020, https://ren.tv/news/v-mire/677798-na-ulitsakh-italianskikh-gorodov-prozvuchal-gimn-rossii retrieved on 15 April 2020.

[24] *EU Commission Warns of Increased Cybercrime during Coronavirus Crisis*, VOA News, 24.03.2020, https://www.voanews.com/science-health/coronavirus-outbreak/eu-commission-warns-increased-cybercrime-during-coronavirus retrieved on 15 April 2020.

[25] Cătălin Cîmpănu, *State-Sponsored Hackers Are Now Using Coronavirus Lures to Infect their Targets*, 13.03.2020, https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/ retrieved on 16 April 2020.

[26] *Ibid*.

An Europol report[27] in March also confirms what has already been listed, highlighting the fact that cybercrime has increased significantly during this period. Europol has been monitoring the impact of the *Covid-19* pandemic on the cybercrime landscape from the outset and has published an updated threat assessment on potential further developments in this area of crime.

The main findings of this eval u ation are: the impact of the SARS-CoV-2 virus pandemic on cybercrime was most visible compared to other criminal activities; criminals active in the field of cybercrime have been able to adapt quickly and capitalize on the anxieties and fears of their victims; *phishing* a nd *ransomware* campaigns are launched to exploit the current cri sis and are expected to continue to grow in scope and scale; both criminal organisations, states, and state-backed actors seek to exploit the public health crisis to promote geopolitical interests[28].

During the SARS-CoV-2 virus pandemic, taking as a theoretical basis the NATO definition of information operations, the Russian Federation used mainly information activities to create the desired effects on the will, understanding and capabilities of different audiences. We also observe the planning and execution of influencing activities, activities against command and control capabilities, and information protection activities.

It can be seen that during the SARS-CoV-2 virus pandemic, taking as a theoretical basis the NATO definition of information operations, the Russian Federation used mainly *information activities to create the desired effects on the will, understanding and capabilities of different audiences*. We also observe the planning and execution of influencing activities, activities against command and control capabilities, and information protection activities.

CONCLUSIONS

Although the threat posed by the scale of this pandemic is real and not negligible, the Russian Federation sees this catastrophe as an opportunity to promote and develop plans to carry out information warfare/operations against the West amid the Covid-19 pandemic.

The spread of the SARS-CoV-2 virus has provided a new battlefield in which information warfare/operations is/are the most advanced weapon, currently benefiting from a much faster speed of spread, as well as a wide range of action, contributing decisively to rapidly model and influence both the opinions and actions of target audiences.

---

[27] *Catching the Virus Cybercrime, Disinformation and the COVID-19 Pandemic*, 03.04.2020, https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic retrieved on 16 April 2020.

[28] *Ibid.*

A stake for the Russian Federation in this context is the relationship with Italy, which comes at a time when this country is vulnerable. The growing interest of the Russian Federation in the EU and the provision of assistance to Italy are concrete elements for the implementation of information warfare/operations against the EU and member countries.

From the comparative analysis of the implementation of the domains of information warfare/operations during the Cold War with the specific period of the SARS-CoV-2 virus pandemic, we can see the transition from partial use of information activities specific to the Cold War to the use of all information activities, *to create the desired effects on the will, understanding and capabilities of different audiences*. The typology of the messages used is not a new one, but what is different now is the execution of increasingly intrusive information warfare/operations and use thereof not only to destabilize the US, but also the European Union.

We also consider that the actions subject to the information warfare/operations, carried out by the Russian Federation, are likely *to intensify and develop*, seeking to identify new vulnerabilities, given the countermeasures already taken by the European Union authorities and the US.

As the Russian Federation invests heavily in artificial intelligence research programs, security experts are already describing the new concept of fake news, which will be initiated by the technological capacity of artificial intelligence to faithfully reproduce the voice of the individual, as a human being, as a new field of information warfare/operations of the future.

The spread of the SARS-CoV-2 virus has provided a new battlefield in which information warfare/operations is/are the most advanced weapon, currently benefiting from a much faster speed of spread, as well as a wide range of action, contributing decisively to rapidly model and influence both the opinions and actions of target audiences.

BIBLIOGRAPHY

1. ***, AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009.
2. ***, S.M.G.-66, *Doctrina operațiilor informaționale*, București, 2017.
3. Cătălin Cîmpanu, *State-Sponsored Hackers Are Now Using Coronavirus Lures to Infect their Targets*, 13 March 2020, https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/
4. Alexander Dugin, *Pandemic and the Politics of Survival: the Horizons of a New Type of Dictatorship*, 5 April 2020, https://www.geopolitica.ru/en/article/pandemic-and-politics-survival-horizons-new-type-dictatorship

5. Sarah Jacobs Gamberini, Amanda Moodie, *The Virus of Disinformation: Echoes Of Past Bioweapons Accusations in Today's Covid-19 Conspiracy Theories*, 6 April 2020, https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/
6. Keir Giles, *Handbook of Russian Information Warfare*, NATO Defence College, 2016.
7. Jacopo Iacoboni, *La Stampa*, 25 March 2020, *Coronavirus, la telefonata Conte-Putin agita il governo: "Più che aiuti arrivano militari russi in Italia",* https://www.lastampa.it/topnews/primo-piano/2020/03/25/news/coronavirus-la-telefonata-conte-putin-agita-il-governo-piu-che-aiuti-arrivano-militari-russi-in-italia-1.38633327
8. Filippa Lentzos, *The Russian disinformation attack that poses a biological danger*, 19 November 2018, https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/
9. Jeffrey A. Lockwood, *Insects as Weapons of War, Terror, and Torture*, Annual Review of Entomology, vol. 57:205-227, https://www.annualreviews.org/doi/full/10.1146/annurev-ento-120710-100618
10. Khatuna Mshvidobadze, *The Battlefield On Your Laptop*, Radio Free Europe/Radio Liberty, 21 March 2011, http://www.rferl.org/articleprintview/2345202.html
11. Vicky Peláez, *Scientists: coronavirus would be a weapon of biological warfare*, 13 February 2020, https://mundo.sputniknews.com/firmas/202002131090460452-cientificos-el-coronavirus-seria-un-arma-de-guerra-biologica/
12. Douglas Selvage, Christopher Nehring, *Operation "Denver": KGB and Stasi Disinformation regarding AIDS*, 22 July 2019, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids
13. Faruk Zorlu, *Covid-19: Infodemic spreads faster than pandemic*, 31 March 2020, https://www.aa.com.tr/en/latest-on-coronavirus-outbreak/covid-19-infodemic-spreads-faster-than-pandemic/1786381
14. *A New Chinese Coronavirus Was Likely Elaborated in NATO biolabs,* https://euvsdisinfo.eu/report/a-new-chinese-coronavirus-was-likely-elaborated-in-nato-biolabs/
15. *Catching the Virus Cybercrime, Disinformation and the COVID-19 Pandemic*, 3 April 2020, https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic
16. *Disinformation Can Kill,* 26.03.2020, https://euvsdisinfo.eu/disinformation-can-kill/
17. *EU Commission Warns of Increased Cybercrime During Coronavirus Crisis,* VOA News, 24 March 2020, https://www.voanews.com/

science-health/coronavirus-outbreak/eu-commission-warns-increased-cybercrime-during-coronavirus
18. *На улицах итальянских городов прозвучал гимн России*, 26 March 2020, https://ren.tv/news/v-mire/677798-na-ulitsakh-italianskikh-gorodov-prozvuchal-gimn-rossii
19. *NATO Uses COVID-19 to Mobilise Western Military Forces against Russia*, 19 March 2020, interview with Alexander Artamonov conducted by Novorossia news agency, https://novorosinform.org/808651
20. *The US Defender 2020 Military Manoeuvre Is Explicitly Directed against Russia,* https://euvsdisinfo.eu/report/the-us-defender-2020-military-manoeuvre-is-explicitly-directed-against-russia after Alexander Rahr, *Defender 2020 ist ein Fehler, man muss auf Russland zugehen,* https://www.youtube.com/watch?v=5WCCwneR-DU&feature=emb_title.