This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

Laboratories at Home and Abroad: Russian Information Operations Pre-Deployment

https://www.e-ir.info/2024/09/07/laboratories-at-home-and-abroad-russian-information-operations-pre-deployment/

BOTOND K. KERTI, SEP 7 2024

The study of Russian information operations has seen an explosion since 2014. This is visible in the number of publications on the topic since that year. To illustrate this point, a quick survey of aggregating platforms of academic journals (JSTOR, Taylor and Francis Online, Google Scholar) is sufficient. Querying the platform JSTOR with the search terms ["Russia" "information operations"] produces 169 publications overall, only 40 of which were published before 2014. The platform Taylor and Francis Online produces 19 publications corresponding to this search term with a publication date up to 2014, and 40 overall. Google Scholar produces 628 results published before 2014, and 2200 overall.[1] Furthermore, institutions that specialise in studying, documenting, and counteracting Russian information operations were set up after 2014. The two most notable ones are the NATO Strategic Communications Centre of Excellence (Bentzen, 2016, p. 3) and the East Stratcom Task Force under the European External Action Service (Vilson, 2016, p. 127).

Such an explosion of academic interest is explained by the annexation of Crimea by the Russian Federation in March 2014 (Giles, 2016, p. 2) and the extremely successful informational component that it featured (McIntosh, 2015, pp. 299-300). Russian information operations were studied pre-2014. Examples are the 2007 cyberattacks against Estonia (Lange-Ionatamisvili, 2015, p. 3) and Georgia's "victory" on the informational front in the 2008 war (Thomas, 2010, pp. 279-282). However, the Crimean operation reshaped the field, producing a streak of multidisciplinary, comprehensive studies between 2014 and 2016.

Following 2016, the field underwent a second shift. The intervention of the Russian special services into the US presidential elections made clear that "hybrid warfare"—including information operations—was more relevant than thought even after Crimea. This operation globalised the scope taken to study Russian information operations. If the US was vulnerable, so was everybody else. As a consequence, regional projects started appearing, investigating Russian information operations in the local language. This led to the splintering of the field geographically, and to the decreased attention to the common trends of Russian information operations, one of the key subjects of the literature around Crimea.

One of these trends is the subject of this dissertation. More precisely, I propose that the internal Russian information space is used to test narratives before they are deployed in Russian information operations. Such a mechanism would be especially effective against the countries of the post-Soviet space. These states are typically more vulnerable to Russian information operations due to the presence of ethnic minorities, as well as a shared historical memory with Russia that is easy to exploit for manipulative purposes.

To explore the viability of this hypothesis, I will present the case of the Richard Lugar Center for Public Health Research (Lugar Lab) in Tbilisi, Georgia. During the COVID-19 crisis in 2020, a narrative was deployed first in Russia and then in Georgia, alleging the involvement of the laboratory in the creation and spreading of the COVID-19 virus as part of US biological warfare against Russia. Through a detailed analysis of this case, I hope to illustrate the theory of the Russian information space as a testing ground for information operations. I use the term "information operations" throughout the dissertation because it is inclusive of everything that might form part of such an operation from Russia. Information operations in the Russian understanding include everything from network-based activities,

influence campaigns, intelligence, economic activities, deception, elite corruption, special operations, etc. (Giles, 2016), and are aimed at altering the public consciousness of the adversary populations in ways advantageous to Russia. Despite the shift away from such terminology in Western literature after 2016, I deem it useful, as it provides the necessary scope to understand operations as a whole.

In the following section, I will summarise the key features of post-Crimea literature to highlight the more substantial attention paid to the general understanding of Russian information operations. Following the 2016 shift within the field, I will narrow my focus to the studies that make the connection between the Russian internal information space and Russian information operations. In order to explore this connection, I will elaborate on my hypothesis. The similarity of methods between Russian internal informational control and Russian information operations, administrative ties, and the logical rationale behind testing narratives before deploying them abroad represent the key elements. To highlight how this mechanism of testing might operate, the case of the Lugar Lab will serve as an example.

The aim of this dissertation is not to prove conclusively that this mechanism exists. It is to illustrate the potential for conducting further, potentially more quantitative research on this particular question, as well as the general topic of how the Russian information space is used and interacts with Russian information operations. An understanding of these phenomena would undoubtedly aid in detecting, counteracting, or preventing altogether Russian activities that aim to exploit divides within societies to further Russia's objectives. From the theoretical point of view, the dissertation aims to widen the scope of existing research on the connection between the Russian information space and Russian information operations.

Literature on the Crimean Operation

The Crimean information operation was perceived as extremely successful, even paradigm-shifting within NATO (McIntosh, 2016). Hence, the aim of the literature on the operation was to gain a deep understanding of Russian information warfare and be able to react to similar operations in the future. This being the common topic, a few common features stand out: **1)** a search for a common logic to these operations in Russian-language theoretical pieces on information warfare and strategic documents of the Russian Federation; **2)** a search for historical precedent and analogues with Soviet operations as well as concepts such as "active measures" or "reflexive control theory"; **3)** an attempt to highlight the difference from Soviet "special propaganda" and current Russian information operations, especially ideologically and technologically; **4)** documenting and disproving the narratives deployed in operations; and **5)** anticipating what might happen in the future and how to counteract such operations.

In one of the first examples, Jolanta Darczewska (2014) attempts to uncover the goal of information warfare in Russian doctrine. This goal is located in exerting psychological influence on adversary societies in accordance with the interests of the Russian state. To contextualise this goal, Darczewska analyses the philosophical underpinnings of information warfare from the "Dugin" and "Panarin" schools of thought. Both rely on the concept of societal confrontation between "Western" values and their "Eurasian" counterpart. Information warfare is viewed as historical by both Panarin and Dugin, fought between the "West" and different iterations of the Russian state. The main difference between Soviet times and the present is in method (i.e. mass communication technologies) and not aims or strategy. Such an all-encompassing conceptualisation conditions the ongoing nature of Russian information warfare in theory and in practice.

Thus, Darczewska's paper looks to philosophy to identify the aims of the operations (1), tries to locate the origins of present doctrine and practices in the Soviet past (2), but it also pays attention to the technological and ideological changes since then (3). Narrative analysis focuses on the "Dugin network", a set of online communities curated by the philosopher (4). Finally, the article notes that the annexation of Crimea follows from Russian strategic documents, the application of Soviet techniques in the modern context, and calls to limit the space of Russian information operations by disproving their narratives (5).

Another paper by Darczewska (2015) is devoted to the analysis of the Military Doctrine of the Russian Federation of December 2014 (1). Darczewska argues that the new doctrine inscribes the lessons of the Crimean operation in

Russian doctrine. The main takeaway is that *information* has turned into a weapon and should be treated as such. This conclusion is attributed to Russian "strategic culture", that is, the conspiratorial worldview of the Russian military-political elite, seeking total control at home and effective tools of confrontation abroad, in constant opposition to and under assault from Western values seeking to destroy Russia (2, 3). Such a conceptualisation makes Russian information warfare essentially incomparable with its Western counterpart, the focus of which is limited to concrete military operations, and not confrontations of civilisational magnitude. As such, Western concepts should not be applied when analysing Russian information operations (5).

Lange-Ionatamisvili's 2015 paper is focused on "strategic narratives", translating the conspiratorial worldview outlined above. The author locates these narratives in strategic documents from 2007-2009 (1). The main narratives can be summarised as the "defense of the Russian information space from NATO", the defence of "compatriots" (Russian-speaking minorities in countries of the Former Soviet Union), and the consolidation of the Russkiy Mir ideology, seeking to expand Russia's rightful influence over the post-Soviet space (4). Lange-Ionatamisvili identifies Russia's methods as an entirely new form of warfare that the West is unprepared for (5). Current strategies, such as the control over internal media, are identified as a continuation of Soviet practice and are contrasted with the new state ideology of the Russkiy mir, as well as novel domains of confrontation such as online mass media (2, 3).

In sharp contrast, Maurer and Janz (2014) focus exclusively on operations in the cyber domain, that is, the vulnerabilities of the infrastructure that channels information (TV networks, internet cables, phone operators, data storage centres, etc.). This paper highlights the difficulty in reconciling the all-encompassing nature of Russian information warfare with the much narrower, network-centric interpretations of NATO. The authors call on NATO to define its threshold for the activation of the collective defense clause of the Washington Treaty in case of an "information attack" as a response to the emerging form of Russian information warfare (5).

Snegovaya (2015) accentuates the Soviet origins of present Russian information warfare techniques. The main focus is the Soviet concept of "reflexive control theory", designed to force the adversary to act in ways advantageous to the attacker (1). Hence, Snegovaya deems the discourse around Moscow's new informational capabilities as part of a reflexive control campaign, designed to deter the West from reaction (2). Due to these judgements, the author simply calls to reexamine counter-reactions to Soviet information operations (5). Snegovaya also tries to highlight the ineffectiveness of Russian information operations, citing the limited reach of propaganda outlets such as RT and Sputnik (3, 4), as well as the limited convergence between Western public opinion and Russian narratives about Crimea.

Pomerantsev's 2015 article is an outlier. It locates the source and effectiveness of Russian information operations in the internal Russian information space. The key element of this effectiveness is expressed in the full control of the Presidential Administration (PA) over most channels of internal media. The PA administers a system described as a "highly developed industry of political manipulation" (p.42), propagating "engaging, sensationist drama" (p. 41). According to Pomerantsev, the Kremlin's goals do not differ when it comes to internal and external operations. It is always to blur reality enough so that the concept of truth itself becomes suspicious (1). Such a strategy helps undermine social cohesion in all countries, including Russia, and exacerbates existing societal tensions. The solution proposed by the author is to come up with more compelling *and* truthful narratives compared to the ones propagated by the Kremlin (5). By establishing the similarity of the techniques used for internal informational control and external-facing information operations, the author also calls to attention the increased ideological space of Russian information warfare compared to Soviet practices based on communist ideas (2, 3).

The 2015 publication of Sazonov, Müür and Mödler by the NATO Strategic Communication Centre of Excellence was produced in light of the 2014 Military Doctrine of the Russian Federation. The collection of essays is based around the concept of "Information Superiority". Information Superiority is defined as employing informational activities during peacetime in order to reduce the fighting capabilities of the adversary. Such a concept follows directly from the so-called Gerasimov doctrine of 2013 (Gerasimov, 2013), which argues that control over information is the driving force of modern warfare. Thus, the paper sets out to analyse how this concept of information superiority was implemented during and after the Crimean operation, as well as what countermeasures might be taken by NATO in future conflict scenarios with Russia (1, 5).

The implementation of this concept relies on Russia's control over information about itself, which allows it to create manipulative narratives about its past and present. These narratives form part of the modern Russian state's ideology (Russkiy mir/Russian world) that represents Russia as a separate, special civilisation based on elements from the imperial past, eastern Orthodoxy and the idea of Moscow as the Third Rome, the Soviet empire (2), as well as the Russian ethnos's special role in civilising and ruling over the rest of Eurasia. To implement this ideology, two concepts form the basis of Russia's information warfare doctrine. One is that this special civilisation is under constant attack and hence must be defended, the other is that the most effective way to do this is via the information space. These concepts are elaborated by theorists of Russian information warfare, such as Chekinov, Bogdanov, Semenov, Bukharin, and Gareev (1). Their arguments converge on the idea that information is more powerful than weapons, hence it must lead and not follow kinetic warfare. This, however, requires longer implementation and draws Russia into constant information warfare to achieve its aims. The main method in the operation against Ukraine was the crafting and spreading of narratives based on historical memory that portrayed the Government of Ukraine as Nazis, Fascists, a Junta, illegal, or Russophobic. The paper analyses how these narratives were propagated in different forms via a tabloid newspaper, the official TV channel of the Ministry of Defence of Russia and an analytical website to cater to different audiences, both in Russia and in Ukraine (4). A Facebook group is also examined to analyse the importance of the relatively novel field of social media campaigns (3). The authors propose more thorough historical education on Russia in order to reduce the effectiveness of deceptive historical narratives (5).

András Rácz and Katri Pynnöniemi (2016) begin by locating the roots of information operations practices and theory in the tradition of Soviet active measures (1, 2). Further, the study presents metanarratives of Russian information warfare against Ukraine. The most important ones are the labelling of the Kyiv government as a Junta, Fascists, Nazis, Banderovtsy, and a threat to the Russian world (4). The overall aim of such metanarratives is defined as discrediting any resistance to Russia's foreign policy interests, blaming the conflict on the Ukrainian government, representing the separatist fighters as freedom fighters and Russia as a simple passive bystander (1). What is innovative about the paper is that it also investigates and analyses these metanarratives used in information operations against eight other countries (Germany, Estonia, Finland, Sweden, Hungary, Poland, Czechia, and Slovakia). By taking such an approach, the study established the further development of the field, inasmuch as country-specific analysis of Russian information operations becomes ubiquitous after this initial phase of literature. Furthermore, it also establishes the connection between the Russian information space that produces these narratives and Russian information operations that adjust and deploy them against different countries (5).

Finally, the NATO Handbook of Russian Information Warfare (Giles, 2016) represents the culmination of the first phase of studies. The aim of the book is to establish a baseline for further research on the subject. As such, most of it is dedicated to providing common terminology and directions for further study. Most importantly, the book translates the Russian concept of information warfare into relevant NATO disciplines (1, 2, 3), defining it as the sum of computer network operations, psychological operations, strategic communications, intelligence, counterintelligence, disinformation, deception, electronic warfare, and more. In line with this thought, the book highlights the dangers of applying NATO concepts to Russian activities. The fundamental goal of Russian information warfare is defined as influencing the consciousness of adversary populations to achieve Russia's strategic goals (1). The importance of the "defence" of the Russian information space in Russian doctrine is also elaborated. To provide context, the history of the development of the present concept of information warfare is summarised (2). A chapter is dedicated to the newest techniques used in information operations, such as troll farms that are used to amplify narratives on social media and the internet (3). Finally, the book tries to anticipate the form that future operations might take for corresponding research and design of countermeasures. These include more frequent covert influence actions in the online space, sabotage attacks on communication infrastructure, the convergence between fields of activity that are traditionally considered to be separate (intelligence, media, military), as well as more sophisticated targeting of population groups and even specific personnel (5).

Shifts in the field post-2016

After 2016, there was a noticeable change in the study of Russian information operations. An important factor behind this change is demonstrated in the NATO Handbook of Russian Information Warfare: studying this field in a comprehensive way requires a range of knowledge that is simply rare.

Furthermore, the Russian interference in the 2016 US presidential election expanded the scope of the studied subjects from Ukraine and the former Warsaw Pact countries to the rest of the world. As a consequence, scholarship splintered geographically, requiring local language knowledge for each specific country/region.

Moreover, the two components of the 2016 interference in the US election revealed a further divide. The hacking of the Democratic National Convention was analysed as a cybersecurity incident, which was interpreted as separate from the other part of the information operation. The second direction was based on the disinformation campaign on Twitter, namely the investigation of influence operations through media campaigns. An example of investigating cyber activity is the study of the Stanford Internet Observatory (Diresta and Grossman, 2019, pp. 3-99) on Russian military intelligence-curated (GRU) fake organisations and personas. An example of investigating influence campaigns is the StopFake project and its continuous research on disinformation operations.[2]

In an attempt to bridge the post-2016 geographical-thematic divides, I will conceptualise the role of the Russian information space in Russian information operations. The next section will establish the connection between the two entities through the discussion of cases where narratives were used in both the Russian and a foreign information space. This connection was mentioned quite frequently in the literature related to Crimea because it is immediately apparent. The main avenue for Russian narratives into the information space of other countries during the first phase of literature was Russian state television. This was possible since the studied countries are almost exclusively from the post-Soviet space, and many of them were translating Russian state television at that time. (examples include, for Latvia, Berzina, 2016, pp. 171-205; and for Ukraine, Snegovaya, 2015, pp. 18-22). Even though some of these direct avenues were removed after 2014 (Snegovaya, 2015, p. 19; Stolze, 2022, pp. 7-8), the practice of using internally focused narratives in information operations against post-Soviet countries did not cease.

Historically manipulative narratives based around the Russian/Soviet victory in the Second World War also continued to be deployed both in addressing the Russian population and against Estonia, Finland, Poland, and Latvia (Juurvee, 2020). “Information laundering”—defined as the gradual distortion of an original source and its subsequent dissemination—became one of the practices of delivering Russian narratives to diasporas abroad, especially after the restrictive measures on more direct avenues following the 2022 full-scale Russian invasion of Ukraine (Stolze, 2022, pp. 4-36). The Baltnews Telegram channel continued to narrate the war from the Russian point of view to the ethnic minorities of the Baltic republics, often citing statements from Russian official bodies, disguising their true source through proxy outlets.

Russian information operations against Georgia make for a particularly fruitful example (Lange-Ionatamisvili, McMillan). Russia targets Georgia’s information space through proxies, since openly pro-Russian narratives are unpopular (pp. 38-39). However, the similarity between the narratives used within Russian and against Georgia is striking. A frequent Russian narrative contrasts “decadent Western values” with “Conservative and Orthodox Georgian (Russian)” ones, exploiting ordinary Georgians’ fear of modernisation. Another example is framing Georgia’s ties to NATO as destabilising, which plays on the country’s historical insecurity, exacerbated by the 2008 war with Russia. NATO as aggressive and destabilising is one of the key ideas of Russian President Vladimir Putin, since at least 2007 (Putin, 2007). The defense of traditional values is also a key tenet of modern Russian state ideology, highlighting how narratives used internally are also used in information operations.

In conclusion, the same narratives are often used for both internal Russian audiences and information operations abroad. The implications of this connection are explored below.

Thesis outline

In spite of the fact that the connection between the Russian information space and Russian information operations is documented, the potential implications of this connection are hitherto left unexplored. I could locate no publications that address this particular issue, suggesting that the phenomenon is either assumed to have no significance or it has not been studied yet. The present dissertation attempts to challenge this assumption and start filling this gap. I will try to demonstrate that one of the functions of the Russian information space in information operations against post-Soviet countries could be that of *testing* the narratives before they are deployed in live operations. Thus, the

hypothesis of the dissertation can be formulated thus: *Narratives employed in information operations against post-Soviet countries are tested within the Russian information space.*

There are a few factors that make such a hypothesis credible. First of all, the countries of the post-Soviet space are especially vulnerable to narratives that are also used against the Russian population. In most of them, a significant section of the population speaks the Russian language and receives information from Russian news sources directly or through acquaintances. Ukraine, Latvia, and Estonia stand out, as in these countries, the Russian-speaking population is also a semi-marginalised ethnic minority, and hence a lot more receptive towards narratives hostile to its home state (Kuprashvili, 2021, p. 58). Furthermore, Russia's "Compatriots" foreign policy initiative (Zakem et al., 2015, pp. 37-45) provides a set of avenues for information operations through state-curated NGOs. These organisations work on strengthening the Russian state's ties to ethnic Russian or Russian-speaking minorities abroad, and are highly effective at spreading the Kremlin's narratives. Moreover, shared historical memory between the Russian population and these groups provides fruitful ground for information operations due to its emotional content and its potential for manipulation (Juurvee et al., 2020). Thus, these conditions produce an unusually permissive environment (Giles, 2016, pp. 22-26) for Russian information operations.

Furthermore, the Russian state apparatus deploys identical strategies to achieve internal informational control as in information operations. Internally, troll factories serve to distort impressions of popular opinion online, while the much more advanced and ideologically charged strategy of "littering of the information space", provides engaging but misleading content in large amounts that makes it impossible to distinguish between truth and falsehood Kiriya (2021, pp. 16-26). The similar "firehose of falsehoods" strategy (Paul and Matthews, 2016, pp. 1-11) is used in external-facing information operations. The key features of this strategy are described as: "1. High-volume and multichannel 2. Rapid, continuous, and repetitive 3. Lacks commitment to objective reality 4. Lacks commitment to consistency" (p. 2). These two strategies result in very similar content, both in terms of quality and volume.

Such similarities should not be surprising. First, according to Russian information warfare theory, controlling Russia's information space and exercising external informational influence are the components of the same overall strategy (Thomas, 1998). As such, the organisations responsible for internal propaganda and information operations are best conceptualised as part of the same, highly centralised administrative structure. At the head of this structure is the Presidential Administration of the Russian Federation, directing each participant of these activities, including the country's main media holdings, NGOs, journalistic outlets, digital media, as well as the Special Services (Kuzichkin and Hanley, 2021, pp. 13-31).

A recent incident serves to highlight this interconnectedness. Following Russia's full-scale invasion of Ukraine in 2022, much of the infrastructure of the Special Services used for information operations within the European Union was dismantled. This included many media organisations, agents of influence, diplomats, digital services infrastructure, money laundering schemes, and so on. Due to this loss of capabilities, a profound restructuring took place within the services to replace the lost infrastructure as well as improve coordination between the different branches of the information operations apparatus. This restructuring was led by Sergei Kirienko, deputy head of the Presidential Administration (Watling, Danylyuk and Reynolds 2024, pp. 8-9). Kirienko's usual portfolio is Russian domestic politics, including media and propaganda (Pertsev, 2022; Insikt Group, 2022, pp. 4-5). Thus, the person in charge of internal propaganda has also played the leading role in reorganising information operations capabilities, highlighting the coalescence between the administration of internal and external-facing information operations.

Another factor supporting the hypothesis is that testing narratives internally would help determine their effectiveness before they are deployed. Measuring the impact of information operations is a problem as old as the discipline itself, which has become even more acute with the move into the online space (Rid, 2020, pp. 429-432). For example, the Twitter disinformation campaign during the 2016 US presidential elections turned out not to have had any serious effect in and of itself despite the initial apprehension following its discovery (Rid, 2020, pp. 403-409; Eady, Paskhalis, and Zilinsky et al., 2023). This initial error in impact measurement is in part attributable to the fact that the US information space is difficult to delineate and is so volatile that isolating the effects of a narrative on public opinion is next to impossible. In contrast, the Russian information space's specific characteristics make such impact measurements possible. The Russian information space is extremely well controlled. By 2019, close to 90% of

information content within Russia was produced by just three companies, all under the direct or indirect ownership of the state and direction of the Presidential Administration (Kuzichkin and Hanley, 2021, p. 13). The Russian information space is also closely surveyed. The Kremlin uses public opinion surveys to assess the effectiveness of narratives propagated through traditional and social media channels, and to target and adjust them accordingly (Rogov and Ananyev, 2019, pp. 210-212). This ability to gauge the effectiveness of any given narrative and adjust it as needed greatly mitigates the measurement problem that is otherwise inherent to information operations. Finally, in the case of the post-Soviet countries, narrative testing is possible internally since certain sections of the Russian population have their close equivalents in post-Soviet countries. This is based on their similar education, age, language, habits of consuming information, as well as the shared historical memory, as discussed previously. This provides the Kremlin with the necessary target audience at home to test its narratives before using them against post-Soviet states.

To summarise, the factors that make possible the testing of narratives used in Russian information operations against post-Soviet states are: 1) the specific characteristics of the Russian information space, 2) the role of the Presidential Administration in managing both internal informational control and information operations, 3) the ensuing similarity of applied strategies, 4) the value of initial feedback on the effectiveness of narratives before deployment, and 4) corresponding population groups in Russian and post-Soviet states. To illustrate how this testing mechanism might work in practice, the case of the Lugar Lab in Georgia is examined below.

The information space

In order to be able to see whether the narrative was tested in the Russian information space before being used in the Georgian, it is important to draw the line between the two. There are multiple theories of the Russian information space that could be applied here. The *territorial approach* focuses on entities within the state's borders. The *technological approach* concentrates on infrastructural objects. The *social approach* analyses social relations between the producers and consumers of information. The *evolutionary approach* sees the information space in the theoretical structures that are used to process information by the human mind, and the Noöspheric approach describes the complete merger of the biological and mental spheres as the information space (Kovaleva, 2018, pp. 137-141). This dissertation will adopt a combination of the "territorial" and the "social" approaches, since these are the two concepts that are applied in Russian strategic documents. Thus, the Russian information space is conceptualised along two key factors: territory and target audience. Hence, for a source of information to be considered "inside the Russian information space" and potentially used for testing, it will physically have to be within Russia. It will also have to be under the direct or indirect control of the Presidential Administration (PA) in order for deliberate testing to be conceptually possible.[3] Furthermore, the intended target audience of the source will also have to be internal. This is important to state since many outlets under the PA's control such as RT or Sputnik are under the same editorial, financial, and political oversight, but they address audiences outside Russia (Kuzichkin and Hanley, 2021, pp. 13-30).

To summarise, the Russian information space is constituted by sources of information that are physically based in Russia and are addressed to internal Russian audiences, combining for a territorial-social approach. Sources of information that are under the control of the PA but address external audiences will not be considered for testing, but they are paid attention to as amplification devices for Russian narratives in foreign information spaces.

Accordingly, I will detail the case of Lugar Lab as an illustration of the testing mechanism. The narratives used in the operation were extracted from secondary literature and then traced back to their *initial internal source*. The mechanism of "testing" is considered to be ongoing between the appearance of a specific narrative in the Russian information space and the appearance of the narrative in the information space of the target country (Georgia). Further testing is also possible while the operation is already live, in order to make adjustments to the narrative. Hence, it is expected that the narrative will not disappear from the Russian information space after its first deployment in Georgia. A chronological limit is also applied. The examined period starts on the 20th of January 2020 and ends on the 29th of September 2020. This is due to the fact that some information operations using the same narrative continue for years, if not decades (Rid, 2020, p. 180). Such a timeframe is beyond the scope of this dissertation.

The limitations of this methodology should also be noted. The theory of narrative testing is presented through a single case study. Consequently, it should not be considered to be confirmed, even if all the criteria outlined above are met. A much larger sample size would be required to make such conclusions. Furthermore, no "direct" evidence will be provided that the mechanism identified as "narrative testing" exists.[4] Its theory is based on observations of how Russian information operations are conducted, the practical benefits of testing narratives, and the existing infrastructure that makes testing possible. Hence the following case study is meant as an illustration of what the testing mechanism might look like. Perhaps more importantly, it is intended to provide the starting point for further research on this concrete concept, as well as on the interactions between the Russian information space and Russian information operations, hitherto left unexamined.

Case study: COVID-19 emerged from the Lugar Laboratory in Georgia

Context

The Richard Lugar Center for Public Health Research (henceforth Lugar Lab) is a biological research centre located in Tbilisi, Georgia. It was constructed in cooperation with the US Department of Defence from 2004 to 2011, and it has been operational since August 2013. The main narrative of Russian information operations concerning the Lugar Lab has been Washington's alleged use of the facility for biological warfare against Russia, ongoing ever since 2013 (Bolkvadze, 2021, p. 44; Ghvedashvili, 2021, p. 102; see also the example in note [5]). For example, a high-profile operation was conducted against the Lugar Lab in 2018. Igor Giorgadze, former Minister of State Security of Georgia, alleged that an unlicensed drug against Hepatitis C provided by the US was tested on Georgian civilians at the laboratory, many of whom had died as a consequence. This story was run by Russian main television channels, as well as Russia-leaning outlets in Georgia (IDFI, 2020). Versions of the narrative have also been amplified on the official level. In 2018, the radiation, chemical, and biological defense units of the Ministry of Defence of the Russian Federation started investigating "the suspicious spread" of Congo-Crimean haemorrhagic fever, allegedly spread from the Lugar Lab using infected bugs (BBC Monitoring, 2018). The continued nature of these operations suggests that the Lugar Lab was assessed in the Kremlin as a particularly potent object for information operations. With the emergence of the COVID-19 pandemic, this potency was duly exploited.

The operation

On the 26th of January, REN TV, a Russian federal television channel, ran a story called "Mutation, Secret Laboratory or Provocation: Where did the coronavirus come from" (REN TV 2020). The text initially discussed COVID's likely origins in Wuhan and the potential leak from the biological laboratory in the city. Afterwards, the outlet cites comments from Igor Nikulin, "military expert and former member of the commission on biological weapons to the UN", saying that it is likely that the US has artificially created COVID-19. To support this thesis, Nikulin cites the US's apparent interest in wiping out the Chinese population. He also highlights the presence of American "military laboratories" worldwide, without providing any concrete evidence for his claims.[6] Right after Nikulin's comments about the US having made the virus in its military labs, REN TV mentions the Lugar Lab as one of those sites. Thus, the narrative alleging that COVID-19 was made by American military doctors in the "Laboratory of Death" (Vesti, 2018)[7] was born. REN TV's story represents the insertion of the narrative into the Russian information space. Furthermore, REN TV's 900,000-strong audience on the day of publication (Mediascope, 2020) provided the possibility for the Presidential Administration to see whether this narrative was effective in engulfing the laboratory in doubt. According to the theory of narrative testing, the narrative proved efficient and was ready for export to Georgia.

One of the first appearances of the narrative came from an unexpected source. The Georgian counter-disinformation outlet "Mythdetector.ge" published a report on the REN TV emission in Georgian, Russian, and English, debunking its key theses on the same day it appeared. This publication implies that an information assault on the Lugar Lab was anticipated by the Georgian side. The Georgian portal Netgazeti also published an article debunking the narrative, with the head of the Lugar Lab, Paata Imnadze, calling it Russian propaganda (BBC monitoring, 2020a). In parallel fashion, the narrative conflating COVID-19 with the Lugar Lab was run a number of times in the Russian information space, commencing on the 6th February (BBC Monitoring, 2020b). This would have provided further opportunities to the Presidential Administration to test its effectiveness and make the necessary adjustments.

Despite the "prebunking" within Georgia, the narrative was inserted into the Georgian information space on the 18th of March. The online platforms "Georgia and World" and "NewsFront Georgia"—both frequent conduits of Kremlin information operations—published the narrative in Georgian, using almost identical texts (Mythdetector, 2020; Bilanishvili, 2020). On the 24th of March, an interview from the outlet Saqinform also conflated the Lugar lab with the emergence of COVID, calling the virus a biological weapon (Saqinform, 2020). The interview was given to "NewsFront Georgia" by the editor-in-chief of Saqinform, Arno Khidirbegishvili. In two virtually identical interviews with the same participants, the narrative slightly altered. It was now alleged that COVID-19 was created specifically against the populations of the former USSR. This time, however, it was also *reinforced* by co-opting comments from the Nobel-laureate biologist Luc Montagnier, who claimed that COVID-19 might have been manipulated by adding genes of HIV to it (Saqinform, 2020). Conveniently, the narrative of HIV being an American biological weapon is one of the most famous Soviet information operations (Rid, 2020, pp. 299-311), which made for a remarkable comeback. Saqinform similarly took advantage of the comments of the Chairman of the Joint Chiefs of Staff of the USA, Mike Milley (Saqinform, 2020), stating that the US Army could not exclude the artificial nature of COVID.

All three outlets (Georgia and World, Saqinform, and NewsFront Georgia) publish both in Russian and in Georgian. This increases their reach to Georgia's ethnic minority populations, where usually Russian and the native language (Azeri, Armenian) are the only ones spoken. With no access to Georgian news sources, these groups are more vulnerable to hostile narratives of this sort (Chachava, 2021, p.75). Based on the publishing outlets and the language of the publications, the narrative had two principal target audiences: Russia-leaning/anti-Western Georgian political forces and ethnic minority populations. These are the groups that narratives tested inside Russia could be best used against, since they have their close equivalents inside Russia in terms of worldview, historical memory, and political ideas. This first phase of the operation has sown the seeds of doubt within relevant population groups against the activities of the Lugar Lab related to COVID-19. Now it was time to escalate.

On the 17th of April, Russian Foreign Ministry spokesperson Maria Zakharova elevated the narrative to the official level. She declared that it cannot be ruled out that the Americans at the Lab are conducting "work to create and modify various infectious agents of dangerous illnesses, including for military purposes" (BBC Monitoring, 2020c). These statements surged into a diplomatic war of words between the two countries (BBC Monitoring, 2020d). Importantly, using the Foreign Ministry as a channel meant that the narrative could no longer be ignored. It had made it into the mainstream. Lending such authority to these claims gave the impetus necessary for the operation to continue its work of generating mistrust towards the work of the Lugar Lab in the targeted population groups. Correspondingly, "Georgia and World" rehashed the narrative in slightly different forms 5 times between the 26th of April and the 27th of August 2020 (Georgia and World, 2020). The narrative was also kept active in the information space of Russia. The popular tabloid Komsomolskaya Pravda discussed it on the 30th of April (BBC Monitoring, 2020e).[8] The diplomatic campaign also continued throughout the summer. The Russian side demanded full access to the lab on 27th of May (Interfax, 2020). The Georgian side promptly agreed on the 28th of May, as part of an international mission (TASS, 2020), which did not materialise in the end.

South Ossetia, the Russia-backed separatist region of Georgia, provided another axis of the operation. On the 29th of February, only three days after the first case of the virus was confirmed in Georgia, the Security Service of the self-proclaimed republic conflated the Lugar Lab with the spread of COVID-19 (KGB RYuO, 2020), based on the laboratory's geographical proximity to South Ossetia. The Service also called the Lugar Lab a "threat to the entire Caucasus region" (BBC Monitoring, 2020f), thus attempting to discredit its activities in relation to COVID-19. On the 28th of April, the South-Ossetian campaign mirrored the escalation of the Russian Foreign Ministry. The Security Service discussed the spread of the virus in adjacent Georgian regions, then stated that the biggest concern about the spreading of COVID-19 is caused by the Lugar Lab, implying that the virus is from there and is being actively spread by the laboratory (KGB RYuO, 2020).

The narrative reached its pinnacle on the 9th of June, when the Security Service accused the "American curators" of the laboratory of tasking the Georgian personnel with the creation of viruses capable of the precise infection of the South Ossetian population and ethnic group (KGB RYuO, 2020). This declaration was reported by Sputnik South Ossetia (Sputnik, 2020), and a few other outlets of regional significance. This is most likely due to the fact that such a brazen version was meant exclusively for the South Ossetian population, and hence not amplified by larger

Russian/Georgian outlets.

On the 1st of September, the Georgian Ministry of Health suffered a cyberattack, aimed at stealing data related to the Lugar Lab. The attack was blamed on Russian Special Services on the 4th of September by the Interior Ministry of Georgia (BBC Monitoring, 2020g). Foreign Minister Davit Zalkaliani almost immediately identified the attack as part of the ongoing disinformation campaign (BBC Monitoring, 2020h), attempting to pre-empt the effects of any narratives based on real or made-up data acquired about the Lugar Lab. The purpose and effects of this attack are difficult to judge, since no stolen data was used in Russian information operations since it happened. This may be because the intruders did not find valuable data, or because the purpose of the attack was simply to lend credence to previous (and future) claims coming from the Russian side, as well as to showcase Russian cyber power against the "American military biolab". Russian media discussed the incident only passingly.[9]

Finally, this specific narrative blended back into the general Russian campaign around US biological laboratories on foreign soil. On the 29th of September, Nikolay Patrushev, the secretary of the Russian Security Council, voiced the dangers of US biolabs in the post-Soviet space at the meeting of the Shanghai Cooperation Organisation. This warning was reapplied to the Lugar Lab by Sputnik South Ossetia (2020), rehashing their earlier claims about the laboratory and COVID-19. This article concludes the examined period of the operation. However, similar narratives against the Lugar Lab continued to appear and will most likely have future iterations. For example, the South Ossetian Security Service accused the lab of spreading swine flu in July 2021 (Mythdetector, 2021) and of potential bioterrorism in February 2022 (Civil.ge, 2022).

Summary

Overall, the case of this operation illustrates the hypothesis of the dissertation as well as some of the dynamics of Russian information operations described in the literature review. The narrative of the Lugar Lab being part of American biological warfare against Russia and the post-Soviet states has been prominent since before 2020. The emergence of the COVID-19 pandemic and the uncertainty around it created the environment to renew the operation.

Hence, the narrative of COVID having been created at the lab was invented by REN TV on the 26th of January 2020. The federal reach provided by the channel created the conditions to test if the narrative resonated with relevant section of the Russian population. Afterward, the narrative was inserted into the Georgian information space through platforms with target audiences that have equivalents within Russia and are vulnerable to such manipulations. The operation was escalated on the 17th of April via the Russian Foreign Ministry, entering the mainstream. The operation was kept alive and repeated by the relevant actors both in Russia and in Georgia. On the 28th of April, self-proclaimed South Ossetia also entered the fray. The Security Service of the republic claimed that the Americans were tasking the Georgian lab with creating bioweapons capable of exterminating the republic's population. This version of the narrative was amplified by Kremlin outlets such as Sputnik. Finally, a cyberattack was levied against the Georgian Health Ministry, aimed at stealing data related to the Lugar Lab. The outcomes of this attack are so far unclear, but data stolen might be used against the laboratory in the future. While it is difficult to talk about the results of the operation, a public opinion survey from 2021 showed that about one-third of Georgia's population was uncertain about the nature of the work of the laboratory (Chachava, 2021, p. 66). Thus, it is safe to say that the narrative was effective in creating doubt about the laboratory and its usefulness, even if the narrative about it producing bioweapons was not accepted by most.

Conclusion

The aim of this dissertation was to analyse how Russian information operations have been studied up to now, and how they could be studied further. The invigoration of academia following the Crimean operation in 2014 brought the attention of scholars from many disciplines to the subject. This resulted in a search for the internal logic of Russian information operations, continuities with and differences from Soviet practice, and theories of what future operations might look like. In the wake of the intervention of the Russian Special Services into the US presidential elections in 2016, the scope of the field was globalised. This geographical splintering led to a decrease in focus on general trends and internal logic, characteristic of the previous wave of literature. The Russian information space received

little attention, and was studied on a case-by-case basis, not comprehensively. Furthermore, its functions in information operations have yet to be properly theorised. To begin this work, I argued that the Russian information space is used to test the narratives of information operations before they are deployed against the countries of the post-Soviet space. To support this argument, I analysed the structural similarities of Russian information operations and strategies of internal informational control. I also presented the role of the Presidential Administration in directing both of these activities. Taking the perspective of the Russian Special Services, I highlighted the potential benefits of narrative testing, as well as the availability of the infrastructure to do so. Through the case of the Lugar Lab, I aimed to provide an example of what narrative testing might look like in practice.

The methods employed for this research leave room for improvement. First, the minimal sample size prevents drawing general conclusions. Further cases must be studied to confirm or discard this theory. Furthermore, no direct evidence could be provided to prove that the phenomenon observed is indeed testing and not something else. The hypothesis relies on the observation of trends and the logical deduction of the desirability of narrative testing for information warfare operators. Moreover, the similar strategies between internal informational control and information as well as the interconnectedness of the administrative bodies that govern them should be explored in more detail. Finally, the sources used to track potential testing activities should be widened: platforms such as radio, print press, books, and a wider range of social media platforms including private groups and group chats offer some directions to pursue.

Nonetheless, the approach of investigating the connections between the Russian information space and Russian information operations offers a range of opportunities for further research. The benefits of such research are both theoretical and practical. Theoretically, the approach of tying these two phenomena together and examining their relationship offers a wider scope than is presently applied by the field. Practically, the Russian information space is accessible for observation. A better understanding of its role in Russian information operations could help anticipate and counter such activities, reducing their effectiveness. The present dissertation hopes to serve as the starting point of this new direction of research.

Notes

[1] Certain caveats must be applied here. The queries were on the 19th January 2024. The numbers describing the period “after 2014” might have changed as new papers are produced. Furthermore, false positives might well be included in some of the searches. Nonetheless, the corpus that is present on these aggregators is narrow enough for the searches to produce approximately appropriate numbers. These numbers, despite their potential inaccuracies, help illustrate the trend within the studied field, and as such, they fulfil their present function.

[2] A collection of relevant studies is accessible here: https://www.stopfake.org/en/category/news/.

[3] Independent information resources that address the Russian audience also fall within the internal Russian information space, but they cannot be used for testing a narrative used in information operations.

[4] Direct evidence would be memorandums from the Presidential Administration or the Secret Services, directing concrete structures to conduct the testing of a given narrative. The author has no knowledge of the existence, let alone the availability, of such evidence.

[5] RIA Novosti (2014): “Anti-Russian viruses in the laboratories of the American “BioPRO” (Антироссийские вирусы в лабораториях американской БиоПРО) https://ria.ru/20140723/1017236855.html.

[6] In contrast, a report from the Associated Press and the Digital Forensics Research Lab notes Nikulin might never have been employed by the UN (AP, 2020). One thing that is known is that he has been a very frequent guest on Russian TV channels, discussing similar theories. See: https://www.google.com/search?q=Игорь+Никулин+военный+эксперт.

[7] Russian outlets referred to the Lugar Lab as the “Laboratory of Death” frequently after the 2018 operations. See:

https://www.vesti.ru/article/1498355.

[8] For further analysis see: Covid-19 Analysis: Kremlin revives 'US biolabs' claims for virus crisis (https://monitoring.bbc.co.uk/product/c201ouu3).

[9] See: https://yandex.ru/search/?text=хакерская+на+лабораторию+лугара&lr=10522.

Bibliography

Primary sources

BBC monitoring (2018) 'Russian forces to investigate suspicious 'epidemics'', *BBC*, 4th December. Available at: https://monitoring.bbc.co.uk/product/c200hdyx (Accessed: 21.03.2024).

BBC Monitoring (2020a) 'Georgian health official responds to Russian TV's coronavirus conspiracy', *BBC,* 7th February. Available at: https://monitoring.bbc.co.uk/product/c201fwa9 (Accessed: 21.03.2024).

BBC Monitoring (2020b) 'Russian media amplify coronavirus conspiracy theories', *BBC,* 6th February. Available at: https://monitoring.bbc.co.uk/product/c201ftyb (Accessed: 21.03.2024).

BBC Monitoring (2020c) 'Covid-19 Analysis: Kremlin revives 'US biolabs' claims for virus crisis', *BBC,* 8th May. Available at: https://monitoring.bbc.co.uk/product/c201ouu3 (Accessed: 21.03.2024).

BBC Monitoring (2020d) 'Covid-19 Geopolitics: Georgia rejects Russian claims on Tbilisi-based bio-lab', *BBC,* 18th April. Available at: https://monitoring.bbc.co.uk/product/c201mhni (Accessed: 21.03.2024).

BBC Monitoring (2020e) 'Pro-Kremlin tabloid says US labs at Russian borders prepare for biological war', *BBC,* 30th April. Available at: https://monitoring.bbc.co.uk/product/c201oofl (Accessed: 21.03.2024).

BBC Monitoring (2020f) 'Georgia's South Ossetia takes measures against coronavirus', *BBC,* 29th February. Available at: https://monitoring.bbc.co.uk/product/f201hzlz (Accessed: 21.03.2024).

BBC Monitoring (2020g) 'Highlights from Georgian press 4 Sep 20', *BBC,* 4th September. Available at: https://monitoring.bbc.co.uk/product/c20209zv (Accessed: 21.03.2024).

BBC Monitoring (2020h) 'Covid-19 Geopolitics: Georgian officials blame Russia for health database hack', *BBC,* 4th September. Available at: https://monitoring.bbc.co.uk/product/c20209qo (Accessed: 21.03.2024).

Buziashvili, E. (2020) *Bioweapons, secret labs, and the CIA: pro-Kremlin actors blame the U.S. for coronavirus outbreak*. Available at: https://medium.com/dfrlab/bioweapons-secret-labs-and-the-cia-pro-kremlin-actors-blame-the-u-s-for-coronavirus-outbreak-ffc2139c28dd (Accessed: 21.03.2024).

Civil.ge (2022) *Tskhinvali KGB Targets Lugar Center, U.S. Health Facilities*. Available at: https://civil.ge/archives/471025 (Accessed: 21.03.2024).

Georgia and World (2020) *COVID-19, the Lugar Lab and the empty response of the Georgian FM: Where is the lie?* [Covid-19, лаборатория Лугара и ответ-пустышка от МИД Грузии: в чем подвох?] 26th April. Available at: https://geworld.ge/ru/covid-19-лаборатория-лугара-и-ответ-пустышка/ (Accessed: 21.03.2024).

Georgia and World (2020) *Russia must demand the inspection of biolaboratories of the USA at its border* [Россия должна требовать инспекций биолабораторий США у своих границ] 1st June. Available at: https://geworld.ge/ru/россия-должна-требовать-инспекций-би/ (Accessed: 21.03.2024).

Georgia and World (2020) *The effectiveness of an entomological weapon is being tested in Armenia – Media* [В Армении ведется тестирование эффективности энтомологического оружия — СМИ], 27th May. Available at: https://geworld.ge/ru/в-армении-ведется-тестирование-эффек/ (Accessed: 21.03.2024).

Georgia and World (2020) *The secret biolaboratories of the Pentagon at the borders of Russia – investigation* [Секретные биолаборатории Пентагона у границ России: расследование] 26th April. Available at: https://geworld.ge/ru/секретные-биолаборатории-пентагона/ (Accessed: 21.03.2024).

Georgia and World (2020) *Why the Americans need biolabs in Central Asia and the Caucasus* [Зачем американцам биолаборатории в Центральной Азии и на Кавказе] 1st June. Available at: https://geworld.ge/ru/зачем-американцам-биолаборатории-в-ц/ (Accessed: 21.03.2024).

Institute for Development of Freedom of Information (2020) *Russian Information Warfare against the Lugar Laboratory.* Available at: https://idfi.ge/en/russian_information_war_against_lugar_laboratory?fbclid=IwAR1QjwjDvdtfr6ki8XY9fh7Y3g7l2AYsLBmpWi9SQlQq4OwbPoLEYfCkcn8 (Accessed: 14.03.2024).

Interfax (2020) 'Moscow demands that its expert be allowed into all of the biolaboratory of the Lugar Centre in Georgia [Москва потребовала допустить экспертов РФ во все биолаборатории центра Лугара в Грузии]' *Interfax,* 26th May. Available at: https://www.interfax.ru/world/710418 (Accessed: 21.03.2024).

Klepper, D., Amiri, F.,& Dupuy, B. (2020) 'The superspreaders behind top COVID-19 conspiracy theories', *Associated Press,* 15th February. Available at: https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe (Accessed: 21.03.2024).

Mediascope (2020) *Ratings (Рейтинги).* Available at: https://mediascope.net/data/ (Accessed: 21.03.2024).

Ministry of Foreign Affairs of the Russian Federation (2020) *Comment by the Information and Press Department on the Georgian Foreign Ministry's response apropos of the Richard Lugar Centre for Public Health Research* . Available at: https://www.mid.ru/tv/?id=1433757&lang=en (Accessed: 21.03.2024).

Mythdetector (2021) *Disinformation of the so-called "South Ossetian" KGB, as if the African Swine Fever Virus is Spreading from Georgia*. Available at: https://mythdetector.ge/en/disinformation-of-the-so-called-south-ossetian-kgb-as-if-the-african-swine-fever-virus-is-spreading-from-georgia/ (Accessed: 21.03.2024).

Popov, D. (2020) 'Anti-Russian viruses in the laboratories of the American "BioPRO" (Антироссийские вирусы в лабораториях американской БиоПРО)', *RIA Novosti,* 2nd March. Available at: https://ria.ru/20140723/1017236855.html (Accessed: 12.03.2024).

Rosenberg, S., Vernon, W.,& Gobbard, M. (2018) 'Russian disinformation and the Georgian 'lab of death'', *BBC,* 11th November. Available at: https://www.bbc.co.uk/news/av/world-46157507 (Accessed: 21.03.2024).

Saqinform (2020) 'Arno Khidirbegishvili: The coronavirus COVID-19 is a bacteriological weapon, only a few know the whole truth. [Арно Хидирбегишвили: Коронавирус COVID 19 – бактериологическое оружие, всю правду о котором знают лишь немногие]', *Saqinform,* 24th March. Available at: http://ru.saqinform.ge/news/44384/arno-KidirbegiSvili-koronavirus-COVID-19-bakteriologiCeskoe-oruZie-vsU-pravdu-o-kotorom-znaUt-liSi-nemnogie.html (Accessed: 21.03.2024).

Saqinform (2020) 'Sensation! The Georgian analyst revealed the secret of the coronavirus – Khidirbegishvili ended up being right! [СЕНСАЦИЯ: ГРУЗИНСКИЙ АНАЛИТИК РАСКРЫЛ ТАЙНУ КОРОНАВИРУСА – ХИДИРБЕГИШВИЛИ ОКАЗАЛСЯ ПРАВ!]', *Saqinform,* 24th March. Available at: http://ru.saqinform.ge/news/44688/sensaciA-gruzinskij-analitik-raskril-tajnu-koronavirusa—KidirbegiSvili-okazalsA-prav-.html (Accessed: 21.03.2024).

Saqinform (2020) 'The American general did not exclude Gruzinform's (Saqinform's) version [Американский генерал не исключил версию ГРУЗИНФОРМ]', *Saqinform,* 16th April. Available at: http://ru.saqinform.ge/news/44657/amerikanskij-general-ne-isklUCil-versiU-gruzinform.html (Accessed: 21.03.2024).

Sputnik Yuzhanaya Osetia (2020) 'The American curators from the medical research corps of the US Army in Georgia give tasks to the Georgian leadership of the Centre such as the development of a bioweapon that is aimed at precision strikes against the South Ossetian population. [Американские кураторы из медицинского исследовательского подразделения армии США в Грузии ставят перед грузинским руководством центра такие задачи, как "разработка биологического оружия, направленного на точечное поражение югоосетинской популяции"]' *Sputnik Yuzhanaya Osetia*, 5th October. https://web.archive.org/web/20201005125900/https:/sputnik-ossetia.ru/radio/20200929/11195825/V-Gruzii-sozdayut-bakteriologicheskoe-oruzhie—ekspert.html (Accessed: 21.03.2024).

Sputnik Yuzhnaya Osetiya (2020) 'The KGB of South Ossetia published the data on the tasks of the Lugar biolaboratory in Georgia [КГБ Южной Осетии обнародовал данные о задачах биолаборатории Лугара в Грузии]', *Sputnik Yuzhnaya Osetiya,* 28th November. Available at: https://web.archive.org/web/20201128200346/https:/sputnik-ossetia.ru/South_Ossetia/20200609/10702364/KGB-Yuzhnoy-Osetii-obnarodoval-dannye-o-zadachakh-biolaboratorii-Lugara-v-Gruzii.html (Accessed: 21.03.2024).

State Security Committee of the Republic of South Ossetia [KGB RYuO] (2020) *Declaration* [Сообщение]. Available at: https://kgbruo.org/soobshhenie-43/ (Accessed: 21.03.2024).

State Security Committee of the Republic of South Ossetia [KGB RYuO] (2020b) *Declaration* [Сообщение]. Available at: https://kgbruo.org/soobshhenie-52/ (Accessed: 21.03.2024).

TASS (2020) 'Georgia will only let Russian experts into the Lugar Laboratory as part a wider delegation [Грузия допустит экспертов РФ в лабораторию Лугара только в составе более широкой делегации]', *TASS,* 7th June. Available at:https://web.archive.org/web/20200607023737/https://tass.ru/mezhdunarodnaya-panorama/8592423 (Accessed: 21.03.2024).

Vesti (2018) 'The Laboratory of Death under Tbilisi: documentation of experiments on people and biological weapons is published[Лаборатория смерти под Тбилиси: опубликованы записи об опытах над людьми и биологическом оружии]', *Vesti*, 14th September. Available at: https://www.vesti.ru/article/1498355 (Accessed: 21.03.2024).

Secondary sources

Bentzen, N. (2016) *NATO strategic communications – An evolving battle of narratives.* Brussels: European Parliamentary Research Service, pp.1-4. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586600/EPRS_BRI(2016)586600_EN.pdf (Accessed: 07.02.2024).

Bolkvadze N., Chachava, K., Ghvedashvili, G., Lange-Ionatamišvili, E., McMillan, J., Kalandarishvili, N., Keshelashvili, A., Kuprashvili, N., Sharashenidze, T.,& Tsomaia, T. (2021) *Georgia's Information Environment through the Lens of Russia's Influence*. Riga: NATO Strategic Communications Centre of Excellence. pp. 4-121. Available at: https://stratcomcoe.org/publications/georgias-information-environment-through-the-lens-of-russias-influence/212 (Accessed: 28.02.2024).

Darczewska, J. (2014) 'The Anatomy of Russian Information Warfare – The Crimean Operations – a Case Study', *Point of View,* 42*,* pp. 5-33. Available at: https://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study (Accessed: 07.02.2024).

Darczewska, J. (2015) 'The devil is in the details – Information Warfare in the Light of Russia's Military Doctrine', *Point of View*,50, pp. 5-39. Available at: https://www.osw.waw.pl/en/publikacje/point-view/2015-05-19/devil-details-

information-warfare-light-russias-military-doctrine (Accessed: 07.02.2024).

Diresta, R.,& Grossman, S. (2019) *Potemkin Pages and Personas: Assessing GRU Online Operations, 2014-2019* . Stanford: Stanford Internet Observatory. pp. 3-99. Available at: https://fsi.stanford.edu/publication/potemkin-think-tanks (Accessed: 28.02.2024).

Eady, G., Paskhalis, T.,& Zilinsky, J. et al. (2023) 'Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behaviour',*Nature Communications,* 14 (62), pp.1-11. Available at: https://doi.org/10.1038/s41467-022-35576-9 (Accessed: 27.02.2024).

Gerasimov, V. (2013) 'Tsennost' nauki v predvidennii', *Novosti VPK,* 27th February. Available at: https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html (Accessed: 07.02.2024).

Giles, K. (2016) *Handbook of Russian Information Warfare.* pp.3-77. Rome: NATO Defence College. Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf (Accessed: 15.02.2024).

Giles, K. (2016) *The Next Phase of Russian Information Warfare* . pp.2-16. Riga: NATO Strategic Communications Centre of Excellence. Available at: https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176 (Accessed: 07.02.2024).

Hanley M.,& Kuzichkin A. (2021) *Russian Media Landscape: Structures, Mechanisms, and Technologies of Information Operations.* Riga: NATO Strategic Communications Centre of Excellence. Available at: https://stratcomcoe.org/publications/russian-media-landscape-structures-mechanisms-and-technologies-of-information-operations/215 (Accessed: 02.03.2024).

Insikt Group (2022) 'Putin's Potential Successors Part 1: Sergei Kirienko', *Recorded Future,* 4th November. Available at: https://go.recordedfuture.com/hubfs/reports/ta-2022-1104.pdf (Accessed: 02.03.2024).

Juurvee, I., Sazonov, V., Parppei, K., Engīzers, E., Palasz, I.,& Zawadska, M. (2021)*Falsification of History as a Tool of Influence.* pp.6-76. Riga: NATO Strategic Communications Centre of Excellence. Available at: https://stratcomcoe.org/publications/falsification-of-history-as-a-tool-of-influence/16 (Accessed: 27.02.2024).

Kiriya, I. (2021) 'From "Troll Factories" to "Littering the Information Space": Control Strategies Over the Russian Internet', *Media and Communication*, 9(4), pp. 16-26. Available at: https://doi.org/10.17645/mac.v9i4.4177 (Accessed: 27.02.2024).

Kovaleva, N. (2018) 'Russian Information Space, Russian Scholarship, and Kremlin Controls', *Defence Strategic Communications*, 4, pp.133-172. Available at: 10.30966/2018.RIGA.4.5. (Accessed: 03.03.2024).

Lange-Ionatamisvili, E. (2015) *Analysis of Russia's information Campaign Against Ukraine – Examining non-military aspects of the Ukraine Crisis from a strategic communications perspective* . pp.3-39. Riga: NATO Strategic Communications Centre of Excellence. Available at: https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf (Accessed: 07.02.2024).

Maurer, T.,& Janz, S. (2014) *The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context.* pp.1-4.Zurich: ETH Zurich.Available at: https://www.files.ethz.ch/isn/187945/ISN_184345_en.pdf (Accessed: 07.02.2024).

McIntosh, S. E.(2015) 'Kyiv, International Institutions, and the Russian People: Three Aspects of Russia's Current Information Campaign in Ukraine', *The Journal of Slavic Military Studies*, 28(2), pp. 299-306. Available at:

10.1080/13518046.2015.1030263 (Accessed: 15.02.2024).

Osadchuk, R. (2022) *Pro-Kremlin influencers reignite Zelenskyy "green screen" theory*. Available at: https://medium.com/dfrlab/pro-kremlin-influencers-reignite-zelenskyy-green-screen-theory-d827f761d17d (Accessed: 01.03.2024).

Paul, C.,& Matthews, M. (2016) *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. pp.1-16. Santa Monica, CA: RAND Corporation, Available at: https://www.rand.org/pubs/perspectives/PE198.html. (Accessed: 28.02.2024).

Pertsev, A. (2022) *Sergei Kirienko's new sphere of influence*.Available at: https://web.archive.org/web/20220702225709/https://ridl.io/sergei-kirienko-s-new-sphere-of-influence/ (Accessed: 02.03.2024).

Pomerantsev, P. (2015) 'Authoritarianism Goes Global (II): The Kremlin's Information War', *Journal of Democracy,* 26(4), pp. 40-50. Available at: https://doi.org/10.1353/jod.2015.0074 (Accessed: 07.02.2024).

Pomerantsev, P. (2015) *Nothing is True and Everything is Possible – The Surreal Heart of the New Russia* . pp. 60-69. New York: Public Affairs.

Putin, V. (2007) *Speech and the Following Discussion at the Munich Conference on Security Policy (English translation).* Available at: http://en.kremlin.ru/events/president/transcripts/24034 (Accessed: 02.03.2024).

Pynnöniemi, K.,& Rácz, A. (2016) 'Fog of 'Falsehood – Russian Strategy of Deception and the Conflict in Ukraine', *FIIA Report,* 45. Available at: https://www.fiia.fi/en/publication/fog-of-falsehood (Accessed: 15.02.2024).

Rogov, K.,& Ananyev, M. (2018) 'Public Opinion and Russian Politics.' In Treisman, D. (Ed.)*The New Autocracy: Information, Politics, and Policy in Putin's Russia.* pp. 191–216. Washington, D.C.: Brookings Institution Press. Available at: http://www.jstor.org/stable/10.7864/j.ctt1zkjzsh.11 (Accessed: 02.03.2024).

Sazonov, V., Müür, K.,& Mölder, H. at al. (2015) *Russian Information Campaign Against the Ukrainian State and Defence Forces*. pp.4-116. Riga: NATO Strategic Communications Centre of Excellence. Available at: https://www.ksk.edu.ee/wp-content/uploads/2017/02/Report_infoops_08.02.2017.pdf (Accessed: 15.02.2024).

Sazonov, V., Saumets, A.,& Mölder, H. (2016) 'THE CRISIS IN UKRAINE AND INFORMATION OPERATIONS OF THE RUSSIAN FEDERATION', *Estonian Journal of Military Studies, 2*, pp.7-240. Available at: https://www.researchgate.net/publication/364165705_THE_CRISIS_IN_UKRAINE_AND_INFORMATION_OPERATIONS_OF_THE_RUSSIAN_FEDERATION_Estonian_Journal_of_Military_Studies_2 (Accessed: 15.02.2024).

Snegovaya, M. (2015) 'Putin's Information Warfare in Ukraine – Soviet Origins of Russia's Hybrid Warfare.'*Russia Report,* 1*,* pp.7-28*.* Available at: https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare (Accessed: 07.02.2024).

Stolze, M. (2022) *Information Laundering Via Baltnews on Telegram: How Russian State-Sponsored Media Evade Sanctions and Narrate the War*. pp.4-36. Riga: NATO Strategic Communications Centre of Excellence. Available at: https://stratcomcoe.org/publications/information-laundering-via-baltnews-on-telegram-how-russian-state-sponsored-media-evade-sanctions-and-narrate-the-war/257 (Accessed: 28.02.2024).

Thomas, T. L. (1998) 'Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations', *The Journal of Slavic Military Studies*, 11(1), pp.40-62. DOI: 10.1080/13518049808430328 (Accessed: 20.03.2024).

Thomas, T. L. (2010) 'RUSSIAN INFORMATION WARFARE THEORY: THE CONSEQUENCES OF AUGUST 2008.' in Blank, S. J., Weitz, R. (Eds.) *THE RUSSIAN MILITARY TODAY AND TOMORROW: ESSAYS IN MEMORY OF MARY FITZGERALD.* pp. 265–300. Carlisle Barracks, PA.: Strategic Studies Institute, US Army War College. Available at: http://www.jstor.org/stable/resrep12110.8 (Accessed: 07.02.2024).

Watling, J., Danylyuk, O. V.,& Reynolds, N. (2024) *Special Report: The Threat from Russia's Unconventional Warfare Beyond Ukraine, 2022-24.* pp.1-34. London: Royal United Services Institute. Available at: https://www.rusi.org/explore-our-research/publications/special-resources/threat-russias-unconventional-warfare-beyond-ukraine-2022-24 (Accessed: 02.03.2024).

Wilk, A,& Żochowski, P. (2022) *Massive rocket attacks on Ukraine. 228th day of the war.* Available at: https://www.osw.waw.pl/en/publikacje/analyses/2022-10-10/massive-rocket-attacks-ukraine-228th-day-war (Accessed: 02.03.2024).

Zakem, V., Saunders, P.,& Antoun, D. (2015) *Mobilizing Compatriots: Russia's Strategy, Tactics and Influence in the Former Soviet Union*. pp.3-53. Available at: https://www.cna.org/archive/CNA_Files/pdf/dop-2015-u-011689-1rev.pdf (Accessed: 01.03.2024).