The Dangers and Impact of Russian Fake News on the European Union's Common Security and Defence Policy

Essay

Created for the CSDP Olympiad 2024
in Budapest – Hungary

Author:
Áron Bálint

Student of the Ludovika – University of Public Service
Hungary

Budapest, November 2023

Abstract

Fake news is not a new phenomenon; however, it has become quite prevalent and a rather popular tool in the era of social media. Fake news – referred to as disinformation by professionals – is false information presented as actual news, often with harmful intent. Among its goals is hurting the reputation of a public figure, a company, or a news source by mimicking the news source and disseminating incorrect information under their alias, or disseminating false claims regarding the subject that depict it unfavourably. The Russian Federation frequently launches disinformation campaigns against Western countries, their international institutions and states that are aspiring to Euro-Atlantic integration.

The essay presents a case study of Georgia and the most notable Russian disinformation campaigns, which were conducted against the European Union's peacekeeping mission in Georgia, NATO, and even a health research centre.

The research was conducted with qualitative research methods, predominantly document and content analysis, through which first and secondary sources were analysed. The paper searched for answers to three research questions that had been formulated around the topic, with the first being rather simple and general, and the further two having a focus on the European Union Monitoring Mission in Georgia.

Keywords: Fake news, Disinformation campaigns, Georgia, Russian Federation, Hybrid Warfare

1. Table of Contents

2. Preface

I am studying international security and defence policy at the Ludovika – University of Public Service in Hungary. This degree programme is – as its name indicates – centred around security, its components, dimensions, threats, and means to counter them. During my second semester, I had an interesting subject about political discourse and its relation to the media. This was my first encounter with fake news, which later became my third and last field of research. During this same semester, I also joined the Erasmus Student Network – to familiarise myself with the Erasmus+ programme, since I wanted to participate in a mobility later on – and I have become a member of a college for advanced studies to acquire scientific knowledge and be able to participate in conferences and workshops where I can gather practical experience as well. At these conferences, I gave presentations about modern European military equipment and Italian foreign policy. I also got to increase my knowledge regarding psychological and information warfare from other researchers' presentations.

In the Autumn of 2022, I had the chance to execute a long-planned project: I applied for an Erasmus+ mobility programme with the destination city of Rome, Italy. During my mobility period, I had to write some papers regarding the psychological and information warfare used by Italy in peace support operations, while for other subjects I had to present some pieces of propaganda from the early days of the Ukrainian War. Finally, while taking the EUSecure online course at the Sapienza University of Rome, I decided to write a study about the impact of fake news on the European Union and its citizens.

The Olympiad is a great opportunity to acquire additional knowledge regarding the Common Security and Defence Policy, as well as a chance to raise awareness concerning the vast amount of deceptive and misleading content in the media.

3. Introduction

Fake news might seem like a new invention of the 21st century, however, this is not the case. This expression was born at the end of the 19th century, though, spreading incorrect, misleading and deceptive content – disinforming others – had already been present throughout history. The misleading news content had been referred to under different aliases, the most common being "false news". Initially, similarly to conventional media, this "false news" was disseminated via printing technology on paper.[1] With the discovery of radio waves and radio communication at the beginning of the 20th century, a new channel was also found for spreading incorrect content. From approximately the middle of the century, televisions provided an upgrade to deception; besides audio, people now also had visual content. With the invention of Personal Computers, the Internet, social media, and Artificial Intelligence, fake news has also improved consistently. Nowadays it is a rife tool in the hands of internet users, not only states and organisations, but also individuals.

Fake news can be a collective term that refers to manipulative, deceptive and persuasive news content, however, in the academic literature, disinformation, misinformation and propaganda news may also be found for such manipulative communication.[2] According to another specific definition from Lieutenant Colonel Jarred Prier, fake news can be defined as *"a particular form of propaganda composed of a false story disguised as news".*[3] In comparison, other professionals prefer to stick to disinformation and information manipulation as they are deemed more precise definitions. Since both propaganda and disinformation are parts of psychological warfare, fake news also falls under this warfare classification. Psychological warfare is the cognitive capability of information warfare, which is part of hybrid warfare. Hybrid warfare employs political, military, economic, information and civil means of state power. However, hybrid warfare does not have an exact and universally agreed definition and researchers use different approaches to describe hybrid warfare and its contents. In terms of information warfare,

[1] Homepage of Merriam-Webster. The Real Story of 'Fake News'. URL: https://www.merriam-webster.com/wordplay/the-real-story-of-fake-news. [24-8-23]

[2] Jakusné Harnos, É. (2020). Fake News and Social Media as Security Risks. EUSecure: Interdisciplinary training on EU security, resilience and sustainability

[3] Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. Montgomery. Air University Press. Strategic Studies Quarterly. Volume 11. No. 4. P. 60.

they could not agree on whether it is a tool or a domain. In 2021, the EU's Joint Research Centre prepared a report about hybrid warfare at the request of the European Commission, which analysed hybrid warfare's contents as domains. I created a table from their report, which presents the hybrid tools that exert force in the information domain either directly or indirectly.[4] It is important to note that these domains may also affect each other.

Employment of hybrid warfare	
The tool	The domain it directly affects
Physical operations against infrastructure	Infrastructure, Economy, Cyber, Space, Military, Information, Social, Public Administration
Cyber operations	Infrastructure, Space, Cyber, Social, Public Administration, Military
Engaging diasporas for influencing	Political, Diplomacy, Social, Culture, Intelligence, Information
Financing cultural groups and think tanks	Social, Culture, Political, Diplomacy
Manipulating political discourse to polarise societies	Social, Culture, Political, Legal
Creating confusion and contradictory narratives	Social, Information, Diplomacy
Discrediting or supporting political actors and leaders	Political, Public Administration, Social
Using immigration for influencing	Political, Social
Media control and interference	Information, Infrastructure, Social, Culture
Disinformation campaigns and propaganda	Social, Information, Political, Cyber, Culture, Public Administration

Table 1: Employment of hybrid warfare if information is considered a domain[5]

The aim of this paper on the one hand is to discuss the effects of disinformation on European countries and CSDP missions through a case study. On the other hand, to point out gaps where actions should be taken with more efficiency to counter fake news and its impact on the EU and its Common Security and Defence Policy.

[4] Cullen, Patrick et al. (2021). The landscape of Hybrid Threats: A Conceptual Model. Pp. 27-35.

[5] Table created by the author based on Cullen, Patrick et al. (2021) The landscape of Hybrid Threats: A Conceptual Model.

4. Current State of Research

As mentioned earlier, fake news is not a new phenomenon, however, it has become a mainstream expression and a widely used tool in the 21st century. In 2014, when heavily armed men dressed in green uniforms captured Simferopol, the largest city in Crimea, Moscow started a disinformation campaign, in which it denied all accusations regarding Russian involvement and claimed that the "little green men" were local self-defence units.[6] However, it only became a prevalent expression 2 years later during the 2016 US presidential election campaign, when multitudes of biased and falsified stories were published on social media websites – such as Facebook and Twitter – and 45th US President Donald Trump engaged in the widespread use of the expression[7] mostly in interviews and tweets. Later, he even claimed to have invented the expression.[8] As the use of fake news gained widespread popularity in the 21st century, a large sum of literature emerged. These include books, articles and interviews, though useful reports and datasheets can also be encountered. It is important to note that most of the literature is authored by Western scholars, which may correlate to the frequent disinformation campaigns launched against Western-aligned states.

Due to the vast amount of sources available, narrowing the focus was necessary. Therefore, this study focuses on official documents authored by the EU and studies from mostly European scholars. Below the sources that I find the most important can be found.

First and foremost the EUGS and the European Union's Global Strategy: Three Years on, Looking Forward must be mentioned. In the EUGS the improvement of the EU's strategic communications is visualised, which consists of the previously mentioned faster and consistent messaging and the rebuttals of disinformation. The latter is an analysis from 2019, carried out by the creators of the EUGS. It is a summary of the implementation of the EUGS and its significance comes from the part related to information operations, in

[6] Homepage of Radio Free Europe Radio Liberty. From 'Not Us' To 'Why Hide It?': How Russia Denied Its Crimea Invasion, Then Admitted It. URL: https://www.rferl.org/a/from-not-us-to-why-hide-it-how-russia-denied-its-crimea-invasion-then-admitted-it/29791806.html. [30-9-23]

[7] The term "fake news" has strong political connotations and is considered to be inaccurate and unable to describe the complexity of the issue, therefore professionals use other, more precise expressions, such as disinformation and information manipulation. Therefore, in order to be more accurate and professional, from the 3rd chapter, the expression "disinformation" will be used in the study instead of "fake news".

[8] Homepage of The New Daily. Donald Trump takes credit for 'fake news', but dictionary disputes. URL: https://thenewdaily.com.au/news/world/2017/10/09/donald-trump-fake-news/. [30-09-23]

which they welcome the establishment of 3 Strategic Communications Task Forces under the European External Action Service (EEAS), which significantly contributed to successful strategic communication and countering disinformation. The Task Forces – which were conceived as one of the conclusions of the European Council meeting on 19 and 20 March 2015, to challenge the Russian disinformation campaigns – have a flagship project, a website called "EUvsDisinfo". The website is a large database of disinformation cases, articles, learning materials, and audio and video content. The experts' work mainly focuses on the Eastern neighbours of the EU, including Ukraine, Moldova and Georgia.[9]

For the case study Georgia and the CSDP mission it hosts, the European Union Monitoring Mission in Georgia (EUMM Georgia) were chosen. The country is one among those under frequent pressure from the Russian disinformation campaigns, therefore it serves as an ideal research subject. Three scientific articles provide the framework of the case study: Tamar Gamkrelidze's *"Georgia's external frontier on Russia sedimented and unmalleable: engagement politics and the impact of the three-tier warfare"*, *"Russian Anti-Western Disinformation, Media Consumption and Public Opinion in Georgia"* authored by Ralph S. Clem, Erik S. Herron and Ani Tepnadze and *"Prospects of the EU's Common Foreign and Security Policy and Russia's Disinformation Campaign in the South Caucasus"* written by Nino Machurishvili. The first is an analysis of the Georgian engagement politics towards Moscow in the context of Georgian-Russian relations, and the Kremlin's three-tier warfare, which consists of borderisation, cyberwarfare, and disinformation warfare. The second is an analysis of Russian disinformation in Georgia and anti-government protests. The third is a case study of the Russian disinformation in the Republic of Georgia, and Russia's anti-Western narrative. This case study is particularly useful for my research as it assesses different kinds of conspiracy theories that emerged during the 2010s from either media outlets associated with Russia, or pro-Russian politicians, and their impact on the Georgian population. Here, my study gains relevance: What dangers do these disinformation campaigns pose to the CSDP missions – particularly the EUMM Georgia – and the European Union? Is this threat significant at all, or is it marginal? In my study, I will try to find answers to these questions.

[9] Homepage of the EU vs Disinfo. About. URL: https://euvsdisinfo.eu/about/. [1-10-23]

5. Research Gap

There are numerous research projects regarding propaganda and disinformation, also available are papers analysing all kinds of aspects of the European Union's Common Foreign and Security Policy and its Common Security and Defence Policy. Some case studies and research projects have also been conducted concerning Russian disinformation campaigns. However, these studies were conducted before the Ukrainian War, focusing mostly on the impact of disinformation on society. It is also worth noting that, since the outbreak of the war, scholars have mostly been focusing on Russian disinformation directed against Ukraine and Western countries, and no recent research studied the effect of disinformation on CSDP missions. Therefore, an unfilled research gap can be found here. This space allows the author to analyse the dangers that Russian disinformation poses to CSDP missions and indirectly to the EU after the invasion of Ukraine.

The topic of disinformation has even more relevance nowadays than in the previous decade. As the Russian Federation invaded Ukraine, for a long time the first symmetric – the war quickly shifted from asymmetric to symmetric in the initial phase – and large-scale hybrid war broke out. Information warfare is strongly present in the war, regarding significance, it might even be on par with conventional warfare, i.e. the usage of military equipment and soldiers. These information operations require rapid and effective government countermeasures to minimise the damage they might do. Cooperation among the states, the EU and partnership countries could also help on the one hand to detect manipulated information and, on the other hand, to increase the resilience of the European societies.

6. Research Question

So what dangers does disinformation pose to the European Union, specifically to the Common Security and Defence Policy? Are disinformation campaigns dangerous to the stability of Europe, or rather they pose a marginal threat and therefore the EU should not be concerned? I reckon that disinformation poses a significant threat to CSDP missions, they can easily undermine the efforts of the European Union. The topic was broken down into two separate parts in the research, which both try to find answers regarding the subject from slightly different approaches. The first is more general answering the first question, whereas the second presents a case study answering the further two questions.

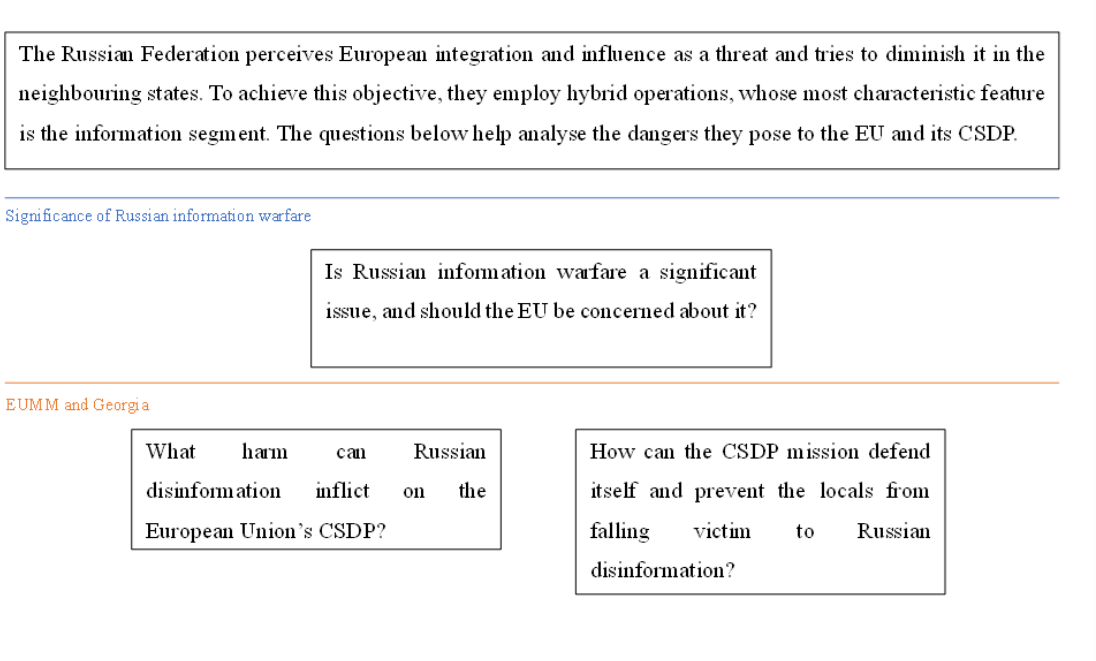

Figure 1: The segments of the research and their respective research questions[10]

[10] Figure created by the author

7. Methodology

To describe the state of the art, an in-depth search was conducted online, from where the necessary information was collected. Methodologically the research is based on qualitative techniques of analysis, such as record keeping – including document and content analysis, – and case study research. To make a theoretical analysis, first I collected a fairly large selection of literature, of which the main sources are internet-based articles, reports, datasheets and documents authored by the European Union, scholars affiliated with the Union, and researchers studying the EU, its external relations and Russian disinformation. I used both primary and secondary sources – published in the official languages of the European Union, including English and Hungarian language, and also Georgian sources – to write this paper. I collected literature from both before and after the Russian invasion of Ukraine on 24 February 2022, as the war shifted the attention of many scholars to Ukraine from other focal points of the neighbouring regions.

The collected information was used to determine whether my hypothesis set out earlier, i.e. disinformation poses a rather significant threat to the European Union, is true or not. The research questions and their answers helped in the process of proving that the issue is real and nowadays it is more relevant than ever before.

8. Research and Result of Research

The Common Foreign and Security Policy is the foreign policy of the EU when its external actions are related to security, trade and commerce, or aid. Even though it originates from the European Political Cooperation, CFSP was established in the Maastricht Treaty in 1993, as the second of the three pillars of the European Union. Its main tool, the Common Security and Defence Policy, was introduced into the framework of CFSP in 2009, with the Treaty of Lisbon.[11] With CSDP, the EU can deploy military and civilian missions to prevent conflicts, maintain peace and increase international security under the principles laid down in the United Nations Charter. These principles are impartiality, non-use of force except in self-defence and defence of the mandate, and consent of the parties.[12] Russia's anti-Western narrative has some influence in certain countries in Europe, and in the 21st century, the Federation has been launching hybrid operations in the continent and the surrounding regions.

8.1. The Hybrid Operations of the Russian Federation, and the Significance of its Information Segment

Nowadays most of the conflicts are hybrid wars, however, the term rose to prominence and became mainstream after the Russian annexation of Crimea in 2014. "Hybrid warfare" does not have an internationally accepted and exact definition, its contents are also subject to different approaches. Previously, I presented the domain-oriented approach, next, I will present the tool-oriented approach. Initially, it was believed that non-state actors employed it by using conventional and non-conventional means of warfare simultaneously with non-military modes of operations. The non-military modes can be horizontally expanded, which would allow the weaker, non-state actor to gain asymmetric advantages over the militarily superior (state) actor. In the case of the non-

[11] Homepage of the European External Action Service. The shaping of a Common Security and Defence Policy. URL: https://www.eeas.europa.eu/eeas/shaping-common-security-and-defence-policy_en. [12-10-23]

[12] Homepage of the United Nations Peacekeeping. Principles of Peacekeeping. URL: https://peacekeeping.un.org/en/principles-of-peacekeeping#:~:text=Consent%20of%20the%20parties,-UN%20peacekeeping%20operations&text=This%20requires%20a%20commitment%20by,carry%20out%20its%20mandated%20tasks. [12-10-23]

state actor, within the horizontal expansion, the most frequent tools are coordinated terrorism and organised crime.

In contrast, a state actor employing hybrid warfare has access to all military and non-military means of state power. States can coordinate and synchronise their instruments of power, which has a synergistic effect. The Russian operations in 2014 and the annexation of Crimea perfectly demonstrated this synergistic effect and resulted in labelling Russia a state employing hybrid warfare.[13] The means of state power can be escalated and de-escalated on a horizontal and a vertical axis, with the former meaning synchronisation among the tools, and the latter adjusting the intensity of the deployed tools.

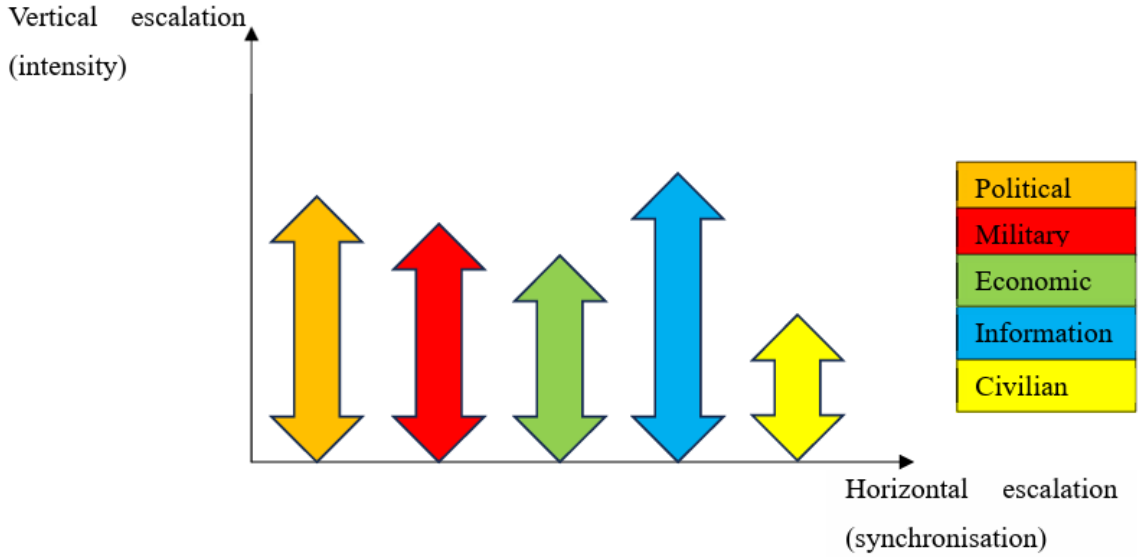

Figure 2: Employment of hybrid warfare if the contents are means of state power[14]

Russian hybrid warfare is characterised by its covert and minimalised use of military force. Instead, they prefer the use of the information segment (e.g. cyberattacks and information campaigns) instead of the deployment of the military. Numerous agents contribute to these operations, including Russian media outlets, bribed European think tanks, Internet trolls, bots and cybercriminals. The most significant pro-Russian media outlets are the state-funded RT (formerly Russia Today), Sputnik News and TASS,

[13] Reichborn-Kjennerud, Erik & Cullen, Patrick. (2016). What is Hybrid Warfare? Oslo. Research Report. Pp. 1-2.

[14] Figure created by the author based on Reichborn-Kjennerud, Erik & Cullen, Patrick. (2016). What is Hybrid Warfare? Oslo. Research Report.

however, the Yevgeny Prigozhin-founded Glavset should also be mentioned here.[15] The Russians try to shape the political discussion to fit the Kremlin's needs and make targeted people question even objective truths. They are most successful in countries with weak legal and anticorruption measures, though, post-Soviet states and demographic groups that share views identical to Moscow's are also in danger.

Russian information warfare, besides using its cognitive capabilities, employs technical capabilities, such as the physical destruction of critical infrastructure and cyberattacks. From the past decade, one could cite quite a large number of Russian information operations that had profound impact. First among the most significant: the 2014 annexation of Crimea, where the "little green men" emerged and Russia had nothing to do with the events occurring on the peninsula until the secessionist referendum in March. Next, during the 2016 US election, Glavset[16] was conducting an information campaign on Twitter in favour of Republicans. These Russian-related tweets caused great concern and became widely documented by researchers and government investigators. However, only a little more than 1% of the American population was exposed to them, and most of this exposure was concentrated among Republican voters.[17] Finally, the most used cyberattacks are ransomware attacks, which have been conducted against numerous hospitals lately. During the fall of 2020, numerous American hospitals were hit by ransomware attacks. The attacks encrypted data stored on the computers and the hospital temporarily had to cancel patient care and several surgeries. Therefore, these ransomware attacks may cause serious harm to people, even death. Russia also targets Europe; in the same year in Germany, a woman died because the hospital she visited for emergency care suffered a ransomware attack.[18]

To conclude this chapter, Russian hybrid warfare and its information segment pose a significant threat to Western societies, which cannot be marginalised. They try to

[15] S. Chivvis, Christopher. (2017). Understanding Russian "Hybrid Warfare". Santa Monica. Testimony Report. Pp. 2-5.

[16] Following the Wagner group rebellion of June 23-24, Glavset was dissolved in July after 10 years of engaging actively in information warfare.

[17] Eady, Gregory 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 behavior. Nature Communications. Volume 14. No. 62/2023. Pp. 2-5.

[18] Nakashima, Ellen & Greene, Jay. (2020). Hospitals being hit in coordinated, targeted ransomware attack from Russian-speaking criminals. Washington D.C. The Washington Post as of 29-10-20. Item.

influence and deceive Western societies, they try to shape narratives to match Moscow's (e.g." Russia is the sole guardian of Christianity and traditional values"), and they are not afraid of launching cyberattacks (e.g. recent ransomware attacks) on Western-aligned countries' institutions that cause serious harm or even death.

8.2. The Russian Disinformation in Georgia, and its Impact on the European Union Monitoring Mission in Georgia

The EUMM Georgia, launched in 2008, is an unarmed civilian monitoring mission, which aims to maintain peace and stability and to ensure that hostilities do not return in Georgia.

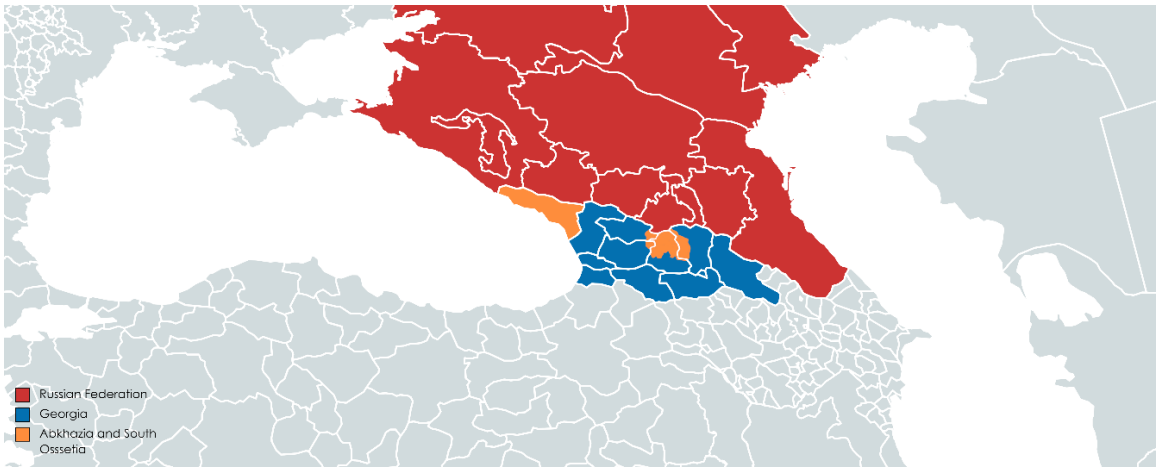

Figure 3: Map of Georgia with Abkhazia and South Ossetia highlighted. They are considered as Georgia, however, they are Russian protectorates currently. The 2 Russian proxy states deny the EUMM access to their territories and frequently participate in Russian disinformation campaigns.[19]

It faces fewer attacks than the EU Delegation in Georgia, however, during the Covid-19 pandemic it was frequently accused of violating the principle of impartiality and having malicious intent towards the separatist states. Russia frequently launches disinformation campaigns in Georgia, intending to increase its influence and diminish the support for Euro-Atlantic integration among the Georgian population. To achieve this, they also target other institutions and events related to the EU or the US, to prove that the West is a threat to Georgian traditions and culture.[20]

[19] Figure created by the author.

[20] Fridman, Ofer & Baudais Virginie & Gigitashvili Gigi. (2023). Enhancing the capabilities of CSDP missions and operations to identify and respond to disinformation attacks. European Parliament coordinator: Policy Department for External Relations, Directorate-General for External Policies. Research Study. Passim.

In 2012 the political space was opened for pro-Russian political parties, NGOs and media outlets in Georgia to ease the tension between the two states. This allowed the previously banned pro-Russian political parties and media outlets to return to the political discourse. Georgian leaders hoped for the normalisation of the countries' relations and Russia's friendly treatment, however, the attacks continued in three tiers: borderisation, cyberattacks and lastly, disinformation. [21] There are multiple topics, claims and sources of disinformation, however, they always share a common, anti-Western narrative. The most frequent ones are shown below in the table.

Source	Subject	Claim
Russian Federation, Separatist KGB, Russian media outlets, Georgian media outlets	Lugar Research Center	The Lab is developing bioweapons, is violating the BWC, is experimenting on humans
Political parties, Russian media outlets	Syrian refugees and EU	The EU integration would oblige Georgia to provide settlement for Syrian refugees
Russian Federation, Georgian media outlets	Turkey and NATO	NATO membership would cause Turkish military deployment and base establishment in Georgia
Separatist KGB, Russian media outlets	Provocative and malicious actions of the EUMM	The EUMM helps Lugar Lab to carry out a genocide of South Ossetians, supports Georgian reconnaissance over South Ossetia, and insulted South Ossetia in 2020

Table 2: The disinformation campaigns. Disinforming actors are all closely tied to the Russian Federation (which is also present as an actor). The most frequently attacked subject is the American-Georgian Lugar Research Center, which has been accused of having committed numerous crimes.[22]

The Lugar Lab has been under attack since its foundation in 2013. Among the most frequent allegations, violations of the Biological Weapons Convention and the development of insects as biological weapon carriers can be found. The claims turned out to be false according to a group of experts from 17 countries, who examined it during an

[21] Machurishvili, Nino. (2021). Prospects of the EU's Common Foreign and Security Policy and Russia's Disinformation Campaign in the South Caucasus. Studia Europejskie – Studies in European Affairs. Volume 25. No. 1/2021. P. 141.

[22] Table created by the author

international inspection. [23] Russia did not participate in it, claiming it to be a Georgian-staged, propaganda act to hide their true intentions. This disinformation campaign tries to create distrust against the US and its allies, claiming that they are carrying out experiments in secrecy that are dangerous to the Georgian population.

Syrian refugees became the subject of disinformation in 2017, after former Austrian foreign minister, Sebastian Kurz, speculated about establishing refugee camps in the migration pathways, including Georgia. Pro-Russian politician, Davit Tarkhan-Mouravi commented that Georgia is not an ideal place for refugees, which indicated that Kurz's theory is the official EU standpoint.[24] Sputnik and pro-Russian media outlets in Georgia reiterated that increasing connections with the West would require Georgia to accept refugees from the Middle East and North Africa. This story relates to Georgian poverty, internally displaced people and fear of immigration.[25]

The third campaign is the simplest; it claims that if Georgia becomes a NATO member, Turkey will deploy soldiers and establish a military base on Georgian soil. This builds on the Georgian fear of Turkish intervention and the tension between them in the past.[26]

The EUMM was also the subject of campaigns, however, they were usually ad hominem attacks or too unrealistic claims. The most ridiculous stories range from the EUMM helping in carrying out a genocide through not noticing machinegun fire on the administrative boundary line to providing unmanned aerial vehicles to Georgia to carry out reconnaissance activities on KGB and FSB positions. The genocide story emerged during the COVID-19 pandemic together with the good old Lugar Lab narrative.[27]

In summary, Russians are threatening the EU and its CSDP, but in this case not directly. Rather, they try to diminish the support for the integration and the EUMM. As countermeasures, the EUMM visited the locals and made public statements rebutting

[23] Gamkrelidze, Tamar. (2022). Georgia's external frontier on Russia sedimented and unmalleable: engagement politics and the impact of the three-tier warfare. Journal of Contemporary European Studies. Volume 31. No. 2/2022. Pp. 547-548.

[24] Homepage of Ipress. Tarkhan Mouravi: Iseti Gantsda Makvs, rom Sebastian Kurtsis ar Esmis Ra Vitarebaa Sakartveloshi. URL: https://ipress.ge/news/politika/tharkhan-mouraviisethi-gan. [25-10-23]

[25] Homepage of Migreurop. Georgia. URL: https://migreurop.org/article2195.html?lang=fr. [26-10-23]

[26] Clem, Ralph S. & Herron, Erik S. & Tepndaze, Ani. (2023). Russian Anti Western Disinformation, Media Consumption and Public Opinion in Georgia. Europe-Asia Studies. DOI: https://doi.org/10.1080/09668136.2023.2220997. Pp. 12-14.

[27] Fridman, Ofer & Baudais Virginie & Gigitashvili Gigi. (2023). Op. Cit. Pp. 9-11.

Russian disinformation. However, they should engage the locals in every channel, including television broadcasts, as they are the most significant media sources in Georgia.

9. Discussion of Results and Personal Conclusions

Russian information operations are dangerous; their cognitive capabilities pose a threat to post-Soviet states with weak anticorruption measures, parts of societies and demographic minorities that can relate to Russian narratives. In contrast, technical capabilities pose a threat to Western states too, as they often target government websites and critical infrastructure (such as hospitals, transportation systems and energy generation). The disruption of these systems causes physical harm and death.

	Russian information operations			
Conducted against	Cognitive capabilities (e.g. disinformation)	Expected result	Technical capabilities (e.g. cyberattacks)	Expected result
Governments	✓	Creating distrust against the government	Distributed denial-of-service attack, phishing, malware, data breach	Overwhelming the government's branches' administrative networks and intranets, stealing, leaking and selling confidential information
Public service websites of the government	×		Distributed denial-of-service attack	Overwhelming the public service websites, so the administrative features and information become unavailable
Media outlets	✓	Creating distrust against the media outlet	Distributed denial-of-service attack, malware	Overwhelming the system to suspend the broadcasts of the media outlet or completely destroy the network's system and bring it off the air
Critical infrastructure	×		Distributed denial-of-service attack, ransomware, malware	Disrupting critical systems, encrypting vital information and demanding ransom payment to make it available, destroying systems to harm the state and its population

CSDP missions	✓	Discrediting CSDP missions	Distributed denial-of-service attack	Overwhelming the missions' networks, so they cannot function properly and the missions become less effective
Population (Western)	✓	Creating distrust against minorities of the society	Crimeware, cryptojacking, phishing, rootkit, data scraping, email frauds	Stealing people's information, money, personal computers, identities, inducing fear in them
Population (Western-aligned)	✓	Creating distrust against minorities of the society, Proving that alignment to Russia is better than alignment to the West		

Table 3: The most used Russian information operations and their possible results[28]

As it turned out, the EUMM is not frequently attacked by pro-Russian agents, in contrast to other Western-aligned institutions, such as the Lugar Research Center. However, the Russian disinformation campaigns are concerning as their principal and common goal is to diminish the Georgian support for Euro-Atlantic integration. Success would mean that Georgians lose their trust in Euro-Atlantic institutions and missions, resulting in the termination of the CSDP mission as the mandate cannot be extended without the consent of Georgia. This would affect rather negatively the European Union's reputation.

According to a survey from 2019, television broadcasts are the dominant source of information among the Georgian population, so pro-Russian disinformation campaigns are frequently disseminated through them. The fact that Georgians prefer television as an information source over the Internet was a significant surprise for me. After I had become aware of it, I immediately thought that television could be the missing link; if Georgians

[28] Table created by the author based on the research and the used literature

prefer TV, then the official CSDP website cannot be more efficient than rebutting Russian disinformation through Georgians' favourite source, the television itself.

It was only at the end of writing the essay that I found an excellent, Georgian-authored research paper that provided more information on the television's success over the Internet and explained that, although Georgians strongly support Euro-Atlantic integration, their knowledge and experience about the EU is minimal. Often not knowing official sources of the EU, they become particularly vulnerable to Russian disinformation.[29] It also advises Georgian leaders to use the medium of television for countering pro-Russian disinformation.

This topic was rather new for me as I had known only the basics of information warfare, but it had importance for me. It might seem evident that Russian information warfare is dangerous to European countries, however, in Hungary, many people are unaware of it, because of the lack of strategic communication and knowledge regarding the topic.

There is space for me to develop in information warfare against post-Soviet countries, and this research could be continued as well, updated with disinformation campaigns after the 2022 Ukrainian War, or even the 2023 Israel-Hamas War, however, I am not planning on doing so. Instead, I consider examining whether Russian information operations against Italy exist and what their characteristics are.

[29] Panchulidze, Elene. (2017). Russian Soft Power: Balancing the Propaganda Threats and Challenges. Georgian Institute of Politics. Research Study. Pp. 14-16.

10. Annexes

10.1. List of Abbreviations

BWC – Biological Weapons Convention

CFSP – Common Foreign and Security Policy

CSDP – Common Security and Defence Policy

EEAS – European Union External Action Service

EU – European Union

EUGS – European Union Global Strategy

EUMM – European Union Monitoring Mission in Georgia

FSB – Federal Security Service (Federal'naya Sluzhba Bezopasnosti Rossiyskoy Federatsii)

KGB – Committee for State Security (Komitet Gosudarstvennoy Bezopasnosti)

NATO – North Atlantic Treaty Organisation

NGO – Non-Government Organisation

10.2. List of Figures

10.3. List of Tables

10.4. List of Literature

1. *About* (no date) *EUvsDisinfo*. Available at: https://euvsdisinfo.eu/about/ (Accessed: 1 October 2023).

2. Chivvis, C.S. (2017) *Understanding Russian*. RAND Corporation. Available at: https://www.rand.org/pubs/testimonies/CT468.html (Accessed: 16 October 2023).
3. Clem, R.S., Herron, E.S. and Tepnadze, A. (2023) 'Russian Anti-Western Disinformation, Media Consumption and Public Opinion in Georgia', *Europe-Asia Studies*, pp. 1–25. Available at: https://doi.org/10.1080/09668136.2023.2220997.
4. Cullen, P. *et al.* (2021) *The landscape of Hybrid Threats: A Conceptual Model (Public Version)*, *JRC Publications Repository*. Available at: https://doi.org/10.2760/44985.
5. Eady, G. *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 behavior', *Nature Communications*, 14(1), p. 62. Available at: https://doi.org/10.1038/s41467-022-35576-9.
6. Frankland, N. (no date) *Donald Trump takes credit for 'fake news', dictionary disputes*. Available at: https://thenewdaily.com.au/news/world/2017/10/09/donald-trump-fake-news/ (Accessed: 30 September 2023).
7. Fridman, O., Baudais, V. and Gigitashvili, G. (2023) 'Enhancing the capabilities of CSDP missions and operations to identify and respond to disinformation attacks'.
8. Gamkrelidze, T. (2023) 'Georgia's external frontier on Russia sedimented and unmalleable: engagement politics and the impact of the three-tier warfare', *Journal of Contemporary European Studies*, 31(2), pp. 536–555. Available at: https://doi.org/10.1080/14782804.2021.2023485.
9. Jakusné Harnos, É. (2020) 'Fake News and Social Media as Security Risks'.
10. Machurishvili, N. (2021) 'Prospects of the EU's Common Foreign and Security Policy and Russia's Disinformation Campaign in the South Caucasus', *Studia Europejskie - Studies in European Affairs*, 25(1), pp. 127–145. Available at: https://doi.org/10.33067/SE.1.2021.6.
11. MIGREUROP (2023) *Georgia*, *MIGREUROP*. Available at: https://migreurop.org/article2195.html (Accessed: 26 October 2023).
12. Nakashima, E. and Greene, J. (2020) 'Hospitals being hit in coordinated, targeted ransomware attack from Russian-speaking criminals', *Washington Post*, 29 October. Available at: https://www.washingtonpost.com/national-security/hospitals-being-hit-in-coordinated-targeted-ransomware-attack-from-russian-speaking-

criminals/2020/10/28/e6e48c38-196e-11eb-befb-8864259bd2d8_story.html (Accessed: 16 October 2023).

13. Panchulidze, E. (2017) 'Russian Soft Power: Balancing the Propaganda Threats and Challenges'. Available at: https://gip.ge/publication-post/russian-soft-power-balancing-the-propaganda-threats-and-challenges/.
14. Prier, J. (2017) 'Commanding the Trend: Social Media as Information Warfare', *Strategic Studies Quarterly*, 11(4), pp. 50–85.
15. *Principles of peacekeeping* (no date) *United Nations Peacekeeping*. Available at: https://peacekeeping.un.org/en/principles-of-peacekeeping#:~:text=Consent%20of%20the%20parties,-UN%20peacekeeping%20operations&text=This%20requires%20a%20commitment%20by,carry%20out%20its%20mandated%20tasks. (Accessed: 12 October 2023).
16. Reichborn-Kjennerud, E. and Cullen, P. (2016) 'What is Hybrid Warfare?', *4 p.* [Preprint]. Available at: https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2380867 (Accessed: 15 October 2023).
17. Schreck, C. (17:01:50Z) 'From "Not Us" To "Why Hide It?": How Russia Denied Its Crimea Invasion, Then Admitted It', *Radio Free Europe/Radio Liberty*. Available at: https://www.rferl.org/a/from-not-us-to-why-hide-it-how-russia-denied-its-crimea-invasion-then-admitted-it/29791806.html (Accessed: 30 September 2023).
18. *Tarkhan Mouravi: Iseti Gantsda Makvs, rom Sebastian Kurtsis ar Esmis Ra Vitarebaa Sakartveloshi* (2017). Available at: https://ipress.ge/news/politika/tharkhan-mouraviisethi-gan (Accessed: 25 October 2023).
19. *The Real Story of 'Fake News'* (no date). Available at: https://www.merriam-webster.com/wordplay/the-real-story-of-fake-news (Accessed: 24 August 2023).
20. *The shaping of a Common Security and Defence Policy | EEAS* (no date). Available at: https://www.eeas.europa.eu/eeas/shaping-common-security-and-defence-policy_en (Accessed: 12 October 2023).

11. Affidavit

I declare that I have written the present essay independently and on my own. I have clearly marked any language or ideas borrowed from other sources as not my own and documented their sources. The essay does not contain any work that I have handed in or have had graded as a previous scientific paper earlier on.

I am aware that any failure to do so constitutes plagiarism. Plagiarism is the presentation of another person's thoughts or words as if they were my own – even if I summarise, paraphrase, condense, cut, rearrange, or otherwise alter them.

I am aware of the consequences and sanctions plagiarism entails. Among others, consequences may include nullification of the essay, exclusion from participation in the CSDP Olympiad. These consequences also apply retrospectively, i.e. if plagiarism is discovered after the essay has been accepted and graded. I am fully aware of the scope of these consequences.

Signature

……

Áron Bálint,

Budapest, Hungary in November 2023