MASTER'S THESIS

Course code: SO330S

Name: Gjelsten, Trude Marielle

Russian Influence Operations on Social Media in Ukraine

Date: May, 18th, 2022

Total number of pages: 84

NORD University

www.nord.no

Acknowledgments

Denne masteroppgaven setter punktum for fem år som student ved Nord universitet. Det siste året som masterstipendiat hos Stabsskolen ved Forsvarets høyskole. Det har vært spennende og nyttig å få en dypere forståelse av Russlands komplekse bruk av sammensatte virkemidler i krig og fred. Ikke minst hvordan Russland har brukt sosiale medier til å påvirke et samfunns holdninger, og hvordan Ukraina har håndtert disse utfordringene.

Mine to år som masterstudent har vært preget av pandemi og digitale undervisninger. Jeg skal ikke undervurdere at dette har vært to krevende, men også lærerike år. Jeg er stolt av at vi likevel fikk til å danne et lite studentmiljø. Takk til mine medstudenter, og min lille kollokviegruppe, for at vi sammen gjorde en usosial studenttilværelse litt bedre.

Videre vil jeg takke veilederen min, Kristian, for å ha ledet meg igjennom en krevende oppgave. Du har vært eksepsjonelt rask og svare på mail, hjulpet meg ut av administrative «krisesituasjoner», og en faglig tyngde og nøyaktighet jeg ikke ville vært foruten. Tusen takk.

Jeg har også vært heldig å få delta i prosjektet «Total Defence Cooperation with Ukraine» ved Stabsskolen. Dette har gitt meg unike muligheter og erfaringer som har bidratt til å løfte oppgaven min. Takk til Tom, for at jeg har fått være masterstipendiat ved prosjektet, og for mulighetene til å reise til Kyiv for å delta på konferanse, danne nettverk og gjøre intervjuer.

Gjennom masteroppgaven har jeg stiftet nye bekjentskaper, venner og gode kollegaer ved Forsvarets Høyskole. Et spesielt takk til kolleger som har brukt timene deres på å lese igjennom og gi gode tilbakemeldinger på oppgaven min.

I would also like to thank all my participants and my colleagues at the National Defence University of Ukraine. Thank you for being welcoming, helpful, and open-minded. Even through challenging times after the Russian re-invasion in Ukraine, you have taken your time to answer my questions. I am looking forward to meeting you all again.

Til sist vil jeg rekke en stor takk til familie og venner. Det er uvurderlig å ha så fine mennesker i ryggen, som heier på meg selv når tiden mellom besøk og kontakt blir lang. Takk for at dere er der.

Trude Marielle Gjelsten. Akershus Festning, 18. mai, 2022.

Abstract

Before and during the war in Donbas, which started in 2014, Russia has actively used influence operations on social media to change the perception of the population in the counties of Donetsk and Luhansk. Ukraine has since 2014 fought an information war, trying to defend itself against Russian aggression and counter Russian propaganda. This study focuses on Ukrainian countermeasures to Russian influence operations on social media. It also discusses whether and how Norway can learn from Ukraine's experiences.

Russian actors have used different methods to reach the targeted audiences in the non-government-controlled areas of Donetsk and Luhansk. Automated bots to spread information at high speed to many people and trolling to reach into people's minds and create tension and polarization in discussions are among the methods used. The Russian social media platforms Vkontakte (VK) and Odnoklassniki (OK), which were the two most popular platforms in Ukraine in 2014, were owned by a Kremlin-friendly oligarch. The Russian security service, FSB, gained access to personal information that people had published on these platforms.

My findings indicate that countering Russian influence operations is about limiting the exposure as well as educating the citizens to be critical of information on social media. The Russian dissemination of disinformation on Vkontakte and Odnoklassniki was extensive before and after 2014, and the content was targeted to touch people's emotions. In the non-government-controlled areas (NGCA), the population was easily attracted because of a high number of people speaking Russian and identifying as Russians. The territory was also largely severed from the rest of Ukraine after the establishment of the "people's republics".

Despite its long-standing desire to adhere to the principle of media freedom, Ukraine decided in 2017 to block the pages of Vkontakte and Odnoklassniki, which gave an immediate effect. The challenges of bots and trolls were harder to counter, and it seems that Russia still has the capacity to build up new botnets and troll farms when one is found and closed. In this case, educating the citizens is important to keep the level of attraction low.

Citizens in Norway are generally aware of the risk of being exposed to disinformation on social media, and the extent of Russian influence operations on social media platforms in Norway has been relatively low. However, the today's situation, where Norway has taken a clear position in support of Ukraine, Russia may attempt to create disorder in Norway using such means. The Ukrainian failure to face the Russian information war in 2014 illustrates the importance of being prepared and able to counter such attempts.

Index

Figures

1.0 Introduction

Since 2014, Ukraine has been Russia's playground for trying out new tools and hybrid methods of warfare. During the Russian annexation of Crimea and the Russian-backed war in Donbas, Ukraine experienced a Russian invasion with a compound use of "little green men," cyber-attacks, influence operations in media and social media, and regular warfare. Well before the Russian annexation of Crimea and the start of the war in Donbas in 2014, Russia influenced the citizens of Ukraine through different types of media and social media. After the Euromaidan protests in the winter of 2013–2014, the Russian influence operations became more aggressive, and the Ukrainian society and government turned their focus to Russian disinformation and propaganda. Russian influence operations on social media in Ukraine, and Ukraine's countermeasures against them, became something other countries could watch and learn from. The Russian influence operations became a source of knowledge about the modern type of warfare, and Ukraine became an arena for experts to observe.

The internet has brought many new opportunities; among them is social media. The social networks that developed with the internet have given us access to keep contact with family and friends worldwide. We can receive live information about what is happening around the world, no matter the distance. We can cooperate worldwide to find solutions to regional and global challenges or join social groups with equal interests and values. Access to social media also brings us challenges. Social networks are also accessible to criminals and actors with hostile intentions. The "weaponization" of social media creates challenges like influence operations, online criminal groups, and mobilization to violent events.

Social media was an effective platform for Russian influence operations during the conflict in Ukraine in 2014. Russia and Russian actors collected personal information from Ukrainians through social media, spread anti-Ukrainian disinformation, and recruited people to violent actions. By influencing and gaining personal information about Ukrainians on social media, the aggressors could target specific audiences by specifying the information campaigns and the narratives and creating polarization and disorder.

Social media allows the aggressor to spread information at high speed to many people. Russia and Russian actors utilized this opportunity to influence Ukrainians and the international society through various means. One commonly used means are bots, automated accounts created by algorithms, similar to typical 'chatbots.' Especially on Twitter, bots have been very active because of the easy access to accounts on the platform. Another means often used is

trolls, who, unlike the bots, are real people that seek to get into the targeted audiences' interests and feelings. Trolls aim to create discussion, polarization, and disorder.

1.1 Research question and main findings

This study seeks to find out if Ukraine managed to counter Russian influence operations on social media at the time of the dramatic events in 2014, and if it is relevant to Norway. How did Ukraine identify such operations? How are they carried out, and how did Ukraine counter them? And what can Norway learn from Ukraine's experiences with Russian influence operations on social media? In short, the purpose of the study is to answer the following research question: ***Did Ukraine manage to counter Russian influence operations on social media in 2014, and is it relevant for Norway?***

My findings indicate that Ukraine had significant challenges in countering the information war in the first part of 2014. The biggest challenge was in the non-governmental areas (NGCA) that include the territory of the self-proclaimed "the people's republics," of Donetsk (DNR) and Luhansk (LNR). This territory is still challenging today, as there are many limitations to getting through with Ukrainian information to the people living there. In an effort to debunk and disprove Russian disinformation to defend Ukraine against Russian aggression on social media, the Ukrainian civil society stepped up. However, debunking and disproving fakes turned out to be ineffective. The strategy changed to lower the exposure of Russian influence information and educate the targeted audience to reduce the level of attraction among the citizens.

Joseph Nye's "soft power" theory may shed light on this strategy. He explains that soft power is about the level of attraction. Ukraine had to lower the Russian actors' ability to attract the targeted audience in order to succeed in the information war. Starting to be preventive in the information security sphere strengthened the Ukrainian military and civil society prior to the Russian re-invention in Ukraine on February 24th, 2022. The Ukrainian experience gives the world a pointer to not underestimate the importance of information security on social media.

This study aims to contribute to the already existing research literature on how Russia has used, uses, and may be using social media as a method of hybrid warfare to influence a target audience. The research might also be helpful for other actors who want to strengthen their defense against Russian influence operations on social media.

1.2 Structure and limitations of the thesis

The thesis is divided into six chapters. Chapter one introduces the topic as well as the research question and the main findings of the thesis. The chapter also draws up the boundaries of the study and explains the rationale behind my choice of time frame and geographical focus area.

Chapter two provides some background information about the Ukrainian media landscape, Russia's capabilities in the field of influence operations, and the environment in which such operations take place. The chapter also gives an overview of previous research on the topic.

Chapter three examines the methodological foundations for the research. The chapter presents details about the research method, data collection, validity, and reliability. It also discusses some ethical concerns that I had in connection with my interviews in Ukraine.

Chapter four presents the theoretical perspectives for the thesis. First, it presents the theory of power by Joseph Nye. Second, it explains the theory of hybrid warfare and the weaponization of social media.

Chapter five discusses central issues related to the conduct of Russian influence operations on social media. The chapter consists of four parts: (1) the target audiences of Russia's influence operations on social media in Ukraine, (2) the Russian narratives on social media, (3) the Russian social media platforms, Vkontakte and Odnoklassniki, and lastly, (4) the challenge of bots and trolls on social media.

Chapter six examines the Ukrainian countermeasures and lessons learned. The first parts, which investigate the Ukrainian countermeasures, are 1) education and information, 2) debunking and disproving fakes, 3) the Russian social media platforms Vkontakte and Odnoklassniki, and 4) closing botnets and troll farms. The last part is about lessons learned.

Chapter seven will shed light on the question to what extent Ukraine's experiences are relevant for Norway. It will give an overview of what factors should be considered in the context of the Norwegian total defense concept.

Chapter eight presents the conclusions of the study. It also summarizes the main findings of the research, limitations, theoretical and empirical contributions, and offers suggestions for further research.

1.3 Limitations

The limitations that should be considered are, first and foremost, the limitations of time and place. My time limitations are between the war that started in Donbas in April 2014 and 2017.

When the war started, the primary focus of the Ukrainian government was on the war on the ground. By limiting my time until 2017, the research can also focus on the measures taken by Ukraine's government. The limitations in time provide the discussion with Ukraine's development in countermeasures in the information war and contribute to the research with important factors of "lessons learned" in countering Russian influence operations.

The territorial focus is limited to the NGCA in Ukraine. These territories are in the Donbas region in eastern Ukraine, more specified, the so-called "Donetsk Peoples Republic" (DNR) and "Luhansk Peoples Republic" (LNR). It is essential to clarify that Russia has recognized DNR and LNR borders, but the territories are not internationally recognized as sovereign republics (Regjeringen, 2022b)

I have chosen the limitations in space to the NGCA because Ukraine had significant challenges countering Russian influence operations in this territory. The consequences of this challenge are important experiences and learning that should be put on the agenda and can be helpful for other countries who want to strengthen the defense against Russian influence operations on social media. In the last part of the research, I will raise my eyes to draw some lines from the Ukrainian experience to today's situation and its relevance to Norway.

A vulnerability of limiting my research to the targeted audiences in the NGCA is that researchers and Ukraine's Government have challenges to collect data from people in this territory. Questions that arise are whether the data is trustworthy and if enough people answer the polls. Another challenge is technology. The Russian jamming makes sure that the government, the media houses, and the social media does not know how many people received certain information the government or the media want to put out.

This research does not analyze Ukraine´s strategic communication for countering Russian influence operations on social media. There are two reasons for this. First, a master's thesis has limitations in time. Analyzing strategic communication (StratCom) would be too complex and time-consuming to consider in this thesis. Second, studying Ukraine's StratCom would have required access to data I cannot access because of the ongoing war in Ukraine or classified information. This aspect should be taken into consideration while reading the study.

I will investigate Ukrainian countermeasures due to the Russian social media platforms Vkontakte (VK) and Odnoklassniki (OK). The two social media platforms were among the most popular in Ukraine before they got blocked by the Ukrainian government in 2017 and created an excellent arena for Russian influence operations. An expert in information security

claims that VK and OK are the best examples of Russian influence operations on social media in Ukraine; “Actually, the best example is the existence of two different networks, Vkontakte and Odnoklassniki. (..) it was definitely under the control of Russian special agency. So, they control everything.” (Interview: 1, 2022). The last chapter will consist of a summary and a conclusion.

2.0 Background

In this chapter, I will present the background for the Russian use of influence operations in social media as a tool of hybrid warfare. First, I will present the relationship between Ukraine and Russia. Second, I will present the Russian capabilities regarding influence operations on social media in Ukraine and the Ukrainian resilience to counter these influence operations. Last, I will present previous research on Russian influence operations in social media.

2.1 Language and identity

After the Soviet Union collapsed and Ukraine became a sovereign and independent country, Ukraine was one of the former Soviet countries where conflict did not break out (Kudelia, 2016, p. 5). At that time, identity was not a big issue among Ukrainians (Interview: 5, 2022). According to Matveeva (2016, p. 25), the foundation of polarization before the war in 2014 was created in line with the cultivation of the Ukrainian identity and language. The Russian language decreased in both educational and public spheres due to a new language law, and the language became more politicized (Matveeva, 2016, p. 27).

In 2004, Viktor Yanukovych was elected president. The electoral process was blamed by many as electoral fraud, and the Orange revolution broke out in December 2004 and lasted until January 2005. The Orange revolution resulted in re-election, where Viktor Yushchenko became the President of Ukraine, and the country became a parliamentary-presidential republic. (Kudelia, 2016, p. 6)

When Viktor Yushchenko was elected as the Ukrainian president in 2005, the 'Ukranization' intensified, and people in the Donbas region were concerned that the education of the Russian language would be taken away as it was the mother language to many people. "In a decade, 2001–2011, the number of Russian language schools in Donetsk oblast reduced from 518 to 176, with the process accelerating since 2004. In 2005, 29.5% of school children of Lugansk oblast studied in Ukrainian, in 2009 they made up 48.5%, although two-thirds of the population considered Russian as their native language", writes Matveeva (2016, p. 27). In higher education, the number of students enrolled in Russian language schools in the same region decreased from 75.7% in 2000 to 37% in 2013 (ibid, p. 27). Regarding the politicization of language in the public sphere, it created challenges for some people in public matters, like in courts or professions like law. According to Matveeva (2016, p. 27), the language law gradually excluded the Russian people from public space.

By the next election in 2010, Yanukovych won with a small margin, and the election was seen as legitimate (Kudelia, 2016, p. 6). In November 2013, the Euromaidan protests started as a

consequence of Yanukovych's decision to withdraw from the free-trade agreements Ukraine was about to sign with the EU. The agreement was set aside on behalf of a customs union between Russia, Belarus, and Kazakhstan (Sotiriou, 2016, p. 51). The Euromaidan protests were not peaceful as the Orange revolution, and about 100 people got killed in the protests. Yanukovych fled to Russia on February 22nd, just a few days before Russia's invasion of Crimea (Mearsheimer, 2014, pp. 4-5). The conflict escalated, and Russia that it had been a coup in Kyiv, supported by the West (Åtland & Hakvåg, 2014, p. 21).

In Donbas, the majority did not recognize the transfer of power to the opposition. In the oblasts of Donetsk and Luhansk, people established paramilitary units, and started a "quiet succession" as the "Peoples Republic of Donetsk" and the "People's Republic of Luhansk" (Kudelia, 2016, pp. 9-10; ibid, p. 13).

2.2 The Ukrainian media landscape

Ukraine did not have the same media and entertainment budget as Russia. Russia continued to dominate the entertainment business in Ukraine. Babak et al. (2017, p. 31) called the differences in the budgets an "unfair competition". According to Forbes, Russia's budget to support the media was 72 billion rubles in 2015 (Galaktionova, 2016). It was natural for Russian-speaking people to watch Russian TV channels (Matveeva, 2016, p. 28), and Ukrainians, independent of their mother tongue, used Russian social media and generally watched Russian entertainment channels.

The social media platforms Vkontakte and Odnoklassniki were two of the most popular social media in Ukraine (BBG, 2014). Vkontakte, meaning 'in contact,' was established as a Russian answer to Facebook and could offer free entertainment such as Russian movies, artists, stand-up shows, etc. VK was launched in 2006 and developed by Pavel Durov. In 2008, it got more popular than Odnoklassniki (Babak et al. et al., 2017, p. 62)

Odnoklassniki can be translated to Classmates, and the social network is developed to unite friends, find love and relatives, and discover job opportunities or professional growth. It was launched in March 2006 by Albert Popkov. OK started with 100 000 accounts which increased to 25 million accounts in 2008 when a mobile version also was launched. In the same year, it was also possible to make groups on the platform, e.g., uniting activists (Odnoklassniki, 2012).

In 2013 OK was ranked as the tenth most popular social network globally, just behind VK. The platforms had respectively 65.3 and 79.4 million users in the same year (Rozumiy, 2013).

According to a poll done by Telekritika in 2015, 8% trusted the information they got on social media, and 17% used it to gain information in the eastern regions of Kharkiv, Donetsk, Luhansk, Odesa, and Kherson (Dutsyk et al., 2015 p. 41). 25% used VK to get news in the same territory, 22% used OK, and 21% used the Western social media platform Facebook. 23% said they did not use social networks (ibid, p. 46).

In line with the Euromaidan protests, the Russian annexation of Crimea, and the Russian-supported war in Donbas, Russian influence operations on social media intensified and got more aggressive. Because of the increasing influence operations, the former Ukrainian President, Poroshenko, decided to block several Russian media, including VK and OK, in 2017 (Freedom House, 2017). The block of VK and OK happened after Ukraine already had banned Russian TV channels (Freedomhouse, 2017b).

The two Russian platforms were still, to some extent, popular among Ukrainians. But after the ban in 2017, the popularity of getting news from VK and OK in the east of Ukraine had decreased to respectively 12.2% and 6.8% in the Region. The popularity of Facebook increased to 35% (Grushetsky et al. 2018, p. 28).

2.3 Russian capabilities

This part will present the Russian capabilities to carry out influence operations on social media. Hybrid warfare implies the coordinated use of several methods of influence that amplify each other to reach a political objective. Hybrid methods blur the line between regular and irregular warfare methods (Kasapoglu, 2015, p. 1). Today, hybrid warfare has reached a new level. The lines between war and peace have blurred, and we see cyberattacks and influence operations being used on a larger scale during peacetime (Schnaufer II, 2017, pp. 20–21).

After the Russian annexation of Crimea and support for pro-Russian separatists in the Donbas region, there has been a greater focus and research on social media as a tool of hybrid warfare. Influence operations on social media played a crucial role during the annexation of Crimea and in the war in DNR and LNR (Demartino, 2021, p. 27).

In 2013, Durov sold out his part of VK. Durov's leaving was a direct consequence of FSB's demand that VK gives up data of the VK users (Babak et al., 2017, p. 63). VK became wholly owned by the Mail.ru group owned by the Putin-friendly Oligarch Alisher Usmanov. OK was also a part of the Mail.ru group. From December 2021, the platforms were sold to Gazprom bank, which is state-owned and controlled by Putin-friendly Yuri Kovalchuk (The Bell,

2021). VK and OK became capabilities where FSB could collect information published on personal accounts.

In addition to VK and OK, Russia uses bots and trolls as tools in influence operations on social media. Bots are automated social media accounts that employ code to replicate human activity to promote a particular message. *Botnets* use real people to monitor their social media accounts. Using real people to monitor the bot can make it easier to get the attention of other users (Helmus, 2020, pp. 153-154). A botnet consists of servers and employees who monitor and regulates the bots. The main purpose of the bots is to create disorder and spread disinformation. (Hurska, 2020).

In 2013, the most famous troll farm created by Yevgeny Prigozhin, also known as Putin's chef, was discovered by journalists from Novaya Gazeta and Moi Raion. The agency was established as the Internet Research Agency, and the troll farm is known as the Trolls from Oligno, or St. Petersburgh Troll farm (Helmus, 2020, p. 155; Mejias & Vokuev, 2017, p. 1034). At the troll farm, hundreds of bloggers had a mission to praise Putin on social networks and other forums and media (Mejias & Vokuev, 2017, p. 1034).

Last, different individuals took part in Russian influence operations on social media. According to Mejias and Vokuev (2017, p. 1028), the war in Ukraine showed that also civilians could create and spread propaganda on social media. These Russian-supportive individuals or actors could be people that already had an influence channel and supporters among the civilians. The influences did not necessarily share the Russian views but were somehow motivated to spread Russian disinformation (Helmus, 2020, p. 155).

2.4 Ukrainian Resilience

Even though Russia had influenced Ukrainians through social media well before the war in 2014, the level of intensity, aggression, and lies was new. The war on the ground took a lot of focus, and the Ukrainian authorities did not have the capacity to focus on Russian influence operations. The civil society aimed to fill the gap in the parallel information war and reconstructed or established platforms to fight the information war against Russia. StopFake.org, Information Resistance, and Detector Media had the goal of debunking and disproving fakes. The Ukraine Crisis Media Centre (UCMC) united journalists, experts, and activists creating a platform to discuss and cover Ukrainian events. UCMC, together with other organizations like the Euromaidan Press, also aimed to spread information to the international society (Babak et al., 2017, p. 50-52; Interview: 5, 2022).

Not before in December 2014, the Verkhovna Rada of Ukraine established the Ministry of Information Policy (today the Ministry of Culture and Information Policy), mainly to counter Russian influence operations. The Ministry's goal was to reach all Ukrainian citizens and carry out social campaigns to educate the population on media literacy (Babak et al., 2017, p. 53). It was challenging to reach the targeted audiences in NGCA in Donbas. The Russian jamming of Ukrainian media channels ensured that information did not get through, and one could not know if information through social media was read or if people believed it (INTERVIEW).

In 2015, the Ministry of Information Policy created "Information Troops" to spread information on social media. The same year, they established the OSINT Academy together with the Institute of Post-Information Society to educate bloggers and journalists in fact-checking and information searches (Babak et al., 2017, p. 53-54).

2.5 Previous research

This chapter will provide a brief overview of previous research on Russian influence operations on social media. The findings from previous research will create a basis for my discussion and analysis. The gaps will be filled by collecting primary data and interviews with relevant persons. These persons are Ukrainian experts, professors, or initiative takers from civil society who contributed to counter Russian influence operations on social media.

The studies on the weaponization of social media are still developing. The first wave of research on Russian influence operations on social media came in the aftermath of the events in Ukraine in 2013/14. The second wave came in 2016 when it was discovered that Russia had attempted to influence the US election via operations on social. The effect of countermeasures and how to challenge Russian influence operations on social media has not been the main focus of previous research, but rather what methods Russian actors use to influence on these platforms.

NGO Internews Ukraine has in cooperation with European Union and the International Renaissance Foundation published an overview of Ukrainian countermeasures, where they also analyzed Russian methods in the information war against Ukraine (Babak et al., 2017, p. 4). They focus on the countermeasures done by both the civil society and the government, lessons learned, and further recommendations. The research says little about how effective the countermeasures are individually, but the recommendations point toward the importance of a "total defense" in Ukraine, where different institutions work together to strengthen the people

of Ukraine (Babak et al., 2017, pp. 120-127). The research also gives an excellent overview of methods and ideas for how Ukraine used different countermeasures against Russian influence operations.

The Ukrainian NGO "Detektor Media" has done some analysis limited to the targeted audiences in NGCA; DNR and LNR. The challenge of getting access has limited the research but given a pointer to what the media habits of citizens in this territory are. The analysis reveals that a lot of people in NGCA still use Ukrainian sim cards (before the Russian re-invasion of Ukraine). On the other hand, fewer people had a smartphone, and therefore more people used traditional (Russian) media as a source of information (Dutsyk et al., 2015, p. 40). The analysis by Detektor Media also reveals that the Ukrainian ban of VK and OK reduced the number of people using these social media platforms, and increased the level of people that used Facebook, as I mentioned earlier. Another analysis from Detector Media shows that the general critical thinking about information in media and social media was higher than expected. The degree of fatigue with political media content was high, and many stayed passive or avoided information like news (Orlova & Shutov, 2018, p. 5).

After the US election in 2016, the general Russian influence operations on social media got a new and more significant focus. There was a lot of research done to discover Russian trolls and bots on different social media platforms, especially Twitter. It turned out that the effect of these bots was not as big as one thought (Helmus, 2020, p.156). It still contributes to creating insecurities and spreading (dis)information to many platforms at high speed. Trolls, who aim to get into people's minds, can be more fruitful as a tool. Trolls can contribute to increasing the tension in comments and groups, and spread articles, videos, and pictures that create discussions (Lange-Ionatamishvili, 2016, pp. 55, 62).

There has been some research on Russian influence operations in Norway. Russian influence operations on social media have not been a much-used method targeted specifically on Norway. FFI (2022, p. 4) did research to discover if it existed any effort of foreign measures to influence the parliamentary election in 2021. The study reported that there was not any foreign hostile influence on social media to detect.

A previous report from FFI emphasizes the general disinformation and conspiracy theories from Russian actors, especially regarding the Covid-19 pandemic. What has changed in the last years, is the content as well as the actors. Russian actors use more pictures, often photoshopped, to avoid being revealed by bad language. In 2020, Facebook tracked people

working for Russian to West African sources. According to the report, the more complex use of actors working to spread Russian disinformation makes it harder to track (Bergh, 2020, p. 24).

This chapter presented the background of Ukraine's challenges of internal issues, the Ukrainian media landscape, Russian capabilities, and Ukrainian resilience. Additionally, it presented previous research on Russian influence operations on social media. The background and the previous research create an empirical ground for my analysis. The data collected through interviews will be presented in the next chapter, "methods and sources".

3.0 Method & sources

This chapter describes the methodology and research design. First, it explains the choice of methods, data collection, and data processing. Second, the criteria for validity and reliability are discussed. Last, it presents some ethical considerations in the research process.

3.1 Research design and conceptual framework

My research concerning influence operations on social media largely depends on social constructions at any given time. Therefore, I have chosen a qualitative methodology to shed light on my research question. The research design includes the choices such as conceptual framework, methodology, research question, data collection methods, and participant sampling (Miles et al. 2020, p. 14).

Qualitative data can be a source of descriptions of social processes and help us find plausible explanations of outcomes. Social media is an arena for social interactions with easy access for everyone who has access to the internet. Russian actors used the access to social media actively to promote the Russian narrative to the Ukrainian people in the NGCA in Ukraine. A qualitative methodology will allow the researcher to "get beyond initial conceptions and generate new understandings" (Miles et al., 2020, p. 3). A qualitative study can provide an understanding of how Russia influences the targeted audiences.

One of the purposes of this study is to examine lessons learned from Ukraine's experience, which can contribute to giving other countries some tools to strengthen their defense against similar influence operations on social media. As noted in my introductory chapter, the thesis aims to explore how Russia carried out social media influence operations targeting audiences in Ukraine, the measure that Ukraine took to counteract the Russian efforts, the extent to which they were successful, and what we can learn from Ukraine's experience.

The conceptual framework for the study has been tight and deductive. I have used the theoretical approaches of soft power, hybrid warfare, and the weaponization of social media that I will present in chapter 4. The reasons for the tight and deductive framework were first and foremost the delineated research question. Second, the limited time to research required avoiding data overload. Third, loose inductive research can be challenging for a student that is new to qualitative research (Miles, et al. p. 14).

I have already mentioned my limitations in time and space. The war in Donbas and the Russian information war against Ukraine create the ground for exploring different methods Ukraine used to counter Russian influence operations on social media.

3.2 Sources and data collection

I started my research by collecting secondary literature. Chapter two presented previous research, which creates an empirical ground for my research. I have used in-depth interviews to better understand how Ukraine faced the challenge of Russian influence operations on social media.

Document analysis

To gain knowledge and an overview of my research study, I started my research by document analysis. In this way, I could orient myself to which previous research had been done and follow up on relevant references for my research (Thagaard, 2013, p. 59-60). I primarily used Nord university´s database "Oria," with search words such as "Russian influence operations" together with "social media," "Ukraine," "Donbas," and "IRA." Also, "Social media" with "Propaganda," "Hybrid warfare," "influence operations," and "Russia," "Ukraine," or "Donbas."

Interviews

I wanted to understand better the considerations behind Ukrainian countermeasures against Russian influence operations on social media. Therefore, I decided to interview Ukrainian experts and civil initiative takers on the theme. Because of the limit in time, place, and the situation with the Russian re-invasion of Ukraine (February 24th, 2022), I did not include the 'common man on the street' or citizens in non-governmental controlled areas in Donbas (NGCA).

An interview is "a conversation with structure and purpose" (Johannessen et al. 2005, p. 135, translated from Norwegian). I did semi-structured interviews. A semi-structured interview gave me the opportunity to prepare for my interviews, which helped me maintain objectivity. Semi-structured interviews still allowed me to follow up on leads that occurred (ibid., p. 137). The opportunity to follow up on leads turned out to be important, as this provided me with new and vital information I wanted to follow up on.

3.3 Interviewing experts – some considerations

For recruiting participants, I had to consider who and how many participants I needed for my research, the strategy of principles, and the strategy for the recruiting process (Johannessen et al., 2005, p. 38). Because of my context and focus for my research study, my samplings were strategic and purposive. The recruiting strategy was homogeneous rather than a maximum variation of participants (Miles et al., 2020, p. 28). On the other side, I recruited persons with

different professions and experiences to shed light on my research question. Additional to interviews, I was in meetings and dialogs with other relevant persons for fact-finding to gain more information.

I limited my recruiting of participants to experts, civil initiative takers, professors, and researchers. An absolute prerequisite was that the participants have experience and knowledge of Russian influence operations in social media. It is essential to consider that my participants are against the Russian aggression and the Russian information war against Ukraine and that some of them have a double role as civil initiative takers in addition to their profession.

As my research study is limited in time, I did five interviews. The participants consisted of three men and two women, all of them Ukrainian citizens. The recruiting was based on network and snowball effect. The snowball effect happens when participants suggest other people who might be relevant informants with information about the phenomenon. (Johannessen et al., 2005, p. 109). I gained a network of relevant people through colleagues at the Norwegian Defence University College (NDUC), the National Defence University of Ukraine (NDUU), and through participating in the 'International Scientific and Practical Conference, Hybrid Aggression of the Russian Federation in Kyiv.

I interviewed experts on "information security" and "hybrid warfare" during my data collection. Mauser and Nagel define "experts" as "agents bearing specific functions within an organizational or institutional context" who "(re)present solutions to problems and decision-making processes" (Bogner et al., 2009, p. 139). All my participants fit Mauser and Nagel's definition of an expert.

An expert appears in three different roles: As an individual, a representative, and a strategist. The interviewer must consider that the participants may present their own meanings and opinions as an individual. If the participant represents an organization, the representative role can give information that is based on the organization's favor. In that way, the researcher can be used as a tool that will gain the organization's own interests. Last, the expert role is explained as the importance of using the right subject status. If the expert gets offended, the expert may hold back information that can be crucial. Interviewing experts can therefore be challenging to validity, reliability, and generalization (Ibid., p. 140).

In my interviews and data-processing, these aspects needed to be considered. I had to accept that the participants could not give out all available information, particularly if it was

classified. I also had to examine if the organization they represented had any own interests that could influence the information they gave me.

As an individual, my participants, to various extent, presented their own meanings. Personal meanings can also be a strength when in this case, the participants' opinions are based on research and experiences of Russian aggression in Ukraine. Many of my participants often underpinned "in my perspective" or "in my view." In this way, I could easier consider how to distinguish between the organization's position and the participant as an individual.

Interviewing the participants gave me a perspective of how Ukrainians experienced the Russian information war against Ukraine. On the other hand, personal experiences made it essential to consider and distinguish between what information was factually Russian influence operations and what information was based on the experience or the feeling of Russian aggression.

3.5 Validity and reliability

Validity is about whether you measure what you intend to measure (Kvale & Brinkmann, 2015, p. 276). One can distinguish between concept validity, internal validity, and external validity.

The question of operationalization turns up in the "concept validity", the concern between the concept and the measurement (Johannessen et al. 2005, p. 71-72). The purpose of this study is to gain knowledge of how to counter Russian influence operations on social media. I have chosen to use three levels for understanding this challenge based on an approach developed by Lange-Ionatamishvili & Svetoka (2015, p. 111). This approach allows me to divide my analysis into three parts: Identify the issues, counter the challenges, and lessons learned. The first part of the analysis, chapter five, will identify and investigate the issues that occurred concerning the Russian information war against Ukraine. Chapter six will examine how Ukraine countered these challenges and the lessons learned from these experiences.

Internal validity is about credibility; the findings must reflect reality (Thagaard, 2013, p. 205). To strengthen the internal validity of my research, I will strive for transparency in my study. The relation between the collected data, the analysis, and the structure are crucial factors for internal validity. The limitations constructed in the conceptual framework for the study, as I mentioned earlier, helped me measure what I wanted to measure to answer the research question.

Good preparations are essential to avoid an overload of data (Miles et al., 2020, p. 64). My data was collected through secondary literature and interviews. Due to preparations, the selection process started already before collecting the data. I had to consider the participants and that the information they gave was relevant to what I wanted to measure. By using a semi-structured interview guide, I was able to limit my interviews within a framework but still follow up on relevant leads. The vulnerabilities of using interviews can be that the individual experience of which events were Russian aggression, and which events felt like Russian aggression but were not. The personal experiences bring us to the external validity and to which extent the findings can be transferred to other situations.

External validity is about to which extent the findings can be transferred to other contexts. In qualitative studies, we talk about transferability rather than generalization because social constructions and understandings of a phenomenon can be various rather than constant (Johannessen et al., 2005, p. 200). The different situations between Ukraine and other countries can vary, but the experience Ukraine has with Russian influence operations on social media is still unique. The focus of transferability in this study will therefore focus on gaining knowledge from how Ukraine countered Russian influence operations on social media.

The research is done from a Norwegian-Ukrainian point of view, with a democratic perspective. Authoritarian states often practice internet and media control. By monitoring the internet, they are less vulnerable to influence operations on social media. Therefore, my findings cannot to the same extent be transferred to authoritarian regimes. Democratic values include media freedom, freedom of speech, and press freedom. This also contributes to the fact that democracies and hybrid regimes practicing these democratic values are extra vulnerable to influence operations on social media. Therefore, this research study can be interesting for countries with democratic values.

There are two aspects worthies of criticism due to the transferability to other democratic countries. These aspects are the low score Ukraine has on democracy and the sanctions on several Russian social media and traditional media channels.

Reliability

The data that I collected and used had to be trustworthy. This is essential for “reliability”. I understand reliability in the following way: Reliability must be considered during the collection of data, the process of choosing which data is being used, and how one processes

the data (Johannessen et al., 2005, p. 46). The relationship between the researcher and the participants and how the researcher recruits participants may influence the reliability.

The conversations and observations will be subjective and crucial for the research. Moreover, it is important to take into consideration that the researcher also is subjective, which makes reliability critical for quantitative research (Johannessen et al., 2005, p. 199). The importance due to the reliability is that another researcher should be able to reproduce the research (Kvale & Brinkmann, 2015, p. 276). Because of the reliability, it is essential to ask open rather than leading questions. Good preparations before the interview, such as an interview guide and test interviews, may decrease the risk of influencing the informant in a particular direction.

For one of my interviews, I used an interpreter. The participant could not speak English, to an interpreter was helpful. However, I had to consider that another subjective person would consume and understand the participant's information before interpreting it into English so I could understand. The interpreter had experience and was recommended by a Norwegian at the Norwegian-Ukrainian cooperation, "the Norwegian Rule of Law Advisers to Ukraine."

During my research study, I have had a scholarship at the NDUC. I have participated in the project "Total Defence Cooperation with Ukraine," which includes cooperation between the NDUC and the NDUU. The cooperative relationship can be a vulnerability for my research. I had to be critical of the information I got due to the cooperation, as there are many feelings related to the war in Ukraine. I also had to consider if my colleagues at the NDUU gave me information that they thought I wanted for the sake of the partnership or the other way around. On the other hand, my scholarship and the project's cooperation with NDUU have allowed me to collect data through a relevant network of people and access crucial information. Also, I have gained help from my supervisor, with great experience in collecting data.

3.5 Ethical considerations

During a research project, several ethical issues may arise. In addition to the ethical issues related to validity and reliability, other ethical issues the researcher must consider might occur. I will describe the ethical issues that I have had to consider in my research study.

The practical skill of exercising discretion, which Aristoteles called *Phronesis*, "is an intellectual virtue that consists in acknowledging and reacting to what is most important in a given situation" (Translated from Norwegian, Kvale & Brinkmann, 2015, p. 95). As an interviewer, it is essential to know the vulnerable position the informant can be in or what

reactions might occur (ibid, p. 97). The interviewer should make good preparations and ensure that the questions are relevant to the research to prevent unethical situations.

Before interviewing people from the Ukrainian culture, I tried to learn what differences between the Norwegian and the Ukrainian culture I could expect and how I should act. I have also been open-minded and thankful for getting the opportunity to learn from another culture. For my interviews, I have a semi-structured interview guide. In that matter, I used the opportunity to ask my supervisor, who has experience in both collecting data and Ukrainian culture. In that way, I gained a critical view of my questions.

To make sure that the participants' personal information was safe, I followed the Norwegian Centre for Research Data (NSD) guidelines for the protection of information. These guidelines include informed consent and allow the participant to ask questions or get their interview withdrawn and deleted. In this research, the personal information about the participant might be crucial, as it is an ongoing Russian invasion in Ukraine.

During the transcription, the participants were anonymized. Due to anonymization, it will be possible to publish my findings without identifying the respondents.

Due to the practical conducting of interviews, other ethical issues can be gender, age, professional, experience, background attitude, and organizational affiliation (Bogner et al., 2009, p. 141). In Norway, the principle of equality between genders has a more significant focus than in Ukraine. As a young lady and a student, I took these considerations before my interviews. It turned out that the interviews were a positive experience as all the participants met me with respect, professionalism, and willingness to share information. My impression was that the participants were happy to have the opportunity to contribute with their expertise to my research regarding the challenge that Ukraine faces with Russian influence operations on social media.

Finally, I will describe the ethical issues with having some of the interviews on video. Because of the limited time, distance, and covid-19 pandemic, it was necessary to do two of the interviews on video. Not all participants might be comfortable giving information over the internet, and technical problems might occur. It might also be challenging for the researcher to see how the participant is reacting to the questions while one cannot see the whole body language.

My experience doing the interviews digitally was that it allowed me to do the interviews I did not have time for when I was in Kyiv. Those two interviews gave me essential perspectives and data. It was also very effective. The participants seemed familiar with digital solutions. What I experienced as challenging was the lack of the good flow a physical conversation creates, which makes it easier to follow up on leads or ask about misunderstood words. I recorded the interviews and had the opportunity to contact my participants after the interview if there were something I needed to follow up on.

This chapter has explained the methodological choices made throughout the research process. The planning and structure that was made formed a conceptual framework for the study. The next chapter presents a detailed explanation of the theoretical perspectives I will use to answer the research question.

4.0 Theoretical perspectives

In this chapter, I will describe my theoretical perspectives. The purpose of using theory is to create a framework for the research that may shed light on the research question and inform the analysis. First, I will explain the theory of power developed by Joseph Nye. Nye's distinction between "soft" and "hard" power may shed light on the Russian use of influence operations in social media. Second, I will present a theoretical framework of hybrid warfare, understood as the complex use of different methods of influence to reach a political objective. Last, I will explain social media as a tool of hybrid warfare. This may help us understand the role of social media in hybrid warfare and how influence operations in social media can affect the course and outcome of an armed conflict such as the one that has played out between Russia and Ukraine since 2014.

4.1 Soft Power

A famous and most relevant definition of power is Robert Dahl's explanation which says that "A has power over B to the extent that he can get B to do something that B would not otherwise do" (Dahl cited in Lukes, 2015, p. 262). Dahl's definition is broad and focuses on actions rather than perception.

A more specified and explanatory definition is developed by Joseph Nye. In the social media context, Nye's definition of power will shed light on my research study: "...power is the capacity to do things, but more specifically in social situations, the ability to affect others to get the outcomes one wants. Many factors affect our ability to get what we want, and they vary with the context of the relationship." (Nye, 2021, p.2).

Further, Nye distinguishes between "soft power" and "hard power." "Hard power is push; soft power is pull." (Nye, 2021, p. 6). Soft power is about the ability to attract; how easily the targeted audiences are attracted to the influence (Kauppi & Viotti, 2020, p. 32). Steven Rothman explains hard power as the use of military and economic resources, or the ability to coerce. Soft power is an institutional and rhetorical resource (Rothman, 2011, p. 51). It is especially the rhetorical resources that are used in influence operations on social media. For instance, the Russian establishment of a pro-Russian and anti-Ukrainian narrative among the targeted audiences at an early stage of the conflict gave Russia a head start. The target audience that believed in the Russian narratives was more easily attracted by Russian social media influence operations such as (dis)information campaigns.

Hard and soft power might be used complementary (Nye, 2021, p. 7). We could see the use of coercion when Russia blocked Ukrainian media channels, and Ukraine did the same to Russian media platforms (Freedomhouse, 2016; Freedom House, 2017). The use of coercion limited the audiences to watch and use specific channels to receive information and entertainment, giving the audience only one point of view and by that, raising the level of attraction. Other factors of hard power that might have a bearing on the level of attraction are the military or economic context. Disorder, insecurities, and dissatisfaction will create an easier arena for the aggressor to influence a targeted audience than a stable situation.

Nye divides power into different levels. The level of power will be defined by the context and depends on the state's resources and the technology to recover them (Nye, 2021, p. 3). Troll farms and botnets are an example of a resource Russia has used to exercise power. It required the right technological competence, like engineering competence to develop algorithms, and psychological competence to reach into people's minds. Russia seems to have both the capabilities and the capacity to implement influence operations in social media.

The ability to attract an audience depends on two factors: The first is internal and relates to how satisfied and united the citizens are. It is easier for Russian actors to create tension and disorder if there already are some dissatisfactions or polarized debates. It will also be easier when the targeted audiences share the same language, beliefs, and culture as the aggressor, which was the situation for many people in the NGCA in Ukraine (Kudelia, 2016, p. 11; Matveeva, 2016, p. 26)

Second, it is about the external factor, which is exposure. If the targeted audiences are exposed a lot to Russian influence operations, the level of attraction may increase (Erlich & Garner, 2021, p. 2). If there are limitations to the Ukrainian perspective, it will be challenging for the audience to be critical. External and internal factors can influence each other. Are there little exposure to Russian influence operations, the discussions on social media may not be so tense. Are the audiences united, satisfied, informed, and have a big trust in the Government, the exposure of disinformation will not affect the audiences to the same extent. How Russia is exposing its targeted audience is essential. Memes, pictures, and videos have turned out to gain a higher attraction than pure text (Lange-Ionatamishvili, 2016, p. 85).

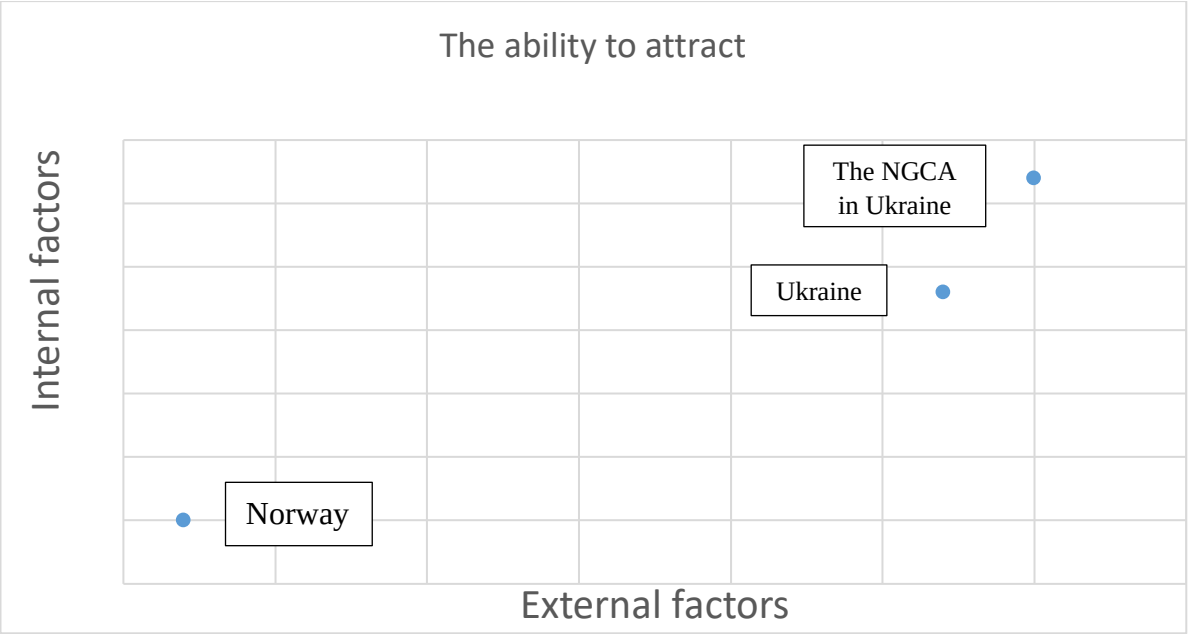

Figure 1 - The ability to attract

"Figure 1" illustrates the depending factors of external and internal aspects of the ability to attract. The figure is not based on statistics but presents a visual example of the level of attraction. As I presented earlier, Norway has a remarkably less exposed to Russian influence operations on social media, as well as the trust in the government and the media literacy is high among the citizens (Forsvarsdepartementet, 2020, p. 21).

In Ukraine, there has been a high exposure of Russian disinformation. In the NGCA, there have also been sanctions on Ukrainian information channels. The content of Russian disinformation and the lack of the Ukrainian perspective heightens the exposure of Russian disinformation in the NGCA in Ukraine.

As I mentioned earlier, the internal factors in the same area are characterized by factors that increase the level of attraction, such as shared language, identity, and war.

4.2 Hybrid Warfare

In 2021, as well as in 2014, hybrid warfare is often defined as a combination of regular and non-regular warfare, as well as a mix of soft and hard power (Reichborn-Kjennerud & Cullen, 2016; Disen, 2018, p. 7-12). The use of the term "hybrid warfare" creates discussions among experts. The phenomenon of hybrid warfare is, among the alternatives, termed 'political warfare,' 'non-linear warfare,' and 'full-spectrum warfare'..'

Mark Galeotti uses the term 'nonlinear warfare', arguing that war is a political instrument in the hybrid warfare context (Galeotti, 2015). Galeotti defines non-linear warfare as "a style of

warfare that combines the political, economic, social, and kinetic in a conflict that recognizes no boundaries between civilian and combatant, covert and overt, war and peace [where] achieving victory – however, that may be defined – permits and demands whatever means will be successful: the ethics of total war applied even to the smallest skirmish (Weissman, 2019, p. 17).

For the sake of simplicity, this research study will use the terms hybrid warfare and hybrid threats. Weissman (2019, p. 18) distinguishes hybrid warfare and hybrid threats as: «Hybrid warfare concerns active measures taken by an actor towards another actor. In contrast, hybrid threats are passive, being real or imagined threats from possible future actions against oneself.»

The Norwegian Ministry of Defense defines hybrid threats as "strategies for competition and confrontation below the threshold of direct armed conflict which can combine diplomatic, informational, military, economic and financial, intelligence, and juridical means to achieve strategic objectives. The use of hybrid methods is often widely distributed, is long-term in its approach, and combines open, covert, and hidden methods"[1] (Forsvarsdepartementet, 2021-2022, p. 15, translated from Norwegian).

The definition by the Norwegian Ministry of Defense, which I will use in this study, presents several hybrid warfare methods. It puts a greater focus on vulnerabilities in the informational domain, which I will focus on regarding the Russian influence operations on social media. The use of hybrid methods aims at reaching a goal without escalating to war or to nuclear weapons.

Incorporating nonmilitary methods in war is not a new phenomenon, neither from Russia nor other states. In newer history, the United States and Russia used different methods trying to win "hearts and minds" among friends and enemies during the cold war (Robinson, 2010, p. 4). Evgeny Messner, Russian Imperial Army Colonel and a former war theorist, explained before his death in 1975 that one of the war's priorities was "a creation of an impression of

[1] The term "hybrid" warfare/threats is a much-discussed term in Norway, and the Ministry of Defense uses another term (in Norwegian) on the same phenomenon. Regards to the translation, I´ve chosen to use the term "hybrid" warfare/threats for the sake of simplicity.

order to obtain new allies and crush the spirit of the enemy's allies" (Messner, cited in Fridman, 2017, p. 45).

Even though the use of different methods in war is not new, the selection and the wide variety of methods are (Galeotti, 2015). The term "Hybrid Warfare" turned up when Frank Hoffman studied different ways of irregular methods Hezbollah used during the Israelian-Hezbollah war, which caused problems for the Israelian state. Hoffman describes hybrid warfare as: 'The blurring of modes of war, the blurring of who fights, and what technologies are brought to bear, produces a wide range of variety and complexity that we call Hybrid Warfare.' (Fridman, 2017, p. 42). Hoffman focused on the synergistic effect that occurs when the aggressor uses regular military methods combined with unregular (Fabian, 2019, p. 310).

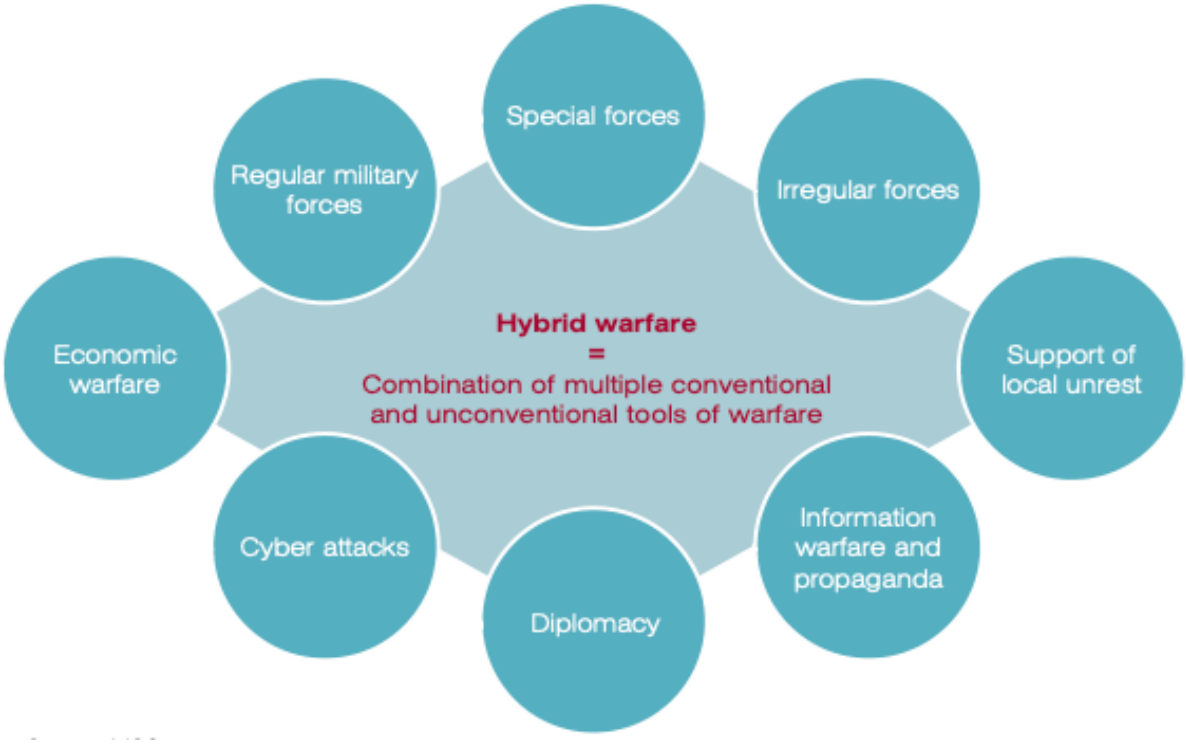

Figure 2 - Hybrid warfare model (MSC, 2015, p. 35)

"Figure 2" presents the different methods of hybrid warfare. The technology has developed at high speed since Hoffman established the term after the Lebanon war in 2006. The development allows the aggressor to create disorder and insecurities in the civil society with a lower cost and less risk for escalation to nuclear weapons or regular warfare (Disen, 2018, p. 9). The result of the low threshold for using hybrid methods is that the line between war and peace has been blurred and created a grey zone with low intensive hybrid attacks, such as influence operations on social media in the absence of war. Hybrid Warfare is used by non-state actors as well as state actors (Reichborn-Kjennerud & Cullen, 2016, p. 1).

The Russian information war in Ukraine has been exercised by non-state actors practicing influence operations on the targeted audiences in Ukraine, such as the Internet Research Agency (IRA) (Dawson & Innes, 2019, p. 3). On the other hand, the FSB demanded personal information from the social media platforms VK and OK to be transferred into their system for surveillance (Babak et al., 2017, p. 63). The different actors working together to reach a goal represents the complexity of how the Russian state, to some extent, can avoid being directly responsible for the influence operations while at the same time they control it.

Using hybrid methods, Russia's goal was to keep the tension at a level that did not develop into a nuclear war, present themselves as not directly involved with certain military actions[2], and use the synergic effect created by hybrid methods to effectively reach their goal that was the annexation of Crimea and creating instability in the eastern part of Ukraine (Cantin et al., 2015, p. 95).

4.3 Social media as a tool in hybrid warfare

Hybrid warfare has been a complex way to influence or wage war, and social media is a new platform to perform at. It is cost-effective in many ways. It can reach many people in a short time and spread misinformation, recruit or coordinate and mobilize during combat or demonstrations. The intense use of disinformation can create insecurity, disorder, violence, and mistrust of the government, and in the worst-case scenario, trigger a '*casus belli,'* which is an occasion for war.

Andrew Hoskins and Ben O´Loughlin talk about the "mediatization" of war: "As a result of changes in the communications technologies available to news media, citizen media and to militaries themselves, media are becoming part of the practices of warfare to the point that the conduct of war cannot be understood unless one carefully accounts for the role of media in it" (Hoskins & O´Loughlin, 2010, p. 4). The trend of easy access to the news has been adopted into social media. Pew Research Centre concluded that 62% of US adults got their news from social media (NATO StratCom COE, 2016, p. 28).

The mediatization of war focuses on all media. A more specific term is the "weaponization of social media". This term is explained as "the utilization of internet resources for 'military'

[2] Russia used «little green men» and supported separatist groups in Donbas for military actions. Russia could reach their goal and at the same time, in the Russian view, get an acceptance for not doing unethical or illegal military actions at the international arena (Cantin et al., 2015).

purposes" (Lange-Ionatamishvili, 2016, p. 21). The Russian actors' goals in using social media as a tool to influence are either "winning hearts and minds" to recruit people, promote themselves as a good role model to gain political influence, or dividing and conquering to saw division and disorder, and lack of trust in the Ukrainian Government, create polarization, and so on (Galeotti, 2017, p. 6; Babak et al., 2017, p. 14).

Messner, cited in Fridman (2018, p. 61) explained these methods as examples of defensive and offensive propaganda during the Cold War, which has presumably been a part of Russian strategy for several years. Today, these strategies play out in social media as information warfare, propaganda, and influence operations (Lange-Ionatamishvili & Svetoka, 2015, p. 104).

According to Bialy and Sanda, the key to success within influence operations on social media is to aim at people's narratives. "Going from conversation to narrative means replacing interest with identification." (Bialy & Sanda, 2016, p. 23). Rumors, or disinformation that may cause chaos, disorder, and insecurities, can be driven by these narratives (Lange-Ionatamishvili & Svetoka, 2015, p. 106). In Ukraine, especially, the people in Donbas have been exposed to the narratives that "Russian speaking people are a part of Russia" and "Ukrainian and Western Nazis are coming to kill them" (Lange-Ionatamishvili, 2016, pp. 47-52).

Automated *bots* and *trolls* are a tool Russia uses in its social media influence operations. Bots are automated, unlike trolls, who are real people (Helmus, 2020, p. 153-154; Babak et al., 2017, p. 66). Bots are often found with hashtags produced in big amounts as automated social media accounts – and 'trolls' are people managing fake social media accounts to get a more realistic portrait of the fake accounts interacting with other individuals or groups on social media.

Ukraine in 2014 demonstrated the importance of understanding influence operations in social media, where Russia used social media as a tool of hybrid warfare, establishing a pro-Russia narrative and influencing the hearts and minds of the Ukrainian people (Lange-Ionatamishvili & Svetoka, 2015, p. 104).

4.4 Social media in a hybrid warfare model

Social media also has a certain role in information warfare. Before social media, the main platforms used in informational warfare were radio, TV, and newspapers, as well as

entertainment such as movies, theatre, and music. Today, social media has taken an increasingly large role in informational warfare (Lange-Ionatamishvili, 2016, p. 19). More people get access to social media and use it not only for communication but also to acquire information, like news and facts. People, groups, or actors know how to utilize social media to influence, presenting disinformation and pure lies as true events.

An aggressor may have different goals for his influence operations in social media, which can be divided into two different categories. In the first category, the goal is to win hearts and minds. Especially if the aggressor has an intention to present itself as a good role model with good intentions. The second category is divide and conquer, which Messner would have called offensive propaganda during the cold war. I have chosen to use the term "divide and conquer" because it can also include the new way of psychological warfare Russia uses, creating insecurities. This type of influence operation is more aggressive and characterizes the Russian information campaigns in Ukraine after 2014.

The various methods in hybrid warfare are several. "Figure 3" illustrate social media's role in the hybrid war context and can be used as a tool in cyber-attacks and information warfare and propaganda. Cyber-attacks in the social media context can be hacking of social media accounts, stealing personal information, or using other people's accounts for hostile intentions. Information warfare and propaganda include the typical spread of Russian disinformation and narratives, aiming at winning hearts and minds and divide and conquer a targeted audience.

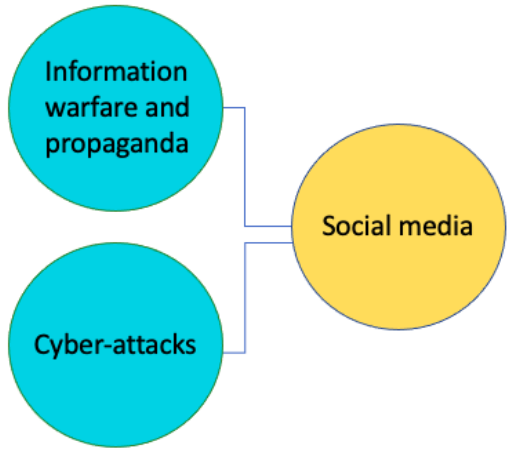

Figure 3 - social media in hybrid warfare

For the sake of simplicity, I use the term "information warfare" in this study. I also talk about FSB's transferring of personal information from accounts on VK and Ok as a part of the information warfare, as well as social media used for combat control and intelligence.

In addition, one can discuss if social media plays a role in other methods of hybrid warfare. Regarding the hybrid warfare model, it presented "support of local unrest", "irregular warfare", and "diplomacy" as dependent factors for hybrid warfare. Creating disorder can be seen as informational warfare as well as irregular warfare by using social media as a tool. Boyte reports that words were used as a "weapon on political warfare (...) to create confusion

and uncertainty world events (...)" (Boyte, 2017, p. 92). Irregular warfare was used by Russia regarding "little green men" or other paramilitary separatist groups in the NGCA. In the irregular forces, social media was used to recruit, mobilize, and communicate. Regarding diplomacy and social media, states as well as non-state actors and individuals have used social media effectively to spread their perspectives and narratives.

This chapter gave a detailed explanation of the study's theoretical framework. The soft power theory sheds light on Russia's ability to attract an audience. The theory of hybrid warfare highlights Russia's use of hybrid methods because of its synergic effect and to avoid an escalation to war or nuclear weapons. Last, the chapter presents social media's role in the hybrid warfare context, and the effectively and low-cost use by the weaponization of social media.

In the next chapter, I will use the theoretical framework to identify and discuss the issues of Russian influence operations on social media in Ukraine. In chapter six, the theoretical framework will shed light on Ukraine's countermeasures against the Russian information war and lessons learned from the experience with the Russian weaponization of social media.

5.0 Russian influence operations on social media in Ukraine – identifying the challenges

In this chapter, I will first discuss the issue of the *targeted audiences*. In the second part, I will examine the most typical Russian *narratives* that have been used in Russian influence operations in the Non-Governmental-Controlled Areas in Ukraine (NGCA). Thereafter, in the third part, I will take an in-depth look at the challenge of two *Russian social media platforms* "Vkontakte" (VK) and "Odnoklassniki" (OK). The fourth and last part of the chapter investigates the issue of *bots and trolls*.

The theoretical perspective of social media as a tool of hybrid warfare will be essential for this chapter and shed light on why Russian actors use different methods to change people's perceptions. Also, Nye's theory of soft power will be essential as it sheds light on Russia's targeted audiences in the NGCA.

5.1 Target audiences for Russian influence operations on social media

I understand the term "targeted audiences" as a group or a specific type of people that the aggressor chooses for their influence operations, seeking to make them act as the aggressor wants. Russian influence operations in social media have been ongoing in Ukraine even before the Russian annexation of Crimea and the conflict in Donbas in 2014.

There are different explanations and understandings of why Ukraine has been exposed to these influence operations. The first explanation is that Russia sees Ukraine as a part of its backyard. The expansion of NATO and the EU increasingly closer to Russian borders may create security issues and insecurities for Russia (FN-sambandet, 2022; Götz & Merlen, 2018, pp. 137-139). The security perspective explains why Russia has targeted the Ukrainian people: keeping or turning Ukraine into an anti-Western and pro-Russian perception. Second, from a Russian constructivist perspective, Russia sees Ukraine as a brother sliding away from the brotherhood toward the West (Tsygankov, 2015, p. 288). As I mentioned earlier, I will focus on the targeted audiences in the NGCA in the Donbas region.

According to Nye, soft power is about the ability to attract. The level of attraction can be influenced by language, identity, wealth, narratives, and experiences (Nye, 2021, p. 6). It is also important to consider that influence operations on social media targeted to an already polarized audience will not be very effective. E.g., if the audience already has attitudes and opinions against the government, this will not change to the same extent compared to a neutral person (Helmus, 2020, p. 156).

First, many Ukrainians speak the Russian language better than the Ukrainian language, especially in the east. According to the high level of Russian-speaking Ukrainians in Donbas, the percentage of people that felt closer to a Russian identity was higher in Donbas than in the other regions of Ukraine (Matveeva, 2016, p. 26-27). The Russian language and the number of people feeling closer to the Russian identity made people in Donbas more vulnerable to Russian targeted influence operations on social media. According to Kudelia (2016, p. 11), as many as 57% of citizens in Donbas would not have supported the independence of Ukraine if there had been a second referendum. This survey was done in 2013, before the war. Donbas was not integrated into Ukraine on the same level as the rest of the country. Almost two-thirds of the citizens saw the Russian President, Vladimir Putin, with a positive attitude.

The war situation in the NGCA increased how susceptible the audiences in the Donbas were to Russian influence operations. As a result of the war in 2014, the Russian proliferation of disinformation to the targeted audiences in the NGCA got more extensive (Erlich & Garner, 2021, p. 2). As a consequence, the Russian ability to attract increased.

On the other hand, language did not seem to be an issue that increased identity polarization before 2014 (Sasse & Lackner, 2018, p. 153). After 2014, language was politicized of Russian actors, e.g. “If you speak Russian, then you are a part of the Russian world” (Interview 5, 2022). It was also politicized by Ukrainian politicians trying to win elections: “And some of them continued politicizing this, like: “what language are you speaking?” (ibid).

The Ukrainians who mainly spoke, read, and listened to the Russian language were language were generally more receptive to Russian disinformation. By reading and following Russian social media and news, they did not get the Ukrainian perspective to the same extent as Ukrainians speaking the Ukrainian language and have access to Ukrainian media and Western social media platforms. People's media habits in the NGCA, as I mentioned earlier, assumed that the audiences preferred and mainly used Russian social and traditional media to gain information. When the narratives on the different platforms are very unlike, the consequence can be an increasing polarization among the Ukrainian citizens, which was the case in Donbas.

Until recently, Russia has also been a big step ahead of Ukraine in the entertainment business, being a leading actor contributing to entertainment for the Ukrainians (Babak et al., 2017, p. 31; Interview: 5, 2022). Russian TV shows are explained as attractive with a broad choice of entertainment, and in 2014 it was reported that 27% of Ukrainians watched Russian TV

channels (Babak et al., 2017, p. 30-31). Entertainment is an effective, additional tool to target an audience because it is associated with authority, and it humanizes the picture of decision-makers. Where the aggressor can not reach their audience through arguments, they can use humor to get their attention and support. (Ozoliņa, 2017, p. 7-8). Russia has a big budget for broadcasting, and in 2015 they used 72 billion rubles (1.2 billion dollars) to support media (Babak et al., 2017, p. 31). Oleg Gazmaniv, a Russian pop singer, is an example of an entertainer popular in Ukraine that presents Ukraine and Crimea as "my country". Popular Russian TV shows are other examples of spreading Russian disinformation and propaganda to polarize, framing Ukrainians as people who violate the law, and Russian TV series that glorify the FSB (Babak et al., 2017, p. 35-36). VK gave access to free Russian entertainment.

After the annexation of Crimea and the conflict had started in Donbas, the Ukrainian signals for TV channels were jammed and unable to reach people in the NGCA. As the jamming blocked the Ukrainian signals, the measure prevented the people from accessing the Ukrainian perspective (Freedomhouse, 2016). When Russia promoted the Russian narratives like "everyone who speaks Russian is a part of Russia," "Ukraine is not able to be a sovereign state," and "the Nazis are coming to kill you," many Ukrainian people in the NGCA believed in these fakes (Interview: 4, 2022; Interview: 5, 2022).

Last, wealth and identity may also be essential factors for attraction. Donbas has been a region for industrial production, whereas the Ukrainian Government has had too little focus. The Donbas region got a social distance from the country. Donbas has also, to some extent, been shut out of the Ukrainian information sphere. Due to the effort to promote and grow the Ukrainian language, and the Ukrainian identity, the Russian-speaking people were de-prioritized. This turned out in the language politics during the "Ukrainization" in Ukraine (Matveeva, 2016, p. 27-28).

Often, social media has no limitations for those receiving the spread of disinformation. It can be hard to distinguish between the target audiences and other audiences for influence operations in social media. On the other hand, the information can be limited to specific groups of people in different closed groups on social media.

Closed groups on VK and OK can often be used as a tool to recruit or coordinate the targeted audiences before or during disorder or combat (Bialy & Sanda, 2016, p. 32). The content in these groups is often more aggressive and violent. People with membership in these groups are often like-minded and can gain trust and comfort in sharing radical content and meanings

(Lange-Ionatamishvili & Svetoka, 2015, p. 105). Closed groups on social media were used in both DNR and LNR.

This part has focused on internal factors for the ability to attract. The next part will examine Russian disinformation and the typical narratives that Russian actors presented on social media to expose the targeted audiences in the NGCA.

5.2 Russian narratives on social media

A famous phrase is, "One man's terrorists are another man's freedom fighters." It may be a cliché, but it also shows the brutal difference between different perspectives. The term *narrative* means the story of how a person sees the world or the reality (Språkrådet, 2017). It is important to consider that it is not only "fakes" and "disinformation" Russian actors use to influence people in NGCA.

The typical narratives Russia has spread are anti-Ukrainian. According to Boyte, the goal is to "...manipulate public perceptions of the events by controlling an element of rhetoric known as narratives." (Boyte, 2017, p. 88). They also use narratives to create skepticism and a critical view of Ukraine's actions. The following presents some examples of Russian narratives flourishing on social media.

"Russophobia"

Ukraine had changed the names of streets and taken away monuments from when Ukraine was a part of the USSR. Russia created a narrative from these actions that Ukraine was a "Russophobic state." The implementation of the Ukrainian language was also being used to establish this narrative, framing it as the Ukrainians are against Russian-speaking people. According to Babak et al. (2017, p. 19), Russian politicians promote this narrative as "genocide of Russian-speaking civilians," "linguistic genocide," and "violent Ukrainianization." Further, he claims that this was the most successful narrative during the Russian annexation of Crimea, which happened just a few months before the war in Donbas started (ibid, p. 19).

The Ukrainian Government is the "Junta," or the "Kyiv authorities."

Framing the Ukrainian Government as the "Junta," or the "Kyiv authorities," aimed at polarizing the citizens away from the Ukrainian Government. An anti-Governmental attitude characterizes this type of narrative. The narratives consisted of rumors such as "the Government wants to destroy everything that is Russian," "This is not the way the society changes" (Interview: 5, 2022), and promoted the Government as an illegal power and that the

Government was neo-Nazi (Babak et al., 2017, p. 15; Lange-Ionatamishvili & Svetoka, 2015, p. 106-107).

Ukrainian soldiers are Nazis.

The last anti-Ukrainian narrative I will present is the one that frames Ukrainian soldiers as Nazis. Rumors that substantiated this narrative was, especially in Donbas, that the "Nazis are coming to kill you" (Interview: 4, 2022) and "Ukraine has become a firing ground of neo-Nazism" (Babak et al., 2017, p. 16). The fakes were often presented in traditional Russian media channels at first before they were transformed into social media platforms and spread. The method of broadcasting the same side of one story effectively increases the thrust of the information (Lange-Ionatamishvili, 2016, p. 7; ibid, p. 13-14). The fakes correspond to the main narratives. Lange-Ionatamishvili & Svetoka (2015, p. 105) distinguish between hate rumors, hope rumors, and fear rumors. Hate rumors "exploit ingrained dislikes and prejudices of a target population. Fear rumours exploit a human tendency to believe the worst." and last, "hope rumours exploit wishes for a favourable turn of events." (Ibid, p. 105).

One famous history is of an emergency physician who was denied to help people who were burnt alive and dying. The story said that nazi occupants denied him and it was shared over 5000 times within 24 hours, only on Vkontakte (Lange-Ionatamishvili & Svetoka, 2015, p. 108). Occasionally it turned out that "Dr. Rozovskiy's profile picture (on Vkontakte) was actually that of a dentist from the North Caucasus" (ibid. p. 109). Fakes like this story were typical during the conflict in Donbas, and we still see these stories today.

The *crucified boy* is a story about a three-year-old boy that a Ukrainian soldier crucified in Slovyansk. This story was shared through an "Eye witness account." The person who "eye-witnessed" was not confirmed by other sources but was shown on the Russian TV channel "Chanel One." Additionally, the story was shared a lot on social media. (Babak et al., 2017, p. 26; Lange-Ionatamishvili & Svetoka, 2015, p. 109). The "eye witness" method was often used in Russian influence operations on social media. These two fakes presented are typical "hate rumors" but can also associate with "fear rumors."

The number of people who used traditional media to gain information was bigger than those using social media to gain information (Dutsyk et al., 2015, p. 41). The use of social media was still an effective tool to target the audiences in the NGCA. Lange-Ionatamishvili (2016, p. 7) emphasizes the effect information on social media gets when it is strengthened from the same information on traditional TV. The connection between the same information on

traditional and social media increases the trust of the information. Russia used this method in lies like the “Crucified boy.”

Another fake story Russia presented was about ‘Ukrainian concentration camps for Russian speakers.’ This lie was in line with the Russian narrative that Russian speakers were not welcome in Ukraine. The concentration camps were described as “separatist concentration camps,” “American secret prisons,” and “refugee screening and filtrations camps,” according to Babak et al. et al. (2017, p. 41). This story is characterized as “fear rumors” as it aims to frighten the Russian-speaking people in Ukraine.

These narratives and fakes were spread on social media platforms. The two Russian social media platforms, VK and OK, were monitored by Russian actors, and the content created a challenge for Ukraine in the information war. The next part will investigate these challenges.

5.3 Russian platforms, Vkontakte & Odnoklassniki

This chapter will investigate Russian influence operations on the social media platforms Vkontakte (VK) and Odnoklassniki (OK). As I mentioned earlier, the effect of using soft power as influence operations will vary depending on the level of attraction. The lower level of attraction, the lower the chance to change people’s perception.

I have chosen to focus on VK and OK because of the high frequency of Russian disinformation and the impact these social media platforms had on the targeted audiences as two of the most popular social media platforms in Ukraine in 2017 (Babak et al., 2017, p. 55). VK and OK had more users in the eastern regions, including the NGCA. The percent of people getting news from VK and OK was representable 25% and 22% in 2015.

The social media platforms VK and OK were used for different purposes in Russian influence operations in Ukraine in 2014. The Russian influence operations aimed to change people’s perceptions, collect personal information, recruit, and combat control. It can be challenging to know who is behind these influence operations, as the accounts on social media can be fake or not represent an actor, pretending they are individuals. The actors behind spreading and promoting Russian disinformation and narratives can also be influencers like famous bloggers, actors, artists, etc. (Helmus, 2020, p. 155; Interview: 5, 2022).

Russia is an authoritarian state, and according to Babak et al. et al. (2017, p. 62), Russia has complete internet control. During the Euromaidan protests in 2013, the FSB demanded all the Ukrainian users at VK be transported into the FSB system. In that way, the FSB could easier

monitor people with VK accounts. The FSB was able to do that with both OK and VK when both platforms were under the control of the 'Mail.ru' group, owned by oligarch Alisher Usmanov. As I mentioned earlier, this was personal information people had published on their accounts. Further, Russia has a 'Ministry of Communication and Mass Media' created in 2008, which controls the internet, its' users, and content (ibid., p. 63-64).

To change people's perception of reality on VK and OK, Russian actors spread disinformation (Boyte, 2017, p. 95; Interview: 2, 2022). As I have mentioned, the disinformation was typical narratives such as that "Ukrainian soldiers were Nazis," and that "Ukraine was not an independent country," and other fakes such as "the crucified boy," "Organs for sale," and "The Ukrainian emergency physician that Ukrainian soldiers denied helping people that were dying."

Russian control over the platforms gave the Russian special agencies full access to personal information posted on the platforms, like friends, family, and networks, where they lived, their interests, religion, and political views (Interview: 1, 2022). As the Russian Federation collected personal information from accounts, they could map who was attracted to Russian influence operations. The mapping allowed Russia to frame an outside reality based on the targeted audiences' interests (Lange-Ionatamishvili, 2016, p. 14-15). "the systems were used (…) for many reasons. Not only to collect information about people but to hire people to become a member of illegal organizations or organize them into Donbas and Crimea to fight against the Ukrainian military. And against state services." (Interview: 3, 2022).

Regarding recruitment and combat control, pro-Russian actors used closed groups in social media to recruit and combat control for creating chaos, rebellions, or even war. The closed groups became a communication platform where they could mobilize. According to my participants, Russia was using groups on VK and OK to "mobilize people on anti-Ukrainian protests, to push the narratives 'Fascists are coming to Kyiv,' and the 'Government wants to destroy everything Russian,' and that 'not the way things change,' 'it is a coup,' and 'you have to fight." (Interview: 4, 2022).

By creating groups, they made a platform to normalize unpopular or controversial opinions. The groups could increase confidence among people to express or increase these attitudes. Normalizing these opinions and thoughts could also frame other targeted audiences to believe in these narratives and lies. Lange-Ionatamishvili (2016, p. 40) explains it as "(..) in the analysis of the propagandist-audience interaction mechanism, it consists of invoking the

audience to adopt the attitudes and beliefs of the 'common man.' This is simply an attempt to convince individuals and groups that the position taken by the persuader reflects the views of the common people. The result is winning the confidence of people who distrust officialdom and state authorities but are likely to trust 'plain folks' – people like themselves."

5.4 Russia's use of bots & trolls on social media

This part will explain how Russia uses bots and trolls on social media. I will further examine how Russia used bots and trolls in their influence operations on social media in Ukraine due to the war in Donbas. I will investigate whether these methods are effective or not in influencing the people in the NGCA in Donbas.

I understand the main issue about bots and trolls on social media as the high exposure of Russian disinformation these methods create, and the audiences "taking the bait". To challenge this, the Ukrainian civil society first tried to debunk and disprove fakes. First, after a while, Ukraine experienced that it was more effective to decrease the exposure to Russian influence operations on social media and educate people to be critical of information and accounts on social media.

Many companies use bots to simplify and improve customer service, and most people using the internet are familiar with typical chatbots. The term "bot" is short for "software robot" and consists of computer algorithms developed to keep a conversation with a human by automatically producing content to interact (Ferrara et al., 2016). In the same way as social media, criminal groups and actors also utilize bots. Bots are a big challenge in the Russian information war against Ukraine, and 'botnet' is described as one of Russia's key elements in the information war against Ukraine (Hurska, 2020). As I mentioned earlier, bots are automated accounts with the purpose to spread (dis)information at high speed to many people.

A bot can be described as "(...) accounts in social networks, created automatically in large quantities and programmed to perform a specific algorithm of actions, first and foremost to disseminate information messages" (Babak et al., 2017, p.64). Botnets, the production, and management of the bots are covert companies of people who create these and manage the automated accounts. We find bots, especially on Twitter, because of the easy access to create large numbers of fake accounts (Babak et al., 2017, p.64). Pro-Russian actors have established several of botnets in Ukraine since 2014 (Hurska, 2020).

What distinguishes bots from trolls, is that trolling consists of real people. The terms are often used together. As I mentioned earlier, trolling aims to get into people's minds through

interests and emotions. Automated bots are not able to do that to the same extent. According to Lange-Ionatamishvili, a troll's behavior is characterized by proactive comments with the purpose of creating a conflict (2016, p. 54).

Russia has troll fabrics, which consist of real persons who create users online to contact persons, start their own campaigns, or establish groups for people with similar opinions. Their goal is to create emotional tension, unlike the automated bots. "So usually, they try to reach not only me, but many people, using some fake accounts. (..) like trolls. Asks for friendship on facebook. Maybe once a month someone tries to reach me. So even using the names of my friends, as my friend Bill from the USA. Probably his account was broken, and they used his name and his ID to reach me." (Interview: 1, 2022)

It registered an increasing number of users due to the conflict in the Donbas region in 2014 (Dawson & Innes, 2019, p. 14). The St. Petersburgh troll factory is a famous example, which is owned by pro-Kremlin hackers and criminal oligarchs called the Internet Research Agency (IRA) (Helmus, 2020, p. 155). In this way, Russia is not "directly responsible" for these troll fabrics. Last, Russian, pro-Russian influencers or others motivated to spread Russian disinformation are a capability Russia used in their information campaigns (Helmus, 2020, p. 155). These influencers are real people spreading Russian propaganda in their media or social media channels, gaining many people to receive their content.

A mapping done by Lena Samokhvalova (2016) presented in figure 4, gives a good example of how one fake account can spread one (dis)information on several social media platforms. This example includes several anti-Ukrainian groups on Vkontakte and Facebook, and Twitter, YouTube, and the chat room Skype. On these different platforms, the trolls behind fake accounts can interact with real people and try to get their attention. Lange-Ionatamishvili (2016, p. 56-58) presents strategy trolls use to gain attraction from the targeted audience: "luring, taking the bait, and hauling in."

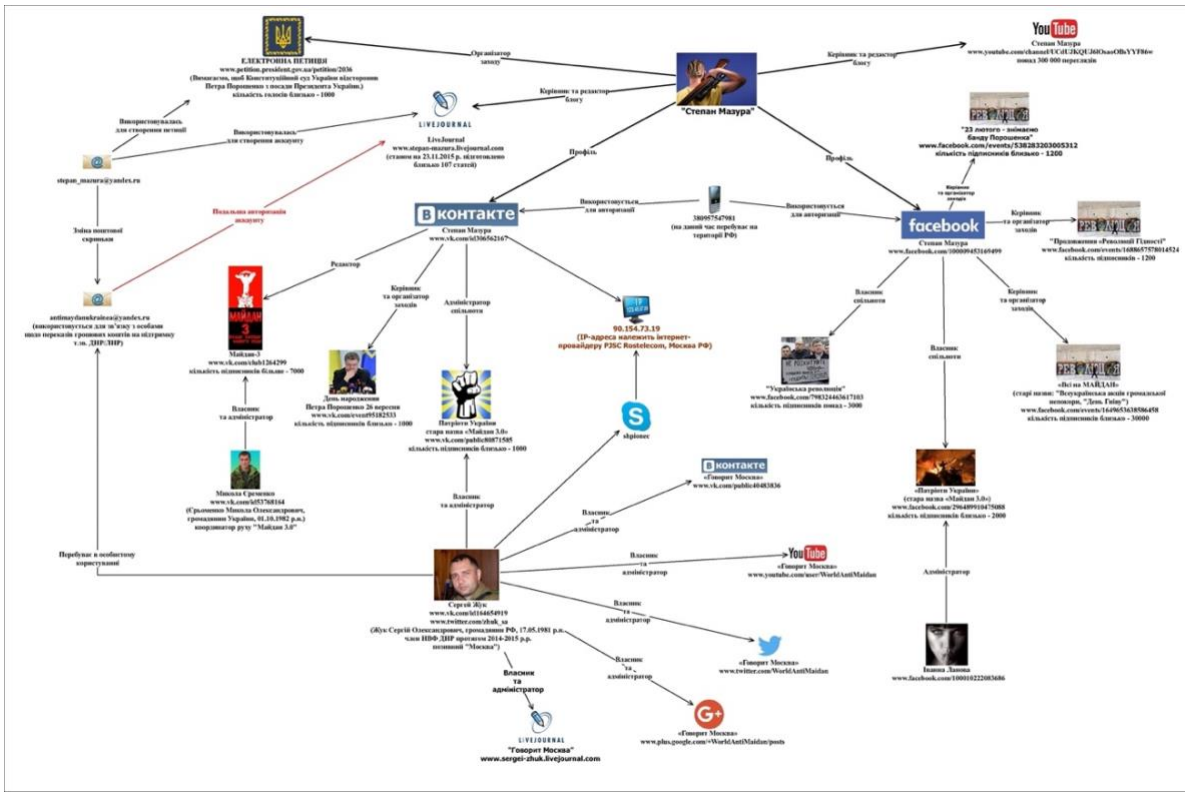

Figure 4 - Spreading disinformation from one account [(Samokhvalova, 2016)](#).

'Luring' is about catching the audience's attention. The content at this stage needs to be interesting, and pictures, memes, and videos seem to be methods which is more attractive to the audiences. Further, the step where the audience is 'taking the bait' is often when a new troll is taking over. This is because it is a different strategy to incite a discussion. In the last step, 'hauling in' is about polarizing the discussion or conversation. The troll is now turning the discussion to other tense content than the article's purpose in the first place.

This chapter has examined the challenges caused by from Russian influence operations on social media in Ukraine, with a special focus on the targeted audiences in the NGCA. Central in this regard were the typical Russian narratives and fakes, the Russian social media platforms VK and OK, and last, the challenge of bots and trolls. The next chapter will investigate how Ukraine countered the Russian influence operations and to which extent these countermeasures were effective.

6.0 How did Ukraine counter Russian influence operations on social media?

In this chapter, I will take a closer look at Ukrainian countermeasures against Russian influence operations on social media. The chapter focuses on four different types of countermeasures. First, it discusses the measure of education on media literacy and spreading information about the Ukrainian perspective. Second, it investigates the debunking and disproving of Russian fakes. Third, it discusses the Ukrainian sanctions on the Russian social media platforms VK and OK, and fourth, the closing of different botnets and troll farms. Last, in this chapter, I will investigate lessons learned from Ukraine's experience with Russian influence operations on social media.

Joseph Nye's theory of soft power and the ability to attract an audience and the theory-based reflections on the use of social media as a tool of hybrid warfare presented in chapter 4, will inform the analysis of Ukraine's countermeasures against Russian influence operations. As I mentioned, Russia's ability to attract an audience is crucial for keeping the influence operations on social media effective. This is regulated by the content and frequency of the exposure and the level of attraction among the audience, which are internal factors that influence how easily the audience will be attracted.

6.1 Education and information

During the first half year of the war, Ukraine had significant challenges countering the Russian aggression in the information war. The situation was characterized by chaos and insecurity, and it was mainly the civil society that countered Russian influence operations by debunking and disproving fakes on social media.

By gaining some experience, experts on Russian influence operations understood that debunking fakes were not the most effective way of countermeasures (Interview: 5, 2022). People in NGCA needed to speak with and see the "outside world." "It is about making people realize that they are being used and being lied to" (Interview: 5, 2022). Ukraine started some programs where children could visit other regions or even other countries. And more importantly, they welcomed people in NGCA to take higher education in Ukraine's government-controlled territories. According to a Ukrainian information security expert (Interview: 4, 2022), there had been told stories by students from NGCA that their parents believed the Nazist were coming to kill all of the citizens. The citizens did not get another perspective, so they believed in these types of lies.

In December 2014, when the Government established the Ministry of Information Policy, the focus turned to both active and preventive measures. These measures included educating citizens to be critical of the information they gained on social media. Regarding the citizens in NGCA, the Government started some social projects to promote the Ukrainian narrative and to give people an opportunity to see with their own eyes that Russian disinformation existed. This included being in the NGCA to speak with citizens, inviting children and students out from the territory and even abroad, and working with journalists to get information (Babak et al. 2017, p. 13; Interview: 4, 2022; Anon 5, 2022).

Many students that started higher education in other parts of Ukraine saw that they had been limited to only one perspective, which consisted of much disinformation. The students could also bring this perspective back home, contributing to a ripple effect of spreading Ukraine's perspective on the information war. These two factors of welcoming young people to Universities outside of the NGCA increase the importance of education and knowledge, not least to young people in NGCA. Young people are easier affected, and they can spread the Ukrainian perspective in a territory the Ukrainian government or other civil initiative takers cannot get in. This is also the generation that takes over when the older generation with experiences from the USSR is gone.

After establishing the Ministry of Information Policy, TV towers were funded to reach people in the east after December 2016 (Babak et al., 2017, p. 53). Not before 2021, the Government also founded the Russian-speaking DOM channel to get out to Ukrainians (Interview: 5, 2022; Prozorro, 2021). In this way, traditional media and social media could strengthen each other to influence the citizens in Donbas. Some challenges arose due to the DOM channel. The limited access to communication with the citizens in NGCA makes sure that the Government cannot measure how many are watching the DOM channel (Interview: 5, 2022). Furthermore, this prevents the Government from knowing how the targeted audiences think or feel. Understanding the audience can be crucial to creating the right content.

Getting through with education on media literacy is important because distinguishing regular social media accounts from bots and trolls can be challenging. Different types of basic behavior characterize a troll's behavior. "Aggression," to cause anger and revenge, "success," if the troll successfully leads the targeted person in an interaction with the troll; and "personal attacks, when the troll aims to start a "personal attack" on both sides. Last, trolling can be for

their entertainment based on *exacerbating a conflict* or causing *disruption* (Lange-Ionatamishvili, 2016, p. 54).

There are also other possibilities to distinguish trolls from real persons. The NATO Stratcom Centre of Excellence's research concludes that "repetitiveness of statements and predictability of reactions make it easier to identify" (Lange-Ionatamishvili, 2016, p. 13).

The complexity of trolls makes sure that analyzing and distinguishing trolls and trolling activity from real persons is hard (Lange-Ionatamishvili, 2016, 54, 58). To perceive the repetitiveness of statements requires vigilance and structure. Therefore, one cannot expect ordinary civilians to disclose trolls and bots in daily life without knowing how to be critical and aware of the threats of trolls on social media.

On the other hand, the analysis discovers that trolling is not as effective as one supposed because propaganda and disinformation trigger counter-propaganda. People also get information through traditional media channels. The issue in the NGCA areas is that the Ukrainian traditional media channels are blocked, and the Russian disinformation on traditional media "confirms" what the audiences have seen and read on social media platforms.

6.2 Debunking and disproving fakes

As civilian initiatives first did the countermeasures, the media houses, bloggers, and experts first began to debunk and disprove Russian fakes. These measures started before the war broke out in Donbas. The civil society was not prepared to counter Russian disinformation, and many organizations had to reconstruct their strategies. According to a Ukrainian analyst within Russian influence operations on social media, the reconstruction of several media- and communication organizations was "a turning point." "Everyone knew that these hybrid war information attacks on Ukraine started way before 2014. But in 2014, even before the revolution of dignity, it was so obvious. It was so clear that no one put like stand aside from it. So that was the turning point for expertise and capacity." (Interview: 5, 2022).

Detektor Media, Informational Resistance, and the Ukraine Crisis Media Centre established or restructured their organization to fight the information war (Babak et al., 2017, p. 50-52). The common ground for these organizations was that they all used social media and strived to give local and international audiences accurate information. The information- and media organizations took a huge step forward in the information security sphere in 2014.

The main focus of these media- and communication organizations was to spread the word to the international society. There was a big focus on getting information in English and Ukrainian on the agenda. According to a Ukrainian information security expert (Interview: 4, 2022), there were some reasons for the international priority: During the Georgian war in 2008, Georgia successfully managed to get information to the international society. The focus on informing the international society gave other countries a perspective of what was happening and helped them be critical of Russian disinformation. When the international society sees the victim state's perspective, one can achieve crucial international support. The Georgian president at that time spoke English well, which was essential to get out information. Similarly, due to the war in Ukraine, Boyte reports that Western counterpropaganda dominated the information war and was influential on an international level (2017, p. 99).

The information where the civil society debunked and disproved fakes reached out to both the international society and Ukrainians, but for the people living in the NGCA in Donbas, one could not know if they received the information. And the exposure of Russian disinformation was still intense on social media with an ability to attract the targeted audience. The people in the so-called DNR and LNR lived under bad circumstances, and it was challenging to know how many received the information.

As I mentioned earlier, Russia blocked Ukrainian signals, and most of the citizens in NGCA used traditional media to get information. Many people already believed in Russian disinformation and narratives and feared Ukrainian soldiers or Western intervention. For those citizens using social media, trolls and bots ensured that the exposure of disinformation was high. The countermeasure would not directly affect the number of fakes by debunking and disproving fakes. However, it was still essential to get the truth on the agenda. Still, it turned out that it was not an effective measure to lower the Russian ability to attract people to Russian influence operations on social media.

6.3 Ukrainian countermeasures against disinformation on Vkontakte and Odnoklassniki

Further, I will examine how Ukraine countered these influence operations by blocking VK and OK. By looking at the level of attraction and the frequency of exposure of Russian influence operations on the platforms versus the democratic values of media freedom, I will seek to find out to which extent Ukraine was limiting media freedom or protecting the target audiences. The analysis presents that it is challenging to fight an information war against

Russia without making decisions that are more equal to the enemy's values than the Ukrainian.

After the former Ukrainian President, Mr. Poroshenko, decided to block these platforms in 2017, today's Ukrainian President, Mr. Zelensky, announced that they would resume the block for another three years in May 2020 (Freedomhouse, 2021).

Ukraine has turned increasingly to the West over the last 30 years. However, according to Freedom House, Ukraine has a "low score" on the total democracy level. Ukraine scored a democracy percentage of 34.52 in 2014 and 39.29 in 2021. The low score gives Ukraine a status as a "Transnational or hybrid regime." (Freedomhouse, 2014; Freedomhouse, 2021). To compare, Russia got 19/100 with the status of "not free" in 2021, and Norway has 100/100 with the status of "free" (Freedomhouse, 2022). Media freedom plays a significant role in democracy and the United Nations' human rights. Article 19 in the Universal Declaration of Human Rights says that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." (United Nations Department of Public Information, NY).

In 2017 Ukraine used hard power to counter influence operations on VK and OK by shutting down these Russian social media platforms. During the interviews, the measure of shutting down Russian social media platforms was frequently mentioned. Among my participants and in meetings with Ukrainian colleagues at the National Defence University in Ukraine, it has been a broad agreement that it was an effective and vital measure. They argue that the decision to block VK and OK stopped the 'tsunami' of disinformation. The discussion was not about whether it was a wrong decision or not. The discussion was about how the international society, especially people who worked for media freedom and freedom of speech, meant it was not a right and democratic decision (Anon; 1, 2022; Interview: 4, 2022; Interview: 5, 2022).

The block of VK and OK created much dissatisfaction. The Russian social media platforms VK and OK offered free access to entertainment like Russian movies and Russian artists. The free entertainment is one of the reasons some Ukrainians are still using VK and OK with access through VPN today (Interview: 1, 2022, Interview: 5, 2022).

Before the ban, many Ukrainians also used VK and OK for communication and business, where they had a network for doing their businesses, including customers and clients. Also, many Ukrainians used the Russian social media platforms VK and OK to keep in touch with family and friends in Russia. After the ban, access was only possible using a VPN, which some Ukrainians did. “As I am told, most of them (editor’ note: Ukrainians) use it to connect with relatives in Russia. Another reason is to get to pirate videos or music that is possible to get on these networks. So, it is mostly young people who like Russian artists and singers.” (Interview: 1, 2022)

The grey zone created by the Russian use of hybrid methods raises the ethical question of whether it is the right thing to do to limit media freedom. As I mentioned earlier, according to the Universal Declaration of Human Rights Article 19, everyone has the right to seek information and express their opinions through any media. The ban stops people from expressing their opinions on these platforms or seeking information through VK and OK. The limitation of media access is one of the reasons that Ukraine has a low democracy score, according to Freedomhouse (2017).

The use of hybrid methods raises challenging dilemmas about if states should make such radical decisions. The question is whether the Ukrainian situation in 2017 was critical enough to legitimize the block of VK and OK. Ukraine had already blocked several media channels after the war, especially in the Donbas region (Freedomhouse 2016). What defines an information war, and where is the limit between protecting the people and limiting their democratic rights?

After the military annexation of Crimea and pro-Russian separatists took control over Donetsk and Luhansk, separatists' pressure on the internet sphere was significant. The citizens in the NGCA experienced limited media freedom and freedom of speech, and some risked their safety to report this issue. Several Ukrainian web pages were blocked in the territory. Ukraine also experienced several hacker attacks from Russian actors (Freedomhouse, 2016). Ukraine, on its side, cracked down on those who spread anti-Ukrainian content on social media. Persons who did this could expect fines or even prison despite Article 34 in the constitution, which says all Ukrainians are granted freedom of speech (Freedomhouse, 2016).

The Ukrainian decision to ban VK and OK was probably not taken without considering the value of media freedom. In 2021, Ukraine abandoned the draft law “on disinformation” because of the importance of media freedom. “Apart from challenges within the country,

Ukraine’s democratic consolidation is also complicated by the insecurity that Russia poses through its military aggression in Donbas and continued occupation of Crimea. For example, Ukraine aspires to shield itself from Russian disinformation, yet the relevant draft law ‘On disinformation’ infringed on media freedom and was abandoned.” (Freedomhouse, 2021).

Ukrainian experts claim that the ban was necessary because of the ongoing war in Ukraine and all the stolen personal data. The Russian collection of personal data was discovered after Ukrainian special forces investigated the issue. The personal data included information about Ukrainian soldiers (Interview: 1, 2022; Interview: 4, 2022; Anon 5, 2022).

Another consideration the Ukrainian government had to take was that blocking the Russian social media platforms would reduce Ukraine's ability to gain information from the enemy, like pictures and videos published by Russian soldiers located in Ukraine. It was a consideration to gain information about the enemy and protect the Ukrainian people in the information war (Interview: 1, 2022; Volchek & Bigg, 2015).

The government’s ban had a positive effect. The media habits in Ukraine changed. As I mentioned earlier, the users of VK decreased from respectively 25% to 12.2%, and from OK, the numbers dropped from 22% to 6.8% in the regions Kharkiv, Donetsk, Luhansk, Odesa, and Kherson. Facebook's popularity increased to 35%.

The decision the Ukrainian government took by blocking VK and OK had significant consequences. The ban meant that it would take too much time and effort for Russian actors to gather the same audience on another social media platform. Additionally, Russia would not have gained the same benefits as entirely Russian control on a Western social media platform. Experts claim that the best way to fight Russian influence operations is to avoid looking at it. The immediate effect of the ban resulted in a lower number of people getting into the Russian (dis)information sphere. One of my participants talked about it as “information hygiene”;

“Keeping your minds clean, keeping your eyes from something you find dirty. So, there is a simulation, walking in the street, you see a huge puddle on the ground. You will not go straight in it, you will pass by it. It is the same for information. You know that they are spreading disinformation and fake news through their media platforms. So the best way for you to deal with it is to avoid being there. Avoid reading their news on their platforms.” (Interview: 2, 2022)

The intentions behind the Russian influence operations were different in 2014 than before. The intensity of Russian information campaigns was high also before 2014 but focused on winning hearts and minds. Around the Russian annexation of Crimea, the information campaigns turned into a divide-and-conquer strategy. The disinformation turned more emotionally and consisted of pure lies, which might be why it was so effective (Babak et al., 2017, p. 14; ibid p. 40). Ukrainian experts and authorities were not prepared for this new intensity of Russian influence operations (Interview: 4, 2022). The Russian military aggression and the aggressive disinformation campaigns made the target audiences more vulnerable. This contributed to raising the level of attraction to Russian influence operations among the targeted audiences.

Moreover, the situation influenced Ukrainians in governmental-controlled areas, which divided families and friends and increased polarization between people. Blocking VK and OK contributed to sparing these people from further influence. Ironically, Russia utilized the situation to shame Ukraine's decision by claiming that the decision limited media freedom (Babak et al., 2017, p.20).

6.4 Ukrainian countermeasures against botnets and troll farms

The challenge with bots and trolls is that one fake account can spread the same information on several platforms (Interview: 3, 2022). The exposure that is created by Russian bots and trolls is still significant. To lower this high exposure, Ukraine closed several botnets after 2014.

Different studies report that at least 8% of accounts on Twitter and 5-11% of Facebook accounts were bots in 2016 (Bialy & Sanda, 2016, p. 33). As I presented earlier, a bot or a troll will often bring the same information to several social media platforms. That method gives one troll or bot the ability to spread one (dis)information to even more people with lesser effort. The platforms they use can have various audiences; “in Viber groups, (...). For example 100 members (editor’s note: in one group), but maybe 1000 groups. The next: telegram channels. For example, more than 220 000 followers.” (Interview: 3, 2022).

On the other hand, by spreading one disinformation to several groups, the trolls and the bots are easier to identify. According to one of the participants, this allowed analytics to find the bots and trolls, and report the fake accounts. “It was clear that it was some kind of coordinated activity. You could see that because of the frequency and the quantity of that information being circulated. Also, these groups started to like pop up, they were created very quickly. And people behind that groups, if you go on and see the accounts, you could clearly

see that they, part of them were bots, or bot accounts with no background information." (Interview: 4, 2022)

However, bots and trolls in groups may be challenging to detect. The platforms can be either Russian-owned or limited to certain people, and Ukrainian security services and Ukrainian analysts may experience it as problematic to get access.

Closing accounts or groups can lower the numbers of fake accounts to some extent, but not necessarily stop the target audiences to believe in the disinformation they have spread. A method for civilian people to detect bots and trolls was to look at the accounts for background information or wrong interpreting of the messages (Interview: 3, 2022). The issue for the targeted audiences in the NGCA was that they have Russian as their mother tongue, the same language most trolls behind fake accounts or bots use. In that way, wrong interpreting was not a big issue for the Russian actors behind the influence operations. "It is easy for them because they are Russian-speaking regions, and still are. If you´re not speaking Ukrainian and use, for example, (editor' note: trolls) working for Russian special services, it is very easy for you to have so many accounts you can manage, because there are no differences in the language, and you can do it very quickly." (Interview: 4, 2022)

Unfortunately, the fact that Ukraine has shut down several botnets shows that Russian actors have the capacity to create new ones. Ukraine established an "internet army" and closed troll farms and botnets to lower the exposure of Russian influence operations and social media.

After all, the effectiveness of bots is various. According to Helmus (2020, p. 156), an analysis of bots showed that this method was not as effective as one thought. This analysis was done on American Twitter users. The IRA's influence operations with bots failed because the audience they targeted already was polarized in their opinions. In that way, the people in the NGCA that stayed neutral towards the Ukrainian government could be more vulnerable, as the Russian bots- and trolls aimed to change their perception toward an anti-Ukrainian view.

The Ukrainian Secret Service attempted to find and close them. In April 2016, the Security Service of Ukraine found and shut down the then world's largest botnet. The server with the botnet was managed from Russia. In March 2019, the botnet "Sapphire" was discovered. The Russian military intelligence GRU set up the "Sapphire" in Luhansk. In 2020, a botnet supported by Russian online services was active in Kyiv, Kharkiv, Dnipro, Dubno, and Irpen with 8000 accounts on different social media platforms. Since 2014, Ukraine has shut down several botnets supported by Russian online services, according to the SSU.

6.5 Lessons learned

This part will sum up and give e brief of lessons learned from Ukraine. The Ukrainian countermeasures highlight the dilemma of winning an information war without becoming what the enemy is. To take away a social media platform from the people, where they can gain information and news, and express their opinions, should not be an easy decision for a democratic state to take. On the other hand, a country in a war – as well as an information war – might be a necessary decision to lower the synergic effect of hybrid warfare. As I mentioned earlier, the synergic effect is created when several methods in war strengthen and streamline each other to reach the same goal. By taking one of them out of the war, Ukraine inhibits the Russian way of warfare.

The Ukrainian Government and the civil society realized that debunking and disproving fakes was a necessary measure but not as effective in lowering the ability to attract. However, education, blocking Russian social media platforms, and closing town botnets turned out to be effective. In that way, Ukraine decreased the targeted audience's exposure to Russian disinformation and lowered the level of attraction among these people. Although these measures were effective, it was still challenging to get through to the targeted audiences in the NGCA. By taking the youth out of the NGCA, they could gain the Ukrainian perspective and bring this side of the story back to DNR and LNR. Ukraine has had big challenges in getting information into the NGCA in other ways. Even by creating channels to reach the targeted audiences, they do not know how many who is receiving the information.

Due to the blocking of VK and OK, this was an effective measure. The changes in peoples' social media habits underpin that the ban decreased the spread of Russian disinformation to many people, which influences the cost-effectiveness Russia has gained from the weaponization of social media. Today, there are still a few persons who use VK, and in some cities, also in Ukrainian-controlled areas like Maripol, Zaporizhzhia, and Mykolaiv, the amount can be up to 20%. But in general, the percentage is around 1% (Interview: 5, 2022).

On the other side, the Russian platforms have later got a built-in VPN working in the NGCA. This also raises the question of the decision to continue the sanctions on VK and OK in 2020 due to the limitations of media freedom.

The Ukrainian Ministry of Culture and Information Policy and the Ministry of Digital Transformation has, in newer times, created a volunteer program, the "Internet Army of Ukraine," to counter Russian influence operations and cyber-attacks. The Internet Army

movement consists of over 310 000 Ukrainian IT professionals, cyber specialists, ordinary people, and creative workers (Hurska, 2022).

However, the challenge trolls and bots create is still considerable. When the Russian re-invasion of Ukraine on 24th February 2022, it was an intensification of bot-driven influence operations on the social media domain. Security Service of Ukraine (SSU) announced that they had shut down five botnets in the Ukrainian oblasts of Kharkiv, Cherkasy, Ternopil, and Zakarpattia. The botnets operated with more than 100 000 fake accounts. Among the equipment they found through searching through the botnets, they also found almost 10 thousand SIM cards of various mobile operators. The goal aimed to spread panic and destabilization among the Ukrainian citizens (SSU, 2022). In 2020, it was revealed 8000 fake accounts on different social media platforms. These face accounts were active in multiple regions of Ukraine (Hurska, 2020).

It is still important to do the job of debunking and disproving fakes to get the Ukrainian perceptive on the agenda. On the other side, the Ukrainian experience shows that preventive measures are the most effective. This seemed to be challenging in NGCA territories because of the limited access due to technical issues as well as lack of communication with the citizens. The technological issue is about not getting through with Ukrainian signals, which stops the sharing of information, especially among the older generation. The younger generation more often uses YouTube or other social media channels and is able to receive information through these channels (Interview: 5, 2022). The lack of communication also makes it hard to know how the citizens in Donbas are thinking and feeling. On the other hand, when young students are coming to Ukrainian-controlled areas to study, they can tell stories of what the DNR and LNR citizens think about the situation. Getting this channel for communication, through young people, underpins that this measure is working.

According to Helmus (2020, p. 164), it is necessary to give the audiences the tools to be critical of the information they receive on social media. This includes the knowledge to identify and consider the sources where they get information and how they can affect others by sharing it. Ukraine made a “Dom-channel” trying to reach out to the Russian-speaking audiences in NGCA. Through this channel, they are sharing Ukrainian information and news in the Russian language. The challenge is that they do not know how many persons are

listening to this information, because of a lack of communication. Ukraine seems not to have found a way to get around the issue of information sharing with this audience.

One of my participants points out the importance of a dialog with social media platforms due to the content on social media. "(…) it is very important to continue the process of establishing their offices in Ukraine. Because there is still this problem that the Ukrainian content is being managed by the office of some social media being located in Moscow".

Another participants education by using teachers and veterans from the war in Donbas. "I think we can create a group of instructors, teachers with 50% of teachers and 50% of veterans from Donbas. To create a channel for information. And it in short terms the information will spread to friends, siblings, and parents." (Interview: 3, 2022). By using people from Donbas to spread information, the audiences trust could increase and there would have been made a "corridor" to get out information to the targeted audiences in the NGCA in Ukraine.

This chapter has discussed the Ukrainian countermeasures against Russian influence operations on social media, and lessons learned from this experience. The next part will briefly investigate to which extent the Ukrainian experiences can be relevant to Norway.

7.0 Are Ukraine's experiences relevant for Norway?

Other countries, including Norway, may have a lot to learn from Ukraine's experiences with Russian influence operations in social media. Both Ukraine and Norway share a border with Russia. At the same time, it should be pointed out that there are several differences between the Norwegian audiences and the audiences in the NGCA of Ukraine. Being a former Soviet republic, Ukraine has a very different history with Russia. In addition, Ukraine has, at least to some extent, been seen as a buffer zone between NATO and Russia.

The Norwegian neighborhood with Russia is different. Norway is a long-standing NATO member. The relation between Norway and Russia has been balanced between cooperation and dialog in the Arctic, and security politics and tension as a representative country for NATO in the north. The balance Norway has in its relation with Russia has probably contributed to a low level of Russian influence operations in Norway. Research done by the Norwegian Defence Research Establishment indicates that Norway was not particularly exposed to foreign influence operations on social media during the parliamentary elections in 2021 (FFI, 2022, pp. 3-4).

Due to internal factors to the level of attraction among the citizens, Norway has a high level of wealth among the citizens. Norway has resources such as oil, gas, and fish, which contribute to the high level of wealth, but also technological development and education. E.g., numbers from 2019 show that about 40% of men and about 50% of women between 25 and 64 years had higher education at a University (Bartsch, 2021, p. 24). Additional to a high level of numbers taking higher education at a University, Norway has had an increasing level of higher vocational education from 2015 to 2021, from 5000 students that completed the education per year to 10 000 students in 2021 (Statistisk Sentralbyrå, 2021). This is different from the people in NGCA, where the wealth and education level is low (Interview: 4, 2022).

On the other hand, today's situation with the Russian re-invasion of Ukraine has changed the security situation in Europe. This will probably also affect Norway and its balanced relationship with Russia. The limits between the society security issues and the state security issues are more blurred because of the increased use of hybrid methods. (Forsvarsdepartementet, 2020, p. 21) One can expect that the use of hybrid methods from Russia can increase. There are several reasons for this:

First, the Russian invasion has inflicted significant costs on the Russian military. There have been losses in both materials and soldiers, and time has shown that Russia has had significant

challenges with logistics and mobilization (VG.no, 2022). Valuable losses additionally to the Russian failure can contribute to a more paranoid Russia in the north. As the northern fleet is weakened and the Russian pride is wounded, the way of low-cost hybrid methods can be tempting, in consonance with the theoretical perspective of hybrid warfare.

Second, Norway has also taken a clear position condemning the Russian re-invasion in Ukraine on February 24th, 2022. Norway has supported Ukraine with economical resources for humanitarian help, military aid in the form of M72 anti-tank missiles and other weapon systems, and sanctions against Russia because of Russia's military actions in Ukraine (Regjeringen, 2022).

Third, influence operations on social media will in general have a lower risk of escalating to regular war. This can lower the threshold to implement such influence operations also in Norway. Creating polarization and tension among the Norwegian citizens can force Norway to place a greater focus on internal affairs, and less focus on foreign affairs. A weak Norway, or a weak Europe, will place Russia in a better position.

Ukraine's experiences show us the importance to be preventive to handle Russian influence operations on social media, both against exposure of Russian influence operations, but also in terms of internal factors to keep the level of attraction low. Factors that might influence these internal factors are higher prices on vital resources like power and food, or essential goods such as fuel. Already polarized debates that create engagement and tension among the citizens, or between the citizens and the authorities, can be utilized by Russian actors who want to influence civilians. Social media is an excellent platform to increase the tension in these debates. Ukraine´s experience brings to light that the most vulnerable and easiest way to influence is through civilian society.

Norwegian actors have actively fronted the importance of being critical of information on social media through education and public awareness programs. Norwegians have a high level of trust in information, as one of the world's most digital countries. At the same time, the technology, strategy, and tactics in the information war are getting more complex (Forsvarsdepartementet, 2020, p. 21).

In periods when hackers find new ways of luring people, banks or other relevant platforms are quick to inform the customers. We are living in a world with an abundance of information. The consequence is that we may miss important information about how to act or react online.

Today, as many as 96% of Norwegian citizens have a smartphone. This number has increased from 57% since 2012 (Statistisk Sentralbyrå, 2022). The fact that most Norwegians have a smartphone, makes sharing of (dis)information easy. On the other hand, the high number of people having a smartphone over a long time has given Norwegians experience and knowledge of how to act safely online.

The older and the youngest generations are probably the most vulnerable. Often, the older generation has a lack of experience with social media. Young people and children often better understand social media than the older generation. However, this group is more exposed as they use social media to a greater extent. They do not necessarily have not developed a knowledge of how to distinguish between fake and true information (Medietilsynet.no, 2021; Medietilsynet, 2020).

When the war in Donbas started in April 2014, the information war had been ongoing for a while. Even though the influence operations got more intense during the Euromaidan protests in December, the spread of pro-Russian narratives on social media had been ongoing for a longer period. It started with regular media channels, and most of the Ukrainian citizens in Donbas got information from traditional media. Therefore, this was an easy platform for Russia to influence on. A narrative was established, which created a ground for further, more intense influence when the Euromaidan protests started, followed by the Russian annexation of Crimea and the war in Donbas.

The slow and patient establishment of a narrative shows us the importance of always being aware of Russian influence operations on social media. As I mentioned earlier, the high number of people having smartphones creates easy access to influence operations. This can be (dis)information spread in high amounts from bots or trolls aiming to cause tension and polarization in discussions. Therefore, it is essential to monitor different social media platforms during specific events or protests that engage the citizens and, in general, make sure that a Russian narrative's slow and patient establishment won’t find a place.

If Russia uses several methods from the hybrid warfare toolbox, this creates a synergic effect. The total defense will therefore be important in this context. How will the citizens react if the vital infrastructure is being sabotaged or personal information is missing in a cyber-attack? If the drinking water is poisoned or TV signals are jammed? Even though there are several differences between the Norwegian society and the society in NGCA in Ukraine, it still shows us that the context these people were living in, characterized by chaos, violence, and

insecurities, raised the level of attraction to Russian influence operations in social media. Also, before the war started in 2014.

Ukraine's experience tells us that being preventive is a much more robust measure than acting after the influence operations have started. The focus on being prepared for Russian influence operations should be prioritized by preventive actions and ready to act when the Russian influence operations on social media take place.

On the other hand, the Ukrainian countermeasure by sanctioning Russian social media platforms will not agree with the Norwegian values of democracy. As I mentioned, Norway has a high rate of democracy. The democratic values are strong and grounded in the Norwegian constitution, which highlighted freedom of the press from early on (Stortinget, 2018).

Another factor is that the context the targeted audiences in the NGCA in Ukraine lived in, differ from the Norwegian citizens in three aspects. First, Norwegians does not share the same language or identity as Russia. This will make it harder to establish a Russian narrative in Norway. Second, the people in the NGCA and the rest of Ukraine was to some extent already polarized before the Euromaidan protests, as I mentioned earlier. Third, the context was characterized of war and insecurities after April 2014. These factors increased Russia's ability to attract. However, the Ukrainian experiences to counter Russian influence operations on social media is unique and bring us important knowledge.

8.0 Summary and conclusion

In this research study, I wanted to understand better how Ukraine countered Russian influence operations on social media and if Ukraine's experiences are relevant to Norway. The research question was: **Did Ukraine manage to counter Russian influence operations on social media in 2014, and is it relevant for Norway?**

To answer the research question, I examined the Ukrainian issues of the targeted audiences in the NGCA in Ukraine, Russian narratives on social media, the Russian social media platforms Vkontakte and Odnoklassniki, and the use of bots and trolls as a tool to influence the audience. Further, I investigated Ukraine's countermeasures against the Russian influence operations on social media and lessons learned from these experiences. Last, I briefly discussed the extent to which the Ukrainian experiences were relevant to Norway.

8.1 Findings

Ukraine's experience challenging Russian influence operations on social media addresses that the countermeasures are about the Russian actors' ability to attract. Ukraine's strategy of lowering the aggressor's ability to attract agrees with Joseph Nye's soft power theory. The ability to attract depends on two aspects: First, the internal issues among the targeted audience, which turns on how easily the people are attracted to Russian influence operations. Second, the external elements of exposure, such as content and methods of Russian influence operations on social media. Many factors can influence these two variables. The external factors depend on the aggressor's capabilities, the content of information, and the frequency of sharing disinformation. The internal factors rely on the audience's knowledge of media literacy and if they are united rather than polarized.

The targeted audiences in NGCA lived in a region with low wealth and low education levels among the people. From April 2014, they also lived in a war zone. The high number of people speaking Russian, and identified as Russian, increased Russian actors' ability to influence these targeted audiences. The Russian narratives turned more aggressive, and many people in the NGCA believed in the anti-Ukrainian narratives. By spreading the narratives, Russia created fear and mistrust among the audiences against the Ukrainian government and military.

When the war broke out in the Donbas region in 2014, Russian capabilities in the information war consisted of access to personal information from personal accounts on VK and OK, botnets and troll farms, and other individual pro-Russia influencers that were able to promote the Russian perspective and spread Russian disinformation.

The FSB's access to personal information through VK and OK allowed Russia to target the audience by reaching out to people based on interests, political views, and networks. Through personal information, it could be easier to target the audience specifically. In that matter, Russia could raise its ability to attract an audience by spreading targeted disinformation.

Using botnets and troll farms, Russian actors such as the Internet Research Agency (IRA) – a company owned by 'Putin's Chef' and located in St. Petersburg - could spread much disinformation at high speed to many people. Bots and trolls produced much disinformation. There were also established botnets in Ukraine. In that event, Russia's influence operations in the NGCA could increase the level of attraction among the targeted audiences. By using trolls, they could reach into peoples' emotions. It lured the audience into taking the bait and then being hauled in. In this process, the goal was to create discussions, increase tension, and create antagonism between the population and the central authorities in Kyiv.

Regarding Ukrainian countermeasures, the Government did not have the capacity to counter the Russian information war when the war broke out. First and foremost, the civil society countered Russian influence operations on social media. Media houses and organizations such as StopFake, Information Resistance, Ukraine Crisis Media Center, Detektor Media, and Europress were established or reconstructed to debunk and disprove Russian disinformation. Some organizations focused on getting the information out to the international society to tell the Ukrainian perspective of the events.

The debunking of disinformation turned out to not be the most effective way to counter Russian influence operations on social media. However, it was a necessary measure to get the Ukrainian perspective on the agenda. In December 2014, the Ukrainian Government established a Ministry of Information Policy and aimed to get information to the targeted audiences in NGCA in Donbas. Get out information to the NGCA turned out to be difficult because of technical issues and unavailability because of the Russian jamming of Ukrainian channels and the ongoing war.

Ukraine started to work proactively. The Government began to welcome children and students to visit and take higher education in Western Ukraine to give them another perspective on Ukraine and the world. Students from NGCA were sometimes surprised by how the situation was, growing up with parents that thought Nazis were coming to kill them. Education of media literacy and the Ukrainian perspective turned out to be a more effective countermeasure, as it lowered the Russian ability to attract.

To decrease the exposure of Russian influence operations on social media, the Ukrainian government decided to block VK and OK. The sanction against the Russian social media platforms worked effectively, and people's social media habits changed to western platforms with less Russian disinformation. On the other hand, the Russian platforms got a built in-VPN that works in the NGCA, and the measure was not in accordance with the human rights of media freedom.

The Security Services of Ukraine shut down several botnets to decrease the exposure further. The issue of bots and trolls is challenging, and new botnets and troll farms are being established. However, it turns out that bots and trolls have various effects and can be prevented by media literacy education.

Norway can learn from the Ukrainian experiences with Russian influence operations. However, Norway cannot adopt measures that violate democratic values like media freedom and need to consider the differences between the Norwegian audience and the Ukrainian audience in the NGCA in Ukraine. The analysis highlights the preventive measures of education and information sharing as one of the most effective measures to keep the Russian ability to attract low.

Norway has not been exposed to Russian influence operations on social media considerably. Nonetheless, because of the Russian reinvention in Ukraine on February 24th, which changed the security situation in Europe, one can expect more frequent use of low-intensity hybrid methods from Russia, also in Norway. Norway should therefore put a greater focus on monitoring social media for Russian influence operations and prepare to act if the exposure gets high. This will be an essential aspect of strengthening the total defense in Norway.

8.2 Avenues for further research

As I mentioned, this study does not examine Ukraine's strategy for strategic communication or its strategy for uniting the Ukrainians with a grounded, common narrative. The Ukrainian people's morals due to the Russian re-invention in Ukraine in 2022 show us that the Ukrainian people are more united in 2022 than eight years ago. In 2014, the war was characterized by chaos, disorder, and polarization. Until May 2022, Ukraine has been a big step ahead of Russia in the information war. Additionally to the Ukrainian countermeasure this analysis examined, it would have been interesting and valuable to know more about the strategic communication that has brought the people more together.

Also, an analysis of different groups of people in Norway that can be more vulnerable to Russian influence operations on social media would have been helpful. This could contribute to a preventive measure against protentional Russian influence operations on social media. As the security situation in Europe has changed, we can expect an increase in low-intensive hybrid methods against Norway and Europe. Examining potential target audiences will give the security services in Norway an opportunity to take preventive measures.

Bibliography

Åtland, K., & Hakvåg, U. (2014). Russlands intervensjon på Krim - Gjennomføring og konsekvenser. *Norsk Militært Tidsskrift*(184), pp. 16-29.

Babak, A. M., Matychak, T., Moroz, V., Puhach, M., Minich, R., Rybak, V. and Yermolenko, V. (2017). *Words and Wars. Ukraine Facing Kremlin Propaganda.* Kyiv: NGO Internews Ukraine.

Bartsch, B. (2021). *Fakta om utdanning 2021 - nøkkeltall fra 2019.* Statistisk Sentralbyrå. Retrieved from https://www.ssb.no/utdanning/artikler-og-publikasjoner/_attachment/442056?_ts=176cc50e7d8

BBG. (2014). *Contemporary Media Use in Ukraine.* Broadcasting Board of Governors. Broadcasting Board of Governors.

Bergh, A. (2020). *Påvirkningsoperasjoner i sosiale medier - oversikt og utfordringer.* Forsvarets Forskningsinstitutt . Forsvarets Forskningsinstitutt .

Bialy, B., & Sanda, S. (2016). *New Trends in Social Media.* Riga, Kalnciema iela 11b, Latvia LV1048: NATO Strategic Communications Centre of Excellence.

Bogner, A., Littig, B., & Menz, W. (2009). *Interviewing Experts.* United Kingdom: Palgrave Macmillan.

Boyte, K. J. (2017, Winter). An analysis of the social media technology, tactics, and narratives used to control perception in the propaganda war over Ukraine. *Journal of Information Warfare, 16:1*, pp. 88-11.

Cantin, J. M., Pendleton, H. D., & Moilanen, J. (2015). *Threat Tactics Report: Russia.* TRADOC G-2 ACE Threats Integration. IHS Jane's Defence Weekly.

Dawson, A., & Innes, M. (2019). *The Internet Research Agency in Europe 2014-2016.* Cardiff University Crime & Security Research Institute. Cardiff: Cardiff University.

Demartino, A. (2021). *False Mirrors - The Weaponization of Social Media in Russia's Operation to Annex Crimea* (Vols. Ukrainian Voices, vol. 13). Stuttgart: ibidem.

Disen, S. (2018). *Lavintensivt hybridangrep på Norge i en fremtidig konflikt.* Forsvarets forskningsinstitutt (FFI).

Dutsyk, D., Shutov, R., Burkovskyi, P., & Chernenko, S. (2015). *Counteraction to Russian Information Aggression: Joint action to protect democracy.* Kyiv: NGO Telekritika.

Erlich, A., & Garner, C. (2021). Is pro-Kremlin Disinformation Effective? Evidence from Ukraine. *The International Journal of Press/Politics*, pp. 1-24.

Fabian, S. (2019, August 09). The Russian hybrid warfare strategy – neither Russian nor strategy. *Defense & Security Analysis, 35*(3), pp. 308-325.

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016, July). *The Rise of Social Bots*. Retrieved April 2022, from Communications of the ACM (casm.asm.org): https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext

FFI. (2022). *Uønsket utenlandsk påvirkning? – kartlegging og analyse av stortingsvalget 2021*. Forsvarets Forskningsinstitutt.

FN-sambandet. (2021, Januar 21). *Tema - Menneskerettigheter*. Retrieved April 2022, from FN.no: https://www.fn.no/tema/menneskerettigheter/menneskerettigheter

FN-sambandet. (2022, 09 05). *Konflikter, Ukraina*. Retrieved 11 2022, from FN.no: https://www.fn.no/Konflikter/ukraina

Forsvarsdepartementet. (2020). *Evne til forsvar – vilje til beredskap Langtidsplan for forsvarssektoren.* Forsvarsdepartementet.

Forsvarsdepartementet. (2021-2022). *Prioriterte endringer, status og tiltak i forsvarssektoren.* Det kongelige Forsvarsdepartement. Regjeringen.no.

Freedom House. (2017). *Freedom on the net 2017 Country Report, Ukraine.* . Retrieved April 2022, from Freedomhouse: https://freedomhouse.org/country/ukraine/freedom-net/2017

Freedomhouse. (2021). *Nations in transit, Ukraine, 2021*. Retrieved 2022, from Freedomhouse: https://freedomhouse.org/country/ukraine/nations-transit/2021

Freedomhouse. (2022, April). *Explore the map, 2022*. Retrieved from Freedomhouse: https://freedomhouse.org/explore-the-map?type=fiw&year=2022

Freedomhouse. (2014). *Nations in Transit, Ukraine, 2014.* Retrieved 2022, from Freedomhouse: https://freedomhouse.org/country/ukraine/nations-transit/2014

Freedomhouse. (2016). *Freedom on the net 2016, Ukraine.* Freedomhouse.

Freedomhouse. (2017). *Freedom in the world 2017*. Retrieved May 12, 2022, from Freedomhouse: https://freedomhouse.org/country/ukraine/freedom-world/2017

Fridman, O. (2017, April 03). Hybrid Warfare or Gibridnaya Voyna? *The RUSI Journal, 162*(1), pp. 42-49.

Fridman, O. (2018). *Russian Hybrid Warfare: Resurgence and Politicization.*

Galaktionova, A. (2016, August 03). *Информация по заказу: влияют ли бюджеты СМИ на их рейтинги?* Retrieved May 2022, from Forbes: https://www.forbes.ru/kompanii/internet-telekom-i-media/infographics/325709-informatsiya-po-zakazu-vliyayut-li-byudzhety-s

Galeotti, M. (2015, 08 19). Hybrid War as a War on Governance. (O. Manea, Interviewer)

Galeotti, M. (2017). *Controlling Chaos - How Russia Manages its political war in Europe.* European Council on Foreign Relations. ECFR.

Götz, E., & Merlen, C.-R. (2018, November 15). Russia and the question of world order. *European Politics and Society, 20*(2), pp. 133-153.

Grushetsky, A., Kruglashov, A., Lygachova, N., Paniotto, V., Petrenko, G., & Shutov, R. (2018). *OPPOSITION TO RUSSIAN PROPAGANDA AND MEDIA LITERACY: results of all-Ukrainian opinion poll.* Kyiv: NGO Detektor Media.

Helmus, T. (2020, October 23). Social Media and Influence Operations Technologies - Implications for Great Power Competition. *Strategic Assessment 2020: Into a New Era of Great Power Competition*, pp. Chapter 7, 153–166.

Hoskins, A., & O´Loughlin, B. (2010). *War and Media: The Emergence of Diffused War*. Cambrigde/Malden, UK/USA : Polity Press.

Hurska, A. (2020, March 3). *Eurasia Daily Monitor: Russian 'Bot Farms'—The New-Old Challenge to Ukraine's National Security*. Retrieved from The Jamestown Foundation: https://jamestown.org/program/russian-bot-farms-the-new-old-challenge-to-ukraines-national-security/

Hurska, A. (2022, April 19). *Eurasia Daily Monitor, Ukraine's Other Front: The Battle in the Cyber Domain*. Retrieved April 2022, from The Jamestown Foundation: https://jamestown.org/program/ukraines-other-front-the-battle-in-the-cyber-domain/

Johannessen, A., Tufte, P. A., & Christoffersten, L. (2005). *Introduksjon til samfunnsvitenskapelig metode* (5. utgave ed.). Abstrakt forlag AS.

Kasapoglu, C. (2015). Russia's Renewed Military Thinking:: Non-Linear Warfare and Reflexive Control. *NATO Defense College.*

Kauppi, M. V., & Viotti, P. R. (2020). *International Relations Theory* (Vol. 6). London, United Kingdom: Rowman & Littlefield.

Kudelia, S. (2016). The Donbas Rift. *Russian Politics & Law, 54*(1), pp. 5-27.

Kvale, S., & Brinkmann, S. (2015). *Det Kvalitative Forskningsintervju* (3. utgave ed., Vol. 2017). Oslo: Gyldendal Akademisk.

Lange-Ionatamishvili, E. (2016). *FRAMING OF THE UKRAINE–RUSSIA CONFLICT IN ONLINE AND SOCIAL MEDIA.* NATO Strategic Communications Centre of Excellence. Riga: NATO Strategic Communications Centre of Excellence.

Lange-Ionatamishvili, E., & Svetoka, S. (2015). Strategic Communications and Social Media in the Russia-Ukraine Conflict. *Cyber War in Perspective: Russian Aggression against Ukraine*, pp. 101-111.

Lucas, E., & Pomeranzev, P. (2016). *Winning the Information War Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe.* Washington: The Center for European Policy Analysis.

Lukes, S. (2015). Robert Dahl on power. *Journal of Political Power, 8*(2), pp. 261-271.

Matveeva, A. (2016, February 25). No Moscow stooges: identity polarization and guerrilla movements in Donbass. *Southeast European and Black Sea Studies, 16:1*, pp. 25-50.

Mearsheimer, J. (2014). Why the Ukraine Crisis Is the West's Fault: The Liberal Delusions That Provoked Putin. *Foreign Affairs, 93*(5), pp. 77-89.

Medietilsynet. (2020). *BARN OG MEDIER 2020.* Medietilsynet.

Medietilsynet.no. (2021, September 02). *Seniorskole: Slik oppdager du falske nyheter og håndterer innhold på nettet*. Retrieved May 15, 2022, from Medietilsynet: https://www.medietilsynet.no/digitale-medier/skole/seniorguide/

Mejias, U. A., & Vokuev, N. E. (2017, January 6). Disinformation and the media: the case of Russia and Ukraine. *Media, Culture & Society, 39*(7), pp. 1027-1042.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). *Qualitative Data Analysis: A Methods Sourcebook* (4th edition ed.). California: SAGE Publications, inc.

MSC. (2015). *Munich Security Report.* Munich Security Conference.

NATO StratCom COE. (2016). *New Trends in Social Media.* Riga, Kalnciema iela 11b, Latvia LV1048: NATO Strategic Communications Centre of Excellence.

Nye, J. (2021, February 10). Soft Power: The evolution of a consept. *Journal of Political Power*.

Odnoklassniki. (2012, July 18). *Archive.today*. Retrieved April 2022, from Odnoklassniki.ru: https://archive.ph/20120718002705/http://odnoklassniki.ru/cdk/st.cmd/helpAbout/tkn/729#selection-355.113-371.145

Orlova, D., & Shutov, R. (2018). *MEDIA CONSUMPTION AND ASSESSMENT OF SOCIAL AND POLITICAL PROCESSES IN UKRAINE BY THE RESIDENTS OF EASTERN REGIONS* . Kyiv : NGO Detektor Media .

Ozoliņa, Ž., Šķilters, J., Struberga, S., Denisa-Liepniece, S., Austers, I., & Kyiak, M. (2017). *Stratcom Laughs: In search of an analytical framework.* NATO Stratcom COE. Riga: NATO Strategic Communication Centre of Excellence.

Prozorro. (2021, October 30). *DOM CHANNEL ADS ALL OVER UKRAINE: COST AND REASONS*. Retrieved Mai 4, 2022, from Transparency International Ukraine: https://ti-ukraine.org/en/blogs/dom-channel-ads-all-over-ukraine-cost-and-reasons/

Regjeringen. (2022). *Tidslinje: Regjeringens håndtering av krigen i Ukraina*. Retrieved May 2022, from Regjeringen.no: https://www.regjeringen.no/no/tema/ukraina/tidslinje-regjeringens-handtering-av-krigen-i-ukraina/id2906711/

Regjeringen. (2022b, February 21). *Ukraina: Norge fordømmer russisk beslutning*. Retrieved May 13, 2022, from Regjeringen.no: https://www.regjeringen.no/no/aktuelt/russland_donetsk/id2901637/

Reichborn-Kjennerud, E., & Cullen, P. (2016). What is Hybrid Warfare? *Multinational Capabilities Development Campaign* (1), pp. 1-4 .

Robinson, P. (2010). Soviet Hearts-and-Minds Operations in Afghanistan. *The Historian, 72*(1), pp. 1-22.

Rozumiy, O. (2013, July 13). *RB.ru* . Retrieved from В ТОП-100 самых популярных соцсетей в мире «ВКонтакте» и «Одноклассники» заняли 9 и 10 место: https://rb.ru/news/v-top-100-samyh-populyarnyh-socsetej-v-mire-vkontakte-i-odnoklassniki-zanyali-9-i-10-mesto/

Samokhvalova, L. (2016, January 1). *Московський слід колорадського Жука, або Хто і як готує «Майдан-3»*. Retrieved from Ukrinform.ua : https://www.ukrinform.ua/rubric-polytics/1948496-moskovskij-slid-koloradskogo-zuka-abo-hto-i-ak-gotue-majdan3.html

Sasse, G., & Lackner, A. (2018, March 29). War and identity: the case of the Donbas in Ukraine. *Post-Soviet Affairs, 34*(2-3), pp. 139-157.

Schnaufer II, T. A. (2017). Redefining Hybrid Warfare: Russia's Non- linear War against the West. *Journal of Strategic Security, 10*(1), pp. 17-31.

Sotiriou, S. A. (2016, February 29). The irreversibility of history: the case of the Ukrainian crisis (2013–2015). *Southeast European and Black Sea Studies, 16*(1), pp. 51-70,.

Språkrådet. (2017, August 14). *Sprakradet.no*. Retrieved Mars 2022, from Spørsmål og svar: https://www.sprakradet.no/svardatabase/sporsmal-og-svar/narrativ-bruk-og-genus/

SSU . (2022, March 28). *ПРЕСЦЕНТР* . Retrieved from службА безпеки України: https://ssu.gov.ua/novyny/z-pochatku-viiny-sbu-likviduvala-5-vorozhykh-botoferm-potuzhnistiu-ponad-100-tys-feikovykh-akauntiv

Statistisk Sentralbyrå . (2021, 12 14). *Statistikkbanken - Høyere yrkesfaglig utdanning*. Retrieved April 2022, from Statistisk Sentralbyrå: https://www.ssb.no/statbank/table/11636/tableViewLayout1/

Statistisk Sentralbyrå. (2022, April 26). *Statistikkbanken - Norsk Mediebarometer*. Retrieved April 2022, from Statistisk Sentralbyrå: https://www.ssb.no/statbank/table/05244/tableViewLayout1/

Stortinget. (2018, 05 09). *Eidsvoll og Grunnloven 1814*. Retrieved May 14, 2022, from Stortinget.no: https://www.stortinget.no/no/Stortinget-og-demokratiet/Grunnloven/Eidsvoll-og-grunnloven-1814/

StratComCOE. (2020). *StratComCOE*. Retrieved 10 2021, from About NATO StratCom COE: https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5

Thagaard, T. (2013). *Systematikk og innlevelse - En innføring i kvalitativ metode* (4. utgave ed.). Bergen : Fagbokforlaget.

The Bell. (2021, December 6). *Russia takes direct control of top social media networks*. Retrieved April 2022, from The Bell: https://thebell.io/en/russia-takes-direct-control-of-top-social-media-networks/

Tsygankov, A. (2015, February 4). Putin's last stand. *Post Soviet affairs, 31*(4), pp. 279-303.

VG.no. (2022, April 01). Dette kan være Russlands neste mål: − De er nødt til å reorganisere. VG.no.

Volchek, D., & Bigg, C. (2015, May 29). *Ukrainian Bloggers Hunt Down Russian Soldiers In War-Torn East*. Retrieved May 2022, from Radio Free Europe, Radio Liberty: https://www.rferl.org/a/ukraine-blogger-hunts-down-russian-soldiers-in-war-torn-east/27043337.html

Weissman, M. (2019). Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework. *Journal on Baltic Security*, *5*(1), pp. 17–26.

Abbreviations

DNR: The «People's Republic of Donetsk"

LNR: The "People's Republic of Luhansk"

NGCA: Non-Governmental-Controlled Areas in Ukraine

SSU: Security Services of Ukraine

StratCom COE: The NATO Strategic Communication of Excellence

Attachments

NSD NORSK SENTER FOR FORSKNINGSDATA

Vurdering

Referansenummer

316818

Prosjekttittel

Did Ukraine manage to counter Russian influence operations in social media – and is it of relevance for Norway?

Behandlingsansvarlig institusjon

Nord Universitet / Fakultet for samfunnsvitenskap / Internasjonale relasjoner, nordområder og miljø

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Kristian Åtland , kristian.atland@nord.no, tlf: 99632623

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Trude Marielle Gjelsten, trudegjelsten@hotmail.no, tlf: 46423346

Prosjektperiode

02.08.2021 - 31.05.2022

Vurdering (1)

08.12.2021 - Vurdert

Det er vår vurdering at behandlingen vil være i samsvar med personvernlovgivningen, så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet den 08.12.29 med vedlegg, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 31.05.2022.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 nr. 11 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse, som kan dokumenteres, og som den registrerte kan trekke tilbake.

For alminnelige personopplysninger vil lovlig grunnlag for behandlingen være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen:

- om lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet.

DE REGISTRERTES RETTIGHETER
NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18) og dataportabilitet (art. 20).

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Office 365 og Nettskjema er databehandlere i prosjektet. NSD legger til grunn at behandlingen oppfyller kravene til bruk av databehandler, jf. art 28 og 29.

For å forsikre dere om at kravene oppfylles, må prosjektansvarlig følge interne retningslinjer/rådføre dere med behandlingsansvarlig institusjon.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilken type endringer det er nødvendig å melde:
https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema
Du må vente på svar fra NSD før endringen gjennomføres.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Kontaktperson hos NSD: Tore Andre Kjetland Fjeldsbø
Lykke til med prosjektet!

Interview guide

Where are you from?

Which kind of job/role do you have in Ukraine?

- Also back in 2013/14?

What is your relation to social media (SoMe)?

- Which platforms do you use yourselves? (back in 2013/14?)
- Which SoMe platforms are popular among the Ukrainians?

The three aspects I am interested in is how to identify, challenge, and learn from experiences of foreign influence operations in social media:

- Identification of foreign influence efforts via social media platforms.
- Efforts that have been made to challenge, neutralize, or reduce the effect of such efforts
- Lessons that have been learned in the process. What has been prepared, and what can be done better?

These aspects are an approach developed to help actors prepare better to meet the challenge of influence operations in social media. The approach is developed by two researchers at the Strategic Communication Centre of Excellence, Sanda Svetoka and Elina Lange-Ionatamishvili. This approach also fits well to structure my research study and for finding whether Ukraine managed to counter-influence operations in social media, and if this experience is in relevance for Norway.

Identify

Have you personally experienced that Ukraine was exposed to Russian influence operations through SoMe?

- Experiences jobwise?
- Experiences on your private SoMe platforms?
- Who was the sender?

What is your experience with Russian influence operations in social media to influence people in Ukraine?

- Good/bad? No experience with this?
- Any specific situations? Personal situations? Related to your job?
- When did it start, and what forms did it take?
- Any variation in the intensity over time?
- Why do you think the operations were initiated? What was the sender's goal?

How did your workplace (government, security agencies, media) seek to identify Russian influence operations in social media?

- Different methods?
- Was it effective?
- What could have been done better?

What do you think is the sender's purpose of these operations?

Challenge

When the influence operations were identified, were they challenged/countered?

- How?
- Did it depend on the method? (Pictures, videos, text, combinations of these?)
- Did it depend on the platform? Purpose? Other factors?
- Do you have any thoughts about something that may have been done differently/better?

Learn and prepare

There is continuous development in the social media platform as well as in the technology for influence operation. How do the Ukrainian state/your section/wo place learn and prepare after these influence operations in 2014?

- What has been done?
- What should be done?

Are there any relevant questions I have missed, or other relevant information you want to share about this theme?

Do you know of any other persons I should contact to collect data for this project?

Do you have any questions/ do you think the interview went well?

Are you interested in taking part in the research project

"Russian Influence Operations through Social Media in Ukraine"?

This is an inquiry about participation in a research project where the main purpose is to seek the extent to which Ukraine managed to counter Russian influence operations in social media, and whether it is relevant for Norway. In this letter, we will give you information about the purpose of the project and what your participation will involve.

Purpose of the project

The project seeks to look at the Ukrainian experience of how to detect and challenge Russian influence through social media. Experiences from employees within the government, security agencies, experts, and the media would strengthen the project. The project is limited to the Donbas region during the period April 2014 to December 2014 from demonstrations in Kyiv to the escalating conflicts in Donbas. The research question for the project is: Did Ukraine manage to counter Russian influence operations in social media – and is it of relevance for Norway? I will seek to find out if Ukraine managed to identify different methods of Russian influence operations in social media, and which methods the Ukrainian state used trying to counter these operations.

The project is a master's thesis associated with the project "Total Defence Cooperation with Ukraine" owned by the Norwegian Defence University College.

Who is responsible for the research project?

Nord University is the institution responsible for the project. I will also use my findings writing a report for the Norwegian Defence University College.

The education and the master thesis are taken through Nord University, with a scholarship through the project "Total Defence Cooperation with Ukraine" at the Norwegian Defence University College.

Why are you being asked to participate?

The selection has been strategical. You have been asked to participate because you are or have been an employee within the government, security agencies, experts, and the media would strengthen the project in the period April 2014-December 2014. You may also have been an employee before/after this or a person with knowledge or competence within Russian influence operation due this period.

What does participation involve for you?

- If you chose to take part in the project, this will involve that you participate in a personal interview with electronic sound recording. Notes will be taken on paper. The interview will take approx. 45 minutes.

Participation is voluntary
Participation in the project is voluntary. If you chose to participate, you can withdraw your consent at any time without giving a reason. All information about you will then be made anonymous. There will be no negative consequences for you if you chose not to participate or later decide to withdraw. It will not affect your treatment at your place of work or employer.

Your privacy – how we will store and use your personal data
We will only use your personal data for the purpose(s) specified in this information letter. We will process your personal data confidentially and by data protection legislation (the General Data Protection Regulation and Personal Data Act).

- The personal data will be accessible for the student and the supervisors.
- To ensure that no unauthorized persons can access the personal data I will replace your name with a code. The list of names, contact details, and respective codes will be stored separately from the rest of the collected data. All the collected data will be either locked away or encrypted.
- The personal data will be processed in Norway. The server where the data is stored is in Norway.

As a participant, you will be anonymous in the publication and your interview will not be published. The interview will be used only for collecting data.

What will happen to your personal data at the end of the research project?

The project is scheduled to end in May 2022. The data will be deleted within a year (May 2023) in case of postponements.

Your rights
So long as you can be identified in the collected data, you have the right to:

- access the personal data that is being processed about you
- request that your personal data be deleted
- request that incorrect personal data about you is corrected/rectified
- receive a copy of your personal data (data portability), and

- send a complaint to the Data Protection Officer or The Norwegian Data Protection Authority regarding the processing of your personal data

What gives us the right to process your personal data?
We will process your personal data based on your consent.

Based on an agreement with Nord University, the Norwegian Defence University College, NSD – The Norwegian Centre for Research Data AS has assessed that the processing of personal data in this project is in accordance with data protection legislation.

Where can I find out more?
If you have questions about the project or want to exercise your rights, contact:

- Nord University via student Trude Marielle Gjelsten, trude.m.gjelsten@student.nord.no Supervisor: Kristian Åtland, kristian.atland@nord.no.
  Supervisor: Tom Røseth, troseth@mil.no
- Our Data Protection Officer at the Norwegian Defence University College: forsvarets.personvernombud@mil.no
- Our Data Protection Officer at Nord University: Toril Irene Kringen
- NSD – The Norwegian Centre for Research Data AS, by email: (personverntjenester@nsd.no) or by telephone: +47 53 21 15 00.

Yours sincerely,

Project Leader (Researcher/supervisor) Student

Consent form

I have received and understood information about the project "Russian Influence Operations in Social Media in Ukraine"? and have been allowed to ask questions. I give consent:

☐ to participate in an interview

I give consent for my personal data to be processed until the end date of the project, approx. May 2023

(Signed by participant, date)

Data processor agreement for the research project "Russian influence operations in social media".

Pursuant to the applicable Norwegian personal data legislation and regulation (EU) 2016/679 of 27th April 2016, Articles 28 and 29, cf. Article 32-36, the following agreement is entered into

between

Nord University
Org.nr. 970 940 243
(data controller)

and

Private Entrepreneur Oleksandra Komarova
(data processor)

24.01.2022

1. Purpose of the agreement

The purpose of the agreement is to regulate the rights and obligations under the applicable Norwegian personal data legislation, and regulation (EU) 2016/679 of 27th April 2016 in respect of the protection of physical persons in connection with the processing of personal data and the free exchange of such data, as well as the repeal of Directive 95/46/EC.

The agreement is intended to ensure that personal data is not processed illegally, wrongfully, or processed in ways that result in unauthorised access, alteration, erasure, damage, loss, or unavailability.

The agreement governs the data processor's processing of personal data on behalf of the data controller, including collection, registration, compilation, storage, disclosure or combinations of these, in connection with the use of/processing in the research study "Russian influence operations in social media".

In the event of conflict, the terms of this Agreement will take precedence over the data processor's privacy policy, or terms of any other agreement entered into between the data processor and the data controller in connection with the use of/processing in the research study "Russian influence operations in social media".

2. Limiting clause

The purpose of the data processor's processing of personal data on behalf of the data controller is to help the data controller translate from Ukrainian to English during an in-depht interview for collecting data.

Personal data that the data processor processes on behalf of the data controller may not be used for any other purpose without the prior approval of the data controller.

The data processor may not transfer personal data covered by this agreement to partners or other third parties without the prior approval of the data controller, cf. point 10 of this agreement.

3. Instructions

The data processor will follow the written and documented instructions for the processing of personal data in the research study "Russian influence operations in social media" which the data controller has determined will apply.

North University is obliged to comply with all obligations under the applicable Norwegian personal data legislation governing the use of the research study "Russian influence operations in social media" for the processing of personal data.

The data processor is obliged to notify the data controller if it receives instructions from the data controller that are in conflict with the provisions of the applicable Norwegian personal data legislation.

4. Types of information and data subjects

The data processor processes the following personal data on behalf of the data controller:

24.01.2022

- The data will be an in-depth interview with one participant. The interpreter will therefore meet the participant.
  - Identifiable
  - Name and profession
  - Receive non-classified information about Russian influence operations in social media in Ukraine

- The interpreter will not be able to store information from the service.

The personal data applies to the following data subjects:

- The information belongs to a project of a master student belonging to Nord University. The information will be used in a master thesis. The interpreter will do the service by helping the student translate from Ukrainian to English during an interview.

5. The rights of registered subjects

The data processor is obliged to assist the data controller in safeguarding the rights of registered subjects in accordance with applicable Norwegian personal data legislation.

The rights of the data subjects include, but not limited to, the right to information on how his or her personal data is processed, the right to request access to personal data, the right to request corrections to, or erasure of their own personal data, and the right to require restriction of processing of their personal data.

To the extent relevant, the data processor will assist the data controller in maintaining the registered subject's right to data portability and the right to object to automated decision-making, including profiling.

The data processor is liable for damages to the registered subject if errors or omissions by the data processor inflict financial or non-financial loss on the registered subject as a result of infringement of their rights or privacy protection.

6. Satisfactory data security

The data processor will implement appropriate technical, physical and organisational safety measures to safeguard the personal data covered by this agreement from unauthorised or unlawful access, alteration, erasure, damage, loss, or unavailability.

The data processor will document its own security organisation, guidelines and routines for security, risk assessments and established technical, physical or organisational security measures. The documentation will be made available to the data controller on request.

The data processor will establish continuity- and contingency plans for effective handling of serious security incidents. The documentation will be made available to the data controller on request.

The data processor will document the training of its own employees in data security. The documentation will be made available to the data controller on request.

- One measure is to sign this contract with agreements on confidentiality

24.01.2022

- The interpreter (data processor) will not be able to take notes or record anything during the interview.
- The data controller will store the data according to Nord university´s guidelines.

7. Confidentiality

Only employees of the data processor, who need to access personal data that is processed on behalf of the data controller in connection with their work, may be granted such access. The data processor is required to document guidelines and routines for control of access. The documentation will be made available to the data controller on request.

Employees of the data processor have a duty of confidentiality in respect of documentation and personal data to which they gain access in accordance with this agreement. This provision also applies after termination of the agreement. The duty of confidentiality includes employees of third parties who perform maintenance (or similar tasks) on systems, equipment, networks or buildings that the data processor uses to provide the service.

Norwegian legislation will be able to limit the scope of the duty of confidentiality for employees of the data processor and third parties.

8. Access to security documentation

The data processor is obliged to provide the data controller, upon request, with access to all security documentation that is necessary for the data controller to be able to meet its obligations under the applicable Norwegian personal data legislation.

The data processor is obliged to provide the data controller, upon request, with access to other relevant documentation that allows the data controller to assess whether the data processor complies with the terms of this agreement.

The data controller has a duty of confidentiality in respect of confidential security documentation which the data processor makes available to the controller.

9. Security Breach Notification

The data processor will notify the controller without undue delay, if personal data processed on behalf of the controller is exposed to a breach of security.

The data processor's notification should, at minimum, include information that describes the security breach, which registered subject is affected by the breach, what personal data is affected by the breach, what immediate measures are implemented to address the breach and what preventive measures may have been established to avoid similar incidents in the future.

The data controller is responsible for ensuring that the Norwegian Data Protection Authority is notified when required according to the data protection legislation.

10. Sub-processors

The data processor is obliged to enter into separate agreements with sub-processors that govern the sub-processor's processing of personal data in connection with this agreement.

24.01.2022

In agreements between the data processor and sub- processors, the sub- processors will be required to comply with all the obligations to which the data processor is subject under this agreement and according to law. The data processor is obliged to submit the agreements to the data controller on demand.

The data processor will verify that sub-processors comply with their contractual obligations, in particular that data security is satisfactory and that employees of the sub-processors are familiar with their obligations and fulfil them.

The data controller approves that the data processor contracts the following sub-processors to satisfy this agreement:

.....
(names of sub-processors)

The data processor may not contract any other sub-processors than those listed above without prior written approval by the data controller.

The data processor is liable for damages to the data controller for any financial loss that is inflicted on the data controller, and that is due to illegal or improper processing of personal data or inadequate data security on the part of sub-processors.

11. Transfer to countries outside the EU/EEA

- The data will not be stored or processed in countries outside the EU/EEA

12. Safety audits and impact assessments

The data processor will regularly implement security audits of its own work with safeguarding of personal data from unauthorised or unlawful access, alteration, erasure, damage, loss, or unavailability.

Security audits will include the data processor's security goals and security strategy, security organisation, guidelines and routines for security work, established technical, physical and organisational safeguards and the work of data security at sub-processors to this agreement. It will also include routines for warning the data controller in the event of security breaches, and routines for testing of emergency and continuity plans.

The data processor will document the security audits. The data controller will be granted access to the audit reports on request.

If an independent third party conducts security audits at the data processor, the data controller will be informed of which auditor is being used and be given access to the summaries of the audit reports on request.

13. Return and erasure

Upon termination of this agreement, the data processor is obliged to return and erase any personal data that is processed on behalf of the data controller under this agreement. The data processor determines how the return of the personal data will take place, including the format to be used.

Erasure is to be carried out by the data processor within 1 (one) day after the termination of the agreement. This also applies to the backup of personal data.

24.01.2022

The data processor will document that the erasure of personal data has been carried out in accordance with this agreement. The documentation will be made available to the data controller on request.

The data processor covers all costs associated with the return and erasure of the personal data covered by this agreement.

14. Breach of contract

In case of breach of the terms of this agreement caused by errors or omissions on the part of the data processor, the data controller may cancel the agreement with immediate effect. The data processor will continue to be obliged to return and erase personal data processed on behalf of the data controller pursuant to the provisions of Section 13 above.

The data controller may require compensation for financial loss suffered by the data controller as a consequence of errors or omissions on the part of the data processor, including breach of the terms of this agreement, cf. also points 5 and 10 above.

15. Duration of the Agreement

This agreement applies during the interpretation at January 25th 2022.

The agreement may be terminated by both parties with a mutual deadline of January 25th 2022.

16. Contacts

Contact person at the data processor for any questions related to this agreement is:

Private Entrepreneur Oleksandra Komarova.
Oleksandra Komarova, sasha.komarova@gmail.com, +380 98 477 2633.

Contact person at the data controller for any questions related to this agreement is:

Adjunct Professor Kristian Åtland, Nord University, Faculty of Social Sciences, email kristian.atland@nord.no (Academic Supervisor of Trude Gjelsten).

17a. Choice of Law and Legal Venue

The agreement is governed by Norwegian law and the parties accept Salten District Court as legal venue. This also applies after termination of the agreement.

***

24.01.2022

This agreement is in 2 – two copies, one to each of the parties.

Place and date

Oslo 24.01.22

On behalf of the data controller	On behalf of the data processor
.....	.....
(signature)	(signature)

24.01.2022