

Bjørnar Fidje Liberg

Risk Perception of Influence Operations on Social Media

Master's thesis in Information Security

Supervisor: Gaute Bjørklund Wangen

Co-supervisor: Vasileios Gkioulos

May 2021

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication
Technology



Norwegian University of
Science and Technology

Bjørnar Fidje Liberg

Risk Perception of Influence Operations on Social Media

Master's thesis in Information Security
Supervisor: Gaute Bjørklund Wangen
Co-supervisor: Vasileios Gkioulos
May 2021

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology



Kunnskap for en bedre verden

Risk Perception of Influence Operations on Social Media

Bjørnar Fidje Liberg

May 28, 2021

Abstract

Influence operations are organised attempts to affect a group's decision-making, beliefs, and opinions, preferably without the group realising they are being targeted. Malicious influence operations have become a valuable tool in the political warfare arsenal of many nations, with perhaps the most well-known example being Russia's attempts to influence elections in the USA. Social Media has played a part in making these operations more advanced, with better tools for reaching more people more effectively. This project looks at the risk perception of the Norwegian public towards malicious influence operations on social media, with a focus on the cognitive dimension of risk perception.

Data for the project was gathered by conducting a survey on the Norwegian population (N=333). The survey revolved around the participants' beliefs of their own familiarity with the subject, their perception of the prevalence of influence operations in Norway, and their perception of how effective these influence operations can be in achieving their goals.

The project found that the Norwegian public perceives malicious influence operations on social media as a moderate risk. Most respondents feel they are at least slightly familiar with influence operations, and very familiar with fake news, a tactic that is widely used by these operations. They believe that Norway is being targeted by both "local" and foreign operations, but that it is not as prevalent in Norway as it is in the rest of the world. They also believe that these operations are moderately effective at making people believe fake information, or making people vote for a certain candidate in an election.

Sammen drag

Påvirkningsoperasjoner kan defineres som organiserte forsøk på å påvirke en gruppe menneskers beslutningstaking, holdninger, og meninger, helst uten at gruppen innser at de blir påvirket. Ondsinne de påvirkningsoperasjoner har blitt et verdifulle redskap i politisk krigføring for mange nasjoner, mest kjent av disse er kanskje Russland sine forsøk på å påvirke amerikanske valg. Sosiale medier har spilt en stor rolle i å gjøre disse operasjonene mer avanserte, med bedre verktøy for å nå flere folk mer effektivt. Dette prosjektet ser på risiko oppfatningen til det norske folk om ondsinne de påvirkningsoperasjoner på sosiale medier, med et fokus på den kognitive dimensjonen av risiko oppfatning.

Data for prosjektet ble samlet inn gjennom en spørreundersøkelse på den norske befolkningen (N=333). Undersøkelsen fokuserte på deltakernes oppfatninger om deres egen kjennskap til temaet, deres tanker om hvor utbredt påvirkningsoperasjoner er, og tanker om hvor effektive de er til å oppnå målene sine.

Prosjektet fant at den norske befolkningen oppfatter ondsinne de påvirkningsoperasjoner på sosiale medier som en moderat risiko. Et flertall av deltakerne føler at de er minst litt kjent med påvirkningsoperasjoner, og veldig kjent med falske nyheter, en av taktikkene som ondsinne de påvirkningsoperasjoner benytter mye. De tror at Norge blir forsøkt påvirket av både "lokale" og utenlandske operasjoner, men at påvirkningsoperasjoner ikke er like utbredt i Norge som det er i resten av verden. De tror også at disse operasjonene er moderat effektiv på å få personer til å tro på falsk informasjon, eller å få folk til å stemme for en bestemt kandidat i et valg.

Contents

Abstract	iii
Sammendrag	v
Contents	vii
Figures	ix
Tables	xi
1 Introduction	1
1.1 Topic covered by the project	1
1.2 Keywords	2
1.3 Problem description	2
1.4 Justification, motivation and benefits	3
1.5 Research questions	3
2 Background	5
2.1 Influence Operations	5
2.1.1 Political Warfare	5
2.1.2 Tactics, Techniques, and Technology	6
2.2 Social Media	7
2.3 Risk Perception	8
3 Related work	11
3.1 Influence Operations	11
3.1.1 Tactics, Techniques, and Technology	11
3.1.2 Challenges	13
3.1.3 Influence Operations in Norway	14
3.2 Social Media	15
3.2.1 Politics in Social Media	15
3.2.2 Social Media and Trust	16
3.3 Risk Perception	17
3.3.1 Biases in Risk Perception	17
3.3.2 Cyber-Security Awareness	18
4 Methodology	19
4.1 Expert Interview	19
4.1.1 Interview Guide	20
4.1.2 Interview Subjects	20
4.2 Questionnaire	22
4.2.1 Design	22

4.2.2	Distribution Channels	25
4.2.3	Data Analysis	27
5	Results	29
5.1	Demographics and Social Media Activity	29
5.1.1	Gender	29
5.1.2	Age	29
5.1.3	Location	30
5.1.4	Education	32
5.1.5	Social Media Use	33
5.2	Familiarity	35
5.2.1	Expert Interview	35
5.2.2	Questionnaire	36
5.3	Prevalence	40
5.3.1	Expert Interview	40
5.3.2	Questionnaire	40
5.4	Effectiveness	43
5.4.1	Expert Interview	43
5.4.2	Questionnaire	44
5.5	Risk Perception of Activities	47
6	Discussion	51
6.1	How familiar does the Norwegian public think they are with malicious influence operations on social media?	51
6.2	How prevalent does the Norwegian public think that malicious influence operations on social media are?	53
6.3	How effective does the Norwegian public think that malicious influence operations on social media are?	54
6.4	Does risk perception of malicious influence operations impact behavior on social media?	56
7	Conclusion	59
8	Limitations and Future Work	61
8.1	Questionnaire Suggestions	61
8.2	Questionnaire Errors	62
8.3	Scope Limitations	62
	Bibliography	65
A	Questionnaire	71

Figures

5.1	Comparison of age distribution of sample versus population. Population is based on data from Statistics Norway (SSB). N=333. . . .	30
5.2	Comparison of location distribution of sample versus population. Population is based on data from Statistics Norway (SSB). N=328. . . .	31
5.3	Comparison of education distribution of sample versus population. Population is based on data from Statistics Norway (SSB). N=332. . . .	32
5.4	Social Media usage across the entire sample. N=332.	33
5.5	Percentage of respondents who said yes to using the following social media platforms.	34
5.6	How often the respondents use social media to do a set of specific activities.	35
5.7	How often the respondents hear about fake news, fake identities, and fake engagement.	37
5.8	Comparison of perceived familiarity between the terms "fake news" and "influence operations".	37
5.9	Comparison of observations of fake engagement between Digital Natives and Digital Immigrants.	39
5.10	Comparison of perceived familiarity in influence operations between male and female respondents.	39
5.11	Comparison of perceived likelihood of a foreign state or Norwegian politician/company using fake news to influence an election	41
5.12	Comparison of perceived prevalence of influence operation between Norway and the rest of the world	42
5.13	Comparison of perceived prevalence between people that have rated themselves unfamiliar and familiar with influence operations. . . .	43
5.14	Comparison of likelihood ratings of achieving the three different influence operation scenario goals.	45
5.15	How much of the population the influence operation can reach. Bin size=10.	46
5.16	Comparison of likelihood between being influenced in the past and being influenced in the future.	47
5.17	Perceived risk levels of the different activities.	48

Tables

4.1	Interview guide questions and how they relate to the research questions.	21
4.2	Questionnaire blocks and how they relate to the research questions.	23
4.3	Summary of Distribution Channels	26
5.1	Gender distribution sorted on distribution channels	29
5.2	Age distribution sorted on distribution channels	30
5.3	Location distribution sorted on distribution channels	31
5.4	Education distribution sorted on distribution channels	32

Chapter 1

Introduction

1.1 Topic covered by the project

“Influence operations are organized attempts to achieve a specific effect among a target audience. In such instances, a variety of actors— ranging from advertisers to activists to opportunists— employ a diverse set of tactics, techniques, and procedures to affect the decision-making, beliefs, and opinions of a target audience.” [1]

Examples of influence operations include marketing companies trying to make consumers buy a certain product, or politicians trying to make people vote for them in the next election.

A subset of influence operations is however more malicious in nature, for example attempts to incite civil wars, erode trust of traditional news, or otherwise sow division within a country. These operations are based on disingenuous information and secretive tactics, and they have gotten more advanced with social media becoming ubiquitous in all modern societies. Several features of social media make it an extremely valuable tool for influence operations, such as the ability to target advertisements based on highly specific personal information, the low barriers to entry, and the ease of spreading information [2]. A sophisticated social media influence operation, such as those performed by state-funded organizations, uses a combination of automated and manually controlled accounts, spanning across multiple social media networks, with messaging nearly indistinguishable from other social media accounts. [2]

This project aims to uncover how aware the Norwegian public are of influence operations, how they perceive the danger of malicious influence operations, and if there is a correlation between awareness and behaviour.

The project defines malicious influence operations to be any influence operation that uses one or more of the following tactics to achieve its desired effect on the target population:

1. **Fake News** - News stories with deliberately erroneous information.
2. **Fake Identities** - Social media accounts, pages, or groups pretending to be something or someone they are not. These identities will usually have hidden agendas that they sneak into their messaging.
3. **Fake Engagement** - “Likes”, “Shares”, and comments from a network of automated social media accounts, to make a post or user seem more popular than what they are in reality.

1.2 Keywords

Influence Operations, Political Warfare, Information Warfare, Social Media, Risk Perception, Fake News, Social Bots

1.3 Problem description

Social media influence operations as a research topic gained a lot of traction following the 2016 US election, where Donald Trump won against Hillary Clinton to the surprise of many given the polls prior to the election [2]. It was discovered after the election that the Russian company Internet Research Agency operated a covert large-scale influence campaign. The campaign had many goals, including undermining trust in democracy, undermining trust in news, encouraging extremism and bipartisanship, as well as getting Trump elected [2].

Much of the research since then has focused on getting a better understanding of the techniques and tactics these operations employ [2], while others have attempted to create ways to detect these operations [3]. A big problem, however, is finding ways to counter them. Influence operations defy easy categorization, which makes it difficult for governments to create policies or legislation [1].

The entities with the best opportunities to counter influence operations are the social media platforms itself [1]. They have access to more information regarding how their platform is used and can create tailored solutions. Existing policies by social media platforms to address influence operations is however too focused on individual influence activities, rather than the operation as a whole [1].

The problem is worsened by the fact that social media users and the social media platform itself has misaligned incentives. All major social media platforms in use today are privately owned, which means they have an obligation towards their shareholders to prioritize profit gain. Profit is gained from advertisement, and the longer a user spends on the platform, the more adverts they can show. Platforms are therefore designed to encourage the user to find new groups or sites, and to follow more and more people. Content that elicits the strongest reactions, either positive or negative, will find its way to the most amount of users. All of this is easily abused by influence operations.

1.4 Justification, motivation and benefits

The importance of countering influence operations can be seen in the damages it can cause. While it is hard to measure the exact impact of an influence campaign, it is clear to see the *potential* impact an influence campaign can have. Let's say for example that an influence operation, with enough resources and the necessary expertise, is able to successfully alter the results of an election without being detected. This would have immense repercussions on our democratic system. This could even already be the case, and we would have no way of knowing.

Rather than leaving the responsibility of "saving democracy" entirely in the hands of the social media platforms, maybe the problem can be addressed from several angles. This project will look more towards the activities of the victims instead of the activities of the attacker. Maybe the effects of influence operations can be mitigated by making social media users more aware of the dangers that exist. If an attack is too difficult to detect or to stop, maybe the solution is to change the way users engage with certain content on social media.

1.5 Research questions

1. How prevalent does the Norwegian public think that malicious influence operations on social media are?
2. How effective does the Norwegian public think that malicious influence operations on social media are?
3. How familiar does the Norwegian public think they are with malicious influence operations on social media?
4. Does risk perception of malicious influence operations impact behavior on social media?

Chapter 2

Background

This chapter will present the background knowledge necessary for the rest of the project, and gives an introduction into the projects main topics: Influence operations, social media, and risk perception.

2.1 Influence Operations

2.1.1 Political Warfare

The act of attempting to influence the opinion of others has existed as long as opinions have existed, but the types of influence operations that are discussed in this paper have their roots in political warfare. Political warfare is a term that has existed for quite some time, but its meaning has evolved with the emergence of cyberspace as a new domain of war. During the second world war, political warfare was defined as “a systematic process that employs both publicity and propaganda in order to influence the will and so direct the actions of peoples in enemy and enemy-occupied territories” [4]. The tools of political warfare at that time were radio broadcasts, leaflets, reconditioning prisoners of war, or taking over radio stations of enemy-held territories. The term ‘political’ was mainly used to signify the exclusion of kinetic force (e.g. physical violence). Now In the 2010s, the same term gained renewed interest, along with other overlapping terms such as cyberwarfare, information warfare and hybrid warfare. The same tactics now have an infrastructure in the form of the internet that makes it possible to perform activities on a much larger scale, and the importance of political warfare has become more important than ever before. In an article from 2013 on the future of warfare, Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces stated the following: “The very rules of war have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.” [5]

There are several notable examples of influence operations, or some form of political warfare being utilised in recent history. In the time leading up to the Arab Spring, American government-funded organizations promoted democracy in authoritarian Arab states, and trained key leaders of the movement in campaigning and organizing through social media [6]. As mentioned earlier, Russian government-funded organizations attempted, and possibly succeeded, in influencing the 2016 US election [2]. The 2017 election in France is another example of Russian interference, but notably the attempt was unsuccessful [7]. Just two days before the election day, thousands of emails from Emanuel Macron's presidential campaign were leaked, some real and some forged. A combination of luck, preparedness, and a high degree of awareness in the public due to numerous recent examples of interference, resulted in the leaks not gaining as much traction, and the controversy did not take root. There have been no confirmed large-scale influence operations targeting Norway, but the Norwegian Intelligence Service has stated that they believe Norway has been exposed to influence operations from both Russia and China during the Covid-19 crisis [8].

2.1.2 Tactics, Techniques, and Technology

Fake Identities

A fake identity on social media, or a fake profile, is the representation of a person, organization, company, or group that does not truly exist [9]. There are many use-cases for these kinds of fake identities: They can be used for social engineering such as a phishing attack, or they could be used to monitor someone and collect personal information that is shared. Influence operations use fake identities to infiltrate local communities and make it seem like they are part of it. An example of a fake identity is the twitter account "Jenna Abrams", who had 70 000 followers and posted xenophobic and far-right opinions, some of which was picked up and quoted by mainstream news media, believing she was a real person [10].

Fake News

Lazer et. al. defines fake news as "fabricated information that mimics news media content in form but not in organizational process or intent." [11] Fake news has overlap with both misinformation, meaning false or misleading information, as well as disinformation, meaning false information that is purposely spread to deceive people. The use of fake news is a tactic that was widely deployed by the influence campaigns of the Internet Research Agency.

Social Bots

A socialbot is a piece of automation software that controls a social media account, performing normal social media activities, such as posting, commenting, or sending friend requests [12]. Socialbots differ from other bots on social media by the

fact that they are designed to pass itself off as a human being, by using the aforementioned fake identities. It is a technology that is used by influence campaigns to reach a wider audience using less manpower. A socialbot typically operates within a botnet, which means that one bot operates in tandem with many other bots, and they are all controlled by a single entity [12]. Influence campaigns use this to fake engagement on their posts, for example to make a fake news story spread faster. By having hundreds or thousands of bots like, comment, or share a certain opinion, they make it seem like that opinion is more widespread than what it truly is.

2.2 Social Media

Social media can be defined as “the different forms of online communication used by people to create networks, communities, and collectives to share information, ideas, messages, and other content” [13]. The most notable aspect of this definition is the fact that social media platforms are entirely reliant on user-generated content, which encompasses many different types of platforms. Messaging-focused platforms such as WhatsApp and Discord, as well as video-focused platforms such as Youtube and Twitch are all considered social media under this definition, along with more “traditional” social media such as Facebook and Twitter. Social media has many different use-cases, such as communication, entertainment, or event organizing. For businesses it can be an excellent tool for marketing, outreach, and customer service.

Wang et. al. classifies different social media platforms with a defined set of different functionalities [14]. All social media platforms will have all of these functionalities in some form, but different platforms focus more on the various functionalities. The seven defined functionalities are as follows:

- Identity: Self-representation, focusing on who you are as a person.
- Conversations: Communication with others on the platform.
- Sharing: The exchange of knowledge. Pictures, videos, news stories, personal experiences etc.
- Presence: Others’ reality perception of you.
- Relationships: Your relation to others, friends, family, colleagues, etc.
- Reputation: Social standing within the platform.
- Groups: The ability to form communities.

To give an example, we can look at the differences between the two social media platforms Facebook and Reddit. Facebook has a high degree of focus towards identity and relationships. On the user profile page, the user has functionality to enter their name, contact information, place of work, location, interests, hobbies, relationships, the list goes on. On Reddit, users have a username, and a profile picture. Here, the focus is on sharing and groups. Instead of adding friends, the

user joins communities with similar interests, and shares content with everyone in the community.

According to Statistics Norway (SSB), 85% of the Norwegian populace between 16 and 79 years old have used social media in 2019, and 73% use social media daily or almost daily [15]. Out of the 4,5 billion people in the world that use the internet, 3,8 billion of them use social media [16].

2.3 Risk Perception

The concept of risk refers to the probability of experiencing some form of harm or hazard. Probability refers to the likelihood of an occurrence. Risk involves uncertainty, both in terms of the expected outcome of an occurrence, and the likelihood of the occurrence happening. People experience, interpret, perceive, and make judgements on these uncertainties differently, and these reactions are known as risk perceptions [17]. The main difference between “risk” and “risk perception” is the subjective nature of perceptions, which means that the actual probabilities of a risk, and the perception thereof, can differ greatly. Research on health often involves risk perception, as it can be used to explain what hazards people care about, and how they deal with them.

Risk perception has two main dimensions: the cognitive dimension, and the emotional dimension [17], also known as “Risk as Analysis”, and “Risk as Feelings” [18].

The cognitive dimension relates to how much people know about and understand risk. Logic, reasoning, and scientific deliberation are core to the cognitive dimension [18]. Early research in risk perception focused on this dimension, with the thought that risk perception is mainly based on people’s cognitive judgements about the magnitude and likelihood of risks [17]. This view is similar to how risk is viewed in Information Security, where risk is commonly described as the product of impact multiplied by likelihood.

The emotional dimension relates to how people feel about risks. This dimension focuses on the role of emotions such as dread, fear or outrage, both directed towards the risk itself, but also the general mood of a person in the moment they are perceiving a risk. Emotional responses to a risk are more instinctive and intuitive, and can often ignore the “known facts” such as probabilities of a risk [18].

People perceive risk using a combination of both dimensions, but the weighting of the dimensions will vary between different people, as well as between different types of risk. A common assumption is that experts within a field rely more on the cognitive dimension while laypeople rely on the emotional dimension. A study conducted in Norway did however find that cyber security education, or lack thereof, did not significantly change how the participants perceived digital risks [19].

Both the cognitive and the emotional dimension look internally (i.e. within the mind of the subject) for explanations regarding different perceptions, but it is also possible to look at external variables. Media is one such external variable that plays a critical role in forming and affecting risk perceptions [17], both in the form of entertainment media and news media. Several factors have been found to affect the general public's risk perceptions, including amount of media coverage, how risks are presented/framed, the type and trustworthiness of information sources, message format, and type of media.

Chapter 3

Related work

This chapter will present some of the state-of-the-art research within the different topics that this project covers: Influence operations, social media, and risk perception.

3.1 Influence Operations

3.1.1 Tactics, Techniques, and Technology

Diresta et. al. [2] has written a paper on the tactics and tropes of the infamous “troll-farm” called Internet Research Agency (IRA). The paper analyzed a massive dataset of social media posts known to have originated from the IRA, including over 10 million tweets, a thousand Youtube videos, 116 thousand Instagram posts and 61 thousand Facebook posts. These posts had garnered 77 million engagements (likes, shares, comments, or similar) on Facebook, 187 million engagements on Instagram, and 73 million engagements on Twitter. Facebook has estimated that the operation reached 126 million users on their platform.

Diresta et. al. identified the following tactics employed by IRA [2]:

Microtargeting: The IRA targeted specific cultures and interests focused on different social issues within the American society, for example Black Lives Matter, Blue Lives Matter, Christian, Muslim, LGBT, Gun rights, Southern culture, or Feminist culture. Within these cultures, they would create and advertise groups, personas, pages, events and websites to attract an audience. Advertisements would often further target based on location or demographics, and with precise timings. Examples of this are advertising police-brutality pages following officer-involved shootings, or targeting coal-miners following massive layoffs in a region.

Recruitment: IRA’s social media pages would often make posts recruiting people to “their cause” or offering direct contact and counselling. Examples of this are offers of free counselling to people with sexual addiction, and recruiting volunteers to hand out fliers or document protests.

Cross-Platform Brand Building: IRA operated as a digital marketing agency, developing brands and building presences across social media sites. Any given Facebook page would have connected accounts on Twitter, Youtube, Tumblr and more, sometimes even operating their own stores with themed merchandise. Brands would also evolve over time, changing logos and typography.

Memes: Diresta states that “Memes turn big ideas into emotionally-resonant snippets, particularly because they fit our information consumption infrastructure: big image, not much text, capable of being understood thoroughly with minimal effort.” IRA would create or appropriate relevant memes for their target audience, encouraging them to reshare to their personal accounts.

Inflecting a Common Message for Different Audiences: An example of how messages would be highly tailored to their respective audiences can be seen in posts regarding Syria. Feminist groups would focus on suffering Syrian mothers and children, black-targeted groups would advocate for focusing on domestic problems in black neighbourhoods before paying attention to foreign nations, while right leaning groups would advocate for U.S. to get out of Syria to stop Syrian refugee floods, or by saying that the U.S. should focus on ISIS instead.

Narrative Repetition and Dispersal: IRA would repurpose the same story across accounts to create the perception that certain messages or opinions were widespread and worthy of attention.

Manipulating Journalism: IRA impersonated state and local news enterprises on Twitter and Instagram, presenting current events and information about cities and communities they pretended to be from. At the same time, a large effort was made to undermine trust in “real” media. Both by advocating for the creation of niche community media as an opposition to unrepresentative mainstream media, and by actively undermining trust in journalism.

Amplify Conspiratorial Narratives: IRA-controlled Twitter accounts would often advocate for conspiracies such as anti-vaccine narratives, paranormal activity, and domestic political conspiracies (QAnon, Pizzagate). Black-targeted groups were given historical conspiracies, such as “Mozart was black”.

Sow Literal Division: IRA accounts would also promote secessionist and insurrectionist movements, such as independence for California, independence for Texas, or promoting riots and rallies as a response to different local issues.

Dismiss and Redirect: When investigations into Russian interference began, the IRA would create content with the narrative that the whole investigation was nonsense, that investigators were corrupt, and that emerging stories were “weird conspiracies pushed by liberal crybabies”.

Social Bots

Boshmaf et. al. performed a study in 2012 where they created and operated a social botnet to collect data on user behavior in response to large-scale infiltration campaigns [12]. Using a network of 102 socialbots that operated on Facebook for 8 weeks, the bots sent 8570 friend-requests, where 3055 were accepted. They

found several factors that affected how likely a human were to accept a bots friend-request [12]:

- Users with more friends are more likely to accept a friend-request.
- Users with more mutual friends with the bot are more likely to accept a friend-request.
- Female bots are more likely to be accepted.
- Bots shouldn't have too few or too many friends. The highest success-rate for new requests is found when the bot has as many friends as the average user on the network.

Chavoshi et. al. has developed a system ("DeBot") for detecting social botnets by using what they call "Warped Correlation" [3]. Warped correlation is based on the observation that humans cannot be highly synchronous for a long duration, therefore highly synchronous accounts are most likely bots. In essence, if several accounts "like" the same post at the same time, then after waiting a bit, "likes" another post at the same time, then post similar posts at the same time, the likelihood that all of these accounts are in the same botnet is extremely high. "Warped" means that the algorithm takes into account lag that can come from various delays, such as network delays, internal processing on the social network, or from the controller issuing commands to the bots [3]. DeBot has a 95% precision rate and managed to detect 500 000 bots on Twitter in 2016.

Fake News

Lazer et. al. wrote an article titled "The science of fake news", which discussed findings from research with regards to fake news prevalence and impact, as well as potential interventions [11]. Some of the key takeaways from the discussion are as follows:

False information on Twitter is shared by more people, and more rapidly, compared to true information, especially when the topic is politics. The use of social-bots can also magnify the spread of fake news by orders of magnitude.

Even though many forms of fact checking exist, their efficiency has mixed results. The article points towards cognitive biases as a reason. People prefer information that confirms preexisting attitudes, and are more inclined to accept information that pleases them for example. In addition to this, people tend to remember information but forget how they encountered it, and they are more likely to accept familiar information as true. Perceptions can therefore be changed by repeating false information.

3.1.2 Challenges

Thomas et. al. discusses the challenges of countering influence operations by analysing a case study of an influence operation originating in Israel, targeting several english speaking countries [1]. The operation controlled, among several others,

one website under the name “free speech front”, which created fake news stories centered around anti-islamistic messages. The study reviews which social media platform policies that were violated by the campaign, which national or international laws were violated, and highlights the gaps in current legislation.

Thomas et. al. found four activities that are violating policies of all major social media platforms [1]: (1) Posting inflammatory content, (2) Cloaking URLs and redirecting traffic to paid advertisements, (3) Using fake accounts to co-opt existing online communities, and (4) Coordinating inauthentic behavior across platforms. All of these policies address individual activities of an influence campaign, instead of the operation as a whole. Thomas et. al. expresses doubts about whether social media officials truly understand how influence operations work [1].

When it comes to international laws and treaties, Thomas et. al. highlights that current legislation focuses on activities directly orchestrated by one state against another, leaving out activities conducted by civilians or proxy organisations [1]. National laws also face multiple problems; there is a scarcity of laws that are suited to address influence operations, there are many difficulties in proving that a certain activity had malicious intent, and jurisdictional hurdles in the form of extraterritoriality may prevent nations from pursuing a perpetrator even if the identity is known.

3.1.3 Influence Operations in Norway

The Norwegian Broadcasting Company, Norway’s public service broadcaster, performed an influence operation experiment in an episode of the show “Folkeopplysningen” [20]. The episode, titled “Make Lillestrøm Great Again”, followed a school election within a high school in Lillestrøm, where a team covertly attempted to make the least popular political party (Senterpartiet) more popular. Over a period of 6 months, the team used tactics inspired by the Internet Research Agency, such as fake news, memes, and fake identities to persuade the students into voting for Senterpartiet. Senterpartiet received 3,1% of the votes, compared to 2% of the votes two years prior [21]. It is hard to tell how much, if any, the experiment contributed to the increase, but the experiment did evidently not impact the election significantly. The episode has received a mixture of praise and backlash. Some feel it highlighted an important subject and was a good opportunity for learning, while others, including the Norwegian prime minister, view the experiment as unethical [22].

The Norwegian Data Protection Authority has investigated the use of data analysis and microtargeting by Norwegian political parties [23]. They interviewed representatives from all nine parties currently represented in the Norwegian parliament, and found no widespread use of microtargeting technology. They did however identify that none of the parties had written guidelines on how to handle personal data during election campaigns, which makes them susceptible to the use of more invasive technology in the future.

The Norwegian Defense Research Establishment (FFI) has pledged 7,5 million kroner towards a project called Cyber-Social Propaganda and Influence, which aims to research the threat of influence operations. [24] Some of the long term goals of the project includes getting a holistic understanding of the scope and threat of influence operations, identifying how it may damage our society, and finding potential countermeasures. Among other things, the project aims to create practice tools to simulate social media activity to use in crisis management scenarios.

FFI has also published a report from Arild Bergh on influence operations [25]. The report is a socio-technical analysis of previous influence operations, including Russian attempts at influencing the 2016 US election. The main output of the report is a conceptual chain of tools, arenas and activities, which is shown below [25].

A planned influence operation executed by active operators
relies on Affordances of social media
that aids the Amplification and reach
which contributes to the Online information sediments
that are deployed to fight for Individual or group attention
to manipulate Individuals' or groups' opinion making processes
so as to encourage Alternate individual or group (in)actions.

3.2 Social Media

3.2.1 Politics in Social Media

Zhuravskaya et. al. has written a paper on how social media has affected the political landscape [26]. The study reviews literature to see if social media has made an impact on several different aspects of politics:

Voting: In the early days of the internet, it seemed to have a negative impact on the interest in elections of those who had access to it. Over time however, this changed, and the change coincides with the emergence of social media. Zhuravskaya et. al. points towards new populist political actors managing to mobilize voters by connecting to them directly [26].

Street protests: Especially in autocratic regimes, social media made it easier to spread information that is critical of the government, increasing the number of informed and unhappy citizens ready to take part in protests.

Polarization: Social media has made it easier to be exposed to political content that aligns with a person's own beliefs, and to filter out opposing views. This does not however mean that we can conclude that social media increases polarization. People exposed to political content mainly through offline means (e.g. friends, family) get a more skewed picture of political news than those who get their political news online.

Xenophobia: Evidence suggests that extreme voices get propagated more on social media, and that this has had real implications for hate crimes. Anti-refugee sentiment on social media on a particular day is associated with a higher number of violent crimes against refugees in places with high social media usage, and the same effect is nonexistent on days where social media is for some reason inaccessible.

Mathé and Elstad explored how Norwegian 16-17-year-old students perceive and evaluate the communications on social media of certain politicians, including Sylvi Listhaug and Donald Trump [27]. One of the tendencies they identified was that the girls would respond to an egregious post with strong emotions and condemnation, while the boys showed more signs of cynicism. The study also found indications that young people are more careful with sharing their political views online, and that the participants of the study had great confidence in their source criticism abilities.

3.2.2 Social Media and Trust

Wang et. al. researched the effects of trust and risk on individual behavior toward social media [14]. The study collected and summarized the empirical evidence of 43 different studies between 2006 and 2014, with the goal of understanding how trust and risk affects an individual's behavior when it comes to social media adoption and content sharing. Trust includes the belief that the social media platforms are honest and will keep their promises, that they have the skill and knowledge to perform their roles well, and that they are concerned about the interests of individuals, not just their own benefits. They found that both the perception of trustworthiness in the social media platform, and the perception of risk in performing certain activities had an effect on behavior. Trust did however have a stronger effect on behavior compared to risk.

Warner-Søderholm et. al. has also studied trust on social media, specifically trust of news on social media, with the goal of seeing if perception of trust differs with respect to gender, age, social media usage, and platform preference [28]. The study measured trust using five scales; Integrity, Benevolence, Competence, Identification and Concern, all borrowed from previous studies on trust. People who use social media several times a day scored significantly higher in all five categories, compared to those who use social media once a day or less. Similarly, Instagram users scored significantly higher in all categories compared to those who did not use Instagram. For the construct of Integrity, which focuses on expectations of honesty and moral character, females scored higher than males in general, while younger people scored higher than older people. The most trusting group identified by the study was young females who use social media several times a day: *“They believe that most people care about the welfare of others, they are less skeptical about others’ competence, have a stronger sense of belonging to their*

network and believe people are genuinely concerned about others in their network.” [28]

Tinius has performed a survey on “Gen Z” (those born between 1995 and 2005) in Norway and Sweden, where they investigated information habits and attitudes toward journalism, language, brand, and the willingness to pay for something on-line [29]. The survey shows that young Scandinavians have a high degree of trust towards journalism and news media. 64% of Norwegians say they go directly to Norwegian media sites to get updates. When given the statement “I deem information written by a journalist to be more trustworthy than information written by a blogger”, 9 out of 10 Norwegians agree. Similarly, 7 out of 10 Norwegians agree with the statement “I like that information I find is quality assured by a journalist. According to *Aftenposten*’s comments on the survey, 74% of Norwegians between 18-24 say they trust their regular news sites, compared to 43% globally [30]. A similar level of trust was found in a survey from *Medietilsynet*, where 83% of the respondents answered yes to the statement “Norwegian Media can be trusted” [31].

3.3 Risk Perception

3.3.1 Biases in Risk Perception

Slovic et. al. has collected data from various studies to analyse what biases can occur when perceiving risk. The paper identifies 5 different judgmental rules (“heuristics”) that humans employ to “reduce mental tasks to simpler ones” [32]:

Availability: People judge an event as likely or frequent if instances of it are easy to imagine or recall. Recently watching the movie “*Jaws*” will increase the perceived risk of sharks. Slovic references a few studies that looked at estimated number of deaths for various events versus actual number of deaths. The participants would consistently overestimate the number of deaths caused by accidents and underestimate diseases that do not get a lot of media attention. Homicides were judged to be as frequent as strokes, while in reality, strokes as a cause of death is 11 times more frequent [32].

Overconfidence: People can be very confident, sometimes too confident, in the judgements they make. In a follow-up study of cause of death estimations, participants were asked which of two lethal events were more frequent, and more importantly how confident they were with their answers. 99% confidence was given frequently, and about 1 in 8 of these judgements with 99% confidence was wrong.

Desire for Certainty: People tend to reduce the anxiety that comes with facing uncertainty by simply denying the existence of it. Victims of flood have actively denied that floods ever could happen again, believing that previous floods were caused by freak combinations of events.

It Won't Happen to Me: People tend to consider themselves personally immune to risks they otherwise perceive as real. Most people think they are among the most skillful and safe drivers in the population, and most people are unrealistically optimistic when evaluating the chances of their own future life events, such as living past 80 or having a heart attack.

Reconciling Divergent Opinions about Risk: Peoples belief changes very slowly, and initial impressions of a risk tend to form the way subsequent evidence is interpreted. If a piece of evidence is consistent with the initial belief, it is considered reliable and informative, while information contrary to the initial belief is considered unrepresentative or false.

3.3.2 Cyber-Security Awareness

Rahim et. al. has reviewed different approaches of assessing security awareness, and analysed their appropriateness [33]. Out of the 23 reports that were analysed the two most common methods for data collection were surveys (10 of 23) and interviews (5 of 23). Only two of the reports had multiple methods of data collection. Rahim et. al. calls for more research utilising multiple data collection methods, stating that “assessing humans cannot be based merely on quantitative approach” [33].

Gkioulos et. al. studied the security awareness of digital natives, meaning young people born in the digital era [34]. The study utilised survey data from three different groups, where the three groups differed in terms of information security competence, ranging from general, to medium, to high. They found variations in behavior based on security competence, along with variations originating from regional, cultural and financial agents. Across the groups, users tended to prioritize ease of use over security measures, for example by remaining logged in to services they were no longer using. They were also willing to accept security risks if it meant they would be able to gain access to additional services, for example by downloading an application from an unofficial source.

Norwegian Center for Information Security (NorSIS) publishes a report on the digital security culture of Norwegians on a yearly basis [35]. NorSIS defines security culture with eight different areas: Behaviour, Interest, Competence, Trust, Community, Risk Understanding, Control, and Will to digitalize. 2019 was the fourth year of the report, and NorSIS have identified a few trends from 2015 to 2019. Generally, more Norwegians feel that they are exposing themselves to risks by using the internet than before, and more people see it as high risk to utilise public services online. 40% of the respondents in 2019 somewhat agreed or strongly agreed that using social media is high risk.

Chapter 4

Methodology

This chapter will describe the applied research strategies. This project will use a mixed-method design, more specifically an embedded design, consisting of two stages. An embedded design collects qualitative and quantitative data in the same time frame, but one of the collection methods is considered to be the primary data source, while the other serves a secondary, supplementary role [36]. As seen in the Related Works chapter, the two most common methods of collecting data on security awareness were questionnaires and interviews, and there have been calls for more research with multiple data collection methods [33]. This has been taken into consideration when creating the research strategy.

The two stages of the design are as follows: First, two qualitative interviews were conducted with experts on the topic of influence operations. Then, these interviews were used to create a questionnaire targeting the Norwegian public, which will serve as the project's primary data source. The following sub-chapters will describe the two stages in more detail.

4.1 Expert Interview

An expert interview can be defined as a “qualitative interview based on a topical guide, focusing on the knowledge of the expert, which is broadly characterized as specific knowledge in a certain field of action” [37]. The experts in this specific instance are persons who either have a research background, or personal work experience, within the topic of influence operations.

As mentioned earlier, this data will serve a supplementary role to the primary data collected from the questionnaire. Its purpose is to support or contradict potential findings from the primary data source, with the possibility of adding more insight or information than what is possible to gather from the primary source alone. The interviews were also used to shape and align the questions asked in the questionnaire. An example of this is that both experts felt that people generally have a hard time seeing the connection between smaller tactics such as fake

news, and the bigger picture of influence operations, which made it interesting to find out if the level of familiarity and knowledge of the two are different.

The experts are anonymous to comply with requirements from the Norwegian Centre for Research Data. Non-anonymous interviews would require an application, and waiting for approval would delay all subsequent data collection. Due to the time constraints of the master thesis, it was decided to continue anonymously. As a result of this, no recordings could be made of the interviews, and instead notes were written down during the interview. These notes were then sent to the subject after the interview, for them to approve, disapprove, edit, add, or delete any of the notes taken. There are some downsides to this approach, mainly related to loss of information. With an audio recording, there is access to more small nuances, such as exact phrasings and more detailed explanations that there might not be enough time to write down. Additionally, having to write during the interview could stifle the flow of conversation, and could cause the interview subject to try to be shorter in their explanation, losing more detail. This tradeoff between time and information was deemed acceptable in this instance, since the data is not the primary source of the project.

4.1.1 Interview Guide

The interview guide was loosely structured around the project's research questions. A selection of questions and follow-up questions was identified prior to the interview, but more focus was put on the flow of the conversation, to allow the expert to talk about the aspects they feel they know the most about, or feel is most important. Leedy, et. al. recommends limiting the number of preconstructed questions to be between 5 and 7, and to use open-ended questions that do not hint towards particular answers [36]. The prepared interview questions, and how they relate to the projects research questions, can be seen in Table 4.1 below.

4.1.2 Interview Subjects

The interview subjects were given the pseudonyms "Expert Einar" and "Expert Tore". Expert Einar has many years of experience as a developer and IT consultant, and also has a doctorate in Sociology. Expert Tore has a background and experience in professional communication, and has worked with strategic communication in both a private and public sector. Both of them are currently doing research work related to influence operations. Their research has focused more on how influence operations function, and how they can affect Norway as a society. They have not specifically looked into public risk perception of the phenomenon.

Research Question	Interview Guide Questions
How prevalent does the Norwegian public think that malicious influence operations on social media are?	<ul style="list-style-type: none"> • How prevalent are influence operations? • How often do you think the average Norwegian comes across posts from an influence operation?
How effective does the Norwegian public think that malicious influence operations on social media are?	<ul style="list-style-type: none"> • How effective are influence operations? • Is there a limit to how much you could change an opinion, or is there just a question of enough time and enough resources?
How familiar does the Norwegian public think they are with malicious influence operations on social media?	<ul style="list-style-type: none"> • How much do you think that the average norwegian knows about influence operations?
Does risk perception of malicious influence operations impact behavior on social media?	<ul style="list-style-type: none"> • Do you think there is something that makes certain people more or less prone to manipulation? • Do you feel better equipped to detect influence operations with the knowledge you have?

Table 4.1: Interview guide questions and how they relate to the research questions.

4.2 Questionnaire

A Questionnaire is a form of survey research, which involves acquiring information about one or more groups of people by asking them questions and tabulating their answers [36]. The goal of survey research is to learn about a large population by surveying a sample of that population. A series of questions is posed to willing participants, and the answers are summarized into percentages, frequency counts, or more complex statistical indexes, which are later used to draw inferences about the sampled population.

Some of the benefits of questionnaires are the possibilities to distribute the survey to a large number of people, and it is an inexpensive way to collect data from wide geographical areas [36]. Additionally, survey participants can respond to questions while remaining anonymous, which might lead to more honest answers. The method does however also have downsides. Questionnaires often have a low return rate, meaning the majority of people who see or receive the survey do not answer, and since the survey is anonymous one cannot completely guarantee that answers are representative of the population that the survey is constructed for. Additionally, since the researcher is not present when the survey is answered, questions might be misinterpreted, and there are no possibilities for follow-up questions from the researcher.

Questionnaire was chosen as the main data collection method for a number of reasons. Most of the project's research questions are more concerned with how people think rather than why they think the way they do, which suggests that a quantitative approach is more suitable. The geographical area that is surveyed is quite large, and the target population is diverse in terms of age, education, and experience, which means a larger sample size will be more representative for the entire population. Furthermore, previous research on similar topics has preferred using questionnaires according to Rahim et. al. [33].

4.2.1 Design

The questionnaire aims to collect data for all 4 research questions, and revolves mainly around the cognitive dimension of risk perception. The questions take inspiration from the expert interviews from the previous stage, as well as from several of the papers presented in the Related Works Chapter, such as the NorSIS report on digital security culture [35]. The questionnaire is also constructed using guidelines presented by Leedy et. al. [36]. Further quality assurance was done through two sessions of feedback with the supervisors of this project, as well as performing a small test run of the questionnaire on 5 participants.

The questionnaire consists of 20 questions, where a subset of these questions are "matrix questions" with multiple rows that the participant has to answer. The questions can be divided into 6 blocks which are described in more detail below. Table 4.2 also shows a summary of which questions relate to which blocks, and what research question they aim to answer. The full questionnaire (in its original

Norwegian language) can be found in Appendix A.

Question #	Block	Research question/Purpose
1, 2, 3, 4	Demographics	Check for bias in sample
5, 6, 7	Activity and behavior	Does risk perception of malicious influence operations impact behavior on social media?
8, 9, 11, 12	Familiarity	How familiar does the Norwegian public think they are with malicious influence operations on social media? Does risk perception of malicious influence operations impact behavior on social media?
13	Risk perception of activity and behavior	Does risk perception of malicious influence operations impact behavior on social media?
10, 14, 15, 16	Prevalence	How prevalent does the Norwegian public think that malicious influence operations on social media are?
17, 18, 19, 20	Effectiveness	How effective does the Norwegian public think that malicious influence operations on social media are?

Table 4.2: Questionnaire blocks and how they relate to the research questions.

Demographics

Participants were asked about their age, gender, place of residence, and education level. This information was used to control that the survey sample is representative of the whole country, and to look for differences between demographic groups.

Activity and Behavior

This block asked the participants about what social media platforms they use, what types of activities they use them for, and how often they do these activities. In the first question of this block, the participant was given a list of social media platforms, and asked to select all the platforms they use. The main purpose of this question was to expand the participants' perception of what social media is. Some people might for example not think that Youtube or Twitch are considered social media. For the second question, participants were asked how much in general they use social media, on a scale ranging from daily, weekly, monthly, rarer than monthly, or never. The participants were then asked how often they perform a specific set of activities, using the same scale. This list of activities include reading news, sharing news, engaging in debates in comment sections, reading political content, and engaging with political content. All of these are activities that will make a social media user more likely to be exposed to influence operations. This

information was used to see if there are certain activities that the participants avoid, and how exposed they are to influence operations, whether they know it or not.

Familiarity

This block introduced the participant to three different influence operation tactics: Fake news, Fake identities, and Fake engagement, as well as influence operations itself. These three tactics are used to see if there is a difference in knowledge and familiarity towards certain aspects of influence operations compared to influence operations as a whole. The participants first read some information about all 4 concepts, then they were asked about how often, if ever, they hear about these tactics outside of the study, and how much, if anything, they feel they know about the tactics.

Risk Perception of Activity and Behavior

Using the same list of activities that were given in the Behavior block, participants were asked to rate the activities in terms of how much risk they feel they expose themselves to by performing them (specifically with regards to influence operations).

Prevalence

Using the three tactics that were introduced in the familiarity block, the participants were asked about how often they think they encounter these tactics while using social media. They were also asked about how likely it is that a foreign government, as well as a Norwegian politician or company, has used these tactics to influence a Norwegian election. Lastly, the participants were asked how much they think influence operations are used in Norway compared to the rest of the world. These questions will give an idea of how much the participant feels they are directly exposed to influence operations, if certain tactics are more prevalent than others, if certain threat actors are more prevalent than others, and if they think that Norway is more or less exposed than other countries.

Effectiveness

Participants were given a hypothetical scenario of an election in Norway, and that a foreign government is influencing the election with an operation. The operation has three goals: (1) they want a certain candidate to win, (2) they want that 10% of the population believes that the candidate's opponents cheated, and (3) they want over half of the population to not vote, either because of indifference, confusion, or exhaustion. The participants are then asked about how likely they think it is for the operation to achieve each of the goals, how likely it is that the

operation manages to remain hidden, and how much of the population they would be able to reach.

The three different goals represent the three different ways of influencing that was discussed in the expert interview. Having a specific candidate win represents influencing into action and changing opinions. For this to be successful, the influence operation would have to convince someone to actually use their vote, and possibly change their vote from who they originally wanted to vote for. Making 10% of the population believe someone cheated represents influencing an attitude. Here the influence operation does not have to convince people to do something, just to think something, and possibly lose some trust in the system at the same time. The last goal represents the apathy an influence operation can create, by spewing out too much disinformation, and by making political discussions too extreme. Effectiveness is also more than just achieving a certain goal. An influence operation is more effective if it is undetected, and if it can reach more of the population.

Lastly, the participants were asked if they think they have ever been influenced by an influence operation, or if they ever will be in the future, to see if they think that an influence operation could be effective on them personally.

4.2.2 Distribution Channels

The target population for the survey is anyone currently living in Norway or anyone who considers themselves to be Norwegian, regardless of age, gender or any other demographic factor. An important goal for the distribution is to make sure that different ages, genders, and locations within Norway are properly represented. The questionnaire was distributed using four different channels: Facebook, Reddit, Norwegian forums, and Adverts. A summary of the effectiveness of the different channels can be seen in Table 4.3.

The questionnaire was made available using a digital tool called “Nettskjema”, which is developed and maintained by the University of Oslo [38], and is the recommended tool for surveys by NTNU. The tool does not store any metadata of the participants, including for example ip-addresses, so they can remain anonymous. Different distribution channels were given different versions of the same questionnaire, to better track where the data is coming from.

For the Facebook distribution channel, a post was shared on the personal Facebook page of the project author that asked friends and relatives to complete the survey and share it further. A problem was encountered when the post was shared by others, in that the original text of the post sometimes would be automatically removed, leaving only the link to the questionnaire. This might have damaged the spread of the questionnaire, as people could not see what the link contained and the motivation for clicking it. In total, the post was shared 13 times, 4 times with the original text attached, and 9 times with only the questionnaire link. The channel was opened the 12th of February and closed 7th of March, and received

Distribution Channel	Estimated reach (number of views)	Number of questionnaire participants
Facebook	1000-4000	101
Reddit	500-6000	86
Forum	500-1000	57
Advert	4535	89

Table 4.3: Summary of Distribution Channels

a total of 101 participants.

Reddit was also utilised as a channel, specifically the two subreddits “r/Norge”, which is dedicated to Norwegian redditors and Norwegian affairs and interests, and “r/NTNU”, which is dedicated to anything related to the university NTNU. r/Norge has at the time of writing 143000 members, while individual posts generally receive between 50 and 2000 reactions and engagements [39]. r/NTNU has 5200 members and individual posts receive around 5 and 100 reactions [40]. One post was created in each of the subreddits. The post in r/NTNU received 13 “upvotes”, while the post in r/Norge received 14 “upvotes” and 7 “downvotes”. The channel was opened the 12th of February and closed 7th of March, and received a total of 86 participants.

For the Forum distribution channel, the questionnaire was shared on three different public Norwegian forums: “Diskusjon.no”, “kvinneguiden.no”, and “VG Debatt”. In addition to this, a post was made on an internal forum for NTNU students and staff called “Oppslagstavla”. The posts on the public forums did unfortunately not get a lot of traction, collecting a total of 15 answers across the three forums. The post on Kvinneguiden was removed for violating terms of the forum, and VGDebatt has no publicly available information on how many people viewed the post. The post on Diskusjon.no was viewed 151 times and received 2 comments. The post on NTNU’s internal forums however was viewed 354 times and collected 42 participants. The channel was opened the 19th of February and closed 7th of March, and received a total of 57 participants.

For the final distribution channel, a Facebook Site was created to leverage the platform’s tools for advertisement. With a budget of 400 kroner, a post was advertised to random users of Facebook over 4 days. The advert targeted anyone currently living in Norway over the age of 18, and more specifically targeted people that were likely to click advert links. The post was advertised to a total of 4535 users, which resulted in 123 “link clicks”, which in turn resulted in 89 completed

questionnaires. The channel was opened on the 3rd of March and closed on the 7th of March.

4.2.3 Data Analysis

Two digital tools were used in the analysis of the data from the questionnaire. The spreadsheet tool Microsoft Excel was used for descriptive statistics such as medians and averages, calculating percentage-wise distributions, and for data-visualization. Excel can create tables and graphs that are more easily digested and more suitable for presentation. IBM SPSS on the other hand was used for more complex analysis and calculations that are not easily performed using Excel. SPSS is a software platform for statistical analysis, such as bivariate analysis and correlation tests.

The project used SPSS specifically to perform analysis of variance (ANOVA) tests to look for differences between demographic groups on all questions, as well as spearman rho correlation tests. An exception to this was questions with the answer options “Never/less than monthly/monthly/weekly/daily”, where I only report on descriptive statistics due to the non-linearity of the used scale. The demographic groups that have been tested for are age, education, gender, and location within Norway. Additionally, another set of groups was made titled “familiar” and “unfamiliar”, which is described in more detail in the Results section. All differences between the demographic groups that have a statistical significance ($P < 0.05$) will be reported on in the Results section.

Chapter 5

Results

5.1 Demographics and Social Media Activity

A total of 333 people completed the survey, and all questions were responded to by at least 326 people. This sample size compared to the population size gives us a margin of error of 5% with a confidence level of 95%.

5.1.1 Gender

The sample consists of 182 males, 147 females, and 4 people who were either non-binary or did not want to disclose their gender. This gives a slight bias towards males, with a distribution of 55% males against 45% females. A reason for this is the skewness of the Reddit distribution channel, which consisted of 82% males and only 18% females, as can be seen in Table 5.1.

Gender	Facebook			Reddit			Forum			Advert			Tot N	Tot %
	N	Row N%	Col N%	N	Row N%	Col N%	N	Row N%	Col N%	N	Row N%	Col N%		
Male	46	25 %	46 %	70	38 %	82 %	32	18 %	58 %	34	19 %	39 %	182	55 %
Female	55	37 %	54 %	15	10 %	18 %	23	16 %	42 %	54	37 %	61 %	147	45 %
Total	101			85			55			88			329	

Table 5.1: Gender distribution sorted on distribution channels

5.1.2 Age

Table 5.2 shows that age distribution varies greatly between the different distribution channels. Especially the Reddit and Advert distribution channels are heavily skewed, but in opposite directions, and sort of balances each other out. Over 90% of the Reddit sample is 39 years or younger, while 80% of the Advert sample is 40 years or older.

Comparing the age distribution of the entire sample against the distribution of the target population, we see that younger than 20 and older than 70 are under-

Age	Facebook			Reddit			Forum			Advert			Tot N	Tot %
	N	Row N%	Col N%	N	Row N%	Col N%	N	Row N%	Col N%	N	Row N%	Col N%		
<20	1	8 %	1 %	10	83 %	12 %	1	8 %	2 %	0	0 %	0 %	12	4 %
20-29	41	35 %	41 %	48	41 %	56 %	21	18 %	37 %	6	5 %	7 %	116	35 %
30-39	17	25 %	17 %	21	31 %	24 %	18	26 %	32 %	12	18 %	13 %	68	20 %
40-49	8	21 %	8 %	5	13 %	6 %	7	18 %	12 %	19	49 %	21 %	39	12 %
50-59	13	27 %	13 %	1	2 %	1 %	6	13 %	11 %	28	58 %	31 %	48	14 %
60-69	12	34 %	12 %	1	3 %	1 %	3	9 %	5 %	19	54 %	21 %	35	11 %
>70	9	60 %	9 %	0	0 %	0 %	1	7 %	2 %	5	33 %	6 %	15	5 %
Total	101			86			57			89			333	

Table 5.2: Age distribution sorted on distribution channels

represented in the sample, as can be seen in Figure 5.1. Ages 20 to 29 are however overrepresented by 22%. To somewhat remedy this, and to ensure that analysis is done with a large enough sample size, age will be grouped into two categories in most of the subsequent analysis. Ages of 39 and younger will be grouped into “Digital Natives” (N=196), and ages of 40 and older will be grouped into “Digital Immigrants” (N=137). The two terms are often used to differentiate between those who have grown up in the digital age, and those who were born before it. Age distribution for the target population is based on data from Statistics Norway (SSB) [41].

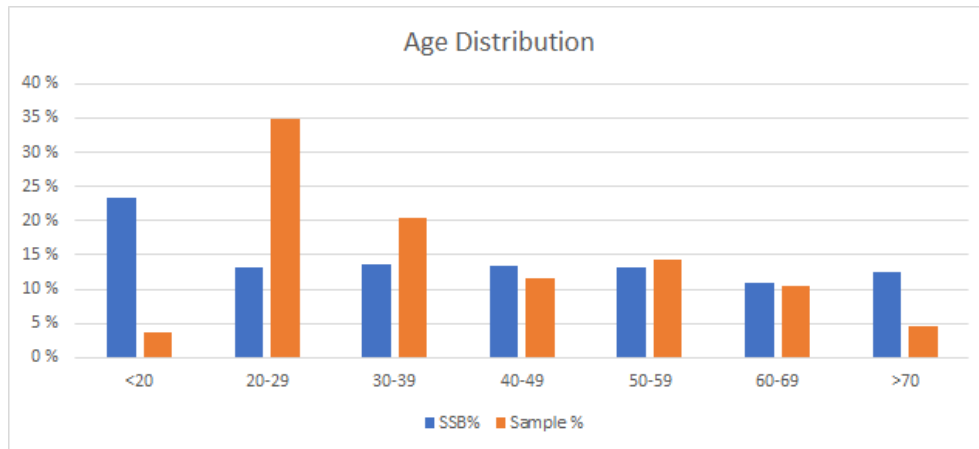


Figure 5.1: Comparison of age distribution of sample versus population. Population is based on data from Statistics Norway (SSB). N=333.

5.1.3 Location

Location distribution has been divided into the 11 counties of Norway, along with an option for anyone currently living outside Norway. Table 5.3 shows the results of the different distribution channels, while Figure 5.2 compares the sample to the target population. With the exception of Viken, Agder and Innlandet, most of the counties are underrepresented in the sample. The largest difference between the

sample and the target population is however Trøndelag, which is heavily overrepresented. All four distribution channels have some degree of overrepresentation of Trøndelag, but the overrepresentation is strongest in the Reddit and Forum distribution channels. There are a couple of possible explanations for this. Firstly, the Facebook distribution channel consists mainly of the project authors family and friends, many of whom are currently living in Trondheim. Secondly, the Reddit and Forum distribution channels both directly targeted people with connections to NTNU, and Trondheim is the biggest and first campus location for the university. Thirdly, although people were chosen at random for the advert distribution channel, people with some connection to the university are possibly more motivated to help students from that university.

Location	Facebook			Reddit			Forum			Advert			Tot N	Tot %
	N	Row N%	Col N%	N	Row N%	Col N%	N	Row N%	Col N%	N	Row N%	Col N%		
Agder	7	44 %	7 %	1	6 %	1 %	0	0 %	0 %	8	50 %	9 %	16	5 %
Innlandet	6	27 %	6 %	5	23 %	6 %	4	18 %	7 %	7	32 %	8 %	22	7 %
Møre og Romsdal	0	0 %	0 %	2	29 %	2 %	1	14 %	2 %	4	57 %	5 %	7	2 %
Nordland	0	0 %	0 %	1	25 %	1 %	0	0 %	0 %	3	75 %	3 %	4	1 %
Oslo	4	15 %	4 %	11	42 %	13 %	4	15 %	7 %	7	27 %	8 %	26	8 %
Rogaland	5	28 %	5 %	3	17 %	3 %	2	11 %	4 %	8	44 %	9 %	18	5 %
Troms og Finnmark	0	0 %	0 %	3	30 %	3 %	1	10 %	2 %	6	60 %	7 %	10	3 %
Trøndelag	27	23 %	28 %	38	33 %	44 %	37	32 %	66 %	14	12 %	16 %	116	35 %
Vestfold og Telemark	1	10 %	1 %	3	30 %	3 %	0	0 %	0 %	6	60 %	7 %	10	3 %
Vestland	2	9 %	2 %	8	35 %	9 %	4	17 %	7 %	9	39 %	10 %	23	7 %
Viken	46	61 %	47 %	11	14 %	13 %	3	4 %	5 %	16	21 %	18 %	76	23 %
Total	98			86			56			88			328	

Table 5.3: Location distribution sorted on distribution channels

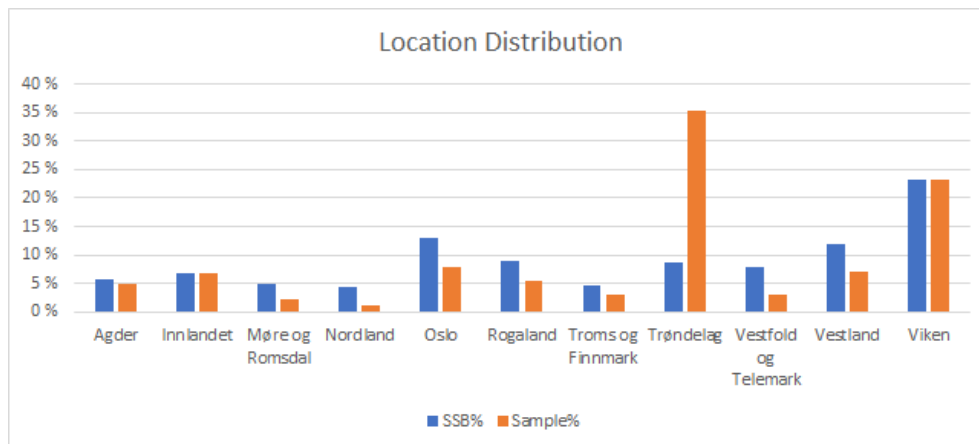


Figure 5.2: Comparison of location distribution of sample versus population. Population is based on data from Statistics Norway (SSB). N=328.

Similar to age distribution, location distribution will be grouped into three categories in subsequent analysis, since many of the counties lack the amount of participants to be representative for the population. The three groups will be “Oslo & Viken” (N=102), “Trøndelag” (N=116) and “Other” (N=110). The “Other” group

will serve as a control group containing the remaining counties. With it we can compare with the two former groups to see if it is likely that different locations are similar in their answers, but we won't be able to see where a dissimilarity lies if one is found. Location distribution for the target population is also based on data from Statistics Norway (SSB) [42].

5.1.4 Education

Education	Facebook			Reddit			Forum			Advert			Tot N	Tot %
	N	Row N%	Col N%	N	Row N%	Col N%	N	Row N%	Col N%	N	Row N%	Col N%		
Primary	4	40 %	4 %	2	20 %	2 %	3	30 %	5 %	1	10 %	1 %	10	3 %
High school	16	23 %	16 %	27	39 %	31 %	9	13 %	16 %	17	25 %	19 %	69	21 %
University	74	31 %	73 %	54	23 %	63 %	44	18 %	77 %	66	28 %	75 %	238	72 %
Vocational	7	47 %	7 %	3	20 %	3 %	1	7 %	2 %	4	27 %	5 %	15	5 %
Total	101			86			57			88			332	

Table 5.4: Education distribution sorted on distribution channels

In the distribution of education of the sample, there is an underrepresentation of lower education compared to the target population, as can be seen in Figure 5.3. Especially primary school is underrepresented, where only 3% of the respondents have primary school as their highest completed education, while the target population consists of 25%. We also see that the sample is heavily biased towards higher education, with an overrepresentation of 37%. In Table 5.4 we can see that the overrepresentation of higher education exists in all four distribution channels. Similarly to the location distribution, a possible explanation for this is that people with some connection to the university could be more motivated to help out by taking the survey. Education distribution for the target population is also based on data from Statistics Norway (SSB) [43].

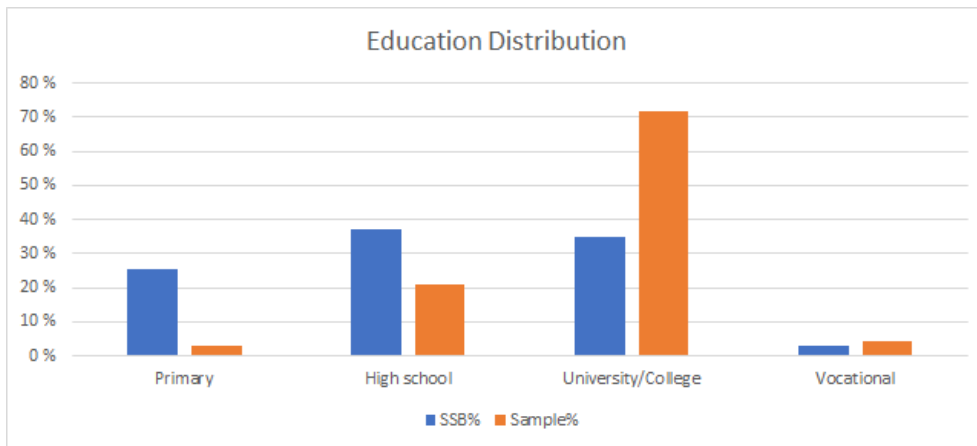


Figure 5.3: Comparison of education distribution of sample versus population. Population is based on data from Statistics Norway (SSB). N=332.

5.1.5 Social Media Use

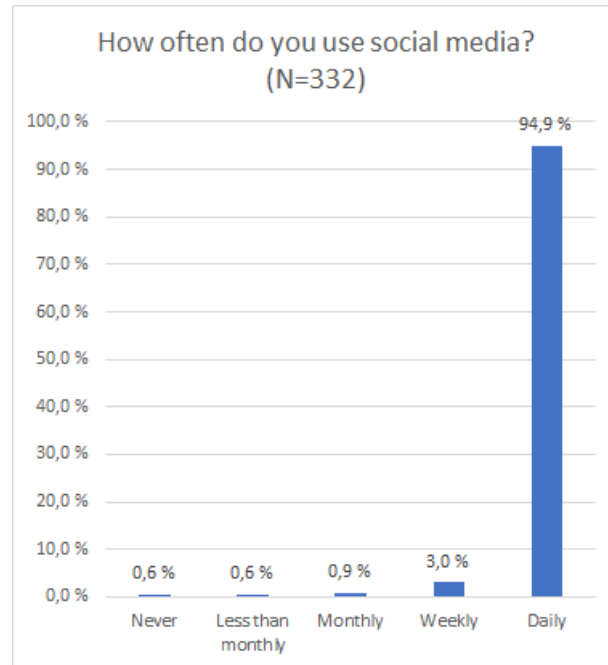


Figure 5.4: Social Media usage across the entire sample. N=332.

As can be seen in Figure 5.4, 95% of the respondents say that they use social media daily or almost daily. Data from Statistics Norway says that only 73% of the target population used social media daily or almost daily in 2019, and that the number of daily users has risen steadily from 54% since 2015 [15]. This overrepresentation is to be expected, since the questionnaire was primarily distributed through social media, and since the subject of the questionnaire is more relevant for social media users.

When it comes to different platform usage, not much certain can be said of the popularity of the different sites, since answers will be heavily skewed towards the platforms that were used to distribute the survey. Something that is noticeable however, is that digital natives are more likely to use a wider array of social media platforms compared to digital immigrants. Figure 5.5 shows that, with the exception of Facebook, all social media platforms are used more by digital natives than digital immigrants.

Respondents were also asked to say how often they use social media to do five specific activities which relates to news, debates and political content. This was asked because it can give an idea of how exposed the respondents are to influence operations, based on what is known of how influence operations operate, and

what has been theorised by the experts. Expert Tore pointed specifically towards political content being a hotspot for influence operation activity.

“As long as there’s a significant disagreement around the given subject, it will be suitable for influence operations. Some form of existential relevance to the person is also important. Climate and immigration are relevant for many people, and the wolf debate is relevant for farmers for example.” -Expert Tore

From the results shown in Figure 5.6, most people prefer to observe without engaging themselves. The most common answer for reading news and reading political content is “daily or almost daily”, while the most common answer for the activities concerning sharing, creating, or commenting is “Never”. Although Digital Natives use a wider variety of social media platforms, it seems that Digital Immigrants do these specific activities more often. For all five activities, there are at least 10% more Digital Immigrants that do these activities weekly or more often. This suggests that Digital Immigrants are more exposed to influence operations, which will be explored further in later sections of the questionnaire.

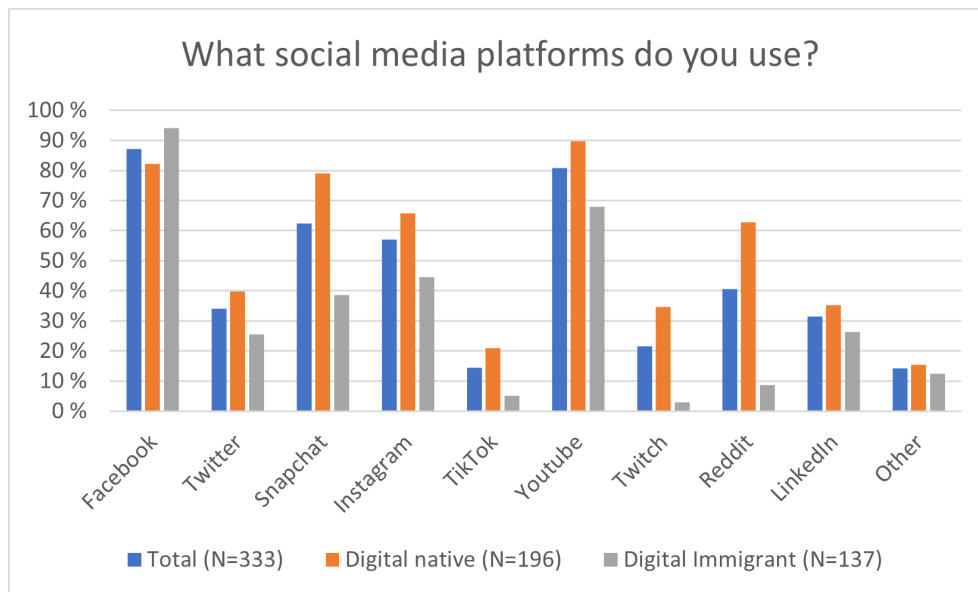


Figure 5.5: Percentage of respondents who said yes to using the following social media platforms.

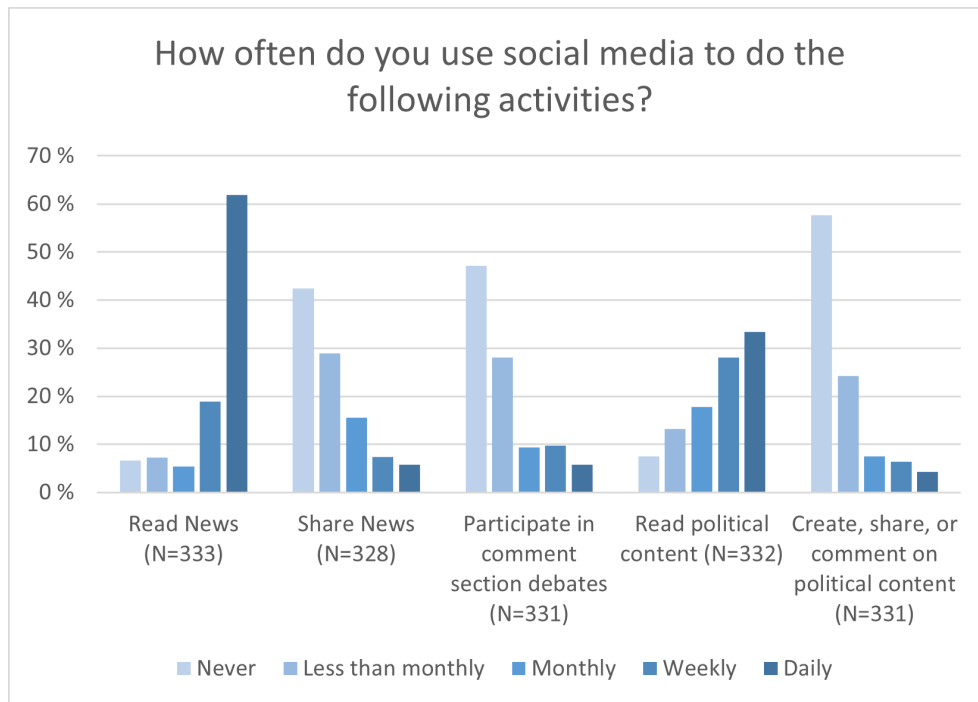


Figure 5.6: How often the respondents use social media to do a set of specific activities.

5.2 Familiarity

5.2.1 Expert Interview

The experts were asked about how much they think the average Norwegian knows about influence operations, and they answered that knowledge on the subject has increased especially in the last year, but there are still some ways to go. Both experts said that awareness especially of fake news has gotten higher, but that many people still don't see "the bigger picture", and that a fake news article is often just a small part of a larger, coordinated, and deliberate attack.

"There's a knowledge of its existence, but a lack of understanding. Influence operations are very often equated to fake news, that they are the same thing. I think the more subtle examples of influencing are harder to understand. So fake news has become a catch all, but an influence operation is much more than just that. So they are able to see "manifestations" of influence operations, but they are not able to understand that they are part of a larger pattern." - Expert Einar

The experts were also asked if they think that knowledge of influence operations can make people less prone to manipulation. The sentiment from both

experts was that it certainly could help, but it won't make anyone immune to manipulation.

“One of the things I have learned is that we are all vulnerable to influencing, regardless of experience and knowledge. Of course, the more you know, the better equipped you are, but you are never immune. Good disinformation is lies spun around a kernel of truth. If you are really good at influencing, you do it so subtle that the information very gradually changes over time, and something like that is very difficult to spot.” - Expert Tore

The experts did however have differing opinions on exactly what type of knowledge is most useful. Expert Tore pointed towards learning how to evaluate the contents of your social media feed, and what to do when you find something that does not seem quite right. Expert Einar on the other hand felt that a better understanding of how society works will make people less likely to believe fake news.

“I don't necessarily think it is that useful to learn directly about influence operations. It becomes a little too narrow, and you just forget about it along with all of the other things you forget in school. But I think it is very useful to learn more about how society in general works and functions. When influence operations find something that people think is unfair, then the operations become very effective. If you for example have the impression that a public service discriminates, or in some way is out to get you. To understand society enough to see the problem from the other perspective will help immensely.” - Expert Einar

5.2.2 Questionnaire

In the familiarity block, three different sets of questions were asked; (1) How often they hear about influence operations and associated tactics through discussions, news, conversations or similar, (2) How often they feel they encounter influence operations and associated tactics through their normal use of social media, and (3) How familiar they feel they are with influence operations and associated tactics. Question 1 gives a sense of how much influence operations are talked about in people's social spheres, while question 2 focuses more on how much people feel they are personally exposed or affected. Question 3 gives an indication of how confident people are in their knowledge of influence operations.

Across all three sets of questions, we see similar distributions for each individual tactic. Fake news for example has a median of 4 and a variance of between 0,95 and 1,05 on all three questions. These similarities are corroborated with a strong spearman rho correlation ($P \geq 0,4$) across all questions for each individual tactic. Comparing the three tactics against each other, there is a clear difference in the level of familiarity, where fake news is the most familiar and fake engagement is

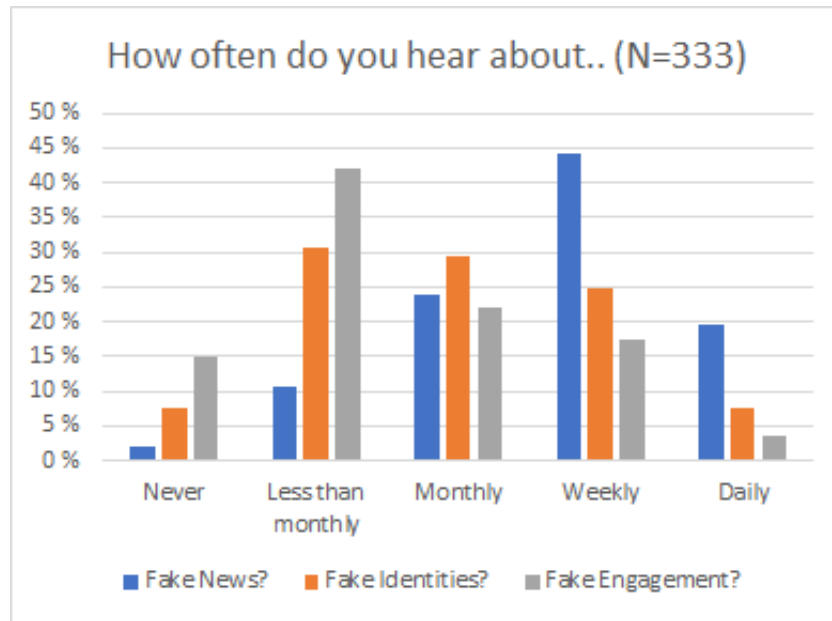


Figure 5.7: How often the respondents hear about fake news, fake identities, and fake engagement.

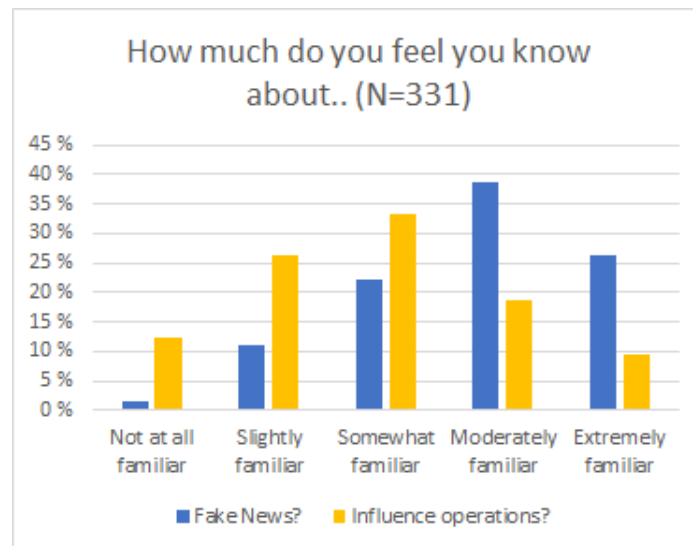


Figure 5.8: Comparison of perceived familiarity between the terms "fake news" and "influence operations"

the least familiar, which matches the theories of the experts. Figure 5.7 shows the difference of how often the respondents hears about the three different tactics, and the difference is similar on the two other sets of questions.

Another initial theory was that familiarity of individual tactics was higher than the broader term of “Influence Operations” (“Påvirkningsoperasjoner” in Norwegian). This is noticeably true for fake news, as can be seen in Figure 5.8, but not as noticeable for the two other tactics. While Influence Operations has the lowest percentage of “Moderately familiar” (19%, $N=62/331$) and “Extremely familiar” (9%, $N=31/331$), Fake Engagement however has the highest percentage of “Not at all familiar” (16%, $N=53/333$) and “Slightly Familiar” (29%, $N=97/333$).

We observed earlier that Digital Natives and Digital Immigrants use social media differently, and there is also a small difference in how often they feel they encounter the different tactics. Fake news had the smallest difference, with less than 5% across the different answers. For Fake identities, 45% of Digital Natives ($N=195$) feel they encounter it weekly or more often, compared to 36% for Digital Immigrants ($N=136$). The biggest difference is however in Fake engagement, shown in Figure 5.9. Digital Natives also feel they know more about Fake Engagement ($P=0,000$). Since the difference lies specifically within Fake Engagement, it could be that certain social media platforms are more aware of, and/or more prone to, this specific tactic.

We also observed a difference in gender, in that males tend to be more familiar. Males feel they know more about all three tactics ($p=0,046$ or lower) and influence operations as a whole ($p=0,000$), and males have a higher median across all three questions regarding fake engagement. Figure 5.10 shows that 15% of males feel they are “extremely familiar” with influence operations, compared to 1% of females.

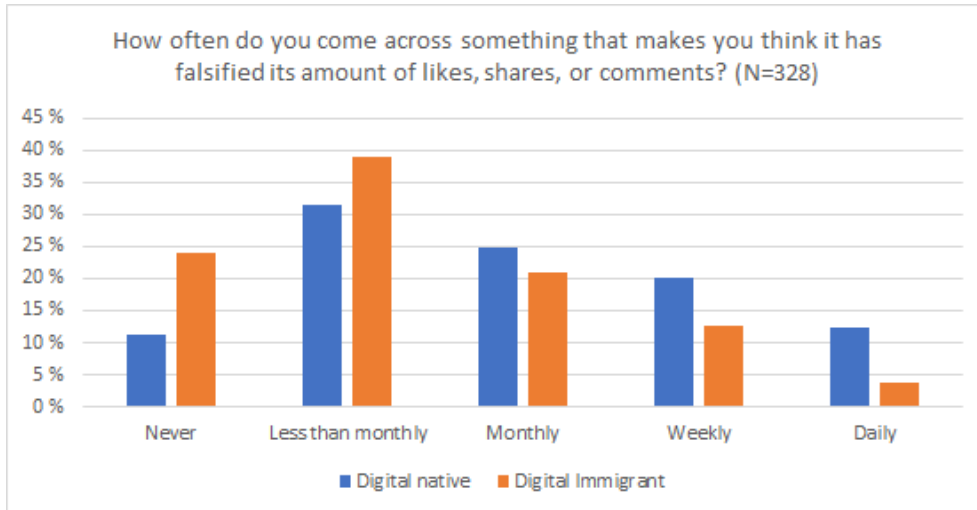


Figure 5.9: Comparison of observations of fake engagement between Digital Natives and Digital Immigrants.

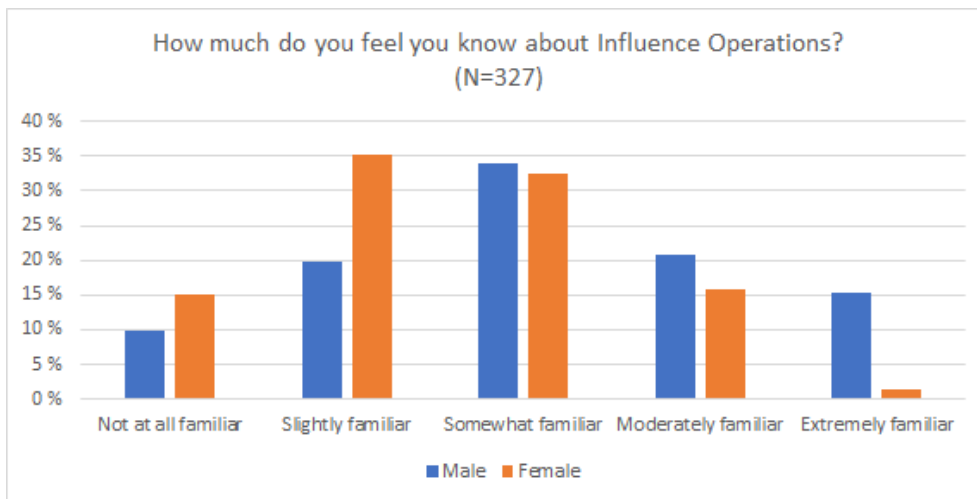


Figure 5.10: Comparison of perceived familiarity in influence operations between male and female respondents.

5.3 Prevalence

5.3.1 Expert Interview

Two questions were asked to the experts that related to the prevalence of influence operations. First, they were asked to give a general sense of how prevalent influence operations are. Expert Einar commented that the quantity of content that a single influence operation can output has been rising, and that more nations and smaller organizations have begun using influence operations. The quality of the content however varies a lot between different influence operations, which affects how much the content is shared, and thus affects how prevalent they are. They specifically point out China, Russia, and Iraq as being the countries that have been discovered using these tactics the most.

“...there has been steadily coming more and more technology to be able to pump out more messages more effectively. It has become very easy to post something. The Russian operation in the USA was also so thoroughly documented that i think a lot of smaller countries got some ideas of their own. Everything is commercialized as well, and with bitcoin among other things it has become possible for smaller groups with the right knowledge to do things only large states could do before. But at the end of the day, it's not that interesting if there's millions of influence operations pushing millions of messages if no one reads them.” - Expert Einar

Secondly, they were asked about their thoughts on how often “the average Norwegian” comes across posts and content from influence operations. Expert Tore says it is almost impossible to tell, and it is highly dependent on the activities you do on social media. They also say that while it is hard to say how often a person is exposed directly, they imagine that it is quite common to be exposed indirectly, for example by having certain topics initially “ignited” by an influence operation be picked up and commented on by different news sites.

“It depends on what types of subjects you normally read about, what types of pages you typically access, and what things you are interested in. I don't know how often people are directly exposed to for example a meme created in IRA's offices, but I think it's quite common to be exposed indirectly to narratives that have been blown up because of an operation. Ideas are planted in different forums, and from there these ideas can spread quite fast, so the chain between original creator and reader can be long.” - Expert Tore

5.3.2 Questionnaire

The Prevalence block also contained three sets of questions. The first set of questions asked the respondent of how likely they think it is that a foreign state has

used fake news, fake identities, or fake engagement to influence a Norwegian election. The second set of questions asked about the same thing, but replaced foreign state with a Norwegian politician or company. Finally, respondents were asked how prevalent the use of influence operations is, both in Norway and in the rest of the world. As can be seen from the questions, a secondary interest along with finding out the perceived prevalence was finding out if there was a perceived difference between Norway and the rest of the world.

The questionnaire responses for the first set of questions are weighted towards “Likely” and “Highly Likely”, with 43-46% of the respondents choosing “Likely” across the three different tactics, and 26-32% choosing “Highly Likely”. The three different tactics had very similar distributions across the first question set, never differing more than 6% in any direction. This suggests that people don’t think certain tactics are more prevalent than others, even though most people feel they encounter fake news the most often.

Comparing question set 1 with question set 2, we see that respondents think it is more likely that an influence operation targeting a Norwegian election will come from a Norwegian politician or company rather than a foreign state. The difference is not huge however, with the largest one being fake news, seen in Figure 5.11. 15% more respondents chose “likely” or “highly likely” that a Norwegian politician would use fake news to influence an election compared to a foreign state. When it comes to fake identities however, only 4% more respondents did the same.

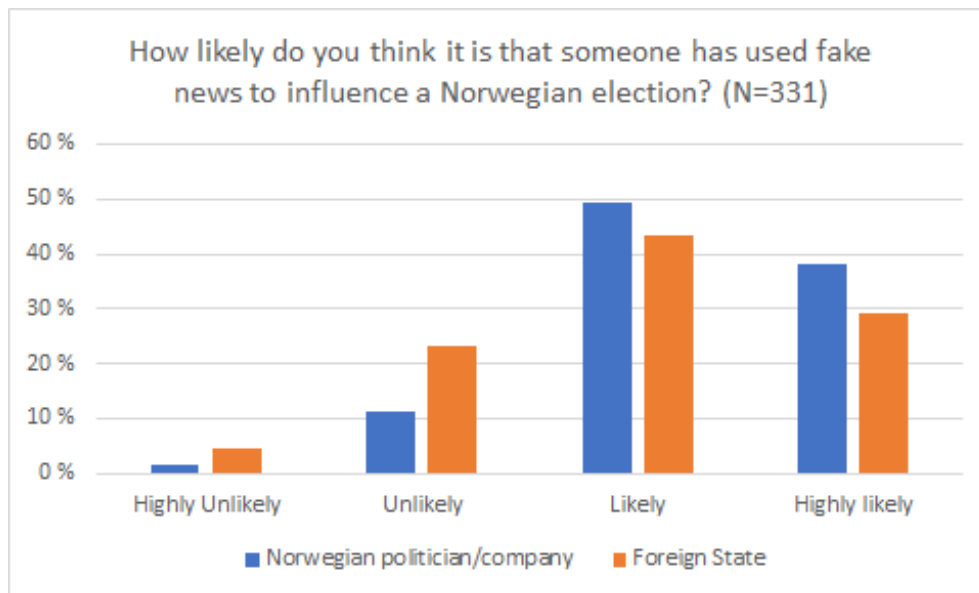


Figure 5.11: Comparison of perceived likelihood of a foreign state or Norwegian politician/company using fake news to influence an election

When asked about how prevalent they think influence operations are, there is a clear difference between the perceived prevalence in Norway and in the rest of the world. 46% of respondents think that influence operations are “Very widely used” in the rest of the world, compared to 12% in Norway, seen in Figure 5.12.

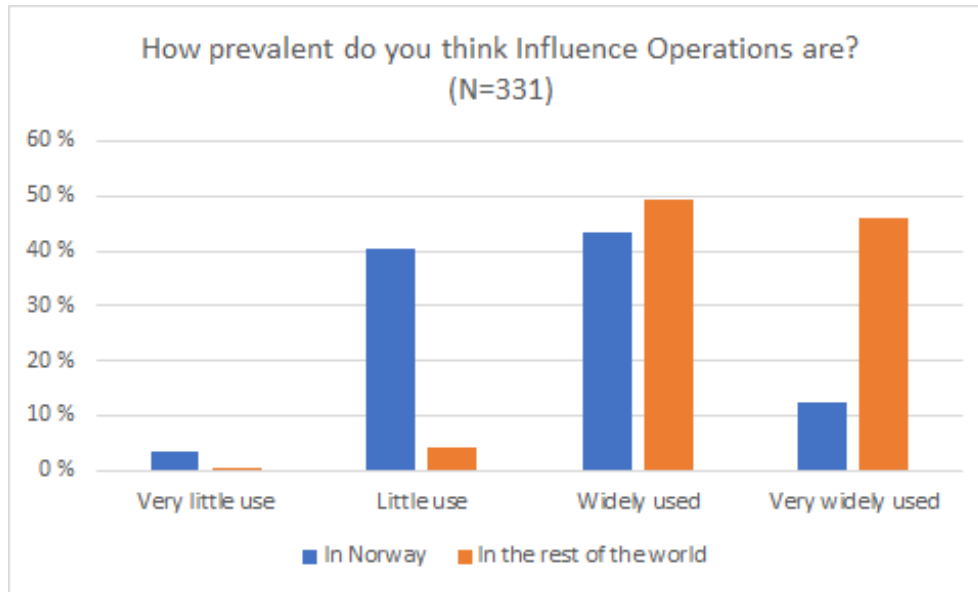


Figure 5.12: Comparison of perceived prevalence of influence operation between Norway and the rest of the world

Comparing the answers of the different demographic groups, there were only a couple of differences found. More males have chosen “highly likely” instead of “likely” when asked about the likelihood that a foreign state has used fake identities ($P=0,021$), and more Digital Natives think that influence operations are “very widely used” in the rest of the world ($P=0,009$).

To look further, the last question from the Familiarity block was used to group people into two categories based on their perceived familiarity of influence operations. Respondents who answered “Not at all familiar” (Ikke i det hele tatt kjent) or “Slightly familiar” (Litt kjent) were categorised as “Unfamiliar” ($N=128$), while respondents who answered “Moderately familiar” (Godt kjent) or “Extremely familiar” (Veldig godt kjent) were categorised as “Familiar” ($N=93$). Respondents who answered “Somewhat familiar” (Middels kjent) were not added to any group. Using these groups, we can see significant differences on all questions in the Prevalence block.

Across all questions, the Familiar group consistently perceived a much higher prevalence than the Unfamiliar group ($p=0,000$ for all questions in question set 1 and 2, $p=0,004$ for prevalence in Norway, and $p=0,023$ for prevalence in the rest

of the world). To give an example, 41% of the familiar group believe it is highly likely that a foreign state has used fake engagement to influence a Norwegian election, compared to only 15% in the Unfamiliar group. 38% of the Unfamiliar group also says the same scenario is unlikely or highly unlikely. This difference is illustrated in Figure 5.13. Based on the information from Norwegian Intelligence Services that was mentioned earlier, it could be argued that the Familiar group has a more realistic perception of the prevalence of influence operations.

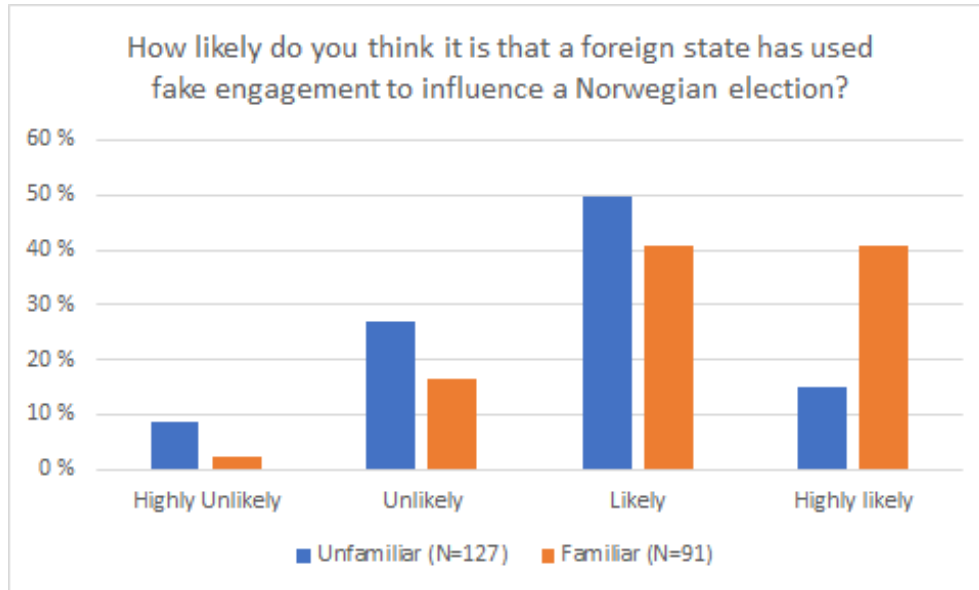


Figure 5.13: Comparison of perceived prevalence between people that have rated themselves unfamiliar and familiar with influence operations.

5.4 Effectiveness

5.4.1 Expert Interview

The experts were asked how effective they think influence operations are, and if there is a limit to how much an opinion can be changed, given enough time and enough resources. Expert Tore says it depends on a lot of different factors. They specifically point out the difference between influencing attitudes and influencing into action, the most difficult of the two being influencing into action.

According to Expert Tore, the goal for an influence operation is often not changing opinions, but creating apathy, polarisation, and distrust by reinforcing existing opinions. Reinforcing opinions exploit people's inherent bias in wanting to be right, in that people will very rarely fact check something they already believe is true. In the same way, opinions can also be strengthened and made more extreme

by “adding fuel to the fire”. For example, if a person believes that a political party’s stances are immoral because it goes against their own beliefs, it is more plausible to make them believe that the same political party would do other immoral things, such as cheating in the election. A side-effect of this also is that by making more people more extreme in one way or the other, people that are not as extreme can become exhausted and confused by the discussions and eventually lose interest and decide not to partake.

Importantly, Expert Tore believes that influence operations lose a lot of its effectiveness against Norwegians specifically, because Norway as a society has a high degree of trust towards one another and towards governmental institutions. This is corroborated by one of the studies mentioned in the related works section, where it was found that 8 out of 10 Norwegians trust Norwegian news media, which is much higher than the global average [31].

“Influence operations rarely try to completely change someone’s opinion, especially if the person already has formed an opinion leaning the opposite way. You don’t try to convince an FRP voter to instead vote for SV for example, that just won’t be very effective. Instead, you target a group that would be realistic to influence. How easy this is depends on the subject.

Something that is much simpler, is to confirm and reinforce an opinion that a person already has. Influence operations often do this, because the goal of the operation more often is to create polarisation or apathy within a society. With regards to threats against democracy this is just as important to be aware of.

It all comes down to trust. Norwegians have a high degree of trust towards one another and towards the government, which makes us more robust against influence operations, and better equipped to deal with crises such as the pandemic, compared to nations with a lower level of trust. The polarisation is just a step towards trying to undermine the trust within a society. Without trust, the society becomes paralyzed into inaction.” -Expert Tore

5.4.2 Questionnaire

Influence Operation Scenario

Participants were asked to envision an influence operation from a foreign state targeting a Norwegian election with three goals in mind: (1) They want a specific candidate to win the election, (2) they want at least 10% of the population to believe that the candidate’s opponents cheated in the election, and (3) they want under half of the population to vote, due to apathy, exhaustion, confusion, or

indifference. The respondents were asked how likely it is to achieve these goals, along with the likelihood of remaining hidden, and how much of the population they would be able to reach with the operation.

Looking at the first goal in Figure 5.14, we see that over 47% of the respondents deemed it “Likely” and 7% “Highly likely” that the influence operation will succeed in getting a specific candidate to win the election. The second goal is very similar, though slightly more skewed towards “Likely” and “Highly likely”, while the third goal is the only one to skew towards “Unlikely” and “Highly unlikely”. There are very few answers in the “extremes” on all questions, with over 75% of the answers being either “likely” or “unlikely”. This could suggest a lack of certainty either way in many responses.

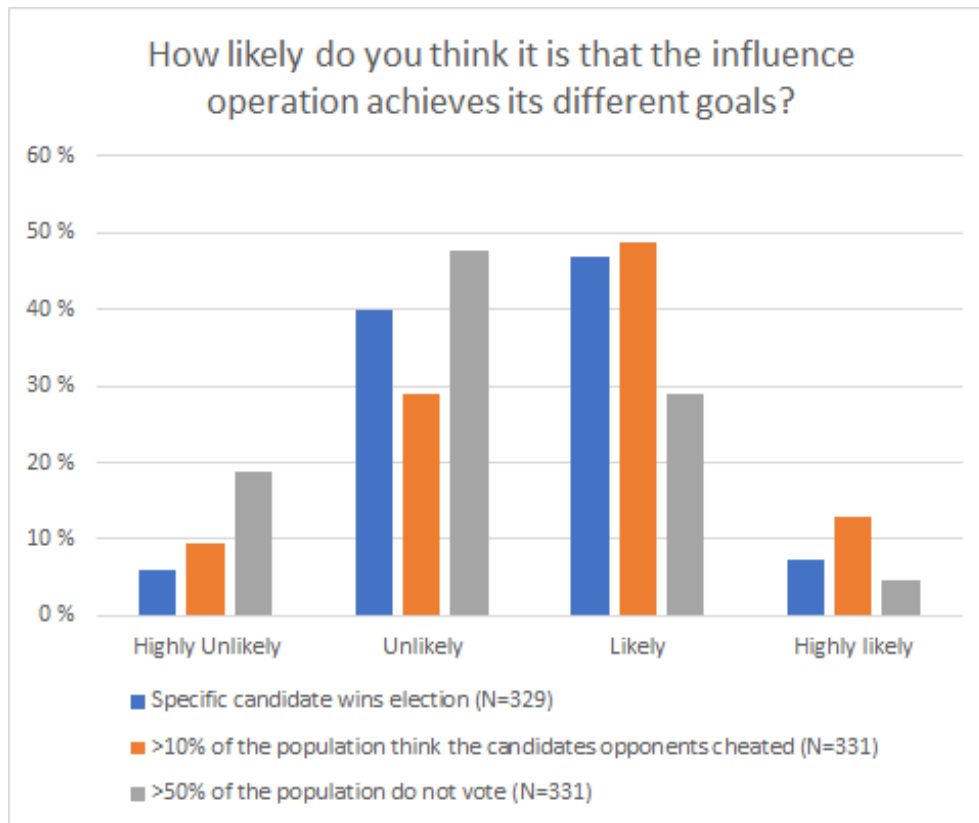


Figure 5.14: Comparison of likelihood ratings of achieving the three different influence operation scenario goals.

There were some differences in the demographic groups, both in location and in gender. Respondents from Trondheim believe it is less likely for the influence operation to achieve the first and third goal compared to other locations (P=0,038 and P=0,000). Males also believe it is less likely for the influence operation to

achieve the third goal compared to female respondents ($P=0,015$). No significant correlation was found between any of the goals and any of the other questions in the survey.

As for the other scenario-specific questions, a majority of the respondents believe it is likely that the influence operation can remain hidden, with 53% choosing “Likely” and 9% choosing “Highly likely” ($N=331$). This is higher than any of the three goals, which suggest that people think remaining hidden is one of the simplest tasks for influence operations.

When it comes to the reach potential of the influence operations, the respondents are clearly divided into two groups which can be seen in Figure 5.15. We see two spikes slightly below and slightly above 50% reach. The most common answer is 30-40% of the population, but the three next most popular answers are 60-90% reach. Surprisingly, there were no significant differences in any of the demographic groups, and no correlation strong enough to explain this division between respondents.

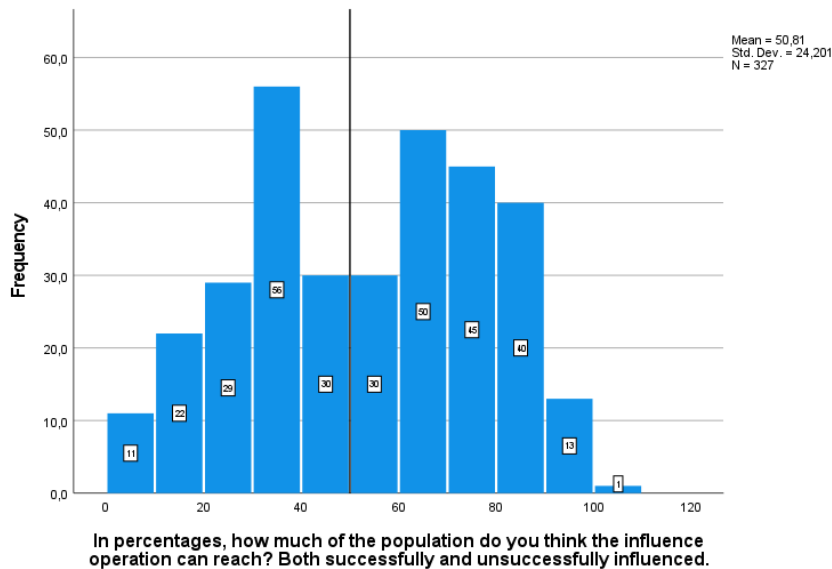


Figure 5.15: How much of the population the influence operation can reach. Bin size=10.

Using the Familiar and Unfamiliar group from earlier, there were no significant differences in any of the scenario specific questions. This suggests that familiarity with influence operations has little effect on how the effectiveness of influence operations are perceived. This is in stark contrast to how the prevalence of influence operations were perceived, where we saw significant differences in all questions.

Personal Effectiveness

The two final questions in the Effectiveness block asked if the respondent thought they ever have been influenced by an influence operation in the past, and if they think they will be influenced in the future. For being influenced in the past, there is a slight majority in “Unlikely” and “Highly unlikely”, with a total of 58% of the respondents choosing one of the two answers. Being influenced in the future however has a slight majority in “Likely” and “Highly likely”, with 55% of the respondents choosing one of these two answers. This is illustrated in Figure 5.16. Once again we see a large majority of respondents choosing between the middle two answers on both questions, with “Unlikely” and “Likely” being 80% of the answers. The two questions are highly correlated (Spearman=0,761).

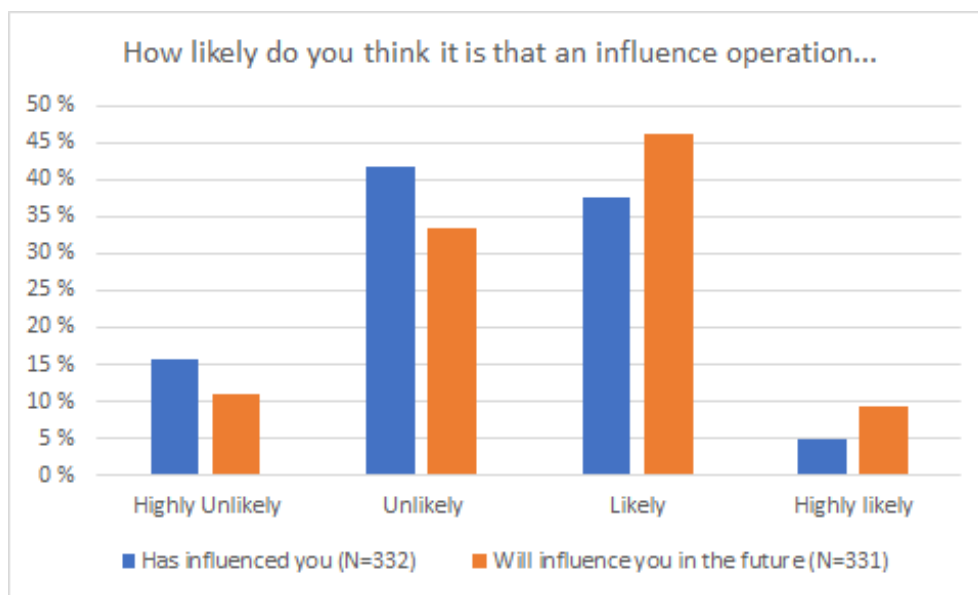


Figure 5.16: Comparison of likelihood between being influenced in the past and being influenced in the future.

There were differences in age and familiarity. Digital Natives think it is more likely that they have been, and will be, influenced ($P=0,048$ and $P=0,000$). The same is true for the Unfamiliar group ($P=0,020$ and $P=0,004$), which suggest that familiarity makes a person feel more resilient.

5.5 Risk Perception of Activities

Questionnaire participants were asked to rate the level of risk associated with the same social media activities that were used to rate their social media use. The main purpose of this question was to compare against social media use, to look for correlations between activity and risk perception.

All of the activities except reading news have very similar distributions, as can be seen in Figure 5.17. Reading news is more skewed towards the “No risk” and “Low risk” options, while the four other activities are more centered. The “Low risk” and “Medium risk” options for these activities are never more than 2% different from each other, staying in the range of 31-36%. Participating in comment section debates is the activity that was deemed the highest risk, with 24% choosing “high risk” and 9% choosing “No risk”.

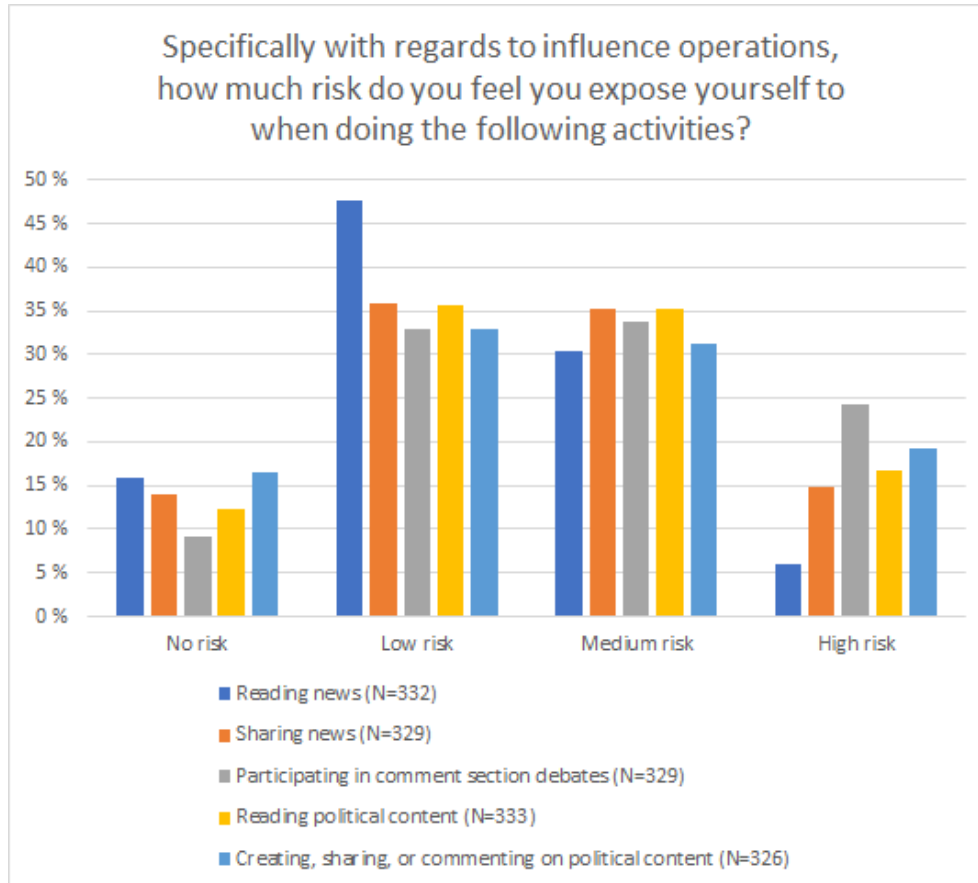


Figure 5.17: Perceived risk levels of the different activities.

In this question, there were once again saw differences in age. Digital Natives attribute a higher level of risk to all activities, with significant differences in reading news ($P=0,000$), comment section debates ($P=0,034$), and reading political content ($P=0,000$). Differences were also found between the familiarity groups, in that the Familiar group attributed a higher risk to comment section debates ($P=0,000$), reading political content ($P=0,000$), and engaging with political content ($P=0,001$).

This is interesting when looking at social media use, and the likelihood perception of being influenced. The Familiar group feel they are more resilient towards being influenced compared to their counterpart, unlike Digital Natives which feel they are less resilient. The Familiar group is also more active than the Unfamiliar group in the three activities that had differences in risk perception, while Digital Natives are less active than Digital Immigrants. This suggests a positive correlation between activity and risk perception in the Familiarity groups, and a negative correlation between activity and risk perception in the Age groups.

Testing for these correlations, there were no significant findings however. There was no correlation between how risky an activity was perceived and how often that activity was done. Correlation was checked for the whole sample, for Digital Natives specifically, and for the Familiar group specifically.

Chapter 6

Discussion

In this section I will summarize the findings from the Results section, with regards to how they relate to the different research questions. I will also discuss possible explanations for the findings, as well as possible implications. Each of the sub-chapters will focus on one of the research questions.

6.1 How familiar does the Norwegian public think they are with malicious influence operations on social media?

From the questionnaire, we saw that there was a clear difference in familiarity between the different tactics, with fake news being more familiar than any of the other tactics as well as the broader term of “influence operations”. The experts also believed this would be the case, and they often experienced that Fake News got equated to influence operations, even though it is only a small part of a larger operation. There are a few possible explanations to this. For one thing, fake news has more applications than just large-scale influence operations. Some sites might for example create fake news stories only for economic gains, using “shock factor” to gain more clicks and in turn gain more ad revenue, such as the influence operation discussed by Thomas et. al.[1]. The term has also gained increased popularity with “populist politicians” that often use it to discredit their opposition or criticism from the media. This can be seen for example in Google Trends, where the search term “Fake News” spiked massively in popularity in November of 2016, correlating with the 2016 US election [44]. The search term has also consistently been more than 5-10 times more popular after 2016 compared to before 2016.

Fake engagement on the other hand, was the least familiar tactic. This could have something to do with the fact that “engagement” does not have a direct translation to Norwegian that encompasses the same social media activities. The questionnaire used “fake popularity” and tried to explain that it involved falsifying likes, comments and shares. Another factor could be that fake engagement is in

many ways the hardest of the three tactics to identify. A news story and an identity involves more information that can be processed to make a judgement on whether it is fake or not, while fake engagement is often from the users perspective just a slight change in a number.

We saw however that some demographic groups were more familiar with fake engagement than their counterpart, specifically Digital Natives. Digital Natives were more familiar with, and felt they encountered, fake identities and fake engagement more than digital immigrants. This is somewhat special because in most cases in the questionnaire, a higher amount of activity on social media correlated with better familiarity of influence operations, and Digital Immigrants were generally more active in the given social media activities. Digital Natives however used a wider variety of social media platforms. The theory here is therefore that the difference in familiarity comes from the fact that certain platforms are more “culturally aware” of social bots, both malicious and benevolent, which are an essential tool for both fake identities and fake engagement. An example of this is that Reddit and Twitch, which is almost exclusively used by Digital Natives only, have a higher amount of automated accounts interacting with normal users as though they were users themselves, but announcing the fact that they are bots. Reddit has an entire subforum called “SubredditSimulator”, which consists entirely of automated accounts that simulate the behavior of users on other specific subforums using artificial intelligence [45]. Twitch has NightBot, which acts as an automated moderator of chatrooms for livestreams. NightBot can delete prohibited words or messages and display automated answers that get invoked when users say a certain word or give a certain command [46]. Seeing bots interact with you in this way can make you more aware of the fact that the same technology can be used in more discreet and malicious ways.

All in all, while some tactics are quite familiar, there is still some way to go when it comes to seeing the bigger picture. There were more people that feel they are unfamiliar with the term “influence operations” than there are people that feel they are familiar, and the majority of respondents place themselves in the center of the scale. The question is then, if a person knows enough about the tactics individually, is it necessary to know that they can be combined? Expert Einar believes it is unnecessary to learn that much specifically about influence operations since most people will forget about most of the information anyways. The most beneficial thing to know would probably be that the threat exists. Not knowing that deepfakes exist for example can make you very vulnerable to misinformation, but knowing exactly how deepfakes work or how to spot anomalies in deepfakes will probably have a lower “return on investment”, considering the effort that would take. I think therefore that if one were to create an awareness campaign around influence operations, the target should be to transfer the “not at all familiar”s to “slightly familiar” rather than trying to make everyone extremely familiar.

6.2 How prevalent does the Norwegian public think that malicious influence operations on social media are?

When it comes to prevalence, a large majority believes that both foreign and national threat agents have used fake news, fake identities, and fake engagement to influence Norwegian elections. The interesting point here is that, although the questions asked were of a subjective nature, we do actually have some information from “reality” to compare against. Norwegian Intelligence Service (E-tjenesten) has confirmed that both Russia and China have targeted Norway in influence operations concerning the covid-19 pandemic [8], and they expect that both Russia and China will seek to influence the election in 2021 [47]. The experts also believe that Norway is targeted by foreign states, and that it is not that uncommon to be at least indirectly exposed to influence operation narratives. So in reality, it is likely or highly likely that a foreign state will influence a Norwegian election in the future.

With this in mind, the perception of the majority is probably close to reality, but the remaining 25-28% of the respondents who said it was unlikely or highly unlikely that a foreign state has used any of the tactics on a Norwegian election is important to note. The implication of this low perception of prevalence is that they might be more susceptible to being influenced by foreign states, since they don't expect to be targeted and therefore might have a higher barrier to detect that something is wrong. While they are the minority, 25-28% is still a lot of people, especially when considering that the experts believe the prevalence will only rise in the future.

The “minority-group” of low prevalence perception is however smaller for influence operations coming from Norwegian politicians or companies, which means that people deem it more likely to be targeted by Norwegian influence operations than foreign ones. This seems a bit counter-intuitive when you consider that most people believe that prevalence is higher in other countries than Norway. If it is used more outside Norway, wouldn't it then make sense that an attacker more often is from outside Norway? A possible explanation for this is that people have a perception of Norway being insignificant in the world and therefore “not on the radar” for the bigger nations. This view is certainly not shared with the interviewed experts however, which mentioned Russian interests in Norway several times.

As mentioned earlier, most people believe that the prevalence of influence operations is higher in other countries than Norway. Whether this perception is realistic or not can be hard to judge, but Slovic's common biases and heuristics in risk perception could give an explanation to why this perception exists. Some of it might be an optimism bias (the “it won't happen to me” heuristic), that people

feel Norway is immune to a threat they otherwise perceive as real [32]. One of the experts felt Norway is more resilient because we have a high degree of trust. It could also be a result of availability heuristics, that people judge an event to be more frequent if instances of it are easy to recall [32]. There haven't been any big news stories of influence operations in Norway, but such stories have been very prominent in for example the US.

Finally, we saw a high correlation between perceived familiarity and perceived prevalence, and that a higher degree of familiarity resulted in what I describe as a more realistic perception of prevalence. A question we are left with however is which of the two affects the other the most? Does learning about influence operations make it easier for people to spot them and therefore give a higher perception of prevalence, or does perceived prevalence make you feel more familiar? Judging by the effectiveness-block which we will look at in the next sub-chapter, it seems that the latter is more likely. Familiarity has no effect on perceived effectiveness, so it seems that the relationship is the other way around, that prevalence affects familiarity.

6.3 How effective does the Norwegian public think that malicious influence operations on social media are?

The results from the effectiveness block stand out from the rest of the questionnaire, especially from the scenario-specific questions. There was no clear pattern in the answers, in that we saw no significant correlation with any other blocks of questions. Demographic groups such as location showed differences when it had not done so on any other questions, while the familiarity groups showed no differences even though it made an impact on all the other blocks. The question regarding potential reach of an influence operation is a good example of all of this. It had a clear divide in the answers, with two clusters forming around slightly under 50% and slightly over 50%. This divide could however not be explained by any of the demographic groups or by any correlation with the other questions, which could suggest that these answers are affected by some variable that were not tested for. A possible explanation is that these answers rely more on the emotional dimension of risk perception instead of the cognitive dimension, and that people have answered based on instinct, feelings, or guesswork rather than some prior knowledge or preconception. This would make sense considering the subject, there is no documented proof of the effectiveness of influence operations, so there is no (factual) prior knowledge available. It is however not possible for us to dig deeper into this without some form of follow up interviews with respondents to ask about their reasoning behind their answers.

In any case, the effectiveness of influence operations was perceived to be at around a "medium risk", with the likelihood of achieving the different goals being

somewhere between “unlikely” and “likely” for most people. Very few people chose either “very unlikely” or “very likely”, which suggests that people don’t see it as a non-existent threat, but they don’t see it as extremely dangerous either. Out of the three goals, the one deemed most likely to achieve was making people believe a candidate cheated, slightly over making a specific candidate win the election.

To get a sense of whether these perceptions are an overestimation or underestimation of influence operations’ actual capabilities, we will try to look at the 2020 US election. It is hard to know exactly how much an influence operation changed the outcome of an event, and there are many differences between Norway and the US that makes it not directly comparable, but there are still some observations that can be made. US intelligence reported that Russian influence operations tried to get Donald Trump reelected in 2020 but was unsuccessful [48]. The election also had accusations of fraud spearheaded by the 2020 Trump campaign. It could be argued whether or not Trump’s accusations should be considered an influence operation or not, but according to surveys from Politico and Yougov, over 70% of republicans believe there was widespread voter fraud. When it comes to voter participation however, participation has been quite stable for a long time in both Norway and the US, meaning no visible change even before and after the inception of social media. To summarize, The most achievable goal seems to be making people believe there was fraud, while the two others are more difficult.

With this in mind, it can be argued that participants have overestimated the capabilities of influence operations to alter election results. This can be corroborated by statements from Expert Tore, where they said that they think Norway should be resilient towards influence operations, and that changing someone’s opinion and influencing into action is the most difficult thing to do. We can also look at Folkeopplysningens influence operation experiments, which had little to no effect on the results of the election [20], but this could also be attributed to a lack of experience and expertise on par with “professional” operations.

Looking now at the questions regarding being personally affected, we once again saw distributions being heavily centered around the middle two options of “unlikely” and “likely”. This gives more reason to believe that influence operations is considered a “medium risk” by most people. Being influenced in the future had a higher perceived likelihood than being influenced in the past, which could suggest that people feel influence operations will become a bigger threat in the future however. Social media influence operations have only become a fairly popular topic in the media in recent years, so people might feel that there haven’t been that many opportunities to actually be influenced yet.

The answers for these two questions are also more “back in line” with the rest of the questionnaire. We once again see the common demographic groups of age and

familiarity showing significant differences, with the Familiar group and the Digital Immigrant group being more confident in their resilience than their counterpart. I will discuss this in more detail in the next sub-chapter in conjunction with some of the other questions.

6.4 Does risk perception of malicious influence operations impact behavior on social media?

My main test for evaluating if risk perception affected behavior on social media was to have the participants note how often they do certain activities, and then ask them to rate how risky those activities were. A negative correlation between these two answers would suggest that a high risk perception can cause people to avoid certain activities. The answer to this research question was however not that simple, as there were no correlation between the two sets of questions. In fact, neither familiarity, perceived prevalence, nor perceived effectiveness had any effect on the risk perception of activities. So if risk perception affects behavior on social media, it is not as easy as saying “I think this activity is risky so i will avoid doing it.”.

Going a more complicated route, one can interestingly find arguments to both support and counter the hypothesis of risk perception impacting behavior. If we look at age for example, we see that Digital Natives consistently have a higher risk perception of influence operations compared to their Digital Immigrant counterpart. They think influence operations are more prevalent in the rest of the world, they feel they encounter influence operations more often, and they think it is more likely that they have been, and will be, influenced by an influence operation. They also feel that several of the activities are more risky than what the Digital Immigrants think. Most importantly, they are less active in these activities compared to Digital Immigrants. So while we cannot find a direct correlation between activity and risk perception, there are some things here that support a theory of high risk perception being in some way associated with lower levels of social media activity.

Things get more muddled however when we look at the Familiar and Unfamiliar groups. The Familiar group has a higher perception of prevalence, and they think that some of the activities are more risky than what the Unfamiliar groups think. But the Familiar group is more active than the Unfamiliar group, which goes against what was found with the age groups. An argument for why this is can be found when looking at the groups perceived resilience towards influence operations. The Familiar group thought it was less likely for them to be influenced than what the Unfamiliar group thought. It could be that the Familiar group relies more on the “It won’t happen to me” heuristic, and view themselves as more immune to the risks they otherwise perceive as real because of their familiarity with the subject.

Combining the two findings together, I argue that there is a connection between risk perception of influence operations and behavior on social media. I think a higher risk perception is connected to a lower level of activity on social media, specifically when it comes to engaging with political subjects. But a high degree of perceived familiarity with influence operations can lead to overconfidence and ignoring the risks, thus the level of activity is not reduced. I also argue however that this connection is weak at best, and that other outside factors will play a much bigger part in the level of activity on social media for any given person.

Chapter 7

Conclusion

This project has looked at the risk perception of the Norwegian public towards influence operations on social media. The focus has been on the cognitive elements of risk perception, and we have looked at three specific elements that can affect a person's risk perception: How familiar they feel they are with the phenomenon, how widespread they think it is, and how well they think it works. We have also looked at the connection between risk perception and social media activity.

When it comes to familiarity, the Norwegian public feel they are more familiar with certain tactics that influence operations employ than they are with the larger operation as a whole. Specifically fake news is very familiar for most people. The familiarity of influence operations as a whole however is still quite high, with 88% of the respondents feeling they are at least slightly familiar with the term.

For the perceived prevalence of influence operations, most people agree that the threat is real, and that Norway will be targeted by both foreign and "local" operations. 25% of the respondents however believe it is unlikely for Norway to be targeted by foreign states, even though Norwegian Intelligence Services is saying we are being targeted by foreign states constantly [8]. Most people also believe that influence operations are more prevalent in the rest of the world compared to Norway.

As for the perceived effectiveness, Norwegians believe influence operations have a moderate chance of success with their different goals. They believe especially that influence operations are good at remaining hidden, and at making people believe in fake information such as alleged fraud in an election. The perceived effectiveness is similar when we ask about them being personally influenced. More people believe however that they will be influenced by an influence operation in the future, which suggests that people believe the threat is rising.

Finally, there was no direct correlation between risk perception of influence operations and social media activity, but there were signs that there exists a weak connection. A higher risk perception was found in certain subgroups of the Norwegian population who also were less active in “political activities” on social media. We do however believe there are other outside factors that will play a much bigger part in the level of activity on social media for any given person.

Looking at different subgroups within the Norwegian population, the demographic attribute that showed the most differences in risk perception were age. Digital Natives generally had a higher risk perception than their Digital Immigrant counterpart. We also saw that familiarity with influence operations played a part especially in the risk perception of prevalence, but familiarity could also lead to a false sense of security in thinking they are more resilient towards the threat.

The summarized version of all this is that the Norwegian public perceive influence operations on social media as a moderate risk. It is probably not something most people actively think about when using social media, but it is not something they perceive as completely unrealistic or harmless either. Due to the nature of the topic, it is difficult to say anymore about what this means. Is moderate risk an accurate representation of the threat? Does it make Norwegians well prepared or unprepared for an eventual large scale operation? Should we do more to be better prepared, and is there even anything we can do to be better prepared? There is still a lot of work that could be done, but like many things in information security, perhaps the only way of knowing how prepared we are is to experience an attack.

Chapter 8

Limitations and Future Work

As a final chapter of this paper, I will discuss some of the limitations of the project and how they could be addressed by future studies.

8.1 Questionnaire Suggestions

The questionnaire had a text box at the end of it, in which the respondents could put their thoughts and feedback on the survey. From this, there were two suggestions that were repeated by multiple respondents, which will be addressed here.

3 participants commented on a desire for more answer options. Most of the questionnaire uses a 4-point scale, and the argument for using this was to make it easier for the participants to answer. My thought-process here was that the more options there are to choose from, the more decisions a respondent has to make, which might lead to decision-fatigue and giving up on the survey. Looking at the distributions for the different questions, I agree that some of them could have benefited from having more options. Especially in the effectiveness block the answers were heavily centered around the two middle options, and increased granularity would give me much better data to analyse. If I were to recreate the survey, I would have probably replaced the 4-point scale with a 7-point or even 10-point scale for most of the questions, as gathering participants wasn't as difficult as I imagined it would be.

8 participants commented on a desire for an "I don't know" option. It was a deliberate choice to not include this option, since all of the questions were of a subjective nature, and I would rather have people guess based on their feelings. This choice was however based on a false notion that an "I don't know" option would not give me any useful information to analyse. I think it would actually be beneficial to have an "I don't know" option especially in the effectiveness block, as it can give a gauge of how much uncertainty there is in the population regarding these questions. I theorised that uncertainty could play a part in the results of the

effectiveness block, but an “I don’t know” answer option could give a concrete answer to that theory.

8.2 Questionnaire Errors

Some problems were discovered with the questionnaire after the data collection, especially in the effectiveness block. As an extra piece of information for the last goal in the influence operation scenario, respondents were told that normal voter participation in Norway is 65%. This is true for county elections, but state elections have a voter participation of 79%. This may have skewed the perceived difficulty of achieving the goal. None of the participants commented on the mistake in the questionnaire feedback, so it is uncertain if anyone noticed the mistake. It is also unknown how many of the respondents had an idea of what the real percentage was, and used that as their reference instead. Because of this uncertainty, it was decided to not put that much weight on this question in the analysis.

The scenario could also be improved in another way. As they were presented in the questionnaire, the different goals aren’t very comparable since they require different amounts of the population to be influenced. A better version of this question would rephrase the goals so that all goals refer to influencing at least 10% of the population in their respective ways, for example like this:

“Imagine an election in Norway, and that a foreign state is targeting the election with an influence operation. The influence operation has three goals in mind:

- *They want at least 10% of the population (who otherwise would have voted on a different candidate) to switch their vote to the foreign state’s preferred candidate.*
- *They want at least 10% of the population to believe that the candidate’s opponents cheated in the election.*
- *They want at least 10% of the population (who otherwise would have voted) to choose not to vote, due to apathy, exhaustion, confusion, or indifference.”*

In this way, it becomes much easier to say something about what the participants think is the easiest to achieve or the hardest to achieve. Future work using a similar research design should apply these corrections.

8.3 Scope Limitations

A notable exclusion in the questionnaire is any questions regarding social media algorithms. Social media algorithms are the mechanics that Social Media Platforms use to sort content based on what they believe will be most interesting to

each individual user, showing the most interesting content first. Both experts expressed that social media algorithms are a huge part of the problem, and that it makes the job of influence operations much easier. This topic was however omitted since the questionnaire was already quite long, and this topic was the most out of scope with regards to the research questions of the project. But seeing how familiar the population is with how these algorithms work and if this impacts their risk perception of influence operations could be an interesting topic to investigate in another study.

As mentioned previously, the questionnaire also focused on the cognitive dimension of risk perception, but that does not mean that there isn't valuable insight to be gained from exploring the emotional dimension as well. The main reason for not going in depth into this dimension was because I felt that questionnaire as a data collection tool was not well suited for it. I think a better way to gather data for the emotional dimension would be to perform qualitative interviews, so the respondents can give their full thoughts and line of reasoning, rather than trying to rate their emotions on some scale. A recommendation here for future work would be to expand the research design with a follow-up interview with questionnaire respondents, to ask about their thoughts regarding the different questions, and possibly some additional questions more specific to what kind of feelings influence operations invoke in them.

Another interesting thing that could be explored by future work is doing a similar research design on a different population. By doing the same study on for example another nation, one could gain increased insight by having a point of comparison. One theory that the experts mentioned was that Norway could be more resilient towards influence operations, because of a high degree of trust towards another. A point of comparison would make it easier to see if this is reflected in their risk perception as well. It could also help with gaining insight into what external variables affect the risk perception of influence operations.

Bibliography

- [1] E. Thomas, N. Thompson and A. Wanless, 'The challenges of countering influence operations,' Carnegie Endowment for International Peace, 2020. [Online]. Available: <https://carnegieendowment.org/2020/06/10/challenges-of-countering-influence-operations-pub-82031>, (accessed: 24-10-2020).
- [2] R. DiResta, K. P. Shaffer, B. Ruppel, D. M. Sullivan, R. Matney, R. Fox, J. Albright and B. Johnson, 'The tactics & tropes of the internet research agency,' 2018. [Online]. Available: <https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf>, (accessed: 24-10-2020).
- [3] N. Chavoshi, H. Hamooni and A. Mueen, 'Debot: Twitter bot detection via warped correlation,' in *2016 IEEE 16th International Conference on Data Mining (ICDM)*, 2016, pp. 817–822. DOI: 10.1109/ICDM.2016.0096.
- [4] A. Nestoras, 'Political warfare: Competition in the cyber era,' Dec. 2018, pp. 4427–4436. DOI: 10.1109/BigData.2018.8622490.
- [5] V. Gerasimov, 'The value of science is in the foresight, new challenges demand rethinking the forms and methods of carrying out combat operations,' *Military Review*, Jan. 2016.
- [6] R. Nixon, 'U.s groups helped nurture arab uprisings,' *The New York Times*, Apr. 2011. [Online]. Available: <https://www.nytimes.com/2011/04/15/world/15aid.html>, (accessed: 24-10-2020).
- [7] H. A. Conley, 'Successfully countering russian electoral interference,' Center for Strategic and International Studies, Jun. 2018.
- [8] O. Kibar, 'Ny type desinformasjon har skutt fart under koronapandemien: - du og jeg sprer det videre,' *DNMagasinet*, Oct. 2020. [Online]. Available: <https://www.dn.no/magasinet/teknologi/etterretningstjenesten/politiets-sikkerhetstjeneste/russland/ny-type-desinformasjon-har-skutt-fart-under-koronapandemien-du-og-jeg-sprer-det-videre/2-1-883373>, (accessed: 24-10-2020).
- [9] A. Aronivich. (2018). 'How to detect fake profiles - understanding phishing,' [Online]. Available: <https://www.cybintsolutions.com/detect-fake-profiles-phishing/>. (accessed: 24-10-2020).

- [10] C. Ladd, 'Jenna abrams is not real and that matters more than you think,' *Forbes*, Nov. 2017. [Online]. Available: <https://www.forbes.com/sites/chrisladd/2017/11/20/jenna-abrams-is-not-real-and-that-matters-more-than-you-think/#3edb8eb53b5a>, (accessed: 24-10-2020).
- [11] D. M. J. Lazer, M. A. Baum, Y. Benkler, A. J. Berinsky, K. M. Greenhill, F. Menczer, M. J. Metzger, B. Nyhan, G. Pennycook, D. Rothschild, M. Schudson, S. A. Sloman, C. R. Sunstein, E. A. Thorson, D. J. Watts and J. L. Zittrain, 'The science of fake news,' *Science*, vol. 359, no. 6380, pp. 1094–1096, 2018, ISSN: 0036-8075. DOI: 10.1126/science.aao2998. eprint: <https://science.sciencemag.org/content/359/6380/1094.full.pdf>. [Online]. Available: <https://science.sciencemag.org/content/359/6380/1094>.
- [12] Y. Boshmaf, I. Muslukhov, K. Beznosov and M. Ripeanu, 'Design and analysis of a social botnet,' *Computer Networks*, vol. 57, no. 2, pp. 556–578, 2013, Botnet Activity: Analysis, Detection and Shutdown, ISSN: 1389-1286. DOI: <https://doi.org/10.1016/j.comnet.2012.06.006>. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1389128612002150>.
- [13] M. Jones. (Jun. 2015). 'The complete history of social media: A timeline of the invention of online networking,' [Online]. Available: <https://historycooperative.org/the-history-of-social-media/>. (accessed: 24-10-2020).
- [14] Y. Wang, Q. Min and S. Han, 'Understanding the effects of trust and risk on individual behavior toward social media platforms: A meta-analysis of the empirical evidence,' *Computers in Human Behavior*, vol. 56, pp. 34–44, 2016, ISSN: 0747-5632. DOI: <https://doi.org/10.1016/j.chb.2015.11.011>. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0747563215302260>.
- [15] SSB. (2019). '11437: Bruk av sosiale medier, etter kjønn og alder(prosent) 2011-2019,' [Online]. Available: <https://www.ssb.no/statbank/table/11437/>. (accessed: 24-10-2020).
- [16] Wearesocial.com. (2020). 'Digital in 2020,' [Online]. Available: <https://wearesocial.com/digital-2020>. (accessed: 24-10-2020).
- [17] H. Paek and T. Hove, 'Risk perceptions and risk characteristics,' 2017. DOI: 10.1093/ACREFORE/9780190228613.013.283.
- [18] P. Slovic and E. Peters, 'Risk perception and affect,' *Current Directions in Psychological Science*, vol. 15, Dec. 2006. DOI: 10.1111/j.1467-8721.2006.00461.x.
- [19] B. Malmedal and H. E. Røislien, 'The norwegian cyber security culture,' Norwegian Center for Information Security (NorSIS), 2016. [Online]. Available: <https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf>, (accessed: 24-10-2020).

- [20] Folkeopplysningen, 'Make lillestrøm great again,' *NRK*, Nov. 2019. [Online]. Available: <https://tv.nrk.no/serie/folkeopplysningen/2019/KMTE50000119>, (accessed: 24-10-2020).
- [21] H. Carslen, 'Folkeopplysningen forsøkte å manipulere skolevalg,' *NRK*, Sep. 2019. [Online]. Available: <https://www.nrk.no/norge/folkeopplysningen-forsokte-a-manipulere-skolevalg-1.14686244>, (accessed: 24-10-2020).
- [22] J. Pettersen and Ø. D. Johansen, 'Nrk må svare for kritikken mot "folkeopplysningen" - elvene får ikke si noe,' *VG*, Sep. 2019. [Online]. Available: <https://www.vg.no/rampelys/tv/i/b5WXVl/nrk-maa-svare-for-kritikken-mot-folkeopplysningen-elevene-faar-ikke-si-noe>, (accessed: 24-10-2020).
- [23] Datatilsynet, 'Digital targeting of political messages in norway,' Datatilsynet, 2019. [Online]. Available: <https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/digital-targeting-of-political-messages-in-norway/>, (accessed: 24-10-2020).
- [24] Norwegian Defense Research Establishment (FFI), 'Slik skal ffi forske på påvirkningsoperasjoner,' *Norwegian Defense Research Establishment (FFI)*, 2020. [Online]. Available: <https://www.ffi.no/aktuelt/nyheter/slik-skal-ffi-forske-pa-pavirkningsoperasjoner>, (accessed: 24-10-2020).
- [25] A. Bergh, 'Social network centric warfare - understanding influence operations in social media,' Norwegian Defense Research Establishment (FFI), 2019. [Online]. Available: <https://www.ffi.no/en/publications-archive/social-network-centric-warfare-understanding-influence-operations-in-social-media>, (accessed: 24-10-2020).
- [26] E. Zhuravskaya, M. Petrova and R. Enikolopov, 'Political effects of the internet and social media,' *Annual Review of Economics*, vol. 12, no. 1, pp. 415–438, 2020. DOI: 10.1146/annurev-economics-081919-050239. eprint: <https://doi.org/10.1146/annurev-economics-081919-050239>. [Online]. Available: <https://doi.org/10.1146/annurev-economics-081919-050239>.
- [27] N. E. Mathé and E. Elstad, 'Elevers vurdering av politikeres bruk av sosiale medier i et postfakta-samfunn og implikasjoner for samfunnsfaget,' *Nordidactica*, vol. 2017, pp. 71–96, Aug. 2017.
- [28] G. Warner-Søderholm, A. Bertsch, E. Sawe, D. Lee, T. Wolfe, J. Meyer, J. Engel and U. N. Fatilua, 'Who trusts social media?' *Computers in Human Behavior*, vol. 81, pp. 303–315, 2018, ISSN: 0747-5632. DOI: <https://doi.org/10.1016/j.chb.2017.12.026>. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0747563217307021>.
- [29] Tinius, 'Oppdatert digitalt - informasjonsvaner blant generasjon z,' Tinius, 2020. [Online]. Available: <https://tinius.com/2020/09/04/ny-rapport-om-gen-z-oppdatert-digitalt/>, (accessed: 24-10-2020).

- [30] A. Veberg and M. T. Pettrém, 'Fersk rapport: Unge i norge og sverige stoler mer på mediene enn unge i resten av verden,' *Aftenposten*, Sep. 2020. [Online]. Available: <https://www.aftenposten.no/kultur/i/P9W87J/fersk-rapport-unge-i-norge-og-sverige-stoler-mer-paa-mediene-enn-unge>, (accessed: 24-10-2020).
- [31] Medietilsynet, 'Åtte av ti har tillit til norske medier,' Medietilsynet, 2019. [Online]. Available: <https://www.medietilsynet.no/om/aktuelt-2019/atte-av-ti-har-tillit-til-norske-medier/>, (accessed: 20-03-2021).
- [32] P Slovic, B. Fischhoff and S. Lichtenstein, 'Facts and fears: Understanding perceived risk,' *Policy and Practice in Health and Safety*, vol. 39, Jan. 2005. DOI: 10.1007/978-1-4899-0445-4_9.
- [33] N. Rahim, S. Hamid, M. L. Mat Kiah, S. Shamshirband and S. Furnell, 'A systematic review of approaches to assessing cybersecurity awareness,' *Kybernetes*, May 2015. DOI: 10.1108/K-12-2014-0283.
- [34] V. Gkioulos, G. B. Wangen, S. Katsikas, G. Kavallieratos and P. Kotzanikolaou, 'Security awareness of the digital natives,' *Information (Switzerland)*, vol. 8, Apr. 2017. DOI: 10.3390/info8020042.
- [35] B. Malmedal and H. E. Røislien, 'Nordmenn og digital sikkerhetskultur 2019,' Norwegian Center for Information Security (NorSIS), 2019. [Online]. Available: <https://norsis.no/norsis-publiserer-rapport-om-nordmenn-og-digital-sikkerhetskultur/>, (accessed: 24-10-2020).
- [36] P. D. Leedy and J. E. Ormrod, *Practical Research - Planning and Design*, Eleventh Edition, Global Edition. Pearson Education, 2016.
- [37] S. Döringer, 'The problem-centred expert interview. combining qualitative interviewing approaches for investigating implicit expert knowledge,' *International Journal of Social Research Methodology*, vol. 24, pp. 265–278, 2021. DOI: 10.1080/13645579.2020.1766777.
- [38] NTNU Innsida. (2020). 'Nettskjema,' [Online]. Available: <https://innsida.ntnu.no/wiki/-/wiki/Norsk/Nettskjema>. (accessed: 31-10-2020).
- [39] Reddit.com. (2020). 'Reddit r/norge,' [Online]. Available: <https://www.reddit.com/r/norge/>. (accessed: 31-10-2020).
- [40] Reddit.com. (2020). 'Reddit r/ntnu,' [Online]. Available: <https://www.reddit.com/r/ntnu/>. (accessed: 31-10-2020).
- [41] SSB. (2021). 'Befolkningens sivilstand, kjønn og alder,' [Online]. Available: <https://www.ssb.no/befolkning/statistikker/folkemengde/aar-per-1-januar>. (accessed: 12-04-2021).
- [42] SSB. (2020). '11342: Areal og befolkning i kommuner, fylker og hele landet,' [Online]. Available: <https://www.ssb.no/statbank/table/11342/>. (accessed: 12-04-2021).
- [43] SSB. (2020). 'Befolkningens utdanningsnivå,' [Online]. Available: <https://www.ssb.no/utniv/>. (accessed: 12-04-2021).

- [44] GoogleTrends. (2021). 'Google trends - fake news interest over time,' [Online]. Available: <https://trends.google.com/trends/explore?date=all&q=fake%20news>. (accessed: 24-05-2021).
- [45] Reddit.com. (2021). 'What is r/subredditsimulator?' [Online]. Available: https://www.reddit.com/r/SubredditSimulator/comments/3g9ioz/what_is_rsubredditsimulator/. (accessed: 24-05-2021).
- [46] Nightbot.tv. (2021). 'Nightbot.tv - your stream, simplified,' [Online]. Available: <https://nightbot.tv/>. (accessed: 24-05-2021).
- [47] K. Persen and S. Saabye, 'E-sjefen: -høstens valg kan bli utsatt for påvirkning-soperasjoner,' *TV2*, Feb. 2021. [Online]. Available: <https://www.tv2.no/a/11939825/>, (accessed: 12-04-2021).
- [48] US National Intelligence Council, 'Foreign threats to the 2020 us federal elections,' US National Intelligence Council, 2021. [Online]. Available: https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf?fbclid=IwAR3fUCw_jNfn1ulX77dkkbBcWpgU9t22FNNmwY0IcAqtutX7ZJn1tdSPYPk, (accessed: 12-04-2021).

Appendix A

Questionnaire

This appendix contains screenshots of the entire questionnaire, using the same style and layout as how it was presented to the participants. This also means that the text is in Norwegian, as the questionnaire was never distributed in English.

Forord

Hva handler undersøkelsen om?

"Påvirkningsoperasjoner på sosiale medier". Det vil si, forsøk på å endre meningen din om noe, helst uten at du legger merke til det selv. Du har kanskje hørt om at Russland prøvde å påvirke det amerikanske valget i 2016? En av måtene de gjorde det på, var å bruke falske nyheter og falske identiteter på sosiale medier.

Hvem har laget undersøkelsen, og hvorfor?

Mitt navn er Bjørnar Liberg, og jeg er en masterstudent på NTNU i Gjøvik, hvor jeg studerer informasjonssikkerhet. Jeg skriver en masteroppgave om påvirkningsoperasjoner.

Undersøkelsen er laget for å finne ut av hva Norges godtfolk vet, tror, tenker, og føler om påvirkningsoperasjoner, selv av de som kanskje aldri har hørt om påvirkningsoperasjoner før.

Undersøkelsens oppbygning

Undersøkelsen er anonym, og det er valgfritt å svare på alle spørsmål. Den består av 20 spørsmål med svaralternativ som er antatt å ta ca 10 minutter å svare på til sammen. Den består av fire deler: Først litt demografisk info som alder og fylke, deretter noen spørsmål om hvilke sosiale medier du bruker, og hvordan du bruker dem. I del 3 blir det presentert litt informasjon om påvirkningsoperasjoner, og du blir spurt om din kjennskap til temaet. Til sist får du noen spørsmål om dine tanker og meninger om temaet.

Andre ting som er kjekt å vite

Hvis du ombestemmer deg og finner ut at du ikke vil ta del i undersøkelsen kan du avbryte innsendingen din underveis, og alt du har skrevet opp til det punktet blir slettet. Jeg kan dessverre ikke slette svar etter du har fullført hele undersøkelsen, da jeg ikke vet hvilke svarsett som tilhører hvem. Dersom du har noen spørsmål, eller om du ønsker å få en kopi av masteroppgaven når den er ferdig, kan du sende en mail til bjornfli@stud.ntnu.no. Forøvrig er oppgaven også veiledet av Gaute Wangen (gaute.wangen@ntnu.no) og Vasileios Gkioulos (vasileios.gkioulos@ntnu.no)

Tusen takk for hjelpen!

Demografisk info (1 av 4)

Hvilket kjønn er du?

- Kvinne
- Mann
- Ikke-binær/Ønsker ikke oppgi

Hvor gammel er du?

Under 20 år

20-29 år

30-39 år

40-49 år

50-59 år

60-69 år

Over 70 år

Hva er ditt nåværende bosted?

Agder

Innlandet

Møre og Romsdal

Nordland

Oslo

Rogaland

Troms og Finnmark

Trøndelag

Vestfold og Telemark

Vestland

Viken

Utenfor Norge

Hva er ditt utdanningsnivå?

Grunnskole

Videregående

Høyskole/Universitet

Fagskole

Aktivitet på sosiale medier (2 av 4)

Hvilke sosiale medier bruker du?

Kryss av for alle som gjelder.

Facebook

Twitter

Snapchat

Instagram

TikTok

Youtube

Twitch

Reddit

LinkedIn

Annet

Hvor ofte bruker du sosiale medier?

Aldri

Sjeldnere enn månedlig

Månedlig

Ukentlig

Daglig/ Nesten daglig

Hvor ofte bruker du sosiale medier til å gjøre følgende aktiviteter?

*Med "politisk innhold" menes: Innhold som omhandler politiske partier eller personer, og temaer som ofte blir diskutert i en politisk sammenheng, f. eks. klima, innvandring, eller bompenger.

	Aldri	Sjeldnere enn månedlig	Månedlig	Ukentlig	Daglig/ Nesten daglig
Lese om nyheter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dele nyhetsartikler	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Delta i debatter/diskusjoner i kommentarfelt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lese eller se på poster/innlegg med politisk innhold*	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lage egne, dele, eller kommentere på poster/innlegg med politisk innhold*	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Kjennskap til påvirkningsoperasjoner (3 av 4)

Denne delen har litt informasjon om tre forskjellige taktikker/temaer som er veldig mye brukt i påvirkningsoperasjoner: Falske nyheter, Falske identiteter, og Falsk popularitet. Først vil hvert tema bli forklart, deretter får du noen spørsmål om din kjennskap til hvert av temaene. Det kan hende du allerede kjenner godt til disse temaene, og det kan hende at du aldri har hørt om dem før.

Falske nyheter

En falsk nyhet er en nyhetssak som med vilje inkluderer informasjon som ikke er sann, med et mål om å villedde mennesker til å endre meningen deres om et tema.

Falske identiteter

En falsk identitet er en konto, bruker eller gruppe på sosiale medier som utgir seg for å være noe eller noen de ikke er. Falske identiteter blir ofte brukt til å etterligne nyhetskanaler, eksperter på et tema, eller "den vanlige mannen i gata".

Falsk popularitet

Falsk popularitet på sosiale medier betyr at man får noe (eller noen) til å se mer populær ut enn hva det egentlig er, for eksempel ved å forfalske antall "likes" på en post eller antall venner til en bruker. En vanlig måte å gjøre dette på er å bruke mange automatiserte kontoer ("Bots") til å like og kommentere på et innlegg. Dette gjør at innlegget blir spredt til flere mennesker, og de som ser innlegget kan få inntrykket av at innholdet er viktigere enn hva det egentlig er.

Hvor ofte hører du noe om disse temaene?

For eksempel fra samtaler med andre, fra nyheter, eller gjennom bruk av sosiale medier.

	Aldri	Sjeldnere enn månedlig	Månedlig	Ukentlig	Daglig/ Nesten daglig
Falske nyheter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falske identiteter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falsk popularitet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Hvor ofte kommer du over noe på sosiale medier som får deg til å tro at det

	Aldri	Sjeldnere enn månedlig	Månedlig	Ukentlig	Daglig/ Nesten daglig
Inneholder falske nyheter?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Er postet av falske identiteter?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Har forfalsket mengden med likes, delinger, eller kommentarer?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Hvor god kjennskap føler du at du har til disse temaene?

	Ikke i det hele tatt kjent	Litt kjent	Middels kjent	Godt kjent	Veldig godt kjent
Falske nyheter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falske identiteter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falsk popularitet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Påvirkningsoperasjoner

En påvirkningsoperasjon er et koordinert forsøk på å få en gruppe mennesker til å endre meningen sin om et bestemt tema, uten at de innser at de blir aktivt påvirket.

Påvirkningsoperasjoner bruker sosiale medier til å lage falske identiteter, som poster falske nyheter, som blir spredt ved bruk av falsk popularitet.

Som et eksempel, så er det blant annet bevist at Russland har brukt påvirkningsoperasjoner for å prøve å påvirke det amerikanske valget i 2016.

Hvor ofte hører du noe om temaet påvirkningsoperasjoner?

For eksempel fra samtaler med andre, fra nyheter, eller gjennom bruk av sosiale medier.

- Aldri
- Sjeldnere enn månedlig
- Månedlig
- Ukentlig
- Daglig/ Nesten daglig

Hvor god kjennskap føler du at du har til temaet påvirkningsoperasjoner?

- Ikke i det hele tatt kjent
- Litt kjent
- Middels kjent
- Godt kjent
- Veldig godt kjent

Følelser og tanker om påvirkningsoperasjoner (4 av 4)

Spesifikt med tanke på påvirkningsoperasjoner, hvor mye risiko føler du at du utsetter deg for ved å gjøre følgende aktiviteter?

*Med "politisk innhold" menes: Innhold som omhandler politiske partier eller personer, og temaer som ofte blir diskutert i en politisk sammenheng, f. eks. klima, innvandring, eller bompenger.

	Ingen risiko	Lav risiko	Medium risiko	Høy risiko
Lese om nyheter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dele nyhetsartikler	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Delta i debatter/diskusjoner i kommentarfelt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lese eller se på poster/innlegg med politisk innhold*	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lage egne, dele, eller kommentere på poster/innlegg med politisk innhold*	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Hvor sannsynlig tror du det er at en utenlandsk stat har brukt følgende taktikker på sosiale medier for å påvirke et valg i Norge?

For eksempel Russland, Kina, Nord-Korea, Irak, USA

	Meget Usannsynlig	Usannsynlig	Sannsynlig	Meget Sannsynlig
Falske nyheter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falske identiteter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falsk popularitet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Hvor sannsynlig tror du det er at noen innenfor Norge har brukt følgende tak- tikker på sosiale medier for å påvirke et valg i Norge?

For eksempel en norsk politiker eller en norsk bedrift

	Meget Usannsynlig	Usannsynlig	Sannsynlig	Meget Sannsynlig
Falske nyheter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falske identiteter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Falsk popularitet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Hvor utbredt tror du bruken av påvirkningsoperasjoner er?

	Veldig lite brukt	Lite brukt	Mye brukt	Veldig mye brukt
i Norge	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
i resten av verden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Se for deg et politisk valg i Norge, og at en utenlandsk stat prøver å påvirke valget med en på-
virkningsoperasjon. Operasjonen har tre mål:

1. De ønsker at en spesifikk kandidat skal vinne valget.
2. De ønsker at over 10% av befolkningen skal tro at kandidatens motstandere har jukset i valget.
3. De ønsker at over halvparten av befolkningen velger å ikke stemme, enten på grunn av likegyldighet, forvirrelse, eller utmattelse. (Valgdeltakelse til vanlig er rundt 65%)

De tre neste spørsmålene er knyttet til dette scenariet:

Hvor sannsynlig tror du det er at påvirkningsoperasjonen kan oppnå hvert av de forskjellige målene?

	Meget Usannsynlig	Usannsynlig	Sannsynlig	Meget Sannsynlig
Spesifikk kandidat vinner valget	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Over 10% av befolkningen tror at kandidatens motstandere jukset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Over halvparten av befolkningen velger å ikke stemme	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>


Hvor sannsynlig tror du det er at påvirkningsoperasjonen holder seg uoppdaget?

- Meget Usannsynlig
- Usannsynlig
- Sannsynlig
- Meget Sannsynlig

Hvor stor del av befolkningen tror du påvirkningsoperasjonen klarer å nå ut til?

Det vil si, både påvirket og ikke påvirket. Hvor mange som har sett/lest noe påvirkningsoperasjonen har sendt ut.

0% 50% 100%



Verdi

Hvor sannsynlig tror du det er at en påvirkningsoperasjon

	Meget usannsynlig	Usannsynlig	Sannsynlig	Meget sannsynlig
Har klart å påvirke deg?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kommer til å påvirke deg i fremtiden?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Tusen takk!

Har du noen kommentarer eller tilbakemeldinger til spørreundersøkelsen?

