University of Gothenburg
Department of Journalism, Media and Communication
MSc in Political Communication

Information Operations & The Rising Threat in the Cyber Domain

Case Study of Finnish Governments Addressing the Cyber Threat Environment and Policies Countering Information Operations

Tuuli Marjaana Järvinen
Thesis: Master Thesis, 30 ECTS
Course: MK2502
Level: Advanced
Term/Year: Spring 2021
Supervisor: Nicklas Håkansson
Course Administrator: Orla Vigsö

Abstract

Thesis: Master thesis, 30 ECTS

Course: MK2502

Level: Advanced

Term/Year: Spring 2021

Supervisor: Nicklas Håkansson

Course administrator: Orla Vigsö

Number of pages: 63 excl. references and appendix. 85 in total

Number of words: 29 096 excl. references, appendix and abstract. 32 487 in total

Keywords:
Information operations, information warfare, cyber environment, Finland, security environment, extended security, policy analysis, hybrid influence

This research was inspired by two courageous Finnish women, journalist Jessikka Aro and PhD Saara Jantunen, who shined a light on Russian hostile behaviour on the Internet and started discussions about *information operations* nationally and internationally all over the world. Due to personally becoming a target of aggressive information campaigns, Jessikka Aro had to move abroad from her home as the Finnish Security and Intelligence Service suggested there is nothing to be done to counter the attacks or safeguard her from getting harassed online and "offline".

The following paper will take a closer look on Finland and its governmental work towards making the cyber domain securer and safeguarding Finnish society from the potential threat looming in the Internet and social media platforms. Information operations in the cyber domain are gaining saliency in the national security conversations. The governments and other actors in the civil society are rushing to find policies which would mitigate the harm information operations are causing in elections, healthy public debates and widely in the democracy as we know it. Finland is known for its technologically savvy industries and the society is highly dependent on technological solutions in all aspects of the nation to work efficiently. The Finnish society, including the political leaders, are broadly integrated in social media and therefore potential subjects of information operations.

The thesis argues, that the obstructions in the cyber domain and information operations have caused security environment to expand from the traditional considerations of the securitisation of military and the state. Rather, the cyber security has expanded similarly like other global issues in multiple fronts: climate change, migration, polarisation and trade. Cyber space offers a domain for the whole global world, where there are basically no boundaries, no governments, no norms of behaviour and in addition, no need for exposing users own identity. The case study of Finland will analyse six governmental texts from the Ministry of the Interior and Ministry for Foreign Affairs from the time period of 2012 and 2020. The years chosen are argued to reflect a change in the Finnish threat environment and policies which have potentially stemmed from the Crimean annexation in 2014. In 2014, Finland and other European countries saw how different hybrid tactics, including information operations, can lead to military conflict which still to this day in 2021, is present in Eastern Ukraine.

The thesis is exploratory in its nature, due to the lack of previous studies which explore the Finnish security environment and policies regarding information operations. The results are argued to reflect and predict a wider change in the international considerations of the threats in the cyber environment and a bigger wave of policies which are meant to tackle and counter information operations globally. Finland has been considered as a front runner in technology as well as in cyber security matters, which indicates that Finland could be one of the countries driving the change and demand more governing in the cyber environment. Finland poses an interesting case to study, since it might be one of the countries initiating broader scales of international norms in cyber space and policies for the future regarding cyber environment, ICT, artificial intelligence, data security and beyond.

Politics in the information age "may ultimately be about whose story wins."

Arquilla and Ronfeldt, 1999

Table of Content

1. Introduction

The cyber environment has become increasingly salient in the global and national security conversations and especially, how civilians are subjected to different information operations in the cyber environment. The traditional domains of war such as air, sea and ground are now accompanied by the global, ungoverned cyber domain, which has the potential to reach more people than ever before and cause potential harm from an unknown origin or an anonymous hostile actor. The operational environment online is characterised being "*without gravity*" (Shallcross, 2017:3) and not bound by the physical world. Previously, the threat could be measured in terms of military strength, territorial advantage or means to develop and security could be guaranteed partially by physical distance from the enemy. In the new operating environment of the Internet and social media, distance is irrelevant and the cyber environment can be weaponised by hostile actors cheaply and effectively, therefore democratising the weapons of war - iPhones, laptops and technology available to almost everyone in some capacity. Therefore, nations have become increasingly aware of the threats and security concerns that are happening and will become even more concerning in the near future. Critical events, such as the Crimean annexation in 2014, the United States elections in 2016 and the European Parliamentary Elections in 2019 have showed signs of information warfare and/or operations which caused a rapid interests in the nations' security authorities and demand for policies to safeguard governmental decision-making, election integrity, healthy public debate, individuals data and *democracy as we know it*.

In Finland, information- and influence operations have gained saliency in the governmental and public discourse ever since the Ukrainian crisis took place in 2014. Finland is not new to the operations which often are linked to its neighbour to the East. Ever since Finland's independence in 1917 and the war with Russia, Finland has experienced propaganda campaigns and information operations coming from Russia. For example, Russia has openly questioned legality of the Finnish independence and actions of historical figures (Rosendahl and Forsell, 2016). Russia media has also produced disinformation campaigns and widely spreading false narrative of Finnish authorities taking custody of children from a Russian family due to their nationality. The Russian media painted the Finnish authorities as cold-blooded, ruthless and Russophobic (Ibid). There are several other incidents in the recent past, which have caused an alarm in the Finnish authorities and there is a rush to find solutions to tackle the challenges of information operations coming from different external actors and also from domestic actors.

Securing the global operating environments, especially the cyber domain, is becoming increasingly complex. The great power competition, global polarisation and dependency in technology are creating new threats. Especially the threats related to technology dependencies are in interest due to the broadness of effects they might have in the individuals, communities and the whole of society (DDV, 2020). Different tactics included in hybrid influencing such as trolls, hackers and information influencing

are becoming harder to counter and hostile actors are developing more efficient ways of using technology for broad attacks and operations (Ibid). The Finnish Digital and Population Data Service Agency (DDV, 2020:6-7) stated in their report that they *do not* believe the Finns are knowledgable and understanding enough of digitalisation or the threats that might rise from the new operating environment. Therefore, new policies and updated knowledge are essential in order to increase citizen's understanding and knowledge about information operations in the Internet and social media.

Over the years, the issue of information- and influence operations have moved from being a threat for the militaries and governments to rather being a broader issue for the civilians, communities and the general public, who are often the by-standers in the national security conversations. The older national security considerations address the threats towards territorial sovereignty, military strength, political elites and the state. The new, global operating environment in the cyber domain has demanded the discussion move from the narrow to broader considerations, further from just the state and military. The extended considerations address multiple global issues such as climate change, human rights or migration as well as the cyber attacks and information operations. The threats in the cyber domain are not just national or regional. The whole global world is using the Internet and social media platforms, communicating without borders, however, there are no governing bodies handling the spread of disinformation, trolling, bots or hate speech. Some progress is seen from governments joining together to tackle the challenge and some companies making changes in their platforms. However, the cyber operating environment is highly ungoverned, acting mostly on commercial incentives and issues such as freedom of speech are debated internationally without consensus on what can be done. The increasing amount of detected information operations have gained saliency in the Finnish discussion and more actors from different parts of the society are joining in to tackle the challenges.

The paper will look at the Finnish governmental response to information operations from the governmental outlook and how the Finnish threat environment and policies have shifted from a narrower to a broader considerations since the Crimean annexation in 2014. The hypothesis is that, as like the international conversation and suggested policies for information operations, the Finnish government's policies have shifted targeting the military and political actors to now increasingly targeting civilians. The research will look at governmental policy reports from before the Ukrainian crisis, right after the events of 2014 and the current standing positions in 2020. The time period of 2012 and 2020 exceeds three different governments and gives an outlook of the progression of the Finnish national security understanding of the cyber related issues and policies that are planned or already set in place for countering information operations.

1.1 Study Aim and Research Questions

The study will focus on the Finnish governments addressing the threat environment related to information operations and what policies have been planned between 2012 and 2020 to tackle them. The study is led by a main question and followed by two specifying questions. RQ2 aims to understand different perspectives of the governments addressing the overall threat environment by Daase's Extended Security Dimension (2010) framework and RQ3 analyses the policies which are set in place or in development for the dimensions of political elite and civilians. The first question gives an outlook of the study as a whole:

RQ1: How has the Finnish threat environment and policies regarding information operations and cyber security developed between 2012 and 2020?

The main research question covers the whole purpose of the thesis and the initial hypothesis that the Finnish threat environment and policies aiming to tackle information operations have developed between 2012 and 2020. There are several different aspects to understand and to study information operations, which will be addressed in the first parts of elaborating on the contexts of information operations: who are involved, where do the operations take place and what are the commonly known tactics. The study will also elaborate the information operations in the Finnish context, what is happening currently and why did the crisis in Ukraine affect Finland. After the background information and developed understanding, the study will tackle on what are the relevant aspects of studying governments addressing information operations and where can we see the changes. Therefore, two further questions are set:

RQ2: Has the Finnish national security moved from the narrow security considerations of the state and military dimension to a broader considerations of individuals and humanitarian dimensions in terms of information operations and cyber security?

The second research question will expand the understanding whether the Finnish national security has evolved from the narrow to a broader outlook. The question will be answered with a framework from Daase (2010) by analysing the Dimensions of Extended Security. The different government reports between 2012 and 2020 are analysed through the framework dimensions and answering to a hypothesis that the threat environment and needs for safeguarding have expanded towards global instead of national environment, humanitarian instead of military and so forth.

RQ3: What specific policies have the Finnish government laid out to the civilian and political elite dimensions?

The second sub-question is aimed to solve whether the Finnish governments' policies have moved focus targeting the military and political elite towards targeting civilians, civil society and the private sector. The dimensions of the political elite, military and civilians are modelled after Daase's (2010) referent object dimension. The government

reports are analysed through the dimensions and policy proposals categorised accordingly.

The following study will aim to expand knowledge of information operations and the threat posed due to the rapid technological development, ungoverned cyber domain, societies dependency on the information and communications technology (ICT) and the challenges finding effective countermeasures against information operations. The study will start with defining information operations, contrasting it to connected concepts and how different actors internationally are addressing the threat of information operations. Then study will move on to the Finnish case and due to the lack of former research on the Finnish case, the thesis is exploratory in its nature. Lastly, the conclusion and discussion will talk about the results found, the future of the field and how the Finnish case could also reflect a larger trend of policy-making in securing the cyber domain and further countermeasures to improve national and global security.

2. Information Operations - Public Diplomacy, Propaganda or Something Else?

"Call it public diplomacy, call it public affairs, psychological warfare, if you really want to be blunt, propaganda"

Holbrooks, 2001

Information operations are discussed in several different terms depending on the context and who is discussing them. Information operations are linked to its doctrinal predecessor of information warfare (Yin & Taylor, 2008:1), as one of the tools in hybrid warfare and often contrasted with concepts of public diplomacy, propaganda and psychological warfare. Information operations are discussed in terms of the actors conducting them or being on the receiving end of them, actions and tactics, countermeasures and the consequences and effects of the actions. In the research, the West is often seen as the victim of information operations and as the receiver of misinformation, trolling, fake news and so forth. When discussing the harmful effects of the actions, the consequences are described as weakened democracies, distorted public opinion, influenced policy outcomes and silenced individuals. Below, information operations are separated from the information warfare term as well as differentiated from connected terms of propaganda, public diplomacy and hybrid influencing. Afterwards, information operations are elaborated in terms where they are happening primarily and how are they conducted, who are traditionally considered as the receivers and senders and what effects information operations are likely to cause.

2.1 Information Operations or Information Warfare

Information operations are discussed often as information warfare or as part of it. However, many would argue that the terms should be separated since they are used in various different ways depending on the context. Information operations are seen as a broader concept than information warfare (Armistead, 2004:16-21). According to Armistead, information warfare refers to an active conflict, which might involve some military operations. In comparison to information warfare, information operations can be described as a strategic campaigns which expand over time of peace and conflict. In this sense, information warfare can be understood as one stage of information operations or an escalation of information operations. Information operations are or can be also part of hybrid warfare, which can be seen as the smarter way of reaching political goals and wanted outcomes without the use of military or violence (Salonious-Palsternak and Limnéll, 2015). In the Finnish context, the term information operations is used rather than information warfare since it covers more widely the influencing tactics used in normal conditions (Ministry of the Interior, 2019:24). The Ministry of the Interior report also notes that information warfare is conducted in order to support military objectives. In this study, the term information operations will be used due to research only focusing on information operations without the means of military operations or violence.

2.2 Public Diplomacy

The concept of public diplomacy is often brought in to the conversation in comparison to information operations. Similar to the purpose and strategy of information operations, public diplomacy is similar by definition due its objective and its aim: influence opinions and advance own interests and values (Gregory, 2008:274). Public diplomacy was first applied in the mid-60s and defined by "*the process by which international actors seek to accomplish the goals of their foreign policy by engaging with foreign publics*" (Cull, 2008:31). A wider use of public diplomacy was adopted at the end of the Cold War (Ibid). Public diplomacy is often connected to propaganda and scholars such as Nye (2008:101) argues, that treating public diplomacy as substitute for propaganda is missing the point. Cull (2008:32-34) defined the key elements of public diplomacy: listening, advocacy, cultural diplomacy, exchange diplomacy and international broadcasting. The term public diplomacy has spread to the wide popular use nowadays and it is used not only by the nation states, but also by non-governmental individuals and organisations (Murrow, 1963 in Leonard, 2002:101).

Public diplomacy is used for multiple different functions: it centres around enhancing international collaboration, achieving policy goals and stimulating trade relations (Bjola, 2020:1). Public diplomacy is discussed as the Western culture's own initiative of advancing values and the public diplomacy efforts are seen as a dialogue and non-propagandist (Alafuzoff et al., 2020:23). Public diplomacy serves as an tool for nation states and non-state actors to engage, understand and influence foreign and domestic publics about issues they are particularly interested in, whether its economy, governance, trade or supporting democracy (Gregory, 2008:276). Communication does not only serve between nations or governments. The aim of public diplomacy is traditionally seen as government to people contact (Cull, 2008a:15). Nye (2008:103) notes, that effective public diplomacy is a two-way communications of hearing the target audiences and adapt own messages accordingly. Public diplomacy instruments include public relations, cultural diplomacy, national branding, broadcasting and exchange programs (Gilboa, 2008:73).

Arguably public diplomacy has similar functions as information operations: to engage with and influence foreign or domestic publics. However, there are differences that scholars separates them with. Pamment et al. (2018:9) noted that public diplomacy "*constitutes legitimate informational power exerted across borders to influence policy outcomes*". In comparison, they argue that information operations are not only utilising, but also exploiting open systems of opinion formation and turning the greatest assets of free and open debate into vulnerabilities. In these descriptions, Pamment et al. specifically discuss the exploitation of the Western democracies and attacks against the Western system. The terms of public diplomacy and information operations are very similar to the actions taken, but what differs is the aspect of legitimacy as well as the motivations behind the actions. The definitions of the concepts are contested depending on the context they are discussed in. In contrast for example, Russian scholar Illya Yablokov explained that promoting conspiracy theories and other information operations are used as specific tools of Russian public diplomacy, which are aimed to

undermine the US government's policies (Illya Yablokov in Jakubowski, 2019). In the Russian context, influence term is not used in for example defence reports and influence term is replaced by terms such as soft power and public diplomacy (Alafuzoff et al., 2020:11). Gregory's quote captures the essence that is the difficulty of defining public diplomacy depending on variables such as: "*Interests, values, identities, memories and geostrategic contexts shape how we think about public diplomacy*" (Gregory, 2008:276).

2.3 Propaganda

Propaganda is often linked to information operations as well as public diplomacy discussed above. Propaganda research and term definition has its long traditions. One of the major scholars in the field, Lasswell, defined the purpose of propaganda as "*to intensify the attitudes favourable to his purpose, to reverse the attitudes hostile to it, and to attract the indifferent or, at the worst, to prevent them from assuming a hostile bent*" (Lasswell, 1927:629). As Lasswell also predicted, what have been in history achieved by violence and intimidation can be done now by argument and persuasion. Doob and Robinson (1935:1) referenced propaganda as the means to employ appeals in the public dissemination that are non-logical and which would modify the ideas, attitudes and beliefs of the receivers. Propaganda as a term suggests a negative and dishonest messaging and it's purpose is to "*deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behaviour to achieve a response that furthers the desired intent of the propagandist*" (Jowett and O'Donnell, 2012:7). A newer definition by Marlin (2013:12) consider also the act of propaganda being organised attempts of communication that suppresses individual's informed, rational and reflective judgement.

Similar to public diplomacy and information operation concepts, propaganda aims to influence attitudes, ideas and beliefs that are favourable to the sender of the message. The age old tradition of propaganda is connected to the information operations happening in the cyber environment and new technologies are just allowing the old propagandist techniques to enter our own pockets (Erbschloe, 2017). The one big difference between propaganda and information operations might be the changes and development of technology. Propaganda have been distributed by channels which allows one-way communication, but information operations are now conducted via the Internet and social media, where general public - who are the targeted - are interacting with the information by liking, sharing and commenting on such messages which are meant for influencing and aiming to distort the discussion.

2.4 Information Operations

Information used as a means of warfare and national power is an old tactic (Shallcross, 2017:2) and the tactics of using information in warfare have been written already by Sun Tzu in the Art of War. Information used in war became more discussed during and after the Gulf War in 1991, when the lack of information flow in the battlefield and uncertainties were meant to be solved with information technology (Lehto & Limnéll,

2017:187). The Cold War is an example, where war was conducted effectively without the military means and primarily with information used for influence and in psychological operations, both for foreign and domestic audiences (Ahvenainen, 2014:21-24; Rantapelkonen; 2014). The tactics are not new to countries, militaries or organisations, however, the cyber environment, rapid development of technology and our lives merging almost seamlessly with social media, has raised the threat levels of the information spreading in the online platforms. The operations using information have become more common due to the emergence and diversification of information channels such as social media platforms, news media and the speed of communications (Ministry of the Interior, 2019). With one like or sharing of a post, video or a meme, anyone can reach millions of people around the world, which is something that the Internet and social media has allowed - in good and bad. Information operations are defined by the illegitimate attempts of influencing opinion-formation, exploiting open and free-opinion formation (Pamment et al., 2018), systematically stirring the public debate and muddy the boundaries between truth or lie (Ministry of the Interior, 2019) and competing for individual's and groups's attention in order to "*enter into and manipulate their meaning making processes*" (Bergh, 2019:3). Information operations aim to distort public debate, influence policy-making and opinion-formation by mimicking legitimate behaviour online to seem truthful whilst disseminating false information which can be targeted to create divisions for example between different ethnic, linguistic and political groups (Renz and Smith, 2016:57).

The operations can be conducted by several actors that benefit their own mission by gaining influence or creating divisions in the targeted publics. Information operations are used by several actors and operations "*represent an evolution in military affairs*" (Shallcross, 2017:2) where the playing field between bigger and smaller powers is lessened due to the availability, effectiveness and low cost of new technology found in everyone's pocket. Information operations include sets of different tactics, which can be employed in different times or concurrently and so that the wanted goal of the adversary is achieved. The different tactics can include for example electronic warfare by attacking IT and network systems, deception by misleading, manipulating, distorting and falsifying or psychological operations in order to influence perceptions, behaviour of targeted groups or individuals (NATO, 2009). In addition, also often key leaders and their inner relationships are used against them by gaining intel of their personalities, stances, ambitions, history, relationships and psychological profiles (Ibid). The personal information about a leader and their personal relationships can be used against them in order to pressure and influence their decision-making.

2.5 Hybrid Influencing

Hybrid warfare has become more salient and it includes more broadly the different types of attacks with means of information and military (Hoffman, 2007; Lehto, 2014). In the Finnish discussion, hybrid influence, - operations, - attacks and - threats have raised interests, however similar to the term information warfare, hybrid influence includes also other methods of hostile behaviour than information. Hybrid influencing is employed by

a range of different methods and by targeting another party from several angles to unbalance them (Merimaa, 2018). Different methods include attacks in the cyber environment, cover military operations and information warfare during the time between war and peace - in the grey area (Ibid). In order to complicate the countermeasures, hostile actors use the space between war and peace (City of Helsinki, 2018: 5-6). Purpose of hybrid influencing, similar to information operations, is for the hostile actor to remain unidentifiable in their actions and use and maintain existing vulnerabilities in the targeted country, community or individual (Ibid). The methods can happen simultaneously and can be employed with more than one at the time. Influence can be gained through information, finances, politics, cyber as well as the threat of physical intimidation and political violence (Ibid). Hybrid influencing can be broken down to five different activities: 1. *creating or maintaining vulnerabilities* through technical, economic or human means by for example supporting news websites that publish misinformation, 2. *observing* the target by collecting information, 3. *testing* the target's actions, reactions or the consequences, 4. *practising* the range of methods and 5. *diversion phase* during which the methods of hybrid influence are utilised to direct attention away with another activity (City of Helsinki, 2018:9). Hybrid influence therefore is a broader set of methods, including informational, which the hostile actors use in order to influence the targeted country, community or individuals. Hybrid influence is separated from information operations, due to the methods ranging from information operations to physical violence and use of military in different operations.

2.6 Information Operations in the Context of this Research

The term information operations is difficult to crystallise since it connects to, as discussed before, to several terms and areas of cyber warfare, hybrid warfare, hybrid influencing, propaganda and public diplomacy. As seen in the later analysis of the Finnish governmental reports, information operation term is used differently depending on who is discussing it and when. For example the Finnish government discussing security and foreign policy, the term hybrid warfare, - influence, - threat, - attack is often used as an umbrella term which includes also information operations. The Ministry of the Interior refers to information operations more than hybrid operations and separates information operations from information warfare due to the methods used. For this thesis, term information operations will be used due to it's relevance as a broader concept than information warfare (Armistead, 2004:16-21). Information operations covers widely different influence tactics which are employed during normal conditions without the means of military or violence (Salonius-Palsternak and Limnéll, 2015). As mentioned, information warfare can refer to an escalation of an information operation and can be understood as one stage of an information operation (Ministry of the Interior, 2019). The government mentions of hybrid influencing/attacks are connected with information operations due to the similarities in methods (information as one of they key methods) and the policies which are planned to reduce the threat and respond to hostile behaviour.

3. Where, Who and How?

Information operations is a complex term and multiple different angles should be elaborated on how can we understand information operations in practice. Information operations should be separated from propaganda, public diplomacy and information warfare due to their purpose (compared to public diplomacy), channels (compared to propaganda) and for being regarded as hostile without the means of military (compared to information warfare). Therefore, information operations are expanded below in terms of their operating environment, who are seen as participants, what are the aims of operations and how are they conducted in practise.

3.1 Where: Cyber Space

Cyber space has become largely discussed as the new domain of warfare and the threat of operations carried out in the cyber space are increasingly alarming to nation states as the new tactics of information operations are getting smarter and the effects are still to be understood. Cyber space can be characterised as a global domain in the information environment, which consists of "*interdependent networks of information technology, infrastructures, and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*" (DOD, 2021).

The new battleground for information operations, cyber intrusions and hacks in the cyber space, the Internet and social media, are not bound by the physical world (Shallcross, 2017:3) in which security or defence might be provided by geography or military presence. When the attacks happen online, the war is beyond limits because the normal rules of traditional domains of ground, sea, air or outer space do not exist and the rules are much wider (Qiao and Wang, 1999). The internet can be considered as an "*ungoverned state of literally billions of people*" which promotes anonymity and thus gives those who conduct information operations a plausible deniability due to the options of being anonymous (Shallcross, 2017:3). This particular tactic was seen in the Russian attacks during the Crimean annexation in 2014, where information was used as part of the hybrid warfare but due to the various possibilities the cyber space offers, the adversaries could deny involvement in the operations. Due to the several alarming events in the recent years, such as the Crimean annexation, the national security discussion has started to centre around how to secure the cyber domain from the consequences which cyber intrusions have caused (Yannakogeorgos, 2016:10). The cyber intrusions cannot be only discussed in terms of the cyber space, but widely as something that has effects through-out the society as well. When more and more of human lives are moved online to cyber spaces, the adversarial actors have more opportunities to influence, sow social division and create further polarisation among societies (Falk, 2020). Yannakogeorgos (2016:10-11) considers the discussion too focused on the technology and solely as a virtual domain, which is divorced from the real world and argues that discussion should focus on the human elements, not only on the computer codes. Divorcing the cyber space from the real-world makes it difficult to understand it as a natural domain such as air, land or sea where harmful operations can

be conducted. The discussions of issues in the cyber space focus on the abstract domain which makes it hard for the policy discussions. For the policy discussions, it would be necessary to understand that the cyber space is not divorced from the laws of physics, space and time and the people behind the cyber intrusions should be held accountable as well as hold states liable for letting malicious cyber intrusions happen in their territory (Yannakogeorgos, 2016:2). Social media has changed information operations drastically and what was seen in the Ukrainian crisis in 2014 and the elections in the United States in 2016 in terms of social media, Goolsby (2019) analysed that the component of social media used in conflicts has developed in use and entered public consciousness.

3.1.1 Operations in Social Media

Social media has added an another function to the cyber space, by introducing new platforms for people to connect, share and organise themselves differently than before and by changing the way we socialise. Social media is a double-edged sword. It creates a platform for people to connect around the world, gives a voice to those who do not have it without and acts as a tool for social advocacy and organising. Social media has empowered the civil societies (Falk, 2020:4) by promoting ways of organising and responding quickly to causes. Black Lives Matter is an example of the power of social media organising, where protests and gatherings for solidarity took place all over the world in the spring and summer of 2020. However, social media also represents a problematic evolution in military tactics where platforms are used for notorious activities and as a weapon (Shallcross, 2017:2). Social media platforms will arguably be the new key arena for influence operations. Especially younger generations can be targeted due to their habits of getting information and news from social media (Stelter, 2008).

As Qiao and Wang (1999) forecasted more that 20 years ago, media has become vital part of warfare and the trend only seem to increase and tactics are getting smarter as they are discovered. Why then, especially social media, has started new conversations of the cyber space being increasingly threatening to societies at large? Several aspects of social media have made it useful for adversaries: it is cheap and effective (Jakubowski, 2019), it connects to worldwide audiences and helps find people (Pier, 2017), it is increasingly used as a source for news amongst young people (Bergh, 2019), the functions to target specific individuals or groups, use of algorithms and creating trends by sharing and liking (Pamment et al., 2018). Ironically, the functions of social media that adversaries are benefitting from are the business models for most social media platforms and now used against those who are signed into the platforms. Scholars and professionals in the field of national security and cyber issues are agreeing that the platforms should be held accountable and hope that they would take the initiative to do something to prevent the platforms for being used in information operations and cyber attacks (see Aro, 2016; Jakubowski, 2019). Aro (2016:128) argues that platforms such as Facebook and Twitter are key actors in information operations and the key enablers who have the potential to solve issues relating to their platforms. Jakubowski (2019:16) agrees that the private companies could be pressured by public scrutiny to change their operations and stopped enabling hostile actors using platforms for information

operations. A survey was conducted in eleven different EU countries' secret services, which implied that Russia is using social media as one of the key tools for influence activities and it is one of the most important avenues (Karlsen, 2019:1 and 6).

As much as our lives are merged with social media, Falk (2020:3) sees also the importance of noting that the battlespace in social media is increasingly creating the civil society into a battlespace in itself. Civil society should be discussed and rethought as the offline and online civil society (Ibid:6). Much of our lives are happening in the information space, in the Internet and social media, and they should not be separated as independent factors which have no influence on offline lives. Jayamaha and Matisek (2019:1) also supports the argument that civil society has been a blind spot in understanding warfare. The civil society has been weaponised in the new online battlespace consisting of the Internet and social media (Ibid:1). The social media warriors consider the online battlespace as a "*unguarded, under surveilled and ill-defined human-to-human interface*" which can be exploited and used for manipulation (Ibid:1). Social media has posed new difficulties in tackling information warfare, since it offers for example anonymity, algorithms and trending function for exploiters to use. Social media is a powerful tool to weaponise and as a tool for hostile behaviour it is "*neither easily wielded nor contained*" (Shallcross, 2017:1). The problematic developments of operations in social media require new skillsets and tools (Bergh, 2019:3) from those who are planning the counterattacks and policies for information operations and also from the civilians using the platforms. Arguably, we have only began to understand the basics of information operations in social media and how they are conducted, but the actual connections and longer-term effects are yet to be discovered since information operations in social media as a field will be quite uncertain.

3.2 Who: Participants

Information operations involve multiple "participants", who are involved by conducting the operations, are the targets of the operations, are exploited or the enablers in disseminating information or the as side-watchers. In information operations, the parties involved are often formerly regarded as nation states and non-state actors and labelled so that the adversary is automatically a foreign actor. The newer research and articles however also point out that there is a larger pool of actors that can be participating in the conducting information operations, not only nation states and non-state actors who are foreign, but also hostile organisations, proxies, proto-governments and individuals who can be either foreign or domestic (see e.g. Pamment et al, 2018; Shallcross, 2017). The conflict and operations are not only between nation states but also between states and proto-governments, non-state actors and individuals (Shallcross, 2017:3). There is also a very fuzzy line between the nation state and non-state actors conducting information operations and it is not easy to detect who are behind the malicious activities. Hostile actors can use several tactics to hide their identify as well as location by routing the attacks via different countries and jurisdictions (Yannakogeorgos, 2016:13-18) and by using anonymity and fake profiles to camouflage the attacks. Due to several functions in the Internet and social media, it becomes hard to find who are

responsible and the question of whether the states should be responsible has come to the discussion. Yannakogeorgos (2016:2) argues, that the states should be responsible for the attacks that are either originating or being routed through their territory.

Literature on the information operations and information warfare often points out to the same hostile actors. Pamment et al. (2018:21-23) elaborated with the examples such as: violent extremists proto-governments or hostile organisations (ISIS/Daesh), hostile states (Russia, China, Iran), hackers and profiteers (individuals with skills in digital systems) and sub-state criminal actors (drug cartels). Consensus in the research is quite solid, who are seen as the adversaries, especially when talking about specific nation states who are responsible for information operations. For example, Russia is often pointed out as one of the main operators and seen as a hostile nation in conducting information operations globally (see Pier, 2017; Shallcross, 2017; Bergh, 2019; Aro, 2016; Jakubowski, 2019; Jayamaha and Matisek, 2019; Janda, 2018; Renz and Smith, 2016). Most research in the field discusses Russia as one of the key actors, but often also Syria and China are pointed out. Russia has been known for using similar tactics of information operations and propaganda from the beginning of the Cold War (Porotsky, 2019). Russia is the first entity fully include the entire social media ecosystem to its information operations and that the operations have been intentionally planned and used for means of warfare (Jakubowski, 2019). Russian President Putin stated in June of 2013, that Russia would "*break the Anglo-Saxon monopoly on global information streams*" (in Jakubowski, 2019:8) and Defence Minister Sergei Shoigu noted that "*Kremlin sees the mass media as a 'weapon'*" (in Aro, 2016:121). The Russian history of using these tactics has given them advantages in developing the further and they are likely now to dominate in the information and social media battle with the use of hackers, trolls, bot network and their intelligence assets (Pier, 2017:66-68). The Canadian Centre for Cyber Security analysed the cyber threat actors similarly to other research discussed before, in which the motivations for conducting cyber attacks are elaborated as being geopolitical, ideological, satisfaction and also for profit. However, this visualisation, even though it gives some idea of what the motivations behind different cyber attacks might be, gives a simplistic motivations and who are likely to conduct attacks for those motivations. Argument could be done, that nation-states, as well as individual hackers can be motivated in ideological and geopolitical terms.

Figure 1: Cyber threat actors

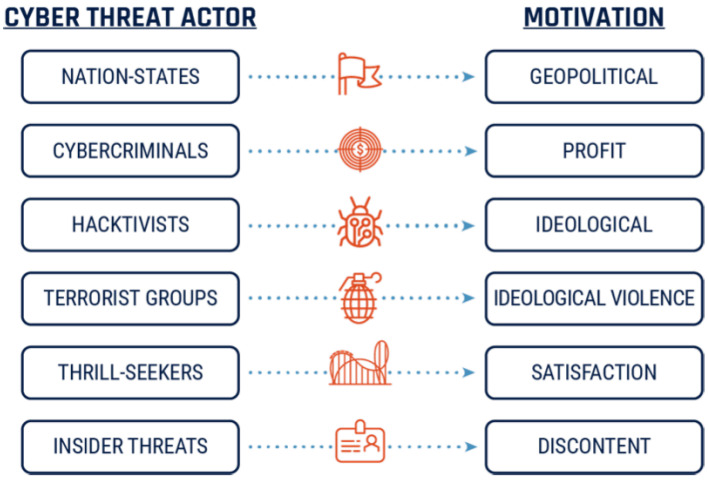

Figure 1: Cyber Threat Actors (Government of Canada, 2020)

Who are seen as the targets and victims then? Similar to the former, the research seems to have a strong consensus who are the targets of information operations. Information

operations are described to be targeted towards the Western countries by exploiting their greatest strengths and making them into vulnerabilities. The adversaries are using and exploiting the Western open systems of opinion formation and robust public debate in their advantage (Pamment et al, 2018). The tactics of using the open public society and debate in information campaigns have been used before. During the Cold War, the communist states were supporting the left-wing political movements in order to shift political attitudes (Jayamaha and Matisek, 2019:13). Now the adversaries are using different channels in order to foment dissent and create polarisation between different ethnic, racial, religious and socioeconomic groups (Ibid). In practise, the adversary can show support on both side of a topic that is already polarising in nature, for example abortion rights or gun laws, and give support on both sides whilst creating further division between the groups of people supporting or against the issue. However, the strategy of fomenting divisions in the public is not successful uniformly. Countries that are more heterogenous, where more cultural, religious and historical cleavages exist, the more easy it is to sow divisions between those cleavages (Jayamaha and Matisek, 2019:23). Information operations in countries with more homogenous publics are likely to have less impact. For example, in Iceland the societal differences stem mostly from economic differences, but for example in the United States, there are more opportunities to create divisions between groups belonging to different religions, races and cultures (Ibid:14). In the research, examples are often given which indicate that West is the likely victim and several information operations have been conducted for example during the Crimean annexation in 2014, European Parliament Elections in 2019, the United States elections in 2016. These specific cases are always brought up as examples of the recent severe information- and cyber attacks towards the West.

Another important participant in information operations is the tools and platforms in which the operations are conducted. Unlike the discussion and consensus about the adversaries and victims, the tools and the actual battlefield is quite debated. Social media has changed the ways in which we communicate, organise and consume information. Different platforms such as Facebook, Twitter and Instagram are used for good purposes such as trade promotion and managing crises (Bjola, 2019:1) but they have also been used as a weapon by hostile states, non-state actors and individuals wanting to sow division, meddle in elections or employ fighters for terrorist organisations (Pamment et al, 2018). The governments are facing challenges in governing social media platforms which are becoming increasingly powerful (Falk, 2020). Platforms are designed to create communities by algorithms and making echo-chambers of people who are like-minded and therefore the individuals within the groups are seeing decreasing number of opposing viewpoints and information from different aspects. Social media platforms are however not the only creators of the echo-chambers, but we are also active in building our own filters due to the hard-wired tendencies of wanting to "*interpret the world around us consistent with already-held beliefs*" (Ibid:4). Social media has been seen as a democratising tool across the globe, where more causes are gaining attention and civil movements like the Arab Spring in 2011 resulted in regime changes. The most divisive debate is revolving around the aspect of responsibility and responses from the social media platforms. The information

operation strategies rely on the Internet and social media platforms and the functions such as anonymity, algorithms, adds, fake profiles, bots and trending lists. The platforms are cost-effective channels that external hostile actors can use in delivering messages with a purpose of sowing division and steer conversations to both undermine specific government or individuals in order to support their own ambitions (Falk, 2020:5). Some scholars have argued that the responsibility should not be on the platforms to respond to information operations (Prier, 2017) and some argue that social media platforms are the key enablers in disseminating messages and allowing influence activities material in their platforms (Aro, 2016). Prier argued that social media companies, such as Facebook and Twitter, are balancing their interests in business and "*betterment of society*" (Prier, 2017:80) and that other institutions should respond to the malicious attacks in social media. Also, Prier (2017:80) noted that by removing functions such as the trending lists, Twitter would devaluate its own usability and it would have an adverse impact from firms that rely on the revenue streams coming from Twitter advertising.

According to Aro (2018:128), the social media platforms are the key enablers for information operations, thus the potential solvers of the issue. By providing a platform for malicious use, Facebook and Twitter should be responsible of what is circulating across the newsfeeds and groups. Aro notes that the platforms are highly connected to information operations since the platforms are also gaining revenue from practises which disseminate disinformation by selling ads on Facebook and pollute Twitter conversation with messages from fake identities. An individual user is helpless when information campaigns are orchestrated in the platforms and thus making the social media platforms responsible for "*cleaning up*" their services from fake profiles and disinformation (Aro, 2016:129). "*Just like any polluting companies or factories should be and are regulated for polluting the air and the forests, the waters, these companies are polluting the minds of people. So they also have to pay for it and take responsibility of it*" (Aro, in CNN, 2019).

3.3 How: Strategies of Information Operations

Information operations term, as discussed before, is connected to multiple different umbrella terms such as hybrid operations, influence activities and information warfare. Information operations itself is also an umbrella for multitude of different operations that academia and security officials have tried to identify and describe how they are conducted in real-life situations in the cyber battlefield. The information environment is "*ripe for misuse*" (Pamment et al., 2018a:4) with offering several possibilities for hostile behaviour conducting information operations online. Watts analysed that information operations in online platforms would become "*the most effective and efficient influence campaign in world history*" (Watts, 2014 in Jakubowski, 2019:8). Especially social media creates a perfect storm for disseminating propaganda when putting together aspects of fake news, conspiracy theories, politics, sensationalism and human nature (Jakubowski, 2019:9). Hostile activities can be series of individual, coordinated operations aimed at achieving "*death by a thousand cuts*" or gaining longer-term influence through

combination of information influence and hybrid activities in a campaign form (Pamment et al, 2018a:6).

Information operations can be employed strategically to different audiences depending on their end-goal. The operation level can be targeted towards general societal level, sociodemographic targets or psychographic targeting (Pamment et al., 2018:9). The general societal level aims to influence and employ operations to mass audiences by different means. Sociodemographic level aims to influence selected groups for example on different sides of political, racial, religious or ideological spectrums. Psychographic targeting aims to use information on individuals to influence their beliefs or behaviour. Psychographic targeting tactic was used for example by Cambridge Analytica where they scraped data from individuals and analysed the data in order to use them for micro-targeted advertisements on Facebook with an end-goal of influencing their voting in elections (Jakubowski, 2019:9).

Figure 2: Levels of Information Operations by Pamment et al (2018)

As discussed before, the success of operations depend on several aspects. A country, where dividing lines between groups and different topics exist, the better it is for the adversary to use those dividing lines for influence. A country which is more homogenous and large fractions between groups do not exist, the harder it is for the adversary is to create and escalate such divisions. Information campaigns are also targeted not only towards the general public, but also politicians, journalists and other public figures (Aro, 2016).

There are several different types of information operations and since the adversaries are always developing and getting more discreet and smart, the work continues to expose strategies employed online and in social media. The operations are conducted in different times, during peace, war or hybrid threat and also on grey-zone situations where the two parties are neither in war nor peace (Pamment et al., 2018a). The typical framework for information operation strategies consists of the following functions (Jakubowski, 2019:9):

- Reconnaissance - Knowing the target audience
- Hosting - Platforms, for example Facebook, Instagram or blogs
- Placement - Placing false items in news outlets that publish them as authentic
- Propagation - Quick spread of wanted narratives

- Saturation - Disseminating information to multiple types of social media platforms, which gives credibility to the false information based on likes, shares and comments

Saturation function is typical for information operations and what the general public is most commonly used for. Information operations benefit from the social media functions by influencing trends and algorithms creating news feeds for individuals. In return, the humans are psychologically wired to believe and further spread the news that are liked and shared by their connections in social media. Beneficially for adversaries wanting to exploit individuals or groups for their operations, the false news stories are spread further and faster than legitimate news. In Twitter, true tweets were studied to reach around with 1000 people, whereas false tweets could usually reach up to 100,000 people (Vosoughi, Roy and Aral, 2018). False information was seen spreading six times faster than legitimate information and information regarding politics spread even faster and became viral (Ibid). Disseminating false information does not rely only on the trolls behind the operations, but the general public and public figures who are spreading the false news in the Internet (Jakubowski, 2019) and giving it more legitimacy in the process. Below, few typical information operations are explained broadly in order to understand the overall picture of such strategies:

3.3.1 Sociocognitive and Psychographic Strategies

The overall aim with sociocognitive and psychographic strategies is to penetrate in to the heads of people in order to create outrage and emotional responses with for example dark ads (Pamment et al.,2018a:10). Dark ads are non-public posts that are only targeted for the specific groups and individuals. For example, dark ads and dark posts were used in the Trump 2016 presidential campaign to depress the Democratic voters, especially the African American voters (Green and Issenberg, 2016).

3.3.2 (Para) Social Hacking and Selective Exposure

Social hacking aims to falsify the public opinion and create trends and saliency for topics that would not be as salient without (Pamment et al., 2018a:10). The public opinion support is gained by likes and shares with a "*bandwagon effect*" where illegitimate news or information gains legitimacy based on the how much it is shared and liked in individuals social media feed (Ibid). The bandwagon effect is created with filter bubbles and echo chambers on social media, where the reality of the world is constructed by algorithms, which usually lack countering information. Algorithms trap social media users in bubbles of their own making and they contribute to alarming effects on a larger scale such as political fragmentation of opinion online due to the personalised newsfeeds (Pariser, 2011). Para-social hacking is created by making one-sided relationships seem two-sided, and social media platforms allow these relations with strangers online. For example, the Digital Caliphate successfully used para-social hacking in their strategy of engaging worldwide online and recruit more fighters to their mission. (Pamment et al, 2018:40).

3.3.3 Disinformation and Fake News

The purpose of disseminating disinformation and fake news are to deliberatively deceive and mislead the audience (Pamment et al, 2018a:11). The campaigns include major disruptive activities to minor falsifications of information. In minor activities, the content is created by being selective with facts, taking facts out of context, advertising, manipulation or satire (Ibid). More disruptive activities can be content manipulation, deep-fakes, trolling and creating fakes sites and platforms which require also more tools and skills than the minor disinformation activities (Ibid). The subtle disinformation is difficult to counter and track to the original sender. The subtle messages are not understood as products of hostile actors and therefore people might be affected by them cognitively and psychologically (Aro, 2016:126). Disinformation is a cheap tactic to employ through social media, compared to for example radio and television, since the reach is far greater online and can be multiplied and spread globally in minutes (Illarionov, 2014)

3.3.4 Trolling

Trolling is an act of purposively disrupt and provoke the public conversation and users' news feeds on social media platforms. The aim of trolling is to polarise discussions, silence people and opinions and distract from other topics that are important (Pamment et al., 2018a:11). For example, Russia has employed "*troll farms*" (Internet Research Agency in St. Petersburg) where people are hired to produce content that is divisive and insert themselves into debates in order to polarise them further. The trolls are focused on inserting themselves into already heated debates Such debates in the US could be for example about gun control, abortions or immigration. The purpose is to pit the citizens against each other and sow distrust by supporting both viewpoints by highly divisive messages (Barsotti, 2018). Trolling is also used for example by China with its so-called "*50 cent party*" troll army (Pamment et al., 2018:64). The purpose is slightly different than Russian trolling, where the Chinese trolls are using 'cheerleading' in order to dominate the information flow of positive messages of China and crow out the dissenting opinions (Ibid). This can be used as a tactic domestically and abroad to support and create a narratives, that the message sender is aiming towards in the information campaign. Trolls are used also in making their own "*investigations*" to target specific individuals and harass them, as of the Finnish journalist Jessikka Aro experienced. The investigations are conducted by trolls going through the individuals public profiles on social media and other information found. For example in Aro's case, she received direct threats, phone calls and trolls claiming her father to be dead and that someone is following her (Aro, 2015:123). The attacks are modified with false personal information with an aim to silence individuals with threats and delegitimise their journalistic work, which happened to Aro, when she exposed Russian troll farms in the Finnish and international media.

3.3.5 Humour and Memes

Humour and memes are also a common tactic where they are used to attract attention in social media and gain followers for social media profiles (Pamment et al., 2018a:11). The messages disseminated through memes and humour can legitimise edgy and controversial ideas by spreading content that is highly accessible, shareable and "infectious" when individuals share them further (Ibid). Humour and memes are quick messages and material, that might contain sensitive issues wrapped in funny pictures and witty texts. Such content tends to spread fast and wide in social media compared to longer texts that require time and focus from readers.

There are several other tactics that are discovered to be part of information operations, but the above are the common noted in multiple articles and studies. However, there are arguably several other that are smart and subtle enough to have gone unnoticed. Countering information operation campaigns is a double-edged sword. When the information campaigns are not detected and left unchallenged, the influence is gained; when the campaigns are revealed and published, publics trust in media and confidence in institutions might be further undermined (Pamment et al., 2018:11). When information operations are exposed and several news items are labelled as fake news, it creates a crying wolf effect, which will erode credibility and polarise audiences on both sides, whether they believe or not in the issue at hand (Ibid:5-11). The situation is therefore great for the adversary: when the receivers of the messages are fighting over who is right and wrong, audiences are further angered and polarised it benefits the purposes of the information campaigns of hostile actors (Ibid). Another issue are the effects of information operations and how the operations have effect at large either in institutions, nation states, civilians or communities. The effects are still very unresearched and often researched only after an event has occurred where information operations have been seen to have an effect for example in election turnouts or what happened during the Crimean annexation in 2014.

3.4 Effects of Information Operations

Research on information operations in cyber spaces and in social media are still quite novel. Arguably, only a small fraction of the operations and tactics have been discovered and traced back to the original senders. What might be even more unknown, is what the actual effects of information operations might be and there is little exploration done on the information campaign effects (Bergh, 2019:3). The research thus far points out to several different factors which might be effected by information operations in terms of society as a whole, the effects on individuals and other targeted groups. The effects can be also understood having short-term and long-term effects depending on the employed operations and campaigns. Shorter goal might be silencing individuals on specific issues or effecting the electoral behaviour for targeted elections. Longer-term goals could be effecting societies trust on each other and the governments/authorities loosing credibility. Information operations such as dissemination of disinformation, trolling and fake news can impact democratic societies negatively by disturbing public

debate and elections and manipulate public opinion (Pamment et al, 2018) and therefore destabilise countries or regions as a result of successful hostile information campaigns. Democracies enjoy public debate, trust and freedom of speech, and those are exactly the main avenues for hostile actors to exploit in order to create distrust, distort debates and present false information as "*alternative*" facts. Hostile actors entering conversations with offensive language can lead people believing what is the "*normal use of free speech*" (Aro, 2016:125) and lead to escalations in online spaces, as have been seen in the Internet and social media with spread of hate-speech. With the benefits of the Internet and social media, hostile actors can pose as citizens who are involved and interested in the democratic debate, but actually are disturbing the conversation with untrustworthy information which aims to provoke and polarise with a set end-goal from the message sender. These sort of information operations can contribute to the polarisation of social cohesion and increasing social mistrust (Pamment et al., 2018a:6). In addition to the bigger effects on the society as a whole, the information operation also can have effects widely on smaller groups and individuals.

Disinformation campaigns are designed to effect the receiver's feelings and can lead to outcomes for example of self-censorship and silencing individuals such as journalists or politicians when commenting on certain topics. Journalists, such as Aro (2016) have been personally targeted and she has noticed that journalists or researchers are less willing to publish findings because of the fear to receiving attacks and hate-speech. In addition to journalists and researchers, also individuals have stopped commenting for example Russian-related topics online due to the aggressive trolls attacking them and in effect being silenced by trolls online (Aro, 2016:124). The fear is also that the hate-speech and attacks online do not stay in the cyber environment, but move on to physical context. Successful information campaigns can in the extreme lead to mobilising people to committing "*serious actions outside the information sphere*" (Ibid:130).

The effects of information operations can be wide in terms of decreasing social trust, effecting election results, distorting public debate, oppressing and confusing people in the receiving end. The difficulty of understanding the effects is having to track the initial messages and origins of disinformation to the senders behind the anonymous accounts and fake profiles that might or might not be part of bigger campaigns directed from hostile states or non-state actors. Information operations which have moved from online to offline are difficult to completely understand without wider investigations and see whether there are linkages between the events happening online and offline. As mentioned before, the effects are widely lacking research and exploration, but there is wide understanding of what the tactics might look like. The issue of understanding information operations seems to be the difficulty of linking and proving the operations and pointing to a specific hostile actor or a nation state directing the information campaign.

4. Theoretical Model

Information operations in the cyber environment and the policies aiming to tackle information operations, are quite unresearched and therefore a theoretical model to research this issue had to be developed. The theoretical model is inspired from previous research on information operations and particularly how different actors, or participants, are involved in the issue. There are several parts to research in terms of understanding the overall Finnish threat assessment of information operations and the cyber security in general and how policies are targeted to actors in the political elite, military or in the civilian society. In the recent years, states such as Finland recognise that a narrow understanding of the security regarding solely own territories does not cover the issues such as climate change, migration or pandemics. Threats are broader and interconnected with the whole global world. A national health crisis can turn into a worldwide pandemic or the increasing global temperature can have massive impacts on the environment, migration patterns, conflicts and human lives everywhere - also in Finland.

The similar consideration are seemingly happening in the cyber security conversations where the threats are not seen only for the military intelligence and ICT infrastructure, but as a bigger threats to democracy, human rights, freedom of speech and healthy democracy. Research questions two and three were constructed to elaborate the overall threat dimensions and analysing whether policies have moved from the political elite and military dimension onto the civilian dimension. The overall threat assessment will follow Daase's Dimensions of Extended Security (2010) framework to understand whether development and extensions of the dimensions can be seen in the Finnish governmental discussions. The policy analysis will look into the policies which are aiming to decrease the risks and counter information operations. Policies are categorised to the two dimensions which are connected to Daase's referent dimension of the state, society and individuals. With the policy analysis and the dimensions, the aim is to see whether the Finnish governments have developed in their national security thinking in cyber related issues and whether Finland is focusing on creating policies which will secure the civilian society, rather than the policies focusing on the political elite and the Finnish military.

The research *hypothesis* is as follows: due to the Crimean annexation in 2014, Finland has started considering information operations and threats in the cyber space as an increasingly salient issue for the national security. From 2012 to 2020, the threat assessment and policies have developed and moved from narrow perspective of the state and military to the broader perspective of civilians, civil society and the private sector. The changes are argued to have stemmed from the events of 2014 in Ukraine, digitalisation of societies, lives merging with social media and the effects that have been seen in online spaces with for example increasing hate speech, polarisation and unidentified profiles disrupting conversations in social media.

4.1 Dimensions of (Extended) Security

Understanding different dimensions of security can help guide in the process of analysing Finland's considerations of information operations, how the government assess the threats to Finnish national security and how a transformation can be seen between the selected years 2012 and 2020. Security concept can be described as a change in political discourse but also explain the changes in political practises and international society generally (Daase, 2010:22). The changes not only describe the policy adaptions but also signals of broader fundamental changes that are underlying in the security culture (Ibid). The security culture is the "*sum of beliefs, values and practises of institutions*" and the individuals who determine what are considered to be the dangers or insecurities in broader sense and how the dangers should be countered and by which means (22). In order to analyse the Finnish security considerations between 2012 and 2020, an understanding of conceptual changes should be the focus point. The changes in language regarding security environment signifies political transformation (Koselleck, 1985; Skinner, 1969).

The dimensions of security have changed and expanded over time due to events that have taken place and thus required broadening security considerations. With the classical view of security, protection of the nation's territory lies at the core of national and international security thinking (Hirsch Ballin, Dijstelbloem and de Goede, 2020:13). Basis of the international order is formed by the key task of defending national territories and sovereignty of states (Ibid). In the 1950s and 1960s, the dimension on security was *narrower* and mainly focused on the traditional military threats towards national territories (Daase, 2010:26). Today, the security dimensions have *broadened* towards individuals and increasing concerns for human rights and economic and social development (Daase, 2010; Hirsch Ballin, Dijstelbloem and de Goede, 2020). The dimensions are ever more interconnected: the global financial crises or climate change can have significant effects on the stability of states, the general public and individuals. A pandemic such as Covid-19 can threaten the global supply chains and causing lack of hospital equipment or food supply across the globe. Formerly, the security has been narrowed to focus on the "*national survival of states and communities*" facing threats such as world war or nuclear annihilation whereas now, other factors such as human, economic, global, internal and external dimensions have extended the overall consideration of security (Daase, 2010:27). The dimensions have expanded beyond the classical view, however the expansion is not a linear process extending from the narrow state and military centrists view to the individual and humanitarian centrists view. The dimensions can be separated to four main categories, which Daase (Ibid:27-34) refers to as:

- Reference Dimension: Whose security should be safeguarded?
- Issue Dimension: Which issues should be safeguarded?
- Spatial Dimension: How far does security concerns reach in terms of geography?
- Danger Dimension: How is the danger considered: risk, vulnerability or threat?

4.1.1 Reference Dimension

Reference dimensions analyses and answers to the questions of whose security should be safeguarded. In the history, the reference dimension has been narrower and mainly considered the state's security and that only legitimate actor in international politics is the nation state. The narrow security is considered as the state security, meaning the nation's territory and defence of state borders. A broader perspective of human security became prominent after the Cold War where not only the state or social collectives were the objects of security policies, but the individuals also (Daase, 2010). The individual security approach challenged the traditional security dimensions from being solely looked at in terms of the state and social groups. The human security approach is an untraditional way of looking at security, where traditionally the state and social groups generally have been considered only. Securing humans does not only mean protecting individuals and communities from forms of violence and war. Human protection goes beyond that and its purpose is to protect humans in ways that "*advance human freedom and human fulfilment*" (Thakur and Newman, 2004:37).

4.1.2 Issue Dimension

The dimension focuses on the different categories such as military, economic, ecological and humanitarian issues. Traditionally, the security considered only the military aspect, since the biggest threat was seen to be military attacks and danger of being conquered (Daase, 2010). Expansions of the dimensions and different considerations for security threats had to be developed after the Cold War and 9/11 attacks. 9/11 demonstrated that smaller hostile actors could cause damage and challenge greater power's national security and due to which, the concept or security refers to hostile states and in addition to non-state actors as military threats (Ibid). Since the expansion, aspects of economic, environmental and humanitarian were added. Economic security such as vital resources need to be safeguarded in order to reduce the state and society vulnerabilities if being embargoed, having shortages or in the event of natural catastrophes. Environmental security are increasing due to the destruction of natural habitat and climate change which could potentially lead to mass migration and conflict. Lastly, the humanitarian security is the most recent extension which refers more broadly on human rights of groups and individuals. Humanitarian dimension includes aspects of economic and social development (Hirsch Ballin, Dijstelbloem and de Goede, 2020:13) and safeguarding individual's freedoms and human fulfilment (Thakur and Newman, 2004).

4.1.3 Spatial Dimension

Spatial dimension answers to the question of how far does the security concern reach geographically. Again, in the traditional sense, security policy only reached nation's borders, disregarding other countries and regions. Realists considered broader security policies that reach beyond a nation state foolish and that only an international agency could help those: "*World-shaking problems cry for global solutions, but there is no global agency to provide them*" (Waltz, 1979:109). National security considers the

security of the territorial states and securing national interests, international security includes more broadly inter-state cooperation and the stability of the international system for the common good. The dimension have expanded from securing own national borders, into creating better conditions internationally in order for all the nations to enjoy security. Institutions, conventions, regimes and organisations are considered as the tools for multilateral preservation of international security (Martin, 1992; Haftendorn et al., 1999). Beyond international security, the global security concept comes in question. Whereas international security focuses on the nation states, global security considers broadly human beings globally as the object to be safeguarded. Global security links to the issue dimension of human security, where for example environment is to be protected in order to secure food and clean water access.

4.1.4 Danger Dimension

Last dimension is focused on the operationalisation of danger. Level of threats have been measured in different ways traditionally based on what is know about the enemy actor, their hostile intentions and military capabilities (Cohen, 1979; Knorr, 1976). Crisis situations have showed however, that hostile actors and their military capabilities are not necessarily the only measures that should be considered, especially when we are increasingly interdependent globally. New ways of measuring insecurities were developed and the security debate has moved onto one's own weaknesses, instead of focusing solely on enemy strengths (Daase, 2010). In the current discourse of international politics, risks dominate the conversation. During the Cold War, threats posed "*clear and present danger*" and since then, they have been replaced by the unclear and future "*risks and challenges*" (Ibid:33). Issues of today, such as transnational terrorism, environmental degradation and proliferation of weapons of mass destruction are present in the political discourse in terms of uncertainties and risks (Ibid). The change in the political discourse on security is important due to the newer concept of risks which are existential dangers of which do not necessarily exist yet, but have the potential to pose severe danger in the future. Danger dimension extending to uncertainties changes the fundamental demands for security policy (Daase and Kessler, 2007), meaning that the uncertainties and risks require proactive measures from policy-makers, instead of reactive measures during the Cold War. The proactive measures reduce possible dangers by focusing on causes and effects of risks with preventive or precautionary ways. Proactive strategies or prevention and precaution may be for example cooperation, intervention, compensation and preparation (Daase, 2002:9-35). By proactive strategies, the aim is to be more active and offensive compared to traditional security policies, where the aim is to avert threats and mitigate vulnerabilities. In terms of the states, the prevention of dangers is done internally (civil rights of citizens) and externally (sovereign rights of states) (Ibid).

4.1.5 Framework in Practise

Daase's security dimensions give a framework for analysing the Finnish security assessment regarding information operations. With the dimensions, information operations considerations from different years can be situated to see whether for example the information operations are considered to be a danger to the state, society or individuals. The possible transformation of the security considerations explain the need for new policy adaptions and which signal fundamental changes (as mentioned above) in the security culture. The new extended security dimension does not only consider threats to be for territorial spaces or nation's borders, but more widely to "*natural and social nexuses in which even individual is embedded*" (Daase, 2010:34). The extended concept of security is therefore de-nationalised and simultaneously globalised and individualised. Below, a visualisation of the Four Dimensions of Extended Security.

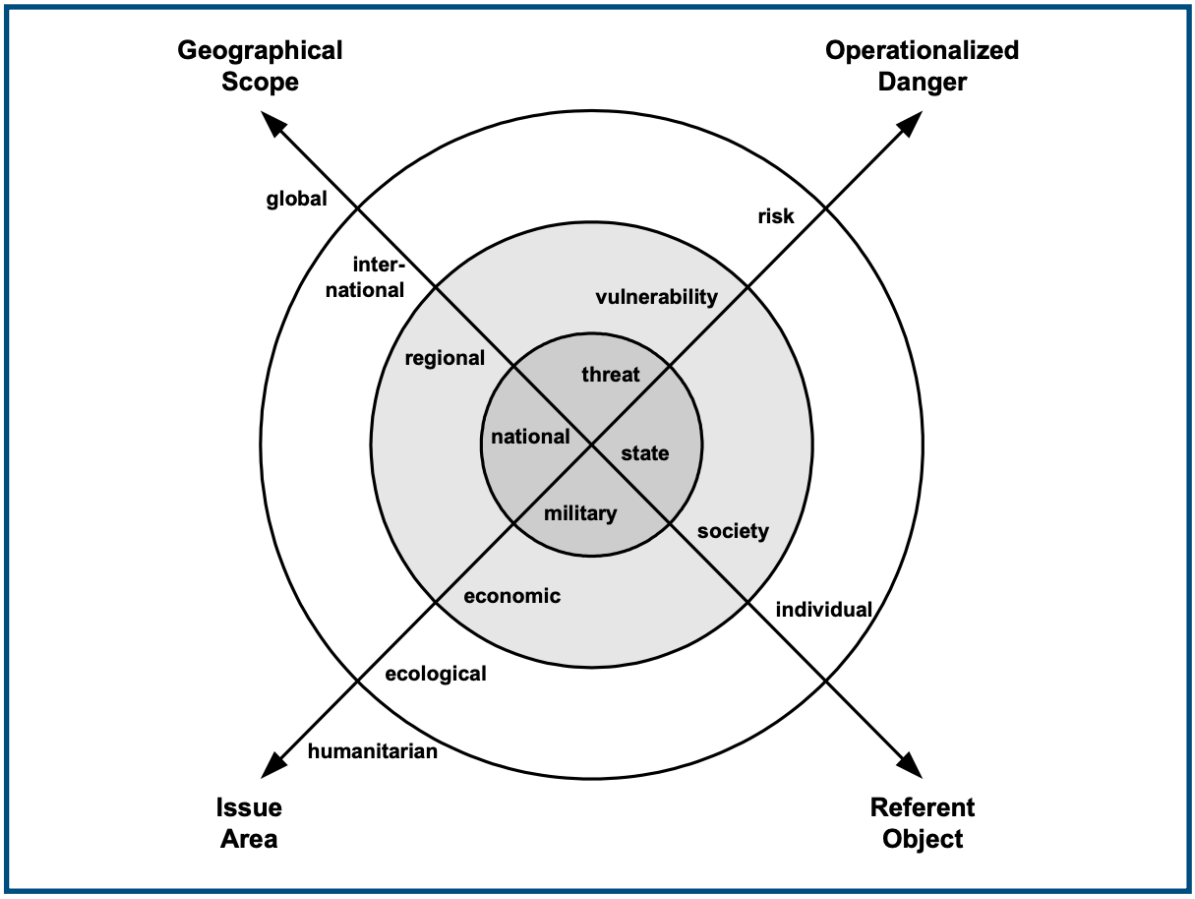

Figure 2: Four Dimensions of Extended Security (Daase, 2010)

4.2 Policies in the Referent Object Dimensions: Political Elite, Military and Civilians

For the purpose of analysing the Finnish information operations policies further, two different dimensions are introduced to help dividing the policies according to the Daase's referent object dimensions of state, society and individual. The two categories involve the perspective of the civilians (individuals and society) and the perspectives of

the political elite, including the military (the state). As discussed before, changes in the security practises and policies do not only describe policy adaptations, but they signal also broader fundamental changes in the security culture (Daase, 2010). Over time, the security dimensions have extended significantly from the narrower perspective focusing on the military and national territories to broader considerations of general public, individuals and global human rights (Ibid). Daase's dimensions of extended security suggests that states are widening their understanding of national security by considering now more than solely own territories and rather shifting into considering the security of the global world. According to the literary review and research on information operations, the readings suggest that cyber security and information operations have shifted from the narrow perspective of being a threat to the state and military to being a threat to individuals and threat largely to the Western, democratic countries. The policies are assumed to have shifted over time towards broader considerations and to reflect the demands for securing civilians and the general public, rather than solely focusing on governments and militaries. Therefore, the policies will be categorised to two dimensions: 1) Political Elite and Military Dimension and 2) Civilian Dimension. The clear policies are taken from the government reports and categorised according to what they aim to be doing: secure the state (elite) or secure the civilians and with what measures.

4.2.1 Political Elite and Military Dimension

Elite refers to "*a group or class of people seen as having the most power and influence in a society, especially on account of their wealth or privilege*" (Lexicon Dictionary, 2021) or "*the richest, most powerful, best educated or best-trained group in a society*" (Cambridge Dictionary, 2021). The people or organisations, who are considered elite, are the best or the most powerful compared to others (Ibid). Elite is a minority group within a larger social collectivity and it exercises influence within that specific collectivity (Roberts, 1971). A elite which exercises political influence in a certain collectivity is called the ruling elite or the political elite (Ibid). The political elite consists of the power holders i.e. leadership or the top power class (Lasswell, 1961). The decisions made by power elites have major consequences and they are in command of hierarchies and organisations in modern society (Mills, 1959).

4.2.2 Civilian Dimension

Broadly, civilians are described as persons without arms, i.e. persons who are not members of the police or the armed forces (Lexicon, 2021a; Cambridge Dictionary, 2021a). In this category, also the civil society and private sector i.e. commercial entities are considered due to their representation as the "*persons without arms*" and persons who are not part of the police, armed forces or the political, ruling elite.

4.2.3 Dimensions Collaborating in the Cyber Security Matters

Both dimensions are seen broadly important in the fight for a secure cyber domain and in setting up frameworks of norms for behaviour in the global online spaces. Security issues in the cyber domain are becoming increasingly concerning for the national security. The cyber arms race has escalated from governments in order to win wars in the cyber domain (Deibert, 2011:23-26). In addition to the cyber arms race, governments are pressured to regulate the global networks and the global civil society has been recognised as an important actor in the matter of governing the cyber space (Ibid). However, the global civil society cannot be summed up as one homogenous group wanting the same norms for cyber environment, but rather include citizens who are wanting to secure democracy, human rights and to have secure and open global communications space (Ibid). Deibert sees the securitisation of cyber domain as one of the most important factors shaping the global communication ecosystems. Securitisation is often associated with the defence industry, intelligence and military operations and civil society and civilians are not included - only as bystanders. However, when the operations moved online and the civilians were used for operations, the dimensions of security had to be extended to fit the new scale of the looming threat. Due to the threat increasingly involving civilians, the cooperation of the civil society, civilians, political elite and military are seen necessary to tackle the challenge. For both dimensions to be effective, strong cooperation is required from the civil society in operationalising normative cyber security framework for trustworthy and stabile ICT ecosystem as well as strong support from government and the private sector (Stifel, 2019). Stifel notes, that the multi-stakeholder process is effective in reducing cyber risks, discuss effective norms and regulatory practises. The civil society could have broad impact on the operationalisation of the agreed norms of behaviour online, however, support from the governments and private sector is needed to sustain the efforts (Ibid).

Many countries consider the highest levels of government, for example the prime minister or the president, as the entities responsible for coordinating cyber policies due to the decision-making reaching and impacting factors such as the economy, international relations and balance between security and privacy and civic liberty issues (Heinl, 2016:37-44). Governments and civilian ministries in most cases, are responsible for coordinating incident responses and militaries are seen as important stakeholders, usually used as instruments of last resort (Ibid). The private sector has an important role in the cyber security matters, due to the companies providing communications networks and social media platforms and benefitting from them monetarily. The role of the private sector is challenging for the military and public sector, since the commercial interests are usually different than of the government's will to securitise communication networks. The challenges between the private and public sectors in cyber security matters require governments, including military and intelligence, collaborating with private sector actors (Ibid). In cyber matters, militaries are dependent on the civilian and private sector infrastructures which are increasingly network-enabled (banking, health, energy, transport) and the reliance on commercial providers and products expose the militaries/ government to same threats as civilians and the private sector (Centre of Excellence for

National Security, 2015) The issue is that the military and intelligence community might be unable or unwilling to give out classified information and the private sector is reluctant to share information directly (Heinl, 2016:39) due to the potential losses of revenue and users trust in the services. The information is however crucial for the public in order to prevent influencing or information operations happening online and having an effect for example during elections or other crisis situations (Ibid).

5. Case of Study: Finland

Finland poses an interesting case study to research regarding information operations. Crimean annexation in 2014 has had a significant effect on Europe and Finland's security environment considerations. Due to Finland's history with Russia and as a country with a society highly reliant on information and communication technology (ICT), Crimean annexation poses an interesting point in time to see whether the crisis has effected the threat environment and policy-making. Finland aims to be a top expert internationally in cyber security (The Security Committee, 2019) and sees it as a threat, but also as an opportunity for future business opportunities (Ministry of Finance, 2019). In the recent years, the Finnish society and the government has faced severe data hacks which have lead to further demand for better and more effective policies for tackling and countering information operations and safeguarding the cyber domain. In the following chapter, the case study about Finland is developed by understanding on why Ukraine crisis in 2014 was a pivotal moment and why Finland poses an interesting case and how information operations are preserved in the Finnish governmental context.

5.1 Case Selection Process

Gerring's method (2004:341-354) of a case study will guide the selection process for the case itself and the overall frames of this research. A case study is an in-depth study of a single unit, which is a bounded phenomenon, with a purpose to understand a larger class of similar units (Gerring, 2004:342). The case (N) used for the study can be small or large and evaluated with qualitative or quantitative methods. The case is analysed through a particular type of evidence, for example non-experimental, participant observation, historical or textual research. Case study is defined by the small sample it studies and used typically when the topic is encountered for the first time (Gerring, 2007). When a research is on the beginning phases and in the exploratory stages, a case study grants the flexibility needed to test theories, develop or generate theories (Ibid). Cases are phenomena which are spatially delimited (Gerring, 2004). For instance, the object of the study, can be a country, city or a social group... (Gerring, 2007:19). Typical case study such as country time-series analysis, uses units as countries, cases as the country-years and observations from a range of variables selected (Gerring, 2007:19). Aim is to investigate the "*properties of single phenomenon*" in regards to dominant political unit of a nation state (Gerring, 2007:17-19).

In this study, the typical country time-series analysis will be conducted. The topic is by its nature exploratory due to the lack of previous research and phenomena being encountered for the first time. The aim is to see from the small-N a pattern by which a larger phenomenon can be understood broadly in the future. Information operations are considered as the properties of a single phenomenon and studied through the dominant political unit of nation state, Finland. For the evidence, textual material will be used from government bodies which are selected due to their relevance, involvement in the matter and policy-making power.
The years selected for time-series analysis are from 2012 to 2020. The selection is limited to the years between 2012 and 2020 in order to see the difference and the change in policies and threat environment considerations which are argued to have changed after the Crimean annexation in 2014. A change in policies do not happen suddenly and they tend to rise when a new danger, opportunity, trend has detected or a critical event has taken place (Kugler, 2006:36). In this case, the Ukrainian crisis is seen as the critical event in between the years and research focuses whether the critical event and the perceived danger raised questions and changed the Finnish policies regarding information operations.

5.2 Developing a Conceptual Framework

For the first part, a conceptual framework of the current existing situation in Finland's reality is presented and defined how the new trend, its development and the threat of information operations are addressed from different relevant government bodies. A new threat rises and gains saliency usually when a situation happens either in a foreign country or domestically and it triggers need for policies to address the new national security threat (Ibid). Need for new policies arise from critical events which might present danger or opportunities for the bodies who plan national security policies. The analysis will try to situate the Finnish government policies and assessments to the Dimensions of Extended Security (Daase, 2010) from years between 2012-2020. By looking at the Finnish considerations in regards to cyber environment and information operations, the results can indicate their strategic goal and the desired end-state of what the policies are pursuing in order to defend own national security and interests. Since there is no former research on the topic, the purpose of this research is to explore the signals and the surface of Finnish governmental understanding of information operations over the time period between 2012 and 2020. After analysing the overall threat environment, further analysis will be on the actual policies the Finnish government has proposed to tackle information operations. A further study on the subject could analyse also for example the policy adaptability, costs-effectiveness or implementation strategies. However, at this stage of the study, the purpose is to find key themes and policies and the change between the years and how the Ukrainian crisis in 2014 has possibly effected Finnish government's considerations of information operations.

5.3 Ukraine Crisis in 2014 and its Relevance for Finland

The security concerns related to several hybrid warfare tactics, such as information operations, were heightened in Europe and in the West after Russian annexation of Crimea in 2014. The tensions between Russia and the West and the following Ukrainian crises in 2014 might be the clear starting point of taking communications a serious threat to European values and stability. Russian and West's communication and influence strategies were contested after 2014 in legitimacy and whether they were acceptable and in the realm of free speech (Alafuzoff et al., 2020:23). As NATO addressed in their paper discussing information warfare, the interest towards the growing threat in connection to information operations and warfare grew after the Russian-Ukrainian conflict where Russia used influence tactics to muddy the waters with disinformation and promotion of own perspective over the Crimean annexation (NATO, 2020). Since the Crimean crisis, the research and understanding of Russian information techniques have developed rapidly (Giles, 2016). The studies of information as a tool in warfare have reached also beyond just Russia to other countries, organisations and individuals. The increasing interest stems from, as Giles argues, from the Russian successes achieving information dominance in Crimea (2016:66). European countries and their governments are facing the challenges of what to do in order to prevent event such as the Crimean annexation happening in their respective territories. The Finnish government Report on Foreign and Security Policies (2020) also analysed, that Russia has weakened the security in Finland and Europe's vicinity by annexing Crimea and continuing the conflict in Eastern Ukraine. The European and Russian relations are seen as deteriorated and Finnish government argues that the Russian are aiming for "*a sphere-of-influence-based security regime in Europe*" (Gov, 2020:21).

5.4 Finland: The Cyber Space and Information Operations

Finland has experienced Kremlin-backed information campaigns since the declaration of independence from Russia in 1917. Since the Ukraine crisis, the Council of State saw demand for example government employee's to sharpen their information control skills (YLE, 2016). The threat of information operations has been seen also in Finland ever since 2014, with an increase of fake news stories and targeted propaganda (Standish, 2017) and intensifying media attacks which were led by Kremlin (Mantila, 2016). The Finnish officials saw concerns due to the shifts in battlefield by information warfare moving online. Not too long after the Ukraine crises, Finland sought help from experts abroad to combat the rise of disinformation coming from the neighbour to the east. The understanding of the threat has developed and Finland and other Western countries are challenged on how to tackle information operations and how to involve domestic audiences who are often the targets. In Finland, the President Sauli Niinistö stated that "*We are all national defenders, meaning everyone who receives information, we are Finland's defenders*" (in YLE, 2015). The direction towards public knowledge and involvement was noted by the Finnish Director of Government Communications, Markku Mantila, who stated that the general public "*is alert to information influence*" (In Giles,

2016). Finland has faced also other major cyber attacks just as recently as the end of 2020, when vulnerable data was hacked and used against the hacked individuals (YLE, 2020; Finnish Security and Intelligence Service, 2021).

In November 2020, the Finnish media reported of a database hack to a psychotherapy centre Vastaamo and as a result, hackers stole citizens sensitive data from around 40,000 people, blackmailed the individuals, extorted money and bitcoins for ransom and leaked diagnoses, ID codes, contact information on the dark web (Yle, 2020). The cyber attack is likely to be the most extensive data breach thus far in Finland and the hacker(s) found truly the most vulnerable information to use against tens of thousands of people. After the hack and release of stolen data online, a campaign started in social media, where Finns pledged not to open or read the hacked information (Lehtinen, 2020). A year before in 2019, the Ministry of Finance addressed the exact scenario in their publication of digital health data ending up with wrong hands and how it would greatly threaten the cornerstones of the Finnish society's trust. The publication emphasised the importance of trust and developing society's resilience when faced with situations such as the Vastaamo data breach scandal. Interestingly enough, the paper foresaw what would take place a year later and had laid out a strategy when faced with cyber attacks, hacked information, information operations and hybrid influencing. Arguably due to having the strategy in place, readiness for crisis response and clear messaging to the public and media, the possible mounting crisis and vaster harm to Finnish public was effectively mitigated and somewhat avoided. However, as the paper emphasised, the intentional weakening of trust is one of the most serious threats to Finnish national security (Ministry of Finance, 2019).

"*Our feeling of security has also been eroded by new digital threats. Whether the target is Parliament or individual citizens' health data, the word 'data breach' is not strong enough to describe the problem. Cyber attacks threaten security; the are attacks against not only individuals but also our entire social order. We must improve our ability to foil them, also at the international level*" - with these words, Finnish President Sauli Niinistö addressed the Finnish public on the 2021 New Year's Speech. Finland's efforts to counter information operations have been in the interest globally by foreign governments and other countries have sought to "*copy its blueprint*" of tackling information campaigns. The governmental representatives from multiple EU member states have come to learn from Finland and find ways to approach the issue (Mackintosh, 2019).

Why is it then interesting to select Finland for this case study and why does other countries want to learn from Finland? Finland has a long history with Russia and is "*painfully well-versed in dealing with Russia as it had to do through war and annexation and most recently the Cold War*" (Nyberg in Standish, 2017). After the two wars with Russia, Finland has maintained neutrality with balancing in between the European Union and having good relations with Russia, however, the wars have left a sobering understanding of Kremlin's motives. Nyberg (former Ambassador to Moscow) analysed, that Finland is not the main target, but a "*side dish*" in a larger operation that might involve bigger information campaigns towards the European Union. Crimean

annexation raised concerns about national security in a military neutral country (Rosendahl and Forsell, 2016) and the threat was seen to be increasing when Kremlin led media attacks started intensifying (Martila, in Rosendahl and Forsell, 2016). However, Finland has emerge resistant to information operations waged by Russia and the country has found tools effective to attacks, unlike its neighbours in the Baltic nations. In the recent years, Finland has set up multiple efforts from different government bodies to understand and tackle information campaigns. For example: public diplomacy programs, enrolling government officials in programs about disinformation and different public education initiatives which build critical thinking and (social) media literacy from a young age (Jakubowski, 2018:13). Compared to its neighbours such as Latvia, Lithuania and Estonia, Finland has been very successful of countering Russian information operations (Ibid). However, the reasons are not only the mentioned efforts from government bodies and education but rather bigger characteristics about the Finnish society in general. Finland has a small population which is quite homogenous and with a small population of Russian speakers. Populations (as discussed before) that are homogenous, are hard to exploit for information campaigns and deliberately cause further riffs between general public. In addition, Finland has a high trust for its governmental bodies and due to the complicated history, higher level of distrust for Moscow (Jakubowski, 2018:13). In Baltic nations, Russia have a broader reach due to their bigger Russian speaking population as well as having Russian media, such as Russian Today, at place. However, as the information operations are getting smarter and they might become less dependent on the native speakers and media outlets such as RT operating in the country.

Social media is a global arena, where arguably, Finns are increasingly consuming international news media and therefore can be more exposed to the messages that might be traced back to hostile actors anywhere in the world. Finnish is also a complex language, which is hard to use in a natural way in information operations without causing the native Finnish speaker to suspect it's credibility. However, as technology develops, especially artificial intelligence, the language barriers are becoming lesser. Even though Finns might be "*winning*" the war on information operations for now, the threat is analysed to be increasing and we might not understand yet how the campaigns happening right now will have effects in the years to come. As the former Chief of Communications Specialist for the Prime Minister's office, Jussi Toivanen stated, "*.. Even though Finland has been quite successful, I don't think that there are any first, second or third rounds, instead, this is an ongoing game*" (Toivanen, in Mackintosh, 2019).

6. Methodology

6.1 Policy Analysis

For this research, a set of different methods will be employed to understand the Finnish understanding of the cyber threat environment regarding information operations and the policy changes in between the years of 2012 and 2020. For the overall frame of the research, a policy analysis will be used in order to answer the first research question:

How has the Finnish threat environment and policies regarding information operations and cyber security developed between 2012 and 2020?

Policy analysis offers a great flexibility of looking at the issue of information operations from larger perspective by analysing the threat environment and which actual policies are discussed. General policy analysis does not offer a standard framework how to approach an issue and each case is approached with a different way and they may employ number of different methods to analyse complex problems (Patton, Sawicki and Clark, 2016:6). Thus, theoretical model was created for this purpose. For policy analysis scholars, the core role is to contribute and improve knowledge of the world and describe phenomenas by aims of contemplating the future (Kugler, 2006:14). A functional role of the analysis can help governments reassess or reform policies for example making better decisions for the foreign and security strategy. However, the analysis does not aim to replace demand for reasoned decisions and "*sensible instincts*" from senior officials but rather enhance understanding on the matter (Ibid).

Policies are analysed through systematic procedures that can help tackling contemporary policy issues (Patton, Sawicki and Clark, 2016:3). Policy analysis focuses on issues on the federal level of governments that usually develop the plans and which the state and regional and local government adopt (Ibid:5). Two types of knowledge is sought to produce with policy analysis: empirical knowledge on attitudes and beliefs which define the world around us and directive knowledge which create guidance for how the analysed case will act in particular situations (Kugler, 2006:20). More in-depth policy analysis can also seek to find policy actions that can be categorised for example in terms of direct or indirect monetary and non-monetary actions taken (Patton, Sawicki and Clark, 2016:10-11). Monetary actions can refer to education programs, funds or purchases from the private sector and non-monetary policies can be laying out rules, regulations and standards which aim to modify behaviour through for example informational and promotional efforts (Ibid).

Policy analysis regarding national security issues are often through the defence affairs and military strategies which focus on providing goals and measurable results however, the issues often over lap with also in the political realm. In the political realm, the policy analysis can focus on areas such as diplomacy, regional security affairs, alliances, global economics or crisis management (Kugler, 2006:15). To systematise the information for the analytical purposes, analysis involves tearing up the policy in parts in order to

understand different components and seeing how they add up together (Ibid; Patton, Sawicki and Clark, 2016). Kugler (2006:29-32) suggested that strategic evaluation methodology is applicable for analysing national security policies and strategies through its aim of understanding broad frameworks of policies and strategies with the goals, activities and resource requirements laid out by the government. For strategic evaluation, data is collected though official documents which articulate the policies of the country or other governments (Ibid). Strategic evaluation is a tool for firsts steps exploring a policy issue but it might lack creating precise results (Ibid). For situations that are quite novel, unexplored but seen as increasing threats in the future (such as information operations), the data and information might be hard to gather and not as plentiful. Policy analysis focused on national security looks at the organised actions or already integrated sets of actions that might vary from "*public declarations to waging wars*" with aims to bring wanted results and achieve broader national goals (Kugler, 2006:12).

Policy analysis can be done before or after the policies have been adopted with either historical analysis of the policies implemented or evaluation of policies prior to the implementation (Patton, Sawicki and Clark, 2016:22-24). Descriptive policy analysis focuses on historical analysis or evaluation of new policies which are being implemented: retrospective analysis describes and interprets past policies which answer to what happened, and evaluative policy analysis refers to program evaluation answering to were the purposes of the policy met (Ibid). The policy analysis which analyses the future proposed policy outcomes can be either predictive or prescriptive. Predictive refers to the future stages which are results after adopting the policies and prescriptive recommends actions that are analysed to bring about specific results. However, the policy analysis often corporate both past and the future due to the need for understanding rationales and the impacts of past policies in order to design and evaluate new ones (Ibid). For this purpose, both past and future considerations are studied in order to understand the development and possible trend in the threat environment and planned policies.

6.1.1 Language and Material for the Policy Analysis

Policy analysis, as mentioned before, focuses on the federal level of government which plans the policies for state and local governments to adopt. Policies are geared to exercise power within a certain community i.e. the nation state in this matter (Savski, 2017:1). The exercised power through policies and laws aims to achieve certain objectives with attempts to oblige or forbid actions or practises by constructing a specific picture of the state of affairs in society which reflect sets of social values and the view what the society should be like (Levinson, Sutton and Winstead, 2009). Therefore, the policies are expressions of particular sets of moralities and ideologies in certain contexts (Savski, 2017:4). Policies can be laid out in different forms of laws, strategies, programmes or white papers with having different statuses in the polity (Savski, 2017:5). Analysis of policies include interactions between macro-, micro- and meso-levels of analysis examining sentences in the text with connecting meaning in the immediate co-

texts, the entire texts and the policy practises and agenda that produced the sentences (Ibid). However, the entire text and connecting sentences might be interpreted and understood differently depending on the reader and often the policies are also written for varied audiences: in the broader sense to general public or for smaller audiences who play a role in the administrative role (Tiersma, 2010:165-167). Scholar analysis of policies are complex processes where texts are received differently (Yanow, 2000; Stone, 2012). Even when policies are applied and implemented based on the government programmes or laws, the meaning and their function might continue to be debated (Savski, 2017:14). Policies can be studied from different perspectives of the implementation: top-down perspective studying the policy-maker viewpoints of the problems and solutions or bottom-up perspective looking at the implementation process from local actors adapting the policies (Ibid:12). This research will study the top-down perspective from the point of the Finnish government and their viewpoints of the national cyber security and policies discussed in order to counter information operations.

6.1.2 Chosen Material for the Study

For the study, two types of government released reports were chosen in accordance with Kugler's strategic evaluation method of collecting data through official documents which articulate the broad frameworks of policies of the country (2006). The data is collected from The Reports on Foreign and Security Policy from the Ministry of the Foreign Affairs and National Risk Assessment from the Ministry of the Interior. The reports were chosen after the research of relevant bodies of the government, who are mostly involved in addressing the overall threat assessments and bodies, who are responsible of the policy-making in a larger scale for the whole society. The Foreign and Security Policy report "*lays the foundation for steering Finland's foreign and security policy*" (Gov, 2020:9), analyses the current operating environment, and present the key priorities and goals. The report's analysis of the Finnish operating environment informs the Ministry of Defence, which prepares the Defence Report based on the analysis made by the Ministry of the Foreign Affairs (Ibid). The National Risk Assessment is prepared every three years based by all of the Member States on the decision by the European Parliament (Ministry of the Interior, 2018).

The National Risk Assessment is produced by different actors in the various administrative bodies and collects all relevant "*threat scenarios and serious disruptions affecting critical social functions and infrastructures at the national level*" (Ministry of the Interior, 2018:5). The National Risk Assessment is selected due to its connectivity and reach between the administrative bodies in all of the Finnish ministries. Both the Report on Foreign and Security Policy and the National Risk Assessment give a comprehensive picture of the government's framework of the national security, salient issues and the policies which are planned to tackle issues in the cyber security field. For more specific information and plans for policies, reports from different ministries such as Ministry of Education, Ministry of Defence, Ministry of Justice and Ministry of Transport and Communications could be looked into to have a better picture of how they are planning

to implement the policies from the wider framework given by the Ministry of the Foreign Affairs and Ministry of the Interior. For this research, the overall threat environment and indications of policy plans are considered only to give an idea of what is happening in the Finnish context. By the strategic evaluation method, data collected will give an indication of the broad frameworks and enhance understanding on the matter (Kugler, 2006) However, in the further study other reports should be looked into to understand the implementation processes and specific means to tackle and counter information operations. Outside of the ministerial and government reports, other Finnish organisations and non-governmental bodies should be considered due to their advocacy and effect on the Finnish threat assessment and policy-making. A relevant non-governmental body is for example The Security Committee which assists the Government in broad matters related to comprehensive security and has published the implementation program for Finland's Cyber Security Strategy (The Security Committee, 2021).

6.2 Key Word Occurrence

For the first part of the analysis, simple key word search is conducted for the selected governmental reports in order to get a sense of recurring words. The key word search is modified after Ryan and Bernard's Techniques to Identify Themes (2003) which will guide the process. With Ryan and Bernard's technique, the aim is to look for recurring themes from the data and identify "*topic that occur and reoccur*" (Bodgan and Taylor, 1975:83). Themes might come both from the data as well as researcher's prior understanding of the phenomenon under study (Ryan and Bernard, 2003). Before reading the reports from the Finnish governments, assumptions of the themes and key words were established due to reading previous studies and having former knowledge of information operations. A simple word list processing technique was created to find key word occurrences. The words on the list were identified from previous studies and publications from professionals in the field (for example Falk, 2020; NATO, 2009; Aro 2016; Jakubowski, 2019): information operations, information warfare, cyber security, cyber environment and so forth. More key words were added to the list after reading the reports and identifying words connected to issues around information operations and cyber security in the Finnish context. The added words, after reading the Finnish government reports, were words such as hybrid influencing, trolling, public attribution, psychological resilience and disinformation. The words were found after looking through the initial words in the list and locating them in the texts. The key word search is only a one step in the analysis, where a sense of saliency of information operations and cyber security in the Finnish government report can be established.

However, the method has its problems and is not comprehensive enough to prove whether the initial hypothesis is correct. The word search only indicates the word saliency between governments, but further research is needed to understand the context the words are in and whether they are actually connected with the topic of interest. For example, the key word search only indicates the number of mentions for each word or word combination in the text. However, further look into the occurrences is

needed in order to see whether the words are located on headlines, table of content, references or in the actual text. In addition, there might be differences between governments and how the phenomenon is addressed especially when the reports from Katainen's government (2012) are only found in Finnish language. There are also quite stark differences between the lengths of the reports which can influence the issues addressed and issues that are left out. For example the National Risk Assessment varies between 64 to 95 pages and the Government Report on Foreign and Security Policy varies between 30 to 115 pages. If the reports were similar to size, the word saliency might look very different. This poses a challenge for the research, however, the most salient issues for the government are believed to be in the reports and discussed even shortly, whilst less salient issues of the time of publishing are not addressed.

The word list and word saliency is only the first step in the process to see whether the initial hypothesis might be valid, however, further research is needed to strengthen the hypothesis. From the word occurrences, only a vague pattern could be established. Next step is to look into the words and in which context they are discussed in to confirm that they are actually connected to the key issue of information operations and cyber security. The reports from Marin's government (current versions) and Sipilä's government are published in Finnish and English but Katainen's publications are only found in Finnish. The word list was mainly established based on the English terms found in previous studies and publications on the topic and they were translated to Finnish in order to find the word occurrences from the oldest reports (Katainen's government). The words were found to be correctly translated from English to Finnish, due to the occurrences found in the Foreign and Security Policy reports (2012). However, the National Risk Assessment 2012 lacked completely any mentions of the words on the list and it raised questions. The table of content was checked and the reports skimmed, and nothing suggested that there were any mentions of information operations or even anything on cyber security. The key word search serves as a first step in the thesis in order to see whether a pattern supporting the hypothesis can be seen and whether the thesis research should be continued to further analyse the Finnish government reports with Daase's (2010) framework of Extended Security Dimensions and analysis of the policies for information operations.

6.3 Weaknesses of the Theoretical Model and Methods

Due to the exploratory nature of the study, an own theoretical model was created. Policy analysis research offers flexibility on how to conduct a study and different methods are employed in order to analyse complex problems (Patton, Sawicki and Clark, 2016:6) such as information operations in the cyber space and policies aiming to tackle the potential risks for the Finnish state and the Finnish society. The nature of the national security analysis is complex and it involves issues from the defence and military realms, but also overlaps heavily on the political realm as well (Kugler, 2006). The study thus demands considerations from a wide perspective when wanting to establish a broad framework in which the Finnish government operates in. For this purpose, two different types of reports were selected to give answers for the study, which is exploratory and

aiming to improve knowledge and describe the phenomena of information operations. However, the theoretical model and the different methods chosen provide quite vague information which only indicates the direction and current issues that the Finnish government is facing. In addition, the time-series chosen is very limited and aims to connect one crisis event (Crimean annexation) to what is happening in the Finnish national security discussion. The phenomena of information operations and cyber security are not new and if the time-series would be extended, a larger trend would be potentially detected especially due to the Finnish history with Russian influence attempts and events such as the Cold War.

The data collected from the Finnish Ministry of the Interior and Ministry of Foreign Affairs reports give broad indications of the Finnish security evaluations and threat assessment. To analyse the reports, qualitative and quantitative methods are employed in order to get various perspectives of understanding of the issue at hand (Patton, Sawicki and Clark, 2016). However, analysing policies is a complex process where scholars might receive and interpret texts in different ways (Yanow, 2000; Stone, 2012). If the study was conducted by another person, the theoretical modelling and results might look different due to different ideas of how to analyse the complex issue and interpreting the texts under analysis. As a native Finn and an active follower of the Finnish political discussion, own potential bias has to be acknowledged especially when comparing different governments and interpreting the world events from the perspective of a Finnish native. Some scholars argue that researcher bias cannot be completely avoided, since researchers are part of the subject matter (McCullagh, 2000) and researchers have different set of ethics, values and morality which might potentially have an impact on qualitative research to a certain level. The impartiality and bias should be minimised and avoided by different methods such as adopting multi-perspective approach which presents multiple and opposite viewpoints (Ibid). In addition, combinations of qualitative and quantitative data is suggested to reduce research subjectivity on the matter (Rajendran, 2001:5-7). Different sets of methods are used in this study to not only rely on own interpretations of the Finnish government reports, but to back up the argument with employing quantitative methods together with qualitative methods.

The subject matter under the research is also very complex. Information operations and cyber security are interconnected with multiple issues in national security and topics are discussed in different terms, as mentioned in the second chapter. Information operations overlap with hybrid influencing and several other terms, which creates difficulties of interpreting whether the threat assessments and policy proposals are connected with the exact issue of information operations. However, based on the governmental discussion and descriptions, the terms are connected due to the use of information for hostile operations and the policy proposals linking hybrid - and information operations together. Another researcher might separate the two, but for this study, information - and hybrid operations are argued to be connected.

7. Finnish Security Environment 2012-2020

The Finnish security environment is analysed through two governmental reports from three different governments during the time period of 2012 to 2020. For the analysis, two different types of methods were employed in order to analyse the security environment through the governmental reports. Data to analyse national security for strategic evaluation (Kugler, 2006) is collected from official documents which address policies and strategies of the respective country, in this case Finland. Strategic evaluation is a tool for the first steps in exploring policy issues and analyses broad frameworks laid out by the government (Ibid). In the following, the research will be complemented with short section on the governments to give context, overlook of the reports with a word analysis of the key themes and observations of how information operations and cyber issues are addressed in the National Risk Assessments and the Reports on Foreign and Security Policy.

7.1 Governments Under Analysis

For the analysis, context on the governments will be given on specifics of the parties in government, the gender ratio and what the official headline was/is laid out by the party coalition in power. This research does not argue that the government specifics necessarily effect largely the results and it is more likely that the security environment and policies are changing due to the global events which have taken place. However, the security environment and the considerations beyond the Finnish territory might be arguably linked to the party coalition characteristics and ideological stances of the coalitions.

In 2012, the Prime Minister Jyrki Katainen's government formed a "six-pack" coalition which included the National Coalition Party (Katainen's party), the Social Democratic Party, the Left Alliance, the Greens, the Swedish People's Party of Finland and the Christian Democrats. In the ministerial positions, 11 out of 25 were women and out of the six parties, five had men as chairs of the party (Valtioneuvosto, 2020). The government's programme headline was "*An open, fair and confident Finland*" (Valtioneuvosto, 2011). During the release of the two reports under the analysis, the National Risk Assessment released by Ministry of the Interior was led by the Christian Democrats. The Report on Foreign and Security Policies by the Ministry of Foreign Affairs was led by the Social Democrats.

In 2015, the Centre Party won the Prime Minister's seat and the PM Juha Sipilä formed a government with the Centre Party, the Blue Reform Party and the National Coalition Party which were all chaired by men. Out of the 23 ministers, nine were women (Valtioneuvosto, 2020). National Risk Assessment was spearheaded by the National Coalition Party and Foreign and Security Policy Report by the Blue Reform Party. The government's program headline was "*Finland, a land of solutions*" (PM Office, 2015).

In 2019, the former PM Antti Rinne stepped down and the newly formed coalition by the in-coming PM Sanna Marin created worldwide attention. An unusual government is

currently led by a coalition, where all the five party leaders are women, most under 35-years-old. The current government is formed by the Social Democratic Party (Marin's party), the Centre Party, the Greens, the Left Alliance and the Swedish People's Party of Finland. Out of the 21 ministers, 13 are women (Valtioneuvosto, 2020). Both reports were published by the Greens who are leading the Ministry of the Interior and the Ministry of Foreign Affairs. The newest program's headline is "*Inclusive and competent Finland - a socially, economically and ecologically sustainable society*" (Valtioneuvosto, 2019).

7.2 Overlook of the Reports

In the following, a short overlook of the reports will be done. There are significant differences of how issues regarding information operations are addressed. In order to understand the structures and saliency of the issues, number of methods are employed to analyse complex problems (Patton, Sawicki and Clark, 2016). Therefore, quick analysis with simple key word research was done in the beginning to find the key themes and saliency of "*topics that occur and reoccur*" (Bodgan and Taylor, 1975:83). Quite big differences could be seen in the reports and how cyber security and information operations are addressed between the selected time period. In National Risk Assessment 2012, mentions of cyber security and information operations are completely missing and in comparison to the newest report, information operations has its own chapter under threat scenarios. The hypothesis, as mentioned before, is that the Crimean annexation in 2014 changed the threat environment and thus themes and words such as information operations, influence, cyber and hybrid warfare are gaining more saliency when moving from the reports from 2012 to the current government reports in 2020. However, the key words search does not address in what the context they are nor where the words are situated. The key word search only gives an idea whether there is a change in saliency and from that point, it is easier to move onto taking a closer look on the contexts they are discussed in.

Key Word	2012	2015	2018
Information Operations	0	4	23
Hybrid (ends with warfare/threat/ influence/operations/ actions)	0	3	19
Influence (ends with cyber, data, political decision-making, attacks, elections)	0	8	14
Cyber	0	70	25
Cyber Environment/ Domain	0	18	2
Disinformation	0	0	3
Trolling	0	1	2
Cyber Attack	0	0	7
Social Media	0	2	13
Psychological Resilience	0	1	25
Ukraine	0	7	1
Russia	0	23	6
Crimea	0	1	0

Figure 3: National Risk Assessment (Ministry of the Interior)

7.2.1 National Risk Assessments 2012-2020

The National Risk Assessments were published in 2012, 2015 and 2018. The 2018 is the most recent National Risk Assessment published. The three reports show significant difference on how information operations and the related topics are positioned in the papers and how the key words have gained saliency over the years. The first report under analysis from 2012, does not mention information operations, disinformation, Crimea, Russia, cyber domain, hybrid (ending with warfare, threat, influence) or other related words throughout the report. This shows, that in 2012 there were other pressing issues to address and the threats in the cyber space were not considered as a risk for national security in comparison to other salient issues. In the 2015 report, the Crimean crisis is novel and thus the difference from the former is quite stark. The key words mentioned before are in double digits and clearly, the threat environment regarding cyber space and information operations have raised concerns. In the latest report from 2018 many words such as information operations, have gained significant saliency and also other words have come up such as psychological resilience, disinformation and hybrid (ending with warfare, influence, operation). Only in the newest 2018 report, information operations are addressed in its own chapter with long description of the threat, who is it effecting and what should be done. In the 2015 report, the key words are separated in different sections, usually regarding overall risk scenarios and cyber-related issues and cooperation.

Key Word	2012	2016	2020
Information Operations	2	3	0
Hybrid (ends with influence/threat/ action)	0	11	27
Hybrid influencing	0	8	14
Network (ends with warfare or attack)	3	0	0
Cyber security	8	3	1
Russia	163	30	34
Cyber	35	9	13
Cyber environment/ domain	5	2	1
Ukraine	6	2	3
Crimea	0	1	2
Public Attribution	0	0	1
Dividing lines	3	0	6
Crisis resilience	0	8	12
Disinformation	0	0	1
Information/Data Security	0	18	2
Digital Society	0	0	4
Manipulation (regarding SoMe, cyber, misleading content)	0	0	3

Figure 4: Government Report on Foreign and Security Policy (Ministry of Foreign Affairs)

7.2.2 Government Report on Foreign and Security Policy 2012-2020

The reports of Foreign and Security Policy are not as clear in terms of key word saliency increasing from 2012 to 2020. Firstly, the main key word of interest *information operations*, is addressed in the 2012 and 2016 reports, but does not exist in the 2020 report. In 2020, the word hybrid (ending with influence, threat, action) has gained saliency from being non existent in 2012. In 2020, hybrid with different ends were mentioned 28 times. Hybrid tactics/operations are noted to be inclusive of information operations and hostile tactics using information. Contrary to the older reports, also new word regarding the counter/retaliatory measures is introduced: public attribution. Mentions of two different information operation tactics, manipulation and disinformation, are also

mentioned few times in 2020 which do not exist in the reports before. The Finnish and global society is analysed vulnerable due to the technological developments and a society transforming into a "digital society".

7.3 Finnish Security in Daase's Dimensions of Extended Security Framework

In this section, the Finnish security environment will be analysed through Daase's Dimensions of Extended Security framework. The aim to see whether the national security considerations have moved between 2012 and 2020 and see whether the threat environment has broadened or narrowed in terms of four categories: geography, operationalisation, issues and referents.

7.3.1 2012 - Katainen's Government

7.3.1.1 Geographical Scope

In geographical scope, the Western countries are seen vulnerable for information- and influence operations due to their resilience on ICTs and cyber-enabled systems. Ministry of Foreign Affairs analyses, that there are several areas which are creating conflicts in the international community regarding cyber security: "*Cyber security issues cause contradictions and divisions within the international community. They are based on economic and security interests, as well as differing perceptions of human rights and the role of states in the relationship to individual freedoms*" (Gov, 2012:22). In 2012, cooperation in cyber issues are discussed to be happening between the EU, NATO, OSCE and the UN and between different groups of countries. It is not established how Finland is participating in these conversations, rather that they are happening in general between such bodies. Government notes that in order to secure free and trustworthy use of common global operating environments (sea, air, space and human created cyber space) "*the importance of international regulation should be emphasised*" (Ibid:21). Government supports close Nordic cooperation and creation of knowledge network for preventing cyber attacks. The report notes that international development in the cyber environment is increasing threats and Finland has been subjected to cyber operations from insider and outsider actors (Gov, 2012). Katainen's government is therefore analysed to regard the national, regional and international dimensions in demand for safeguarding and emphasising on regional (Nordic) cooperation in the issue.

7.3.1.2 Issue Area

In terms of the issue area, Foreign and Security Policy report considers most of the levels, except the ecological, to be safeguarded for cyber attacks. Katainen's government sees the military, economy and humanitarian dimensions to be under threat in the cyber environment and subjected to information - and influence operations. "*In*

addition to traditional military operations, operations involve a variety of asymmetric means, such as information and cyber warfare, political-, economic- or military pressure, and combinations of these. This is taken into account in the development and use of defence capabilities" (Gov, 2012:37). Humanitarian dimensions is also acknowledged with analysing the threats in cyber environment are becoming more dangerous for the whole of society and that the impact may not just be harmful for the armed forces, but for the society at large. "*The changing nature of conflicts means that securing the civilian population is even more challenging*" (Ibid:38). Katainen's government report on Foreign and Security Policy notes the military, economic and humanitarian dimensions as vulnerable, leaving out the ecological dimensions.

7.3.1.3 Referent Object

In answering who should be safeguarded, Katainen's government addressed the society and the state needing security in the referent object dimension but disregards safeguarding of the individuals. As mentioned before, the whole society at large is seen as vulnerable for information operations and cyber attacks and the securitisation of the civilian population is becoming challenging. The Finnish state and society are seen potentially at risk due to the high reliance on cyber enabled networks and services and government see essential for the upcoming years that "*securing the cyber environment is essential for the information society*" (Gov, 2012:12).

7.3.1.4 Operationalised Danger

The operationalised danger dimensions are analysed through threats, vulnerabilities and risks by Katainen's government. Threats traditionally are analysed based on what is known of the potential enemy actors and the government addresses this by noting their knowledge of Russia developing its cyber warfare capabilities (Gov, 2012:40). Government acknowledges the vulnerabilities in the Finnish military and the development demands in defence capabilities. The operationalised danger dimension of risks and vulnerabilities seem to be more present than threat dimension. Government mentions Russian military capabilities once, but focuses on the Finnish vulnerabilities and the potential risks that cyber attacks and information operations might pose in the future. The logic of shifting from "clear and present dangers" towards the unclear "risks and challenges" (Daase, 2010) seem to be the case in 2012. "*Warfare can begin in time of peace with pressure and information operations. The line between political influence and warfare is blurred*" (Gov, 2012:37). The government analyses that the separation of state and non-state actors and identifying the origins of the threats are becoming challenging.

7.3.2 2016 Sipilä's Government

7.3.2.1 Geographical Scope

The Report on Foreign and Security Policy from Sipilä's government follows the report from 2012 with considerations of national, regional and international dimensions in the geographical scope. The developments in Finland's vicinity are seen threatening stating that "*Finland, for the sake of its security, must carefully monitor the military capabilities and aspirations of the actors that impact our immediate surroundings, in particular.*" (Gov, 2016:14). This could be argued to be directed to Russia and Finland analysing Russia's goal of becoming a sphere-of-influence-based security regime and the demonstrated capacity of reaching Russian objectives by employing military force in Crimea (Ibid:13-14). Finland sees demand in strengthening cyber security by cooperating with the European Union, NATO and bilaterally between states. Difference between 2012 to 2016 is, that the National Risk Assessment addresses information operations and cyber attacks which are missing from the 2012 assessment. National Risk Assessment considers national and regional dimensions in a need for safeguarding - stating that Finland and European Union can be potentially subjected to information operations and cyber attacks: "*Different combinations from the range of instruments have been used in recent European military conflicts. The probability of the hybrid threat against Finland is low-average.*" (Ministry of the Interior, 2012:26). Government analyses that Finland might face potential economic or political retaliations as a EU Member State from anti-EU actors during a larger crisis or conflict (Ibid:26).

7.3.2.2 Issue Area

Sipilä's government seem to have broadened the security in terms of the issue area considering the traditional dimensions military and the economy (Foreign and Security Policy Report), and in addition some elements of the humanitarian dimension (National Risk Assessment). In the Foreign and Security Policy report, the focus lies at the economic and militaristic considerations mostly: "*The picture of war has become more complex. In order to achieve political objectives, political, economic and military pressure, forms of information and cyber warfare, combinations of all of the above and other forms of hybrid influencing, among other things, are used in a coordinated fashion on top of the constantly developing military means*" (Gov, 2016:14). Finland is cooperating with NATO's operational, training and exercise planning and cyber-defence cooperation to develop Finland's national defence and capabilities to defend own territories (Ibid:24). In the National Risk Assessment, the issue area is expanded from military and economy to humanitarian aspects also with acknowledgements that the pressure can be targeted to hinder public opinion, misinformation dispensed through the media and negatively impact social order. "*The pressure can target political decision-making or public opinion, it may include interference in the activities of the authorities, enterprise, services or financial and payment systems as well as obstructing and hindering, and military violations of territorial integrity or troop concentrations near our borders*" (Ministry of the Interior, 2015:25).

7.3.2.3 Referent Object

Sipilä's government acknowledges the referent object extending to the state and society dimensions and disregarding the individuals on both reports. Government sees Finnish society vulnerable due to being an advanced information society which "*creates favourable conditions for a successful attack*" (Ministry of the Interior, 2015:25). Attacks are analysed to employe against the state of Finland or Finnish society with the aim of influencing Finnish political decision-makers and state leadership. If attacks towards society and the state are not successful, government analyses that the cyber-attacks would target "*society's vital functions, decision-making and management systems, critical infrastructure included*" (Ibid:18).

7.3.2.4 Operationalised Danger

Similar to the 2012 operationalised danger considerations, Sipilä's government seems to follow the similar logic by acknowledging the risks and vulnerabilities that cyber environment and information operations pose for Finland. However, the knowledge from 2012 of the actual risks and challenges have become more concrete and the government addresses quite extensively different threat scenarios which might take place in Finland and in Europe. The knowledge is argued to have developed due to the events in Ukraine and Finland is considers it "*as an example of a crisis in which political, economic and military as well as special forces and, especially, information operations are used*". (Ministry of the Interior, 2015:27). The threat of information operations and different cyber attacks to the Finnish state and society have become clearer with describing the most likely scenarios of pressure attacks and campaigns. "*The adversary may want to deny third party access close to this area, or establish a military buffer zone to protect his strategic targets. Limited operations may also include the occupation of certain areas and air/sea denial. Alongside the armed forces, limited operations may target society's vital functions such as telecommunication networks, energy and electricity distribution networks, transport hubs, logistics centres or foreign trade connections. In addition, they may include psychological operations and other information operations as part of the use of force*" (Ibid). Unclear and looming risks and challenges have become clearer threat scenarios with detailed descriptions of the avenues of influence, military operations and potential harms. The Finnish risk scenario seems to be influenced by Crimean annexation and what took place during the conflict in 2014. Comparison to the former government, the threat of information operations is a clear threat, not only a potential risk or a vulnerability.

7.3.3 2020 - Marin's Government

7.3.3.1 Geographical Scope

Out of all the reports from 2012 and 2016, the National Risk Assessment of 2018 is the broadest in terms of the geographical scope, taking in consideration national, regional,

international and global dimensions. The government sees influencing of large masses to be enabled by the new global communication environment in which the hostile actors can reach more people than ever in real time. In accordance with most research on information operations, the Ministry of the Interior sees the threat towards the Western democracies by operations attacking trustworthiness of the elections. "*Questioning the integrity of the election can threaten the trustworthiness of entire Western democracy*" (Ministry of the Interior, 2018:24). Government notes that international and especially EU-wide collaboration is highly important in preventing information operations and hybrid influencing. The Foreign and Security Policy report supports and emphasises also the EU and NATO cooperation which would benefit both parties and enhance European security and capabilities. Finland supports better EU countermeasures by adopting uniform approaches to cyber security which "*the Member States must effectively execute the jointly agreed measures*" (Gov, 2020:40).

7.3.3.2 Issue Area

Marin's government National Risk Assessment discusses widely the humanitarian aspects of information operations and why safeguarding is highly demanded to secure access to trustworthy information, secure the Finnish unity and identity and keeping citizen's safe from making harmful decisions or act in violation of own interests due to influencing. Finland have noticed that "*the statements of our leading politicians have been distorted, journalists and scholars have been threatened and pressured*" (Ministry of the Interior, 2018:25). In addition to the decision-makers, scholars and journalists, the Ministry adds their close ones as potential receivers of pressure, threats and even physical threats. The Foreign and Security Policy Report focuses expectedly more on the military and economic dimensions of the issue area with regards to the new developments in technology, which has impacts on the Finnish defence capabilities. "*Technological development, particularly in the areas of digitalisation, AI, machine autonomy, sensor technologies and new operational environments, also has an impact on every area of national defence*" (Gov, 2020:16). The government notes that the security perspective demands wide outlook in multiple areas: "*Finland examines security from a wide perspective that observes not only the military threats, competition between great powers and hybrid influencing but also the impacts of the global challenges in sight, such as climate change, health threats, human rights violations, migration, economic crises, increasing inequality, terrorism and international crime. Many of the global phenomena affecting security are characterised by their ever closer interconnectedness*" (Gov, 2020:25). As comparison to other governments, Marin's government examines security threats to be highly interconnected and that solutions for wide-ranging preparedness against multifaceted threats are needed in order to maintain society's well-being and security. The government aims to have "*an open, free and safe cyber operating space, where ethical aspects, and privacy protection and freedom of speech issues are also taken into consideration*" (Ibid:39). Therefore, all dimensions of the issue area are analysed to be noted by Marin's government.

7.3.3.3 Referent Object

As predicted, the current government, recognises all the referent object dimensions as vulnerable for information- and/or hybrid operations in both of the reports analysed: state, society and individual. While the International Security Assessment focuses highly on the individual's perspective by noting on the strategies how civilians can be used for disseminating false information and influencing citizen's to make harmful decisions to themselves or act in violation of their own interests (Ministry of the Interior, 2018). The information operations targeting civilians have consequences on the larger society by its "*aim to weaken the operating capacity of the society and trust in the authorities and government*" (Ibid:24). Civilians working as journalists, politicians and their close-ones are also addressed to be one of the main targets for influencing, threatening, pressuring and even physical threats. The Report on Foreign and Security Policy focuses more on the state and society at large dimensions by noting that "*disturbances and hostile activities in networks may affect the transfer of information, data integrity, the functioning of telecommunications, and the ability of states to act in times on crisis*". (Gov, 2020:15) and "the electrification and further networking of societies may make the more efficient but, at the same time, network vulnerabilities may also enable injurious activities" (Ibid). Government sees the state, society as well as individuals and society vulnerable due to the dependencies in ICTs and high reliance on technology - both which makes Finland an efficient but also at risk for disturbances.

7.3.3.4 Operationalised Danger

Similar to Sipilä's government threat assessment, Marin's government seem to have a very clear picture of the threats. However, from 2016 to 2020 the situational picture has developed from understanding the humanitarian and individual threat scenarios in addition to the military scenarios. The threat of information operations (clear and present dangers) for civilians are understood to become more common as a result of the "*transformation and speed of communication, emergence of social media and diversification of information channels*" (Ministry of the Interior, 2018:23). The effects of information operations are threatening to stir up public debate, weaken operating capacity of the society and the trust in democracy and the Finnish elections. The government addresses also vulnerabilities and risks regarding information operations that lie in Finland. As a vulnerability, the government analyses technology and society and state's dependency on it worrying: "*New technologies and changing operating environments, including cybersecurity and the growing security role of space, and the overlapping of conventional and nuclear weapon systems upset the strategic balance and set new requirements for arms control agreements, national legislation and preparedness*" (Gov, 2020:18). Cyber issues have become part of the clear and present dangers similar to conventional and nuclear weapon systems and not only potential risks and vulnerabilities. Vulnerabilities are recognised in the Finnish society, mostly based on the dependency on technology and ICT.

7.4 Summary of Dimensions of Extended Security

As predicted, the security perspectives have broadened from 2012 to 2020 regarding issues around information operations, influence campaigns and cyber matters. In 2012, the cyber security and information operations are seen as unclear and looming issues compared to 2016 and 2020, where the Ukrainian crisis has had an effect arguably. From the unclear and abstract issues, the situational picture in the reports after 2014 have developed more clear and the vulnerabilities and challenges are seen widely in Finland in terms of military, state, economy and individuals. Both reports in 2016 and 2020 provide quite detailed threat and risk scenarios analysing the avenues of influencing, hostile actor's motivations and potential goals and how Finland should be prepared for such operations. The unclear and looming threat of information operations and cyber attacks have become to be clear and present threats, which in 2020 are connected with conventional and nuclear weapon systems.

The National Risk Assessments show interesting development between 2012 and 2020. In 2012 National Risk Assessment, information regarding cyber security, information operations, hybrid influencing or related terminology was completely lacking. During that time, there might have been other pressing issues in happening and therefore cyber security and related issues were not addressed. In 2015, the Crimean annexation had just taken place the year before and the its effect can be seen in the National Risk Assessment. 2016 report is developed vastly from 2012, but the main focus lies on the national-regional, military-economy and state-society dimensions. In 2020, the risk assessment has developed to be inclusive of most of the dimensions on the framework. Underneath, a visualisation of the Finnish National Risk Assessments between 2012-2020 situated in Daase's framework of Extended Security.

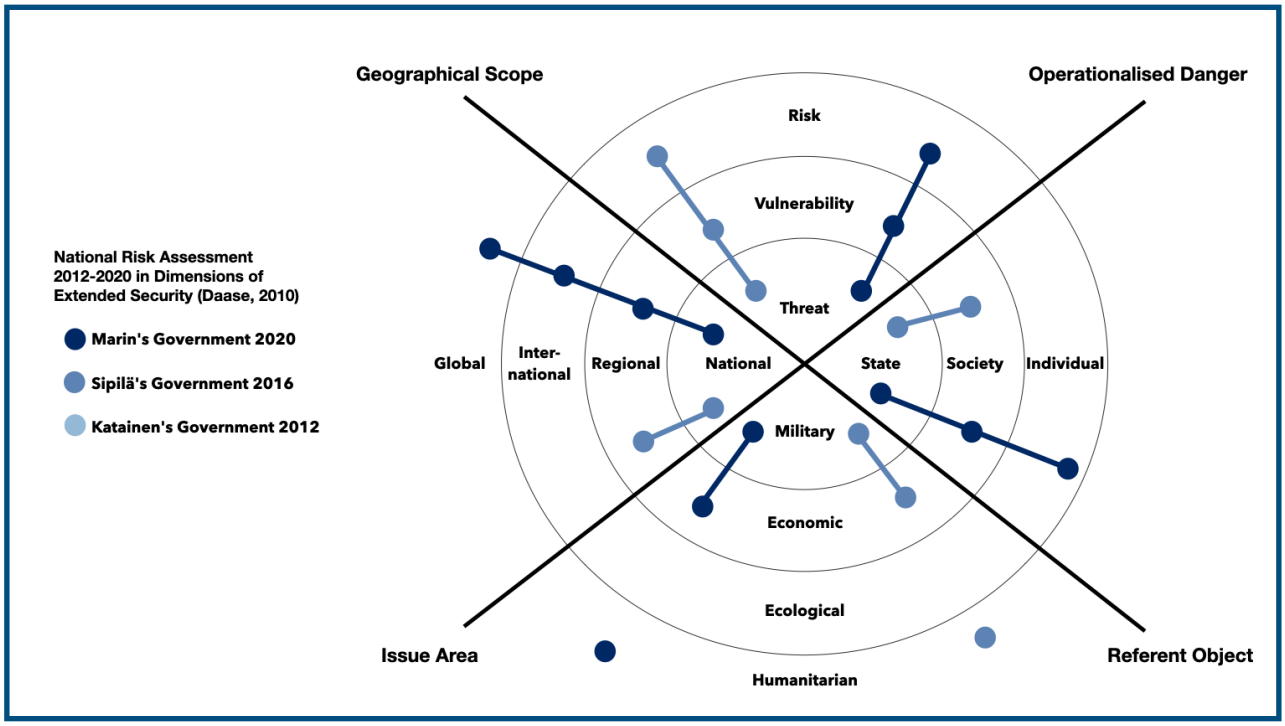

Figure 5: National Risk Assessment 2012-2020 in Dimensions of Extended Security by Daase (2010)

The Report on Finnish Foreign and Security Policy generally focuses more on the militaristic and foreign aspects by its nature. In 2012, the information operations and cyber related issue are present and also addressed quite widely, in comparison to the National Risk Assessment, where nothing on the matter existed. 2012 and 2016 considered dimensions follow mostly the same pattern in the geographical scope, referent object and operationalised danger dimensions. Only difference based on the analysis is that Katainen's government in 2012 regards also humanitarian dimension in the issue area. In 2020, the report is analysed to be differing only based on its considerations of the individual dimension in the referent object. The Reports on Foreign and Security Policy between 2012-2020 are therefore quite consistent in the cyber security and information operation issues, where as bigger change can be seen in reports from the Ministry of the Interior. It could be argued, that the cyber security and information operations have moved from being an issue for the military, Ministry of Foreign Affairs and security officials towards the Ministry of the Interior, civilians and security of the individuals. Underneath a visualisation of the Foreign and Security Policy reports between 2012 and 2020 situated in Daase's Extended Security framework.

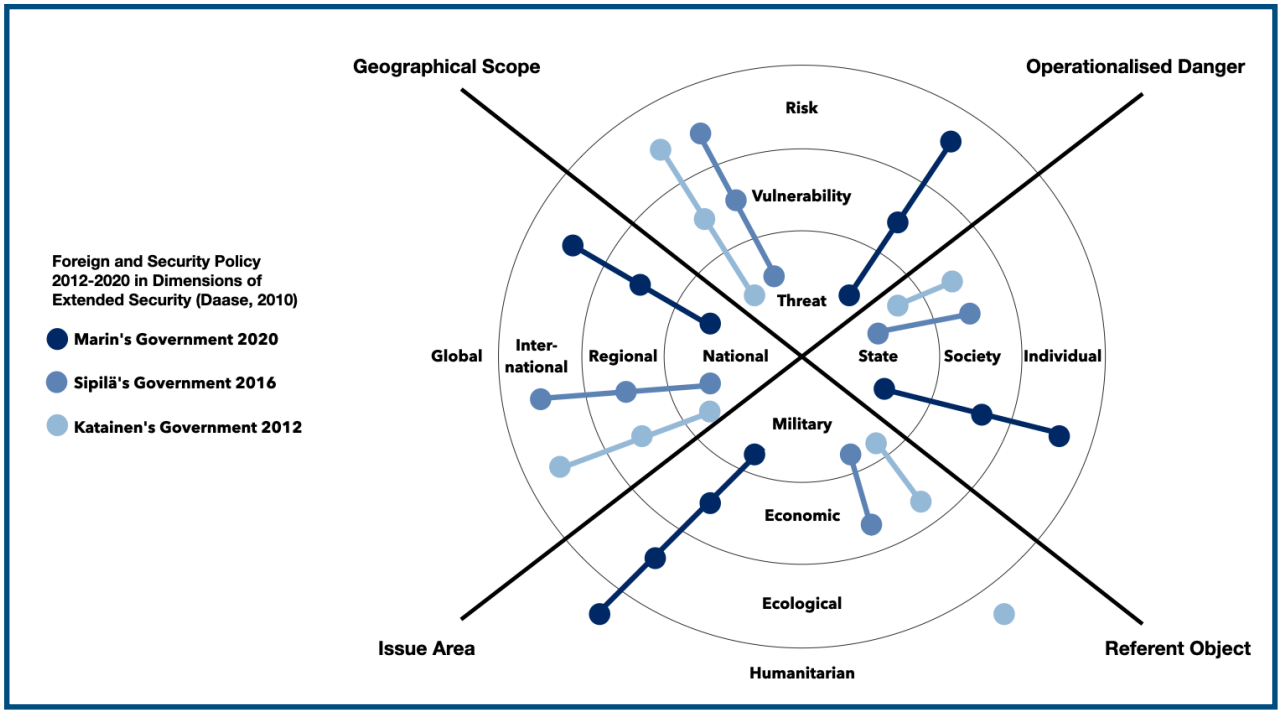

Figure 6: The Report on Foreign and Security Policy 2012-2020 in Dimensions of Extended Security by Daase (2010)

8. Policies into Political Elite Dimension and Civilian Dimension

In the following, the reports are further analysed through the actual policies that the Finnish government has laid out in order to tackle the threat of information operations and related issues such as influencing elections, disinformation and cyber attacks. As elaborated before, the policies are categorised according to their aims of involving the two groups: the political elite and military or the civilians and the public in general. In the following separate sections of each government, both Reports on Foreign and Security Policy and National Risk Assessment are discussed from each year. The policies are elaborated in full sentences and categorised further in the Appendix: 11.1 Katainen's Government, 11.2 Sipilä's Government and 11.3 Marin's government.

8.1 2012 Katainen's Government

8.1.1 Political Elite and Military Dimensions

As the model of extended security dimensions above suggests, Katainen's government and the reports from 2012 present quite a narrow concepts about the security threat that information operations pose. In 2012, the Ukrainian crisis has not happened yet and therefore the threats are not as clear, as compared to the 2020 reports. As mentioned before, the Internal Security Assessment from Katainen's government does not discuss information operations, or any related terms of influencing, cyber security or hybrid operations. The report on Foreign and Security Policy gives a wider outlook on information operations as well as connected issues in the cyber environment. The new warfare is seen developing with asymmetric tactics that are can be political-, economic- and military pressure, information- and cyber warfare or the combinations of them. The warfare can start during the time of peace with different pressure- and information operations and the line between political influencing and warfare is blurring. In 2012, the vulnerabilities of information technology are connected with difficulties of predictability and that in order to better predictability, situational picture, intelligence, analysis and further development are needed to reduce the uncertainties. The policies and also the risk analysis regarding information operations and cyber environment focuses highly on the political elite and military dimension. Government sees that the defence systems and demands for development are often focused on the military: surveillance, intelligence, cyber abilities of the defence forces and the making of the comprehensive national cyber security strategy that gives a starting point for the Finnish actors involved. Cyber security is seen to be creating diving lines and conflict inside the international community in terms of economic and security interests and different understanding of human rights and state's role in individuals rights. The cooperation is done within the EU, NATO, OECD, the UN and amongst different groups of countries. Importance of international regulation and policies for the global, common operating environments of sea, air, space and the human created cyber space is emphasised. In

2012, Finland supports the creation of Nordic knowledge network that would be responsible for countermeasures and retaliation against targeted cyber attacks in the Nordics. For the future, the government sees that the nature of conflicts are changing and safeguarding the civilians and civil society will become more challenging and that the focal point for the information society will need immediate actions to securing the cyber operating environment.

8.1.2 Civilian Dimension

Katainen's government tends to be vague on the policies and concrete actions which are addressing the civilians. Government acknowledges that the influence in the information- and cyber space are targeted towards the society as a whole, not just the military and defence forces. The threats in cyber space have developed to have dangerous effects for the whole society and that safeguarding civilians will become harder. However, no policies regarding the civilians are suggested and the focus of policies and overall threat assessment revolves around the defence capabilities and political elite who are developing security strategies for cyber space.

8.2 2016 Sipilä's Government

8.2.1 Political Elite and Military Dimensions

From the report before, Sipilä's government in 2016 has developed in terms of understanding the threat environment and the potential reach to not only the narrow though of military and decision-makers but also broader considerations of public opinion, infrastructure and economy/enterprises. By the time both of the reports were published, the Crimean annexation in 2014 had just happened and it has potentially sparked the interest of also the Ministry of the Interior. In the former government, Ministry of the Interior lacked any information about the issues in cyber space, however, the same report from 2016 is quite extensive on the issue and also addresses it many times: *"The situation in Ukraine, which escalated in early 2014, serves as an example of a crisis in which political, economic and military as well as special forces and, especially, information operations are used"* (Ministry of the Interior, 2015:27). The shift from complete lack of information in 2012 to these reports in 2016 shows, that a critical event has taken place and the Finnish state sees a vulnerability which now requires more attention than before. In terms of policy suggestions however, the main focus follows the 2012 framework of concentrating on the political elite and military dimensions. In addition to the vulnerabilities of political elite and military capabilities, also the critical infrastructure and IT systems that the society is relying on, data banks and services, are considered to be potentially vulnerable for attacks. The shift indicates that the attacks are moving into the civilian sphere in cyber matters, not necessarily towards civilians themselves but to the services that the society and individuals rely on. For cooperation within the cyber defence, the Foreign and Security Policy report discusses Finnish participation with the NATO operational, training and exercise planning. As a Member State of European Union, Finland wants to strengthen capacities to counter hybrid

influencing and improve cyber security with a joint EU effort to establish a centre of excellence with a focus on hybrid threats. With the efforts internationally with the EU, NATO and other bilateral cooperations Finland aims at "*seizing some of the lucrative prospects offered by the cyber domain and digitalisation*" (Gov, 2016:26). Due to the long history with Russia, the Crimean annexation and Russian goal of a "*sphere-of-influence-based security regime*", the government notes that Finland must monitor the developing military capabilities and aspirations of actors, in particular in the immediate surroundings i.e. Russia. By 2016, Finland has established information and cyber security programmes and development projects such as the Cyber Security Strategy and its national implementation programme. With the program, the situational picture of cyber issues have improved and cyber expertise, cooperation with different societal actors and awareness have been improved. The government also discusses the difficulty and challenges that private industry owning most parts of critical infrastructure pose in for example legislation process. Companies and private sector follow own commercial logic and those create challenges in preparedness for cyber attacks and that legislation cannot be approached uniformly rather according to sector-specifics.

8.2.2 Civilian Dimension

Compared to the former government, Sipilä's government have developed in their considerations of the cyber threats posed for the civilians and the society in general. However, the actual policies are still quite vague and addressing mostly the services and systems civilians use, such as ICT, banking and data transfer. Crimes in cyber environment are acknowledged to possible "*lower the confidence citizens and companies have in the cyber domain*" (Ministry of the Interior, 2015:16) but not for example towards public authorities. The threat assessment of cyber attacks and information operations are evaluated to have serious impacts on the society and society's crisis resilience, though the pressure period is seen to have marginal or non-existent impact on the people and the environment. In terms of economic harm, the impact from interference, obstructing or restricting for example trade is noted to cause harm, however, mentioned in terms of losses of "*tens or even hundreds of millions of euros*". Finland is interdependent of the global economy and technological advancements that make the society vulnerable: *"It is possible to influence the whole society through the cyber domain, which examples both at home and abroad have substantiated in recent years"* (Ibid:16). The government notes that the offensive cyber capabilities of other states and potential threats on the Finnish society demand preparedness, "*one way or another*" (Ibid). Compared to the 2012 reports, the threat environment seems wider and the policies needed for the civilians are considered, however not in very concrete terms. The potential threats are addressed towards the services that society uses and depend on and they are pointed to effect crisis resilience if obstructed.

8.3 2020 - Marin's Government

8.3.1 Political Elite and Military Dimensions

A clear evolution of the policies and threat assessment since 2012 and 2016 can be seen in the latest versions of the current government reports regarding cyber environment and information operations. As the dimensions of extended security suggested, the 2020 reports of Internal Risk Assessment and the Report of Foreign and Security Policy consider the threat environment with the broadest sense and affecting view of who actually needs safeguarding in the cyber environment: *"Finland examines security from a wide perspective that observes not only the military threats, competition between great powers and hybrid influencing, but also the impacts of the global challenges in sight, such as climate change, health threats, human rights violations, migration, economic crises...Many of the global phenomena affecting security are characterised by their ever closer interconnectedness"* (Gov, 2020:25). The similar logic also goes within the descriptions of violations in the cyber domain. The two reports address information operations in different ways: Ministry of the Internal differentiates information operations from information warfare due to information operations being a broader concept and covering the influencing efforts during normal, peaceful conditions. The Report on Foreign and Security Policy discusses hybrid influencing and threats which are inclusive of the use of information for hostile acts. For the policy categorisation and analysis, information operations and hybrid influencing are linked together due to their similarity in terms of policy proposals and for having information as one of the key tools of obstruction.

Reports discuss widely the challenges that different information and influence operations pose for the Western democracy as a whole due to for example manipulating and spreading rumours which question the trustworthiness and legitimacy of elections. Ministry of the Interior analyses that intervening in spread of false information poses challenges legislatively due to the freedom of speech guarantee, for which everyone has the right to voice their personal opinions. In practise, for example supporting candidates or parties during elections through fake social media accounts is not criminalised. In this matter, especially social media is seen as one of the avenues of influencing with different cyber attacks. In social media, both trust in the police and authorities can be systematically doubted and the information operations aim to hinder or complicate the operations of authorities by influencing legislation. The hostile influencing and information operations can come from either foreign actors but in addition from Finnish origin. The authorities are analysed to have difficulties of detecting such efforts and the conclusions are reached relatively late. Ministry of the Interior suggests that a faster identification process of detecting fake news and increasing information flow demands sufficient resources and 24-hour monitoring. They acknowledge that the process can be helped with technology to a certain point, but to understand the situational picture and measures, a deliberation by the authorities is needed. The authorities involved need to be trained and swift collaboration with between different authorities should be promoted. The ministry includes not only

safeguarding the decision-makers, but also their close ones from "*pressuring, threatening and physical threats*" with bettering their physical security and training among other measures (Ministry of the Interior, 2019:26). In order to prevent information operations and hybrid influencing, the Ministry of the Interior sees international and especially EU-wide collaboration important and helpful for sharing experiences that other comparable countries have with information operations and sharing their best practices combating the hostile operations.

The Report on Finnish Foreign and Security Policy regards the cyber security issues as a salient topic of wide international debate and that solutions are sought to manage the risks and reducing dependencies. Government recognises that technological development in the field of digitalisation, artificial intelligence, machine autonomy, sensor technologies and the environment they are operated in has an impact on all the areas of national defence which demand and create opportunities for development in defence capability. The opportunities in practise can support decision-making with gathering accurate data faster than before. However, the technological developments also pose potential threats from the comprehensive security perspective and constant anticipation and preparedness is therefore required. The Foreign and Security Policy report supports the EU and NATO cooperation which benefits both and complements each other in the areas of hybrid and cyber matters, and issues related to digitalisation and disruptive technologies (artificial intelligence). Finland supports the development of EU responding to hostile cyber activities with for example sanctions and demands the EU to continue the development for adopting uniform approach to cyber security which the Member States should "*effectively execute the jointly agreed measures*" (Gov, 2020:40). In addition to the cooperation between the EU and NATO and Finland and the EU, the Finnish government has established The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) which is based in Helsinki. Hybrid CoE is seen as important cooperation platform which supports the EU, NATO and Hybrid CoE member states for finding ways for countering hybrid threats. Cooperation in the EU and in the international level is seen as helping Finland finding a framework for the Finnish activities and contributing to create situational picture, detect and understand hybrid threats and create shared resilience whilst enhancing unity in terms of security and reactiveness to hybrid measures.

The new operating environment demands developing cyber defence as well as data defence in order to rectify false information and guarantee integrity of data. Finland emphasises the importance of trust, which includes both the suppliers of hardware and the stakeholders providing them. Another new aspect in terms of policy proposals and actions against information and hybrid operations Finland has laid out in 2020, is the action of publicly attributing hostile cyber activities. Public attribution is not explained further in the government policy report, however more information can me found from other sources. Finland has joined multiple countries in their willingness to publicly announce the views on the international laws governing cyber operations and publicly attributing the hostile actors behind them together with the other countries (Schmitt, 2020; Ministry for Foreign Affairs, 2020).

8.3.2 Civilian Dimension

The policies especially towards the civilians in the Finnish society have developed broadly from 2012 to the latest reports. Whereas mentions of information operations were completely missing from 2012 National Risk Assessment, in 2019 information operations had its own chapter exploring the term, who is it effecting and what should be done. In the Report of Foreign and Security Policy, the terminology have shifted slightly and hybrid influencing, threats and actions have gained saliency. The term "*hybrid*" is inclusive to different methods employed to influence through diplomatic, economic and military methods, but also through *information and cyber influence* (Gov, 2020:14). The government discusses the threat of information and hybrid operations towards civilians extensively in the current government reports. The threat environment is seen broadly, where in the global communication environment "*it is possible to reach out to larger masses of people than ever before in real time and influence the public opinion*" (Ministry of the Interior, 2019:23). The influencing systematically stirs the public debate and challenges the boundaries between truths and lies. The operations are seen to weaken operating capacity of the society and the trust that the society has for the Finnish authorities and government. The aim of influencing can be to decrease citizens' trust towards decision-makers and for example legitimacy of elections. A typical aim for example of information operations can be influencing elections or effect the voting of individuals.

An important difference of the older reports and the latest one, is the acknowledgement of the danger of outsiders destroying the national story of a sovereign state and questioning the existence of the nation. The nation's unity and identity is based on commonly recognised history and "*the story about who we are*" (Ministry of the Interior, 2019:24). The tactics such as this, were used in the Crimean annexation where the Russian information campaigns were challenging the territory belonging to Ukraine and confusing the rest of the world with their own (Russian) narrative. For such operations, the government sees important to combat information operations that challenge the native story with a strong national story that is based in truth, a high level of education, media criticality and efforts to correct lies systematically. These actions create strong societal structures in which disinformation and manipulation has a harder time spreading and influencing larger masses of people. Without actions on education, media criticality and having a strong national story, hate speech and disinformation can threaten to polarise the national value base and overall trust in the society. However, the efforts to correct lies systematically pose challenges: correcting false information does not automatically mean that already disseminated disinformation and the possible damage it has caused can be mitigated. In addition, information operations that are created to cause emotional responses spread fast and perceptions emerge quickly.

Government acknowledges the importance of the Finnish media in the matter. Media can be one of the key targets of influencing due to its channels and reach of spreading information to large masses as well as journalists being pressured and threatened and as result can lead to silencing them or being more careful on topics that are harming the hostile actor. The famous case in Finland was the journalist Jessikka Aro, who made

extensive research on the Russian troll factories and ended herself being target of massive information campaigns. The case resulted by her moving out of the country to be safe, as the Finnish Security Intelligence Service suggested (Aro, 2015). The government notes that trusted domestic media content is highly important when disruptions and information operations increase. Citizens' should have free access to information that is trustworthy, independent and Finnish content plays an important role in that. Media is under fierce transformation and the Finnish media is also competing with international media. Media companies are receiving less financial support and it poses a challenge when especially the importance of source critique is increasing. In terms of policies, Finland wants to support diverse medias that are committed to good journalistic practises which can expose false information for the citizens. Safeguarding the operations of Finnish broadcasting company YLE is one of the key policy actions. In addition to supporting Finnish media, also education and investments of citizen's media literacy is needed. In the education field, the government notes that teachers and the total education system has a key role in improving citizens skills and resources for "*identifying and assessing the trustworthiness and relevance of information*" (Ministry of the Interior, 2019:26).

In the Foreign and Security Policy report, hybrid methods are discussed widely which are inclusive of information operations. Finland sees for example NATO as important partner in intensifying cooperation in civilian readiness and security of supply in the cyber defence and countering hybrid threats. Finland's goal is to have an open, free and safe cyber environment where also considerations of ethics, privacy protection and freedom of speech issues are included. The government looks at the security from a wide perspective which does not only focus on immediate military threats, great power competition and hybrid influencing but also issues of climate change, human rights violations, migration and economic crisis. The global phenomenas are closely interconnected and affect national security from different fronts. For such security issues, civilians crisis resilience needs to be strengthened with wide-ranging actions to safeguard from threats effecting society's well being and security (Gov, 2020). The government has implemented actions of joint preparedness, planning, training and executing in accordance to the principles of comprehensive security which secure important functions of society by cooperation between various stakeholders.

Both of the reports address the importance of the national story and our own narrative. Foreign and Security Policy report notes that hybrid influencing can be practised "*under the guise of, for example, migration, and different crisis situations or reinterpretations of history.*" (Gov, 2020:35). Reports emphasise, that dividing lines should not emerge in the Finnish society that hostile, external actors could exploit in employing information operations. In addition, external actors should not be able to create new dividing lines in the society by for example deliberatively manipulating social debate and reinterpreting the Finnish history (Ministry of the Interior, 2018).

8.4 Summary of the Policy Analysis

From 2012 to 2020, a clear development of the policies can be seen. Similar to the discussions among the international scholars and national security professionals, Finland is arguably following the similar logic of expanding policy measures from safeguarding the political elite and military towards the civilians, civil society and the private industry. The overall security environment showed signs of extended security (chapter 7) and the policies expectedly correspond to the logic of increasing number of policies which are addressing the issues among individuals and the people who do not belong to the political elite or the military. Out of the two reports from 2012, only the Report on Foreign and Security addressed information operations and cyber related issues. The policies focused on the political elite and the military and suggested policies to build better cyber capabilities for the defence forces, a Nordic network of expertise, further international cooperations to respond to cyber threats and creation of a Finnish governmental cyber coordination central which would operate between all sectors of the government. The connection between cyber security matters and civilians was shortly established and vague. Katainen's government acknowledges the issue of cyber attacks for civilians, but no actual policy plans were given. (Appendix 11.3)

In 2016, the policy proposals for improving cyber security and tackling information operations have increased, especially the policies among the political elite and the military. Sipilä's government addresses the issue on both of the reports, unlike Katainen's government. Policies suggested are focused on the political elite and military dimensions by suggesting strengthened capacity to identify hybrid influencing, proposal to establish a centre of excellence focusing on hybrid threats, cooperation with the EU and NATO, implementation of cyber security programmes, intersectoral cooperation between responsible authoritative bodies, legislative measures and higher readiness of the military defence. Sipilä's government addresses linkages between the civilians and cyber threats, however, policies are not established or proposed and Sipilä's government notes that the Finnish society demands preparedness for potential threats "*one way or another*" (Ministry of the Interior, 2015:16). (Appendix 11.2)

In 2020, a clear increase and development of the policies addressing the civilian dimension is seen. Both reports discuss cyber threats and information operations widely, and National Risk Assessment has an own chapter which elaborates broadly on the issue of information operations. The political elite, military and civilian dimensions are widely connected and the government recognises that collaboration between different authorities and civil society actors is needed to tackle the challenges. The policies proposed for the political elite and military are similar to the former governments: cooperation with the EU and NATO, national legislation and preparedness, development of defence capabilities to support decision-making and sufficient resources for monitoring. The added policies in 2020 are also the Finnish determination of building not only cyber defence, but also data defence, respond to hostile activities with public attribution and joint measures (sanctions) with the EU and also safeguard decision-makers from pressuring, threatening and physical threats with enhanced security and training. For the civilian dimension, the government has laid out multiple

policy proposals to secure individuals outside of the political elite and military. The policies in the civilian dimensions are "softer" measures such as strengthening Finnish unity and national story, a high level of education, media criticality, supporting Finnish trustworthy media and commitment to good journalistic practise, making Finnish content available for citizens, increase investments in citizens' media literacy and safeguarding also the close contacts of the decision-makers from pressure and threatening with enhanced security and training. (Appendix, 11.1)

The results correspond to the initial hypothesis that the Finnish policies have developed and moved from focusing on the political elite and military towards the civilians. The results show that Finnish government has started regarding the "softer" policy measures increasingly and focus has shifted from military intelligence development towards citizens' education, media criticality, unity and reinforcement of common story and shared history.

9. Conclusion

To conclude the study, the research questions will be discussed and how the results reflect the initial hypothesis with the constructed theoretical model. The research hypothesis was that the Finnish government has increasingly started considering information operations and issues in the cyber environment as a threat for the national security, notably due to the Crimean annexation in 2014. It was expected, that from 2012 to 2020, the situational picture has evolved in comprehending the threat environment from a narrower perspective (military/state/national) to the broader (humanitarian/individual/global) perspective. The development of policies was expected to follow the similar logic, where the policies were increasingly involving civilians, civil society and the private sector, instead of the political elite and the military. The dimensions and the inspiration for the core theoretical model was established based on the initial patterns found in the research about cyber threats and information- and influence operations. In the international and Finnish discussions in the cyber security field, the focus was seemingly moving from a narrower intelligence, territorial and governmental discussions towards education, strengthening citizen's media criticality and reinforcing cooperation between governments and civilian actors. Cooperation is emphasised by many Finnish as well as international actors to find solutions for legislation and norms for cyber space and countermeasures towards information operations.

9.1 Research Questions

The research was guided by a question of solving how has the Finnish threat environment and policies regarding information operations and cyber security developed between 2012 and 2020. The first part focused on defining information operations and connecting the research with the Finnish outlook on the issue at hand. From there, relevant further questions were constructed with the theoretical model on how to study the Finnish governmental reports.

RQ2: Has the Finnish national security moved from the narrow security considerations of the state, military and national dimension to a broader considerations of individuals, humanitarian and global dimensions in terms of information operations and cyber security?

Two sets of methods were employed to first gain an overall idea of the Finnish governmental discussion on information operations, cyber security and related issues of hybrid warfare, disinformation, trolling and cyber threats. Starting with the key word search, a pattern could be established. However, the key word search does not indicate the context but gives an idea of saliency between the governments regarding the issue. From there the analysis of the Finnish national security was done according to Daase's framework for Dimensions of Extended Security (2010). The framework aims to indicate changes in the political discourse, explain changes in political practises and generally

the changes in the international society. In the area of cyber security and information operations, change could be seen between 2012 and 2020 and the changes signal political transformations, (Skinner, 1969) changing beliefs, values and practises of institutions (Daase, 2009). The framework include dimensions of reference, issue, spatial and danger, which reflect arguably the year 2010 when the framework was modelled. However, when used for the cyber matters and information operations, the model posed difficulties of situating the safeguarding of the cyber domain. Therefore, it would be suggested for the model to be updated and include cyber as one of the elements to correspond the changes in the threat environment and evermore extending national security considerations - especially in online spaces.

The Finnish national security and the considerations of whom and what should be safeguarded showed signs of broadening. From 2012 to 2020, most dimensions were expanded from the state and military considerations into more global, individual and humanitarian considerations. The objects of safeguarding are not just the national territories and military capabilities, but more the humanitarian aspects of safeguarding and advancing individual freedoms and fulfilment. Formerly, the narrow national security has focused on national survival of the states and communities and now, the broader national security take into account also human, economic and global, internal and external factors (Daase, 2010). The security considerations in the cyber-sphere seem to follow the similar logic in the Finnish governmental discussion - the threat has moved from narrow militaristic and governmental discussions into the civilian discussions over the studied time-series. From 2012, only the Report on Foreign and Security Policy addressed cyber related threats, considering military, economy, and the state in a need for safeguarding, understood the threat by Russian's developing military capabilities and that the Finnish military capabilities should be developed in order to mitigate the possible vulnerabilities. In 2016, the impact of the Crimean annexation in 2014 can be seen. Both reports from the Ministry of the Interior and the Ministry of Foreign Affairs address cyber threats and information operations and the dimensions of security have broadened in many areas for example in terms of geography. Lastly, as expected, the reports from the current government are the most extensive in terms of information operations and other cyber related matters. In the National Risk Assessment (2018), information operations are addressed in its own chapter describing the phenomena, who are involved and what effects do the hostile actors intend achieving.

The framework and theory behind the extended dimensions of security therefore *corresponds* well with the Finnish case. Even though some aspects, such as the operationalised danger dimension, are hard to pinpoint from the texts since the considerations of vulnerabilities, threats and risks might vary between Daase and the Finnish governments. However, signs of the extended considerations can be seen and the logic of expanded security also fits with cyber threats and information operations.

RQ3: What specific policies have the Finnish government laid out to the civilian and political elite dimensions?

When starting the background research for the topic, discussions pointed out the question of who are involved in the cyber security matters and information operations. In the different discussions, information operations and secure cyber environments have moved towards securing civilians and how civilians are used as objects of hostile operations, without their knowledge, understanding or consent. The civilian society in the Internet and social media platforms are the primary avenues of influencing larger behaviour and opinions by hostile actors who have their own incentives of creating information campaigns through trolling, disinformation, bots and manipulation. Therefore, the civilians have become extensions of foreign or domestic disruptive operations which might cause further polarisation, confusion, disrupt elections, harm the open, public debates and effect the Western democracies as we know them. Therefore, the research question three was formed to understand what Finland has done and is planning to do and whether the policies are moving from the militaristic and state-centric considerations towards the civilians as the international discussion on the topic suggests. Two dimensions were elaborated further based on Daase's Referent Object dimension to categorise the policies found in the reports: 1) The Political Elite and Military and 2) Civilians. The understanding of the dimensions collaboration was expanded by notes from scholars and professionals in the field. Close collaboration between different actors in the society are highly proposed and important in tackling information operations by setting up the norms in global online spaces. One can not act without the other: the governments have the legislative power, however, behaviour and issues in the platforms are in the hands of the civilians and the private sector. The private sector incentives pose challenges to the governmental legislative processes often due to monetary reasons and their own logic of providing platforms and services for everyone - even anonymous actors, wanting to distort conversations by creating dark ads and trolling campaigns.

The results and development of the Finnish policies over the studied time period matched the expectations and the initial hypothesis. In 2012, the policy proposals are very limited. Information operations were not as salient as currently and therefore information operations were often linked to cyber attacks regarding for example infrastructure and military intelligence. In terms of policies, Katainen's government in 2012 suggested development of situational picture, intelligence and analysis in order to improve predictability and defence surveillance. In addition Katainen's government analysed that cyber abilities demand improvement along with the creation of comprehensive national cyber security strategy. Regarding the civilians, the connections between information operations and civilians were vague without no concrete actions towards securing civilians. Overall focus in 2012 is on the defence capabilities and collaboration between different states.

In 2016, the clear development is seen in both categories and policies towards the political elite, military and civilians. The government discusses the Finnish collaboration widely with NATO and the EU and Finland's initiative of setting up a centre of excellence focused solely on hybrid threats. Unlike before, Sipilä's government acknowledges that information operations and cyber attacks have effects on the public opinion, as well as infrastructure, economy and enterprises. However, in terms of the policies, government discusses the services and infrastructures that civilians are relying on and securing them (ICT, banking and data transfer) and does not expand to further policies of securing for example journalists and the media, educating civilians and strengthening the national story, as the government policies in 2020 do. The government sees the potential threats on the Finnish society and wants to improve preparedness "*one way or another*" (Ministry of the Interior, 2015:16). Compared to 2012, threat environment and policies have broadened and expanded onto the civilian sphere, however, the policies are not directed towards the civilians and more towards the services they use and are reliant on.

The 2020 reports from the current Marin's government, as expected, are the most developed and extensive when it comes to information operations and threats in the cyber space and policies for securing civilians. Unlike formerly, the National Risk Assessment has its own chapter for information operations and they are discussed widely with suggestions of policies meaning to secure individuals, the Finnish society and the Western democracy. The 2020 policies tackle information operations from different angles and views: the Finnish broadcast media, supporting good journalistic practise, protect decision-makers and their close-ones from pressure campaigns, educating critical media reading and spotting disinformation online and strengthening the Finnish national story, unity and identity. Especially the teachers are seen to have the key role in informing and educating citizens with skills to identify trustworthy and relevant information from dis/misinformation. The government wants to enforce and strengthen media literacy as well as the Finnish national story and narrative, which prevents the possible creation of dividing lines in the society by manipulating open debates or reinterpreting the Finnish history.

The policies in 2020 also address the demands in the political elite and military, where they want to better the identification processes and apply resources to 24-hour monitoring online. The close cooperation of authorities are required for having a better understanding of the situational picture and measures taken. The government wants close cooperation with the EU Member States and the international community by sharing experiences and best practises countering hostile information operations. Finland has joined the group of countries, who are willing to publicly announce views on international laws which would govern the cyber domain. In addition, the Finnish government states that they support the EU's use of sanctions, demand uniform approach from the EU Member States and Finland is willing to publicly attribute hostile actors behind information operations online together with coalition of different countries.

9.2 Looking Forward

Within the international community, Finland has been noted as the one of the front runners in tackling information operations and creating effective measures to secure the cyber spaces from hostile actors creating wider harm in the Finnish society. The Vastaamo data-hack scandal at the end of 2020 will arguably boost further measures securing infrastructure, services civilians use and will increase the demand for actions in reinforcing the crisis resilience strategies for the future possible crisis situations created either by domestic or foreign hostile actors. As a country with a good reputation on cyber matters, Finland has opportunities to create norms and be an advocate in the global level of how to tackle information operations and secure open, public debates from disturbance, secure national elections and educate civilians on media criticality and the threats in cyber spaces. The potential opportunities in the cyber security field in the future has been noted by all the governments since 2012. As the background research suggest, the Finnish policies are moving towards the civilian dimension from the military and political dimensions and the results can be possibly comparable to other, similar countries to Finland. For the future research of information operations and actions taken to counter them, it would be highly interesting to expand the research and go deeper with the policy analysis by studying the implementation processes, effectiveness and whether the Finnish model could be scalable to other countries. The difficulty is, how can one study the effectiveness of reinforcing the national story telling, narratives and the education received at a young age and whether it applies when operating in the Internet and social media platforms?

In order to expand knowledge on the Finnish specific policy proposals and further implementation of them, further research should look into specific ministries in different areas as suggested before. The Ministry of Foreign Affairs and Ministry of the Interior provides only the bigger picture of the framework and situational picture of security environment and proposes policies to tackle issues in the national security. A further study would be interesting to see the actual implementation and costs of the given policy proposals from Ministry of Education, Ministry of Justice, Ministry of Defence and Ministry of Traffic and Communication who are mostly connected in cyber security implementation and legislation in Finland. By studying the specific ministries, better look on the actual policy implementations and programs could be found, as well as some indication of the effectiveness and expenses allocated for the purpose. However, the policies suggested by the current government will take time to be implemented and it will take time to see whether they are effective or not.

10. References

Ahvenainen, S. (2014): Verkkosodan historia ja käsitteen kehittyminen - Kriittinen, systeeminen ja kyberneettinen katsaus vuoden 2003 artikkeliin. In Kybertaistelu 2020, edited by Tuija Kuusisto. Helsinki: Maanpuolustuskorkeakoulu Taktiikan laitos. 7-32.

Alafuzoff, Gergij., Blom, Anders., Kurvinen, Mihail., Pyykkönen, Juha., Luoma-aho, Vilma., Tsetsure, Katerina. (2020): Govorit Moskva - Moskova Puhuu Venäjän Strategisen Viestinnän Erityispiirteet. Published by Valtionneuvoston Selvitys- ja Tutkimustoiminta 2020:16. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162201/VNTEAS_2020_16.pdf

Armistead, Leigh (2004): Information Operations: Warfare and the Hard Reality of Soft Power. Edited by Leigh Armistead, Produced in conjunction with the Joint Forces Staff College and the National Security Agency. 1st edition. Washington, D.C.: Brassey's.

Arquilla, John and Ronfeldt (1999): The Emergence of Noopolitik: Towards American Information Strategy. Santa Monica, CA. RAND Corporation.

Aro, Jessikka (2015): My year as a pro-Russian troll-magnet: International shaming campaign and an SMS from dead father. Kioski, Yle. Retrieved 22/03/2021: https://kioski.yle.fi/omat/my-year-as-a-pro-russia-troll-magnet

Aro, Jessikka (2016): The Cyberspace War: Propaganda and Trolling as Warfare Tools. European View. SAGE Journals.

Aro (2019) in CNN Special Report: Finland is winning the war on fake news. What it's learned may be crucial to Western democracy. Written by Mackintosh, Eliza. Accessed 13/3/2021: https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/

Barsotti, Scott (2018): Weaponizing Social Media: Heinz Experts on Troll Farms and Fake News. Carnegie Mellon University. Heinz College. Retrieved 22/3/2021: https://www.heinz.cmu.edu/media/2018/October/troll-farms-and-fake-news-social-media-weaponization

Beitz, Charles (1979): Political Theory and International Relations. Princeton: Princeton University Press.

Bergh, Arild (2019): Social Network Centric Warfare - Understanding Influence Operations in Social Media. Published by Norwegian Defence Research Establishment (FFI).

Bjola, Corneliu (2019): The 'dark side' of digital diplomacy: countering disinformation and propaganda. ARI 5/2019. Elcano Royal Institute.

Bodgan, R., and S.J. Taylor (1975): Introduction to qualitative research methods. New York. John Wiley.

Cambridge Dictionary (2021): Elite. Retrieved 3/4/3021: https://dictionary.cambridge.org/dictionary/english/elite

Cambridge Dictionary, 2021a: Civilian. Retrieved 3/4/2021: https://dictionary.cambridge.org/dictionary/english/civilian

Centre for Excellence for National Security (2015): Cybersecurity: Emerging Issues, Trends, Technologies & Threats in 2015 and Beyond. Conference Report, Singapore July 2015.

City of Helsinki (2018): Helsinki in the ear of hybrid threats - Hybrid influencing and the city. Publications of the Central Administration 2012:22.

Cohen, Raymond (1979): Threat Perception in International Crisis. Milwaukee: University of Wisconsin Press.

Cull, Nicholas J., (2008): Public Diplomacy: Taxonomies and Histories. The Annals of the American Academy of Political and Social Science, Vol. 616, Public Diplomacy in a Changing World. 31-54.

Cull, Nicholas J., (2008a): The Cold War and the United States Information Agency: American propaganda and public diplomacy, 1945-1989. New York: Cambridge University Press.

Daase, Christopher (2002): Internationale Risikopolit. Ein Forschungsprogramm für den sicherheitspolitischen Paradigmenwechsel. In Internationale Risikopolitik,

edited by Christopher Daase, Susanne Feske and Ingo Peters. 9-35. Baden-Baden: Nomos.

Daase, Christopher and Kessler, Oliver (2007): Knowns and Unknowns in the War on Terror. Uncertainty and the Political Construction of Danger. Security Dialogue 38, no. 4, 411-436.

Daase, Christopher (2009). "Der Erweiterte Sicherheitsbegriff." In Internationale Politik als Überlebensstrategie, edited by Mir A. Ferdowsi, 137-153. München: Bayerische Landeszentrale für politische Bildung.

Daase, Christopher (2010): National, societal and human security: on the transformation of political language. Historical Social Research, 35(4), 22-37.

DDV (2020): Digihumaus 2020. Näkökulmia 2020-luvulle digitalisaation hyödyntämiseksi yhteiskunnassa. Digi- ja Väestötietovirasto. https://dvv.fi/documents/16079645/17691137/Digihumaus-2020-raportti_VERKKO.pdf/18f8adbc-a1d7-08a0-845a-9bc98c8b8bfd/Digihumaus-2020-raportti_VERKKO.pdf

Deibert, Ron (2011): Towards a Cyber Security strategy for global civil society? Global Information Society Watch 2011. Internet Rights and Democratisation. The Canada Centre for Global Security Studies and the Citizen Lab, Munk School of Global Affairs, University of Toronto. 23-26.

DOD (2021): Joint Publication (JP) 1-02, The Department of Defence Dictionary of Military and Associated Terms January 2021.

Doob, Leonard W., and Robinson, Edward,S. (1935): Psychology and Propaganda. The Annals of the American Academy of Political and Social Science, Vol, 179, 88-95.

Erbschloe, Michael (2017): Social Media Warfare: Equal Weapons for All. Auerback Publications.

Falk, Barbara J. (2020): Strategic Citizens: Civil Society as a Battlespace in The Era of Hybrid Threats. Hybrid CoE Strategic Analysis 25, 2020.

Finnish Security and Intelligence Service (2020): Supo identified the cyber espionage operation against the parliament as APT31. Press Release 18/3/2021.

Retrieved 8/5/2021: https://supo.fi/en/-/supo-identified-the-cyber-espionage-operation-against-the-parliament-as-apt31

Gilboa, E. (2008). Searching for a theory of public diplomacy. The ANNALS of the American Academy of Political and Social Science, 616(1), 55–77.

Giles, Keir (2016): The Next Phase of Russian Information Warfare. Nato Strategic Communications Centre of Excellence

Gerring, John (2004): What Is a Case Study and What Is It Good for? The American Political Science Review. Vol 98, No.2. American Political Science Association. 341-354.

Gerring, John (2007): Case Study Research. Principles and Practices. Cambridge University Press. New York, USA.

Goolsby, R. (2019): Developing a New Approach to Cyber Diplomacy: Addressing Malign Information Maneuvres in Cyberspace. Senior Leadership Roundtable on Military and Defence Aspects of Border Security in South East Europe, 141, 105.

Gov (2012): Suomen turvallisuus- ja puolustuspolitiikka 2012. Valtioneuvoston selonteko. Valtioneuvoston kanslian julkaisusarja 5/2012.

Gov (2016): Government Report on the Finnish Foreign and Security Policy. Prime Minister's Office. Prime Minister's Office Publications 9/2016.

Gov (2020): Government Report on the Finnish Foreign and Security Policy. Publications of the Finnish Government 32/2020. Finnish Government, Helsinki 2020. Author: Ministry of Foreign Affairs of Finland.

Government of Canada (2020): An Introduction to the Cyber Threat Environment. Canadian Centre for Cyber Security. Accessed: https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf

Green, Joshua and Issenberg, Sasha (2016): Inside the Trump Bunker, With Days to Go. Bloomberg. Retrieved 15/3/2021: https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go

Gregory, Bruce (2008): Public Diplomacy: Sunrise of an Academic Field. The Annals of the American Academy of Political and Social Science. Vol. 616. Public Diplomacy in a Changing World. Sage Publications. 274-290.

Haftendorn, Helga., Keohane, Robert O. and Wallander, Celeste A. eds (1999): Imperfect Unions. Security Institutions over Time and Space. Oxford: Oxford University Press.

Heinl, Caitriona H. (2016): The Role of the Military in Cyber Space: Civil-military Relations and International Military Co-operation. Pointer, Journal of the Singapore Armed Forces. Vol. 42, no.4. 37-46.

Hirsch Ballin, Ernst., Dijstelbloem, Huub. and de Goede, Peter (2020): The Extension of the Concept of Security. Security in an Interconnected World. Research for Policy. Studies by the Netherlands Council for Government Policy. Springer, Cham.

Hoffman, F. (2007): Conflict in the 21st Century: The rise of the hybrid wars. Arlington: Potomac Institute for Policy Studies.

Holbrooke, R. (2001). Get the message out. Washington Post, B7.

Illarionov, A. (2014): Challenges of (dis)information war for liberal democratic regime and on possible counter-strategy. XIX Open Society Forum: Soft Power. Tallinn.

Jakubowski, Glenda (2019): What's Not to Like? Social Media as Information Operations Force Multiplier. Joint Force Quarterly Issue 94, 3rd Quarter 2019. Published by National Defence University Press.

Janda, Jakub. (2018): How to boost the Western response to Russian hostile influence operations. European View 17(2). 181-188.

Jayamaha, Buddhika B. and Matisek, Jahara. (2019): Social Media Warriors: Leveraging a New Battlespace. Journal of the US Army War College. 48(4). 11-24.

Jowett, G. S., & O'Donnell, V. (2012). Propaganda and Persuasion (5th ed.). London: Sage.

Karlsen, Geir Hågen (2019): Divide and rule: ten lessons about Russian political activities in Europe. Palgrave Communications Vol 5, No. 19.

Knorr, Klaus (1976): Threat Perception. In Historical Dimensions of National Security Problems, edited by Klaus Knorr. Lawrence: University Press of Kansas.

Koselleck, Reinhart. (1985): Futures Past: On the Semantics of Historical Time. Translated by Keith Tribe. Cambridge: MIT Press.

Kugler, Richard L. (2006): Policy Analysis In National Security Affairs: New Methods for a New Era. Center for Technology and Security Policy. National Defence University Press. Washington D.C.

Lasswell, Harold D. (1927): The Theory of Political Propaganda. The American Political Science Review Vol. 21:3. American Political Science Association.

Lasswell, Harold (1961): In Agenda for the Study of Political Elites. Ed. Dwaine Marvick. Political Decision-Makers. Glencoe: The Free Press, 66.

Lehtinen, 2020: Tuhansien ihmisten potilaskertomukset vuosivat verkkoon - Onko Vastaamo-tietojen lukeminen rikos? Retrieved 19/4/2021: https://www.hs.fi/kotimaa/art-2000006700395.html

Lehto, Martti (2014): Kybertaistelu ilmavoimaympäristössä. In Kybertaistelu 2020, edited by Tuija Kuusisto. Helsinki Maanpuolustuskorkeakoulu Taktiikan Laitos, 157-177.

Lehto, Martti and Limnéll, Jarno (2017): Kybersodankäynnin kehityksestä ja tulevaisuudesta. Tiede ja Ase, 75.

Leonard, Mark., Stead, Catherine and Smewing, Conrad (2002): Public Diplomacy. London: Foreign Policy Centre. London.

Levinson, B., Sutton, M. and Winstead, T. (2009): Educational Policy as a Practise of Power: Theoretical Tool, Ethnographic Methods, Democratic Options. Educational Policy, vol 23 no. 6.

Lexicon Dictionary (2021): Elite. Retrieved 3/4/2021: https://www.lexico.com/definition/elite

Lexicon, (2021a): Civilian. Retrieved 3/4/2021: https://www.lexico.com/definition/civilian

Mackintosh, Eliza (2019): Finland is winning the war on fake news. What it's learned may be crucial to Western democracy. CNN Special Report. Retrieved 22/03/2021: https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/

McCullagh, C. Behan (2002): Bias in Historical Description, Interpretation, and Explanation. History and Theory. Vol. 39, No.1, 39-66.

Mantila, Markku in Rosendahl and Forsell (2016): Finland sees propaganda attack from former master Russia. Reuters. Retrieved 14/3/2021: https://www.reuters.com/article/us-finland-russia-informationattacks-idUSKCN12J197

Marlin, Randal (2013): Propaganda and the Ethics of Persuasion. 2nd edition. Broadview Press.

Martin, Lisa L.. (1992): Interests, Power and Multilateralism. International Organisation 46, no. 4, 765-792.

Merimaa, Juha (2018): Hybrid influencing is a grey zone between war and peace - how to resist it? Data Science News Article 14/12/2018. University of Helsinki. Retrieved 10/5/2021: https://www2.helsinki.fi/en/news/society-economy/hybrid-influencing-is-a-grey-zone-between-war-and-peace-how-to-resist-it

Mills, C. Wright (1959): The Power Elite. New York: Oxford University Press, 3-4.

Ministry of the Finance (2019): Glimpses of the Future. Data policy, artificial intelligence and robotisation as enablers of wellbeing and economic success in Finland. Ministry of Finance 2019:22.

Ministry for Foreign Affairs (2020): Finland published its positions on public international law in cyberspace. New item published 19/10/2020. Retrieved 15/4/2021: https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace

Ministry of the Interior (2012): Turvallisempi huominen. Sisäisen turvallisuuden ohjelma. Helsinki 2012. 26/2012.

Ministry of the Interior (2016): National Risk Assessment 2015. Ministry of the Interior Publication 4/2016. Internal Security.

Ministry of the Interior (2018): National Risk Assessment 2018. Internal Security. Publications of the Ministry of the Interior 9/2019.

Ministry of the Interior (2019): National Risk Assessment 2018. Internal Security. Publications of the Ministry of the Interior 2019:9.

Murrow, Edward (1963) in Leonard, Mark (2002): Public Diplomacy. London: Foreign Policy Center.

NATO (2009): Allied Joint Doctrine For Information Operations. AJP-3.10. November, 2009. Accessed: https://info.publicintelligence.net/NATO-IO.pdf

NATO, 2020: Media - (Dis)Information - Security: Information Warfare. Retrieved 4/2/2021: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf

Pamment, James., Nothhaft, Howards., Agardh-Twetman, Henrik. & Fjällhed, Alicia. (2018): Countering Information Influence Activities: The State of the Art. Swedish Civil Contingencies Agency. Department of Strategic Communication, Lund University.

Pamment, James., Nothhaft, Howard., Twetman, Henrik and Fjällhed, Alicia (2018a): The Role of Communication in Countering the Malicious Use of Social Media. Lund University. NATO STRATCOM Coe.

Pariser, E. (2011): The filter bubble: What the Internet is hiding from you. New York: Penguin Press.

Porotsky, Sophia (2019): Analyzing Russian Information Warfare and Influence Operations. Global Security View. Retrieved 9/6/2011: https://globalsecurityreview.com/cold-war-2-0-russian-information-warfare/

Prier, Jarred. (2017): Commanding the Trend: Social Media as Information Warfare. Strategic Studies Quarterly Volume 2, Number 2.

Qiao, L & Wang, X (1999): Unrestricted Warfare. People's Liberation Army. Literature and Arts Publishing House, Beijing. In Commin, G. and Filiol, E., (2015):

Unrestricted Warfare versus Western Traditional Warfare: A Comparative Study. Journal of Information Warfare. Vol. 14, No.1. Published by Peregrine Technical Solutions.

Rajendran, NS. (2001): Dealing Bias in Qualitative Research: A Balancing Act for Researchers. Qualitative Research Convention 2001: Navigating Challenges. University of Malaya, Kuala Lumpur.

Rantapelkonen, J. (2014): Historiasta tulevaisuuteen - informaatiosodankäynnin paluu. Kylkirauta, 265(4), 15-18

Renz, Bettina and Smith, Hanna (2016): Russia and Hybrid Warfare - Going Beyond The Label. Aleksanteri Papers 1/2016. Kikimora Publications at the Aleksantari Institute, University of Helsinki, Finland.

Roberts, Geoffrey (1971): A Dictionary of Political Analysis. New York: St Martin's Press, 79.

Roberts, Walter R. (1994): The conduct of foreign policy in the information age. Speech at the Royal Institute of International Affairs, June 21st, London.

Roberts, Walter R. (2006): The Evolution of Diplomacy. Mediterranean Quarterly 17:3.

Rosendahl, Jussi and Forsell, Tuomas. (2016): Finland sees propaganda attack from former master Russia. Reuters October, 2016. Retrieved 23/3/2021: https://www.reuters.com/article/us-finland-russia-informationattacks-idUSKCN12J197

Ryan, Gery W. and Bernard, Russell (2003): Techniques to Identify Themes. Field Methods.15(1). 85-109.

Salonious-Palsternak, Charly and Limnéll, Jarmo (2015): Suomi Hybridisodankäynnin kohteena. Publication of the Finnish Institute of International Affairs 6/15. https://www.fiia.fi/wp-content/uploads/2017/01/comment6_2015suom.pdf

Savski, Kristof (2017): Policy Documents and Laws. Routledge Handbook of Language and Politics. Editors: Ruth Wodak and Bernhard Forchner. Routledge.

Schmitt, Michael (2020): Finland Sets Out Key Positions on International Cyber Law. Retrieved 15/4/2021: https://www.justsecurity.org/73061/finland-sets-out-key-positions-on-international-cyber-law/

The Security Committee (2019): Finland's Cyber Security Strategy 2019. Government Resolution 10/2019.

The Security Committee (2021): Operations and Responsibilities. Retrieved 12/5/2021: https://turvallisuuskomitea.fi/en/security-committee/

Shallcross, Nicholas (2017): Social Media & Information Operations in the 21st Century. Journal of Information Warfare Volume 16, Issue 1. Published by Peregrine Technical Solutions.

Stelter, B. (2008): Politics via the Internet spreads with new force. The International Herald Tribune.

Skinner, Quentin. (1969): Meaning and Understanding in the History of Ideas. History and Theory 8: 3–53.

Standish, Reid (2017): Why is Finland Able to Fend off Putin's Information Warfare?. Retrieved 14/3/2021: https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/

Stifel, Megan (2019): The Importance of Civil Society in the World of Cybersecurity. Global Cyber Alliance. Retrieved 10/4/2021: https://www.globalcyberalliance.org/the-importance-of-civil-society-in-the-world-of-cybersecurity/

Stone, DA. (2012): Policy paradox: the art of political decision making. 3rd edition. W.W. Norton & Co., New York.

Thakur, Ramesh and Newman, Edward (2004): Introduction: Non-traditional Security in Asia. In Broadening Asia's Security Discourse and Agenda: Political, Social and Environmental Perspectives, edited by Ramesh Thakur and Edward Newman. Tokyo: UNU Press.

Tiersma, PM. (2010): Parchment, paper, pixels: law and the technologies of communication. The University of Chicago Press, Chicago.

Vosoughi, Soroush., Roy, Deb. and Aral, Sinan. (2018): The Spread of true and false news online. Science Vol. 358, Issue 6380. 1146-1151.

Waltz, Kenneth N., (1979): Theory of International Politics. New York: Random House.

Watts, Clint (2014) Testimony: "Russia's Info War on the U.S. Started in 2014" in Jakubowski (2019): What's Not to Like? Social Media as Information Operations Force Multiplier. Joint Force Quarterly 94. National Defence University Press.

Yannakogeorgos, Panayotis A. (2016): Strategies for Resolving the Cyber Attribution Challenge. Air Force Research Institute Papers. Air University Press.
Yanow, D. (2000): Conducting interpretive policy analysis. Sage Publications. Thousand Oaks, CA.

YLE (2015): Presidentti Niinistö infosodasta: Me kaikki olemme maanpuolustajia. Written by Teemu Hallamaa, YLE. Retrieved 14/3/2021: https://yle.fi/uutiset/3-8388624

YLE (2016): US Experts gird Finnish officials for Information Warfare. Retrieved 14/3/2021: https://yle.fi/uutiset/osasto/news/us_experts_gird_finnish_officials_for_information_war/8616336

YLE (2020): Psychotherapy centre's database hacked, patient info held ransom. November, 2020. YLE. Retrieved 19/4/2021: https://yle.fi/uutiset/osasto/news/psychotherapy_centres_database_hacked_patient_info_held_ransom/11605460

11. Appendix

11.1 Appendix 1: Katainen's Government

Katainen's Government	The Political Elite and Military	Civilians, Civil Society and Private Industry
Report on Foreign and Security Policy	**The cyber capabilities of the defence forces are built** as part of the defence command system and the overall security of society.	
	A network of expertise to combat cyber attacks. **A Nordic network** of expertise should be set up to combat cyber attacks on the Nordic countries.	
	Finland's national ability to respond to cyber threats is strongly linked to **international cooperation**. The development of cyber security and the tasks associated with it are an example of the overall security challenge for **all sectors of government**.	
	In addition to the creation of situational picture, continuous prediction and monitoring processes, solutions such as establishing a governmental cyber coordination central are required.	
National Risk Assessment	-	-

11.2 Appendix 2: Sipilä's Government

Sipilä's Government	The Political Elite and Military	Civilians, Civil Society and Private Industry
Report on Foreign and Security Policy	In line with comprehensive security thinking **Finland strengthens its capacity to identify wide-ranging hybrid influencing** against society, the capabilities to counter it and to improve cyber security. As part of the EU's efforts to counter hybrid threats **Finland studies the possibilities to establish a centre of excellence which focuses on hybrid threats**.	
	The capabilities required by cyber security will be strengthened, among others, in the European Union, with NATO and bilaterally. In its international cooperation Finland aims at seizing some of the lucrative prospects offered by the cyber domain and digitalisation	
	Participation in the initial phases of NATO's operational, training, and exercise planning and cyber-defence cooperation.	
National Risk Assessment	**Finland has implemented several information and cyber security programmes and development projects**, the latest ones being the **Cyber Security Strategy and its national implementation programme.** As a result of the guidelines of the Strategy and its implementation programme, among other things, the Cyber Security Centre has been established, the integrated **situational picture has been improved and cyber expertise, awareness and cooperating among all societal actors have been improved.**	When it comes to Finland, its dependency on IT systems and, conversely, the offensive cyber capabilities of other states create the kind of potential threat on **Finnish society that demands preparedness, one way or another.**
	The management of cyber incidents is organised and carried out in accordance with the Cyber Security Strategy, following the existing sector-specific divisions of duties based on statutes and pre-agreed cooperation. T**he competent authority will be in charge and intersectoral cooperative bodies are to support the responsible authority**. At the same time, despite the disruption, the aim is to secure the maximum viability of society. **Different technical solutions can mitigate the impact of the risks.** For example, **critical services can be segregated into their own networks,** which will make it more difficult for them to be attacked.	
	In Finland critical infrastructure is for the most part owned by the private sector and companies tend to follow commercial logic, which creates a challenge for cyber security preparedness. **Legislation** does not take a uniform approach to cyber threats. Rather, legislation in this field is sector-specific.	

11.3 Appendix 3: Marin's Government

Marin's Government	The Political Elite and Military	Civilians, Civil Society and Private Industry
Report on Foreign and Security Policy	Technological development, particularly in the areas of digitalisation, AI, machine autonomy, sensor technologies and new operational environments, also has an impact on every area of national defence. It generates growing demands and creates new opportunities for the **development of defence capability, such as supporting decision-making with provision of more accurate data more rapidly than before.**	Efforts to **intensify cooperation in civilian readiness and security of supply issues**, in the fields of cyber defence and countering hybrid threats and in arms control will continue. (**NATO and Finland cooperation**)
	New technologies and changing operating environments, including cybersecurity and the growing security role of space, and the overlapping of conventional and nuclear weapon systems upset the strategic balance and **set new requirements for arms control agreements, national legislation and preparedness.**	The **crisis resilience is strengthened by means of wide-ranging preparedness** against multifaceted threats against society's well-being and security, including bu not limited to the increase and diversification of hybrid influencing, the impacts of climate change...
	The **EU-NATO cooperation** must benefit both parties and be of complementary nature. The development of the EU security and defence cooperation benefits also NATO as it enhances European security and capabilities. Particularly beneficial areas of cooperation include the hybrid and cyber matters, issues related to digitalisation and disruptive technologies, such as AI, and the promotion of military mobility.	Finland must be also prepared for hybrid influencing practised under the guise of, for example, migration, and different crisis situations or reinterpretations of history. **It must be ensured that no such internal dividing lines emerge in society that external actors could exploit. Similarly, it must be ensured that external influencing does not create new dividing lines.**
	The changes in our operating environment underscore the **need to develop not only cyber defence but also data defence**, which means wide-ranging development of methods for rectifying false information and guaranteeing integrity of data.	
	Finland is prepared for the hybrid influencing to continue and acknowledges that it is necessary to react to hybrid actions, such as hostile cyber activities, through **public attribution**.	
National Risk Assessment	The challenges faced by the authorities is that influencing efforts are often detected relatively late. Faster identification of fake news and an increasing information flow **require sufficient resources and 24-hour monitoring**. Technology may help in screening information, but the right situation picture and measures always require **careful deliberation by the authorities**. Acting in such situations should be trained, which also promotes the emergence of **swift collaboration between the authorities**.	It is necessary to be continuously prepared for information operations. Hate speech and disinformation threaten to erode the national value base and trust in the society. The **most effective ways to combat information operations are a strong national story based on the truth**, **a high level of education and media criticality as well as efforts to straighten lies systematically.** Strong structures of society make it more difficult to spread lies.
	International and in particular EU-wide collaboration is important in preventing both information operations and hybrid influencing more extensively. **International co-operation facilitates comparing information operations in comparable countries**; what kind of influencing different countries have experienced, and sharing best practices to combat influencing.	**Trustworthy and independent media** is important to citizens' free access to information. In addition, media services and **the availability of Finnish content** play an important role in the stability of the society as a whole and functioning of the democratic system. The role of trustworthy domestic media content is emphasised in all disruptions and even more clearly as information operations increase.
	The means also include safeguarding decision-makers and their close ones from pressuring, threatening and physical threats through training and enhanced physical security, among other means.	For media companies, the fierce transformation of the communications field and weakening financial support has been a tremendous challenge in a time where the importance of source critique has increased. **Diverse media must be supported** so that media committed to **good journalistic practice** can expose fake news on behalf of the citizens. **Dialogue between the media and citizens** increases bilateral trust in the truthfulness of communication. **Safeguarding the sufficient operational preconditions of Yleisradio**, the Finnish broadcasting company, also plays a key role
		In a time of web-based services, **increasing investment in citizens' media literacy is required**. Critical use of social media is important to identify fake accounts, for example. Media literacy prevents social confrontation and dissemination and spreading of black- and-white views. Teachers and the entire educational system have an important role so that citizens have the skills and resources for identifying and assessing the trustworthiness and relevance of information.
		The means also include safeguarding decision-makers and their close ones from pressuring, threatening and physical threats through training and enhanced physical security, among other means.

University of Gothenburg
Department of Journalism, Media and Communication

Tuuli Marjaana Järvinen
MSc in Political Communication
Master Thesis