DETECTING AND COUNTERACTING DISINFORMATION; IS THERE A ROLE FOR SECURITY INSTITUTIONS?

The potential role of the Dutch Defence Cyber Command in fighting disinformation

Charlie van Delden
Supervised by Dr. H. Swedlund
Master's thesis
Human Geography: Conflicts, Territories and Identities
October 22th, 2021

Author:	Charlie van Delden
Student number:	s1065867
Education:	Human Geography; Conflicts, Territories and Identities
Assignment:	Master's thesis
Institution:	Radboud University
Supervisor:	Dr. H. Swedlund
Second reader:	S. van der Maarel
Date:	October 22th, 2021
Number of words:	23381

Disclaimer: This thesis is the individual final product of Charlie van Delden's Master programme at the Radboud University and is written from a scientific perspective solely. Therefore, the thesis is not based on Defence Cyber Command policy and does not contain any formal statements by the Defence Cyber Command or Dutch armed forces in general. In addition, the thesis is, after review by and in consultation with the Integral Security Department and Chief of Staff of the Defence Cyber Command, classified as 'unclassified' and therefore open to the public.

Preface

In front of you lays my master thesis 'Detecting and Counteracting Disinformation; is there a role for Security Institutions?', the final product of my Master's *Human Geography; Conflicts, Territories and Identities* at Radboud University. Writing this thesis was an interesting and instructive experience, with ups and downs along the way. Worth mentioning is the COVID-19 pandemic, which led to the fact I did this Master's almost entirely from home. Although I really missed having face-2-face lectures on campus and meeting new people, I am really happy and proud to finish this Master's under these unusual circumstances.

There are several people I would like to thank for their help during the process of wiring this thesis. Firstly, I want to thank my supervisor Haley Swedlund. I want to thank her for her help and support, for structuring my thoughts and providing me with new insights. Secondly, I want to thank all the respondents, this thesis would not have been there if it wasn't for you. I really enjoyed listing and talking to you and I feel honoured you trusted me with your ideas and opinions on this, sometimes sensitive and complicated subject. In addition, I want to thank the Defence Cyber Command (DCC), for the opportunity to do an internship within your organisation and provide me with new insights and answers, and maybe even more new questions, in the elusive field of cyber, fighting these threats and the future developments in this field. Moreover, I would like to thank my colleagues at the DCC for the warm welcome they gave me and for seeing me as one of them. Lastly, I want to thank my family, friends, roommates and boyfriend; Bas, Franki, Fé, Julia, Daan, Gido and Pieter. I want to thank you, not only for your help, support and motivation but for your patience and the sometimes necessary distraction as well.

I hope you enjoy reading my thesis.

Charlie van Delden
Amsterdam, the Netherlands
October 22th, 2021

Abstract

It can be stated that the targeted misuse of information, collectively called disinformation, can be seen as the next big weapon and a threat to societies all over the world because of its undermining character. An important question in the debate on limiting disinformation and its effects is who should take a leading role in fighting it. The aim of this research is therefore to provide insight in the debate on who can and should fight this threat, and more specific whether a national security institution like the DCC can and should take this role or not. The research was conducted through semi-structured interviews and observations during my internship at the Defence Cyber Command. The interviews were conducted with staff members of the Defence Cyber Command and other experts, related as well as non-related to the Dutch armed forces.

This research has shown that, despite the fact that all respondents see disinformation as a serious threat to Dutch society, a vast majority of the DCC staff members do not perceive a leading role for the DCC in fighting this threat. However, the majority of the DCC respondents state their unit could play a supporting role, if they would get the needed mandate to do so.

The interviewed experts, both related and non-related to the Dutch armed forces, are divided on the subject of fighting disinformation. Some of them plea for a role for the DCC to fight disinformation, where others are against this. The main reason for the latter is because they think this could be at the expense of the democratic values of the Netherlands. On the other hand, all interviewed experts are of the opinion that (more) action against disinformation is necessary and should be implemented. However, they are divided on the desired interventions and strategy as well as on which organisation or organisations should take action on this.

In addition to the question concerning the role of the DCC, it turns out that the DCC's ability to act when disinformation occurs is limited. An important reason for this is the fact that the current laws, rules and legal framework do not allow the DCC to detect or counteract disinformation. This is, to a large extent, caused by the fact that disinformation is, at this moment in time, not seen as a so called 'use of force', which is an important condition for obtaining a (legal) mandate to perform countermeasures. The limited ability of the DCC in order to fight disinformation is in fact not based on a lack of knowledge and skills, but on the current (legal) frameworks and the absence of the necessary mandate.

Table of contents

List of Abbreviations

AIVD	General Intelligence and Security Service
Covid-19	Coronavirus disease 2019
CWTC	Cyber Warfare and Training Centre
DCC	Defence Cyber Command
EU	European Union
LIMC	The Land Information Manoeuvre Centre
MIVD	the Military Intelligence and Security Service
NATO	North Atlantic Treaty Organization
NCTV	National Coordinator for Security and Counterterrorism

1. Introduction

On the 4th of November 2020, the day of the American presidential elections, *The New York Times* reported that Twitter had attached warnings to multiple tweets posted by presidential candidate Donald Trump. The warnings attached to Trump's tweets messaged the reader about the fact that the concerning tweets could contain misleading information. The reason for Twitter to attach these warnings was that Trump kept tweeting unproven and baseless claims regarding fraud during the presidential elections of 2020 (Vigdor, 2020).

Although it might seem that disinformation is a threat to the United States in particular, disinformation is a worldwide and growing threat to all societies (Bader, 2019). During the COVID-19 pandemic for example, countries all over the world had to deal with COVID-19 related disinformation, not just about the virus but about the vaccines against this virus as well (O'Connor, 2021; Rathenau, 2020). Another well-known example of a case in which disinformation played a role, in particular relevant for the Netherlands, is the MH17 case. MH17 was the flight number of the passenger plane that was shot down at the 17th of July in 2014 above Donetsk, Eastern-Ukrainian territory claimed by pro-Russian rebels (Williams, 2017). In 2017, Bellingcat, an independent international collective of researchers, presented evidence for the spread of disinformation around the MH17 case by Russia, trying to influence the public debate and convince people of their innocence and non-involvement in the case of MH17 (Bellingcat, 2021).

The earlier presented examples show cases of disinformation about different themes. Disinformation is seen as a growing threat to (democratic) societies all over the world, including the Netherlands (Bader, 2019; Rademaker et al., 2017). When disinformation is spread it is often to influence certain people or processes to the advantage of the spreader. This can in particular be seen as a threat to democracies, independent elections and the administration of justice (NCTV, z.j.). Besides, the spread of disinformation can lead to unrest, confusion and distrust in society, with a growing number of people believing in conspiracy theories as a result. Correspondingly, (political) debates get more hostile and people do not trust their government anymore, which make societies more divided, unstable and eventually easier to influence (Bader, 2019).

Waltzman (2017) states that information, and with this the misuse of information, can be seen as the next big weapon. Fact is that the spread of disinformation is increasing and that it is often spread by social media platforms as Twitter or Facebook (Bader, 2019; Landman, 2020). Since this is the case, one of the questions asked (worldwide) is who should play a role in fighting disinformation to limit its influence and threat; big tech-companies, governments, national security institutions, people themselves, any kind of independent organisation or a combination of those?

1.1 Research objective and research question

Based on the introduction above, one can say that disinformation, appearing on different themes, in different forms and for different reasons, is a current and growing threat for the Dutch society. For this reason, all the different options on how to tackle this threat and limit its damage should be explored. This thesis will contribute to the debate about which actor(s) should play a role in the process of detecting and counteracting disinformation in society, and more specifically on the question whether

national security institutions like the DCC, a cyber-focussed unit of the Dutch armed forces, should be one of those actors. For this thesis the following central research question has been formulated:

> *How does the Defence Cyber Command perceive its role in the process of detecting and counteracting disinformation in the Netherlands, and what is their ability to act in moments of disinformation?*

To provide an answer to this question, seventeen semi-structured interviews with DCC staff members as well as with different (other) experts on the subject are conducted. This way the debate about the question whether national security institutions could and should fulfil a role in the process of detecting and counteracting disinformation is observed and presented from multiple perspectives.

1.2 Societal relevance

As stated, disinformation is a growing threat to (democratic) societies all over the world, including the Netherlands (Bader, 2019; Rademaker et al., 2017). Multiple studies have shown that the people in Dutch society, as well as the Dutch government, are worried about the spread and influence of disinformation (and fake news). In 2017, I&O Research found that 82 percent of respondents stated they see disinformation as a threat to Dutch democracy and the rule of law (I&O Research, 2017). As stated before, a relevant question is who should take a leading role in fighting the threat of disinformation.

About 67 percent of the Dutch citizens state that they think the responsibility for limiting the influence of disinformation (and fake news), and making it easier to recognize, lies with big tech-companies as Google and Facebook (Rijksoverheid, n.d.). While the (societal) pressure on these big tech-companies to change their policies concerning disinformation is rising, their handling of disinformation on their platforms is in many cases still very slow and unclear (Schiffrin, 2017; Beckett, 2021). In addition to these private actor efforts, the Dutch government is also focussed on finding solutions for the threat that disinformation is. While Dutch citizens are attributing responsibility mostly to the tech-companies, the Dutch government places the responsibility mostly with its citizens by trying to make them more aware of the presence of disinformation and learning them how to recognize it (Rijksoverheid, n.d.). On top of the efforts made by the Dutch government, the European Union is developing multiple campaigns and plans to counteract the influence of disinformation on the European level and scale (European Commission, 2019). The question here is which role a government could and/or should play in this matter, while maintaining democratic values at the same time.

In order to establish ways of detecting and counteracting disinformation, to protect democratic societies as the Netherlands from unwanted and damaging interference and growing social division, more research should be conducted. It is particularly interesting to do more research on the opportunities the Netherlands has to protect itself against this threat. One of the potential instruments the Dutch government has at its disposal in its fight against disinformation is the DCC; the subject of this thesis. Doing research on a potential role for the DCC to fight disinformation is relevant because of the fact it will clarify if there is or could be a role for the DCC, comparable other (military) units and/or the Dutch military organisation in general. If this turns out to be the case, the DCC should seriously be considered a suitable actor and should start fighting this threat as soon as possible, preventing the Netherlands to get overrun by disinformation and the Dutch democracy and society to become the victim of someone else's hidden agenda and covert influences.

1.3 Scientific relevance

Noteworthy is the fact that, although there is scientific debate about fighting disinformation and its effects and who should lead this fight, the potential role of national security institutions in this debate is quite limited. The fact that little scientific research is (being) done into the role these institutions could fulfil in this process, can be seen as a missed opportunity, since national security institutions are in general well informed about the national security situation. This little scientific research, resulting in a knowledge gap concerning the potential role of national security institutions in the process of detecting and counteracting disinformation, is the reason this thesis will focus on the question whether the DCC or Dutch armed forces in general, as a national security institution, could and/or should fulfil a role in this process. In addition, this thesis especially focusses on how DCC staff members perceive their role in this process. By researching new potential actors for this task, in this case the DCC, this research aims to add new insights to the broader scientific debate about how, why and by whom the spread and influence of disinformation in the Netherlands should be handled.

1.4 Thesis outline

This thesis consists of eight chapters, of which this introduction is the first one. Chapter 2 presents a literature overview of the state of-the-art regarding the debate concerning disinformation and fighting it. In addition, chapter 2 also presents the hypothesis and operationalisation. The third chapter of this thesis is the methodology chapter, in which the choices made concerning the methodology of this thesis are presented, explained and evaluated. Chapter 4 is the Case description and first empirical chapter of this thesis. In this chapter the organisation and tasks of the DCC and Dutch armed forces in general are illustrated and explained. Chapter 5 presents how the DCC staff perceives their role in the process of detecting and counteracting disinformation and how other experts look at this. Chapter 6 presents what the DCC can do when disinformation appears. The seventh chapter contains the discussion, in which the research outcomes are interpreted, connected to the literature and explained. The closing chapter of this thesis, chapter 8, is the conclusion and presents an answer to the research question, limitations of this thesis and recommendations for further research and in praxis.

2. Literature review, hypothesis and operationalization

2.1 Literature review

This literature review provides an overview of the state of-the-art regarding views on the debate concerning disinformation and fighting it. Firstly, the concept of disinformation, the threats posed by disinformation and the role of social media in this will be explained. Secondly, the concept of hybrid-warfare and the role of disinformation in this will be provided and explained. Thirdly, the discussion about what kind of measures could be taken to fight disinformation are presented and discussed. Lastly, the debate whether national security institutions could and/or should be seen as suitable actors to fight disinformation and limit its influence will be cited.

2.1.1 Disinformation

There are multiple definitions of disinformation in the scientific and societal debate. In this research, disinformation is defined as; false and deceptive information that is distributed deliberately and on purpose by an individual, group, company, organisation or government to reach a specific objective (Wardle & Derakhshan, 2018; Karlova & Fisher, 2012). Important here is the fact that the distributor of disinformation is aware of the fact the information he or she spreads is false and has the intention to mislead people (Fallis, 2015). The difference with misinformation is that the distributer in this case spreads false information accidentally, referred to as 'inaccurate information' by Karlova & Fisher (2012) (Wardle & Derakhshan, 2018). According to Bader (2019) and De Ridder (2021), disinformation can appear in different forms of which 'fake news', a current popular concept in society, is an example.

Disinformation is being spread in different domains and with different objectives. According to Fallis (2015) it is without a doubt that the overall objective of disinformation spreaders is to mislead people, often for their own gain. But, depending on the domain where the disinformation is spread, the spreader can have additional objectives like making money or gaining more influence. The fact disinformation appears in vital domains as the political-, investment- or medical domain makes it can cause harm with serious consequences (Fallis, 2015). The spread of disinformation in the investment sector and stock market could, for example, lead to financial losses when people get misled and invest in the wrong fund or company. Disinformation can for example be used to lower a share price, creating a change for others to buy stock at a lower price, or to attract more investors based on false grounds (Isa, 2017; Gillham, 2021). Besides, disinformation is present in the political domain. In the political domain the intended objective of the spreader can for example be to gain more influence in another country (indirectly) by influencing the elections. This can be done by pushing voters to a certain candidate or party by manipulating polling data, influence the public debate, undermine another political actor or candidate or to influence and mislead people in general by undermining the general trust in the political system (Bader, 2019).

2.1.1.1 The threat of disinformation

As stated before, disinformation is spread with the general objective to mislead people, often in favour of the spreader (Fallis, 2015). Clear is that disinformation is used when a certain goal is to be reached that cannot be reached in a transparent and democratic way. According to Fallis (2015) and Bader (2019), the danger of disinformation is that people read it, believe it and act on it with possible political, social, emotional, financial, or even physical harm as the result. In other words, when people start to

act on the basis of disinformation, the untransparent and undemocratic objectives of the spreader of this disinformation will become reality.

A case where the spread of disinformation has led to physical conflict is the storming of the United States Capitol in 2021. Here, former Republican President Donald Trump claimed, without providing any evidence, that the elections were stolen by the Democratic Party. By sending tweets, Trump (indirectly) called his supporters to reclaim the elections and the United States of America, with the result that his supporters stormed the Capitol (Sullivan, 2021). The storming of the Capitol can be seen as an attack on democracy, incited by the spread of disinformation (Drutman, 2021).

Defining the real influence disinformation has had on elections and democracies before is hard, but proof has been found that disinformation has played a role in, among others, the American presidential elections of 2016 and the Brexit (Schriffrin, 2017). Bader (2019) states that the pressure disinformation puts on democratic societies and their elections is worrying, and that the prospects are not that positive, since it seems that the spread of disinformation will not decline in the near future. He states this, since disinformation could be seen as *"a low-cost strategy with a potentially high impact"* for individuals, groups, organisations or governments with the desire to legitimize undemocratic elections, delegitimize democratic elections or undermine specific candidates or parties (Bader, 2019, p. 34).

2.1.1.2 Disinformation and social media

Despite the fact disinformation is not a new phenomenon, the rise of the internet and social media has provided new opportunities to spread disinformation (Landman, 2020). Since the rise of internet and social media platforms as Facebook and Twitter, a bigger amount of information, and with this disinformation, can be spread. Besides, the spreading goes much faster and reaches more people (Fallis, 2009; Bader, 2019). At first, the fast exchange of information was seen as an opportunity, especially in conflict situations. Around 2011, people were hopeful about social media and its societal opportunities, since Facebook was seen a platform that could bring more democracy to the world and Twitter could function as a warning system in case of emergency (Schiffrin, 2017; Niekerk & Maharaj, 2013). But, around 2016 the conclusion could be drawn that Facebook could not fulfil its promising role to bring more democracy to the world, and moreover, actually played a role in breaking some of them down (Schiffrin, 2017). It turned out that social media was not the promising 'tool' it was believed to be. Where the fast and easy spread of information was earlier seen as an opportunity, it is nowadays mostly seen as an unpredictable threat and potential danger for especially, but not only, democratic societies, because of the spread of disinformation (Schiffrin, 2017).

Social media differs from mainstream media on multiple aspects, which makes social media more suitable for the spread of disinformation (Herik et al., 2020). Firstly, in (most) mainstream media, information is passed from a journalist or expert to society, from a few (qualified) people to everyone (the public). In the reality of social media you do not have to be a journalist or expert to say or state something, everyone has the means to inform one another or to share their thoughts and opinions, with the result that a lot of incorrect and unverifiable information is presented. This phenomenon is called citizen journalism. Citizen journalism, in combination with the fact that more people start to use social media as their primary news source (Waltzman, 2017), makes that more people judge the information they read on social media as true and take decisions on it. Besides, Herik et al. (2020) state that where mainstream media often use fact checkers and editorials who rate the content, make judgement, take decisions on the quality and truthfulness of it and by doing do guarantee the quality

of publications, this is not the case on (the great majority) of social media platforms. The result of this is that dis- and misinformation get free play, since not everyone spreads false information on purpose (Karlova & Fisher, 2012; Wardle & Derakhshan, 2018). As a result of this, people can get confused and disorientated by the amount and contradictory information that is provided to them, they do not know what to believe anymore and start to lose trust in society, the political system and each other (Rosenberger, 2020).

The fact that everyone can post everything on social media without it being fact-checked, in combination with distribution-algorithms, makes that people can end up in a so called 'rabbit hole'. The term rabbit hole refers to the situation in which someone's algorithm on social media keeps providing the same kind of articles that could include disinformation, which seem to confirm each other with the result it starts to seem like reality (Takken & van Dijk, 2021). Thorson (2016) presents the following-up problem, namely the so called *belief echoes,* referring to the effects that exposure to (political) disinformation has on people. Thorson (2016) shows that, even when disinformation has been refuted and corrected, people who have been exposed to the disinformation will keep it in mind and might question the correction instead of the disinformation. This shows that the spread of disinformation should be seen as a problem in which 'prevention is better than the cure'.

2.1.2 Disinformation in hybrid-warfare

As presented before, disinformation campaigns appear in different places and forms. Besides, disinformation campaigns are an often deployed strategy in the so called hybrid-warfare and can also be referred to as a hybrid-threat. Despite the fact Lasonjarias & Larsen (2015) state a comprehensive definition of hybrid-warfare is absent, they do summarize it as the following themselves; *"the true combination and blending of various means of conflict, both regular and unconventional, dominating the physical and psychological battlefield with information and media control, using every possible means to reduce one's exposure"* (Lasonjarias & Larsen, 2015, p.3).

In other words, and summarized by Vuković et al. (2016), hybrid-warfare is a form of warfare in which regular and irregular military forces are involved and support each other in order to reach political-strategic goals. According to De Wijk, Bekkers & Sweijs (2020), hybrid threats should be seen as a strategy used by a party that cannot win a conflict or war by just military means. Because of this fact, they decide to use other, often non-military means to weaken its opponent(s) by undermining their political unity and societal support. Examples of these non-military means to weaken and undermine the opponent are economic-, information- and cyber operations, or more specific, disinformation campaigns (MIVD, 2017).

Disinformation as a hybrid-threat is not new. Spreading disinformation for military goals has been done for years as a method to influence and mislead the opponent (Fallis, 2009; Waltzman, 2017). Operation Bodyguard might be one of the most known examples of an 'old school' military disinformation campaign, which took place during the preparations of D-Day in World War II. During Operation Bodyguard, the Germans were misled by the Allied forces about the time and place of their attack by misleading and conflicting information. As a result the Germans were not fully prepared on or able to stop the attack of the Allied forces.

However Operation Bodyguard shows that disinformation campaigns have been used as a strategy for a long time, the number of disinformation campaigns seems to increase (Bradshaw & Howard, 2019).

Bradshaw & Howard (2019) found that in 2019 at least 70 countries had to deal with organized social media manipulation campaigns, in contrast with 48 countries in 2018 and 28 countries in 2017.

De Wijk, Bekkers & Sweijs (2020) state that one of the reasons why targeted disinformation campaigns (against the West), in the hybrid warfare context are increasing is because of the power of the European Union and NATO alliance. The European Union and NATO form a strong (military) front against the rest of the world, what makes countries that are not part of these institutions or alliance feel threatened. These counties feel threatened because of the fact they know they will never beat the EU or NATO based on just military power. For this reason, they use hybrid threats as a way to undermine the political cohesion and social resilience of the member states of these institutions with destabilisation as the result (De Wijk, Bekkers & Sweijs, 2020).

Another notable fact of hybrid-warfare is that it is a strategy generally used by autocratic countries and less by democratic countries (De Wijk, Bekkers & Sweijs, 2020). Autocratic countries use this hybrid-warfare strategy more than democratic countries because of the fact that autocratic leaders are able to insert different 'debatable' tools without contradiction, where democratic countries have to deal with *checks and balances*. These checks and balances are an important part of democratic societies since it monitors and evaluates the decisions made by politicians (Britannica, n.d.). A drawback of these checks and balances is, according to De Wijk, Bekkers & Sweijs (2020), decision-making goes slowly, what is one of the reasons why some of the countries in the West do not have a successful counter-hybrid strategy (yet).

2.1.3 Fighting disinformation

One of the main questions in the debate about disinformation and its influence is the one of who's responsibility it is to limit this threat. While limiting the threat and influence of disinformation, it is important to, at the same time, transgress democratic norms and values as freedom of speech. The big tech companies are often seen as the suitable actor to fight disinformation, since a lot of it is being spread on their social media platforms (Herik et al., 2020). Despite the fact pressure is applied by governments and civil society on these big tech companies to change their policy concerning disinformation, there is no consensus concerning the effectiveness of this (Rijksoverheid.nl, n.d.; I&O Research, 2017; Robbins, 2019). As a result of this, some national governments and the European Union take measures against disinformation themselves (European Commission, 2019). Some countries choose to implement laws and rules against (the spread of) disinformation, others are more focussed on alternatives like rising awareness, self-regulation by its citizens and improving the resilience of society as a whole (Landman, 2020; Brinkel, 2017). There is no consensus on which approach works best. Measures to limit disinformation and its influence can be divided in different categories; political measures and societal measures. However, there can also be an approach in which both kind of measures are implemented. The different categories of measures will be explained in more detail in the following paragraphs.

2.1.3.1 Political measures

Some countries, as France and Germany, made the decision to fight disinformation by implementing laws and rules to limit the influence of disinformation. Another example of political measures taken to fight disinformation is that former British Prime Minister Theresa May created a new security task force to fight disinformation and fake news, called the UK National Security Communications Unit (Landman, 2020; Ingram, 2018; Levush, 2019).

The aim of creating restrictions and organisations like these is for governments to try and protect their democracy and society from undesired influences. But, not everyone agrees with this approach. One of the critiques, mostly expressed by scientists, journalists and activists, is that government-led developments like these could be a way for governments to limit democratic rights in their country and moreover for autocratic regimes to use as an excuse to tighten their control on their citizens (Landman, 2020; Rademaker et al., 2017). The discussion on who's responsibility it is to fight disinformation actually comes down to the question whether you should want the government to play an active role in this or not. Landman (2020) and Rademaker et al. (2017) express their concerns and resistance towards a role for the government in this by stating we have to be careful with, or actually should not, counteract disinformation by implementing laws and rules against it. According to Landman (2020) this will, paradoxically, negatively influence the fundamental principles of democracy, as the freedom of speech and press.

2.1.3.2 Societal measures

Measures to limited disinformation and its influences in which the government is not actively involved can come from society. Rademaker et al. (2017) state that solutions against disinformation should come from society, citizens and tech-companies and should not be government-led. According to them, the media and the scientific world should play a supportive role in this by making citizens more aware by making it an important subject in education programmes or by establishing an independent organisation who actively presents, disproves and communicates about specific cases of disinformation.

Another theory in this debate is the one about resilience and deterrence. Brinkel (2017) defines resilience as the extent to which a society can deal with threats and shocks, how it adapts and how fast it recovers from a threat or attack. In this sense, resilience is a way to determine the immunity of a society against conflicts or hybrid threats as disinformation. Besides, Brinkel (2017) states that a society with a high amount of resilience has a deterrence strategy as well, since it is unattractive to attack a country with hybrid means like disinformation, if it does not touch them. An important note to make about resilience as a (deterrence) strategy is that, despite the fact it might offer good opportunities in theory, building resilience in society can be a challenge (Brinkel, 2017; Francart, 2010). This challenge has to be taken seriously and handled well before the strategy will pay off, otherwise it could create confusion in society and might even worsen the situation.

2.1.3.3 Political- and societal measures in hybrid form

However, the line between political- and societal measures is not static, since these sectors can decide to work together in their fight against disinformation (Robbins, 2019). Collaborations like these are often seen in East-European countries as the Balkan countries and the Czech Republic, since these countries have to deal with disinformation, especially from Russia, more than other European countries (Krekó, 2020; De Wijk, Bekkers & Sweijs, 2020). In Estonia for example, volunteers, referred to as 'elves', since they are fighting against the disinformation-trolls, work together with the Ministry of Defence to fight disinformation (Debunk.EU, n.d.). Partly because of this initiative, Estonia can be seen as one of the frontrunners in the fight against disinformation.

2.1.4 The (potential) role of national security institutions

In line with the earlier presented debate about the desirability of a role of the government in detecting and counteracting disinformation, the question arises whether there is a role for national security

institutions in this. National security institutions are institutions with the task to provide and maintain the safety of a State or an organization against criminal and subversive activities such as terrorism, espionage and other potential dangers (Marotta & Nunzi, 2011).

2.1.4.1 National security institutions fighting disinformation

On the one hand, the discussion about the potential role of national security institutions in detecting and counteracting disinformation is hard because of the fact that these institutions are an extended part of the national government. This means that the earlier presented worries and critiques about the interference by the government on, among others, the freedom of speech and press, by Landman (2020) and Rademaker et al., (2017) count here as well.

On the other hand, detecting and counteracting disinformation can be seen as a suitable task for national security institutions, since it is their job to protect society and its citizens against unwanted influences and threats (Costa & Geltzer, 2019; Rademaker et al., 2017). Both Costa & Geltzer (2019) and Rademaker et al. (2017) state that fighting disinformation could be a task for national security institutions, since these institutions are often already aware of the current (national) developments and threats, which gives them an informed position. As an example, Costa and Geltzer (2019) state that the US intelligence agencies could, and even should, play a role in this. They state the US intelligence agencies have been focussed on safeguarding government secrets for too long and should start taking responsibility to protect the country to unwanted influences on social media and by disinformation. Costa & Geltzer (2019) plea for the US intelligence community to "*identifying disinformation spread by foreign adversaries and swiftly debunking it before it can "go viral""* (Costa & Geltzer, 2019). In addition, former US NSA general counsel Glenn Gerstell called, during an interview with CBS news in 2020, for more attention to the threats of disinformation and plead especially for other and more political measures to tackle this problem. More concrete did Gerstell propose "*an integrated disinformation centre"* hosted by the federal government or a national security institution (CBS News, 2020).

Despite their earlier presented critiques and worries, Rademaker et al. (2017) do agree with the fact there could be a role for the intelligence services in the process of detecting and counteracting disinformation, but under certain requirements. They state intelligence services could have a role in the process of detecting disinformation under the condition that detecting and reporting would be their only tasks. The intelligence services should not get involved into the further course of the process as debunking or tackling disinformation at any time. This is to prevent these institutions, or actually the government as a whole, from getting too much power in the process and on deciding what is the truth and what is not.

2.1.4.2 Military organisations

An example of a Dutch national security institution is the Dutch military organisation. Military organisations are, among others, known for their characteristic organizational culture. An organisational culture tells something about the way people act (often in the workplace), and can be defined as; *"the collection of values, expectations, and practices that guide and inform the actions of all team members."* (Wong, 2020).

Despite the fact the specific culture of the different departments of a military organisation differ, the military culture in general is especially known for their discipline, strictness and unification. Snider (In

Levesque, 2013) states that military culture is generally based on four elements; discipline, a professional ethos, tradition and cohesion. This organisational culture is needed, or at least helpful, in order to fight battles and reach certain goals in a safe and in a functional way.

But, there is critique on this military organizational culture as well. The elements that lead to the functionality of this organisation, can, at the same time, be seen as the 'Achilles heel' of the organisation (King, 2020; Chinn & Dowdy, 2014). According to Levesque (2013) and King (2020) this is the case since these jeopardized order, discipline, cohesion and entrenched organizational interests can lead to a lack of efficiency, operational effectiveness and rejection of innovation and change in the organisation at the same time.

Since King (2020), Chinn & Dowdy (2014) and Levesque (2013) all state that military organisation are not that open to change, a relevant question for this thesis is how military organisations look at and handle (new) hybrid-threats and whether they are able to reconsider and possibly reform their 'policy'. Since this thesis focusses specifically on the potential role of a military unit in detecting and counteracting disinformation, it is important to know about the military organisational culture. The reason for this is that the military organisation culture could have an influence on how DCC staff members perceive their role in fighting new or emerging hybrid-warfare threats, as disinformation.

2.1.5 Conclusion literature review

Disinformation can be defined as information that is false and deceptive and that is distributed on purpose with the aim to mislead people (Wardle & Derakhshan, 2018; Karlova & Fisher, 2012). Disinformation is spread by different people, for different reasons and in different domains and should be seen as a serious threat to society because of its undermining effects. Despite the fact multiple parties feel the urge to restrict disinformation and its unwanted influences, there is still a lot of uncertainty and disagreement about how these measures should look like and if they should be societal based, political based or organised in hybrid form.

In addition, there is not much knowledge on the potential role of national security institutions in the process of detecting and counteracting disinformation yet. What is known is that military organisations are very disciplined, structured and hierarchical, what is functional for fighting battles, but can at the same time be an obstacle for innovation and change. For these reasons this thesis will add to the debate whether and how national security institutions, as a military unit, could play a role in detecting and counteracting disinformation, specifically in the Netherlands.

2.2 Hypothesis

The following question is the central research question in this thesis:

> *How does the Defence Cyber Command perceive its role in the process of detecting and counteracting disinformation in the Netherlands, and what is their ability to act in moments of disinformation?*

During this research I expect to find that the DCC sees detecting and counteracting disinformation in the Netherlands as one of their tasks. The reason I expect this is since disinformation campaigns can be seen as a hybrid threat towards the Kingdom of the Netherlands. Since protecting the Kingdom of the Netherlands against threats is one of the main tasks of the Dutch armed forces, including the DCC,

I expect to find that they see it as their duty to fight disinformation. In fact, I expect to find that the DCC plays an active role in detecting and counteracting disinformation or at least thinks about how they could do so, considering the fact they are the specialised cyber unit of the Dutch armed forces, and disinformation is increasingly being spread by the internet and social media in particular. In addition, I expect to find that the interviewed experts think about a potential role for the DCC in fighting disinformation differently than the DCC respondents themselves. I expect this since experts, and scientists and journalists in particular, are often more focussed on finding solutions without the involvement of a governmental party, as the DCC is, in societal and civil rights sensitive issues like this, since they are worried this will be at the expense of democratic values.

2.3 Operationalization

When doing scientific research it is important to be clear about what is meant exactly by the use of certain concepts and terminology. Besides, as a researcher one should be clear about how these concepts are 'measured' and what their role is during the research. In table 1, the key concepts of this thesis are presented including their used definition, how they will be measured and an explanation of their role in this thesis.

2.3.1 Key concepts

Key concept	**Definition of the concept**	**Use of the concept**
Disinformation	Disinformation is defined as; information that is false and deceptive and that is distributed on purpose to reach a certain goal (Wardle & Derakhshan, 2018; Karlova & Fisher, 2012; Bader, 2019). As presented in the literature review, disinformation can appear in different domains and with different objectives.	In this thesis the focus is on what should and could be done to limit disinformation and influence and not about what disinformation is or is not, meaning the concept itself is not measured or discussed directly.
National security institutions	National security institutions are defined by Marotta & Nunzi (2011) as; institutions with the task to provide and maintain safety of a State or an organization against criminal activities such as terrorism or espionage and other potential dangers.	In this thesis the focus is on if and how national security institutions could play a role in protecting the Netherlands to hybrid- and cyber related threats.
Defence Cyber Command	The DCC is an unit of the Dutch armed forces that performs offensive and defensive military actions in the cyber domain. The DCC was established in 2014 with the aim to protect the Dutch cyber space as well as to support operational military missions.	In this thesis the DCC is the Dutch national security institution that is the central case.
'Perceive its role' [in the process of detecting and	Perceiving its role in the process of detecting and counteracting disinformation is defined as the way the DCC staff members thinks about what they could, should and can do in	Since the DCC is an organisation and cannot perceive a role itself, the perceived role of the DCC is

counteracting disinformation]	the process of detecting and counteracting disinformation and how they look at this.	formed by the staff members of the organisation and will be measured by interviewing them.
'Ability to act' [in moments of disinformation]	Having the ability to act in moments of disinformation is defined as having the legal base, necessary resources as knowledge and skills to do so.	The ability to act of the DCC is measured by asking the staff members of the command about the legal framework, and resources as knowledge and skills to act if they get the assignment to do so during the interviews.
Fighting disinformation	In order to fight disinformation, there are two pillars; - detecting disinformation: professionally searching for disinformation and its source - counteracting disinformation: action taken to end disinformation being spread and present in the Netherlands	'Fighting disinformation' is a term used for detecting and/or counteracting disinformation.
Table 1: Operationalisation key concepts		

3. Methodology, methods and techniques

In this chapter, the choices made concerning the methodology of this thesis are presented, explained and evaluated. A complete and detailed methodology chapter is important since it increases the reliability and replicability of the research (Bryman, 2016).

3.1 Qualitative inductive research

This thesis research project is done by the means of qualitative research methods. Qualitative research methods are regularly used to find out why something happens or how, and why, people think about certain issues in a particular way. When doing qualitative research, as a researcher you want to gain insight into thoughts and experiences of people (Bryman, 2016). Qualitative research methods are most suitable for this thesis since the aim of this thesis is to find out how people think about disinformation and how the DCC perceive its current and potential role in the process of detecting and counteracting disinformation.

While doing scientific research, a deductive or inductive approach is used. The difference between these two approaches it that deductive research starts from a theoretical basis with the aim to verify or disprove these theories, where inductive research starts without a theoretical basis and dives into the empirical world immediately with the aim to develop or built theory (Bryman, 2016). This thesis can be described as an inductive and explorative research project since there has not yet be a lot of (scientific) research about the role of national security institutions in fighting disinformation yet. This makes that this research did not start with a theoretical basis or theory but by diving into the empirical world (almost) immediately. The aim of this thesis is to bring innovative theoretical insights into the debate of fighting disinformation and have a role in building theory about the role of national security institutions, as the DCC, in detecting and counteracting disinformation, especially in the Netherlands.

3.2 Research design

A common research design used in qualitative research is the case-study design. The aim of a case-study is to study one or a few cases very intense and detailed (Bryman, 2016). When doing case-study based research, as a researcher you get less diverse data, but the data that you collect are detailed and in-dept. The detailed and in-depth data makes that you as a researcher get a real understanding of how a case is structured, how it works and its (potential) complexities.

This thesis project is done on the basis of a single case-study. Since this thesis is focussed on the potential role of the DCC, a Dutch national security institution, in the process of detecting and counteracting disinformation in the Netherlands, the DCC is the central case here.

3.3 Data collection

This research is based on semi-structured interviews. This way of collecting data has been chosen for multiple reasons. First, semi-structured interviews are one of the best ways to get to know more about what people experience and think. Second, the semi-structured interviews will provide more insight

into-, and a better understanding of the current situation or dominant discourse (Bryman, 2016). Since the focus in this thesis is on how the DCC staff members perceive their role in the process of detecting and counteracting disinformation in the Netherlands and on how certain other experts think about disinformation and fighting it more generally, doing semi-structured interviews is an essential part of this research.

Doing these interviews in a semi-structured way, makes that both the interviewer and the respondent has the time, space and freedom to explore the subject in-depth and in a wider perspective during the interview. While doing semi-structured interviews, the interviewer does have an interview guide to make sure none of the themes or questions are forgotten, but, at the same time, has the freedom and flexibility to react on the interviewee, ask in-dept questions and improvise during the interview (Bryman, 2016). For the respondent this means there is more space to talk about, for example, specific experiences and ideas concerning the DCC or the disinformation debate in general, since there is space to elaborate on themes that are not on the interview guide. The fact the interview is not limited by the interview guide makes that the data is more detailed and in-dept. The interview guides used during the semi-structured interviews can be found in the appendix of this thesis.

3.3.1 Respondents

This thesis is based on semi-structured interviews with different people, with different backgrounds and perspectives from different organisations. In this paragraph, the respondents included in this research are presented. To secure the reliability and replicability of this research, information concerning the date and length of the interview, as well as the medium used are presented as well. In total seventeen semi-structured interviews were conducted.

The respondents can be divided in three groups; staff members of the DCC, others attached to the Dutch military but not to the DCC, and experts outside the Dutch military. The reason to include these three groups instead of just the DCC staff members is because this way multiple perspectives are included. Therefore, a more complete overview of the topic can be presented and discussed. The respondents who cooperated in this thesis have been specifically selected because of their position and/or knowledge. The DCC respondents are selected because of their position at the DCC. The experts are selected for their knowledge on the subject and are, for this reasons, called expert interviews. These ways of sampling is called purposive sampling (Bryman, 2016). Besides, the method of snowball sampling is used, what means the respondents have provided names and contact details of people they taught could be interesting to include in this research as well (Bryman, 2016).

Because of the fact this thesis is mainly focussed on how the DCC perceives its role in the process of detecting and counteracting disinformation in the Netherlands, the first group of respondents are staff members of the DCC. Table 2 *'Overview of interviewed staff members of the DCC' provides* an overview of the respondents from the DCC. Because of privacy- as well as safety reasons the respondents of the DCC are all anonymized and are referred to by a number.

'Name'	**Date of interview**	**Length of interview**	**Medium used**
Respondent I	19th of May 2021	70 minutes	Face-to-face
Respondent II	19th of May 2021	45 minutes	Face-to-face
Respondent III	20th of May 2021	30 minutes	Face-to-face
Respondent IV	20th of May 2021	70 minutes	Face-to-face
Respondent V	3th of June 2021	60 minutes	Face-to-face

Respondent VI	4th of June 2021	60 minutes	Skype
Respondent VII	22nd of June 2021	32 minutes	MS Teams
Respondent VIII	15th of July 2021	60 minutes	Face-to-Face
Table 2: Overview of interviewed staff-members of the DCC			

The second group of respondents are people who are attached to the Dutch military but not to the DCC. They are included in this research because of the fact they have valuable information and experience in the cyber domain or with disinformation and can, for this reason, provide a different perspective on the issue. Table 3 *'Overview of interviewed experts related to the Dutch armed forces'* provides an overview of who are interviewed and some basic information of the interview.

Name and function	**Date of interview**	**Length of interview**	**Medium used**
Han Bouwmeester - Professor at the Netherlands Defence Academy	31st of May	45 minutes	MS Teams
Paul Ducheine and Peter Pijpers - Professors at the Netherlands Defence Academy and University of Amsterdam	31st of May	60 minutes	MS Teams
Lauren Heida - Staff member of the Counter Hybrid Unit	11th of June 2021	41 minutes	MS Teams
Table 3: Overview of interviewed experts related to the Dutch armed forces			

The third group of respondents are people who are experts in the field of cyber, the cyber domain or disinformation and fighting it. They have been included in this thesis because of their knowledge on the subject and, since they are not part of the Dutch military, they add an 'outsider' perspective on the matter. Table 4 *'Overview of interviewed experts not related to the Dutch armed forces'* provides and overview of who are interviewed.

Name and function	**Date of interview**	**Length of interview**	**Medium used**
Bart Jacobs - Prof. dr. at Radboud University	16th of April 2021	23 minutes	ibestuur.nl
Sico van der Meer - Research Fellow at the Clingendael Institute	21st of April 2021	32 minutes	Skype
Robert van der Noordaa - Multiple functions, a.o. journalist and co-founder of Trollrensics	23st of April 2021	70 minutes	Zoom

Jeroen de Ridder - Associate Professor at the Vrije Universiteit	29th of April 2021	34 minutes	Zoom
Daniel Romein - (Former) Bellingcat staff memeber	6th of May 2021	120 minutes	In person
Isabelle van Duyvesteyn - Prof. dr. at Leiden University	7th of June 2021	35 minutes	Skype
Table 4: Overview of interviewed experts not related to the Dutch armed forces			

3.4 Data-analysis

Before the collected data can be interpreted and conclusions can be drawn, it is important to make the collected data comprehendible. This happens in the data-analysis phase and can be done in multiple ways. In this thesis, the semi-structured interviews are coded on the basis of the interview guide. The aim of coding is to create a structured overview of the collected data in order to draw conclusions later on. Coding is done by labelling certain phrases, topics or themes with a code every time that they are mentioned in the semi-structured interviews. When this is done, all the codes have a collection of labelled phrases, topics or themes and are ready to be compared and processed. During the data analysis I coded the data manually, meaning I worked out all the data in schedules and overviews per group of respondents. This way I was able to quickly see similarities and differences between the respondents.

The process of coding is done as introduced by Strauss & Corbin (in Bryman, 2016). Strauss & Corbin are presenting the process of coding as three phases; open coding, axial coding and selective coding. Open coding is the first round of coding and is about labelling the useful phrases and with this separating the unusable parts of the interview. When finishing the open coding phase, you often have a lot of different codes. The axial coding phase is about combining and regrouping different overlapping codes from the open code phase into broader categories. This way the data becomes more structured. The last phase, the selective coding, is about finding relations between these categories and is the starting point of the theory building phase.

Analysing the semi-structured interviews is the easiest when they are recorded and transcribed, what was the case with all the conducted expert interviews. But, the interviews with the DCC staff members are not recorded because of privacy- and safety reasons or because some of the respondents did not feel comfortable to talk freely when being recorded. This has had consequences for the process of analysing this data, since those interviews are not transcribed. During the interviews that are not recorded, notes are made. Afterwards an interview report is made containing a substantive summary and a description of the interview setting, atmosphere and other notable things. These interviewed are analysed manually by comparing the interview notes and interview reports with one another.

3.5 Ethical considerations

When using interviews as a way to collect data, it is important to respect the respondent's rights. This is called informed consent and means that you as a researcher should be open and straightforward

about the aim of the research, the role the respondents have in it, and the way you will use their answers. By discussing this on forehand, the risk that the respondents get negatively surprised or even dissatisfied with your research or the way they are presented in this is being minimalized (Bryman, 2016). In addition, all the respondents were asked if they gave permission to use their real name or wanted to be anonymised in the thesis. In order to respect the anonymity of the, in case of this thesis DCC respondents, none of their names or functions are mentioned on the interview notes or in the thesis and the interviews are not recorded or transcribed. Lastly, with some of the respondents I agreed with deleting the interview- recordings and transcripts when finishing this thesis, what I will do with all the interviews the moment I completely finished my thesis.

4. Case description

To get a better understanding of the DCC and about what they can and cannot do, it is important to understand the Dutch Defence Organisation as a whole and its relation to politics. For this reason, this first empirical chapter is a case description and will provide more insight into, among others, the chain of command, general set up, tasks and authorizations of the Dutch Defence Organisation, and specifically of the DCC.

4.1 Instruments of power

Before describing the Dutch military and DCC in more detail, it is important to understand in which context military power can be placed. The deployment of military means is one of the four instruments of power a State can insert to achieve their objectives and safeguard their interests. The other three instruments of power are; diplomatic, informational and economic. These instruments of national power can be used separately or together, depending on the situation and the intended purpose (Defensiestaf, 2019).

Since this thesis focusses on the DCC and its potential role concerning disinformation, this case description solely describes the conditions under which the military category as an instrument of power can be deployed.

4.2 The Dutch military and deployment of military means

The role and deployment of the Dutch military is incorporated in the Dutch constitution. The first, for this case description, relevant article is article 97.

In the Dutch constitution, article 97 is presented as the following (Ministry of the Interior and Kingdom Relations, 2019, p. 21);

1. *There shall be armed forces for the defence and protection of the interests of the Kingdom, and in order to maintain and promote the international legal order.*
2. *The Government shall have supreme authority over the armed forces.*

Article 97.1 of the Dutch constitution, as presented above, formulates the tasks of the Dutch armed forces very broad, formal and political. In her own words, the Dutch Defence Organisation states that its committed to keep safe what the Netherlands is dear and thinks is important. In addition, they strive towards a world in which everyone, inside and outside the Netherlands, can live in safety and freedom (Ministerie van defensie, 2021). The Dutch Defence Organisation strives towards this goal on the basis of three main tasks derived from article 97 of the constitution. The Dutch Defence Organisation presents its three main tasks as the following (Defensiestaf, 2019, p. 52):

1. *Protection of national and allied territory, including the Caribbean part of the Kingdom*
2. *Maintenance and promotion of the internal legal order and stability*
3. *Support for civil authorities in national law enforcement, disaster relief and humanitarian aid, both nationally and internationally*

Article 97.2 of the Dutch constitution states that the Dutch government has supreme authority over the Dutch armed forces. This means that the Dutch armed forces always operates under the responsibility and guidance of the Minister of Defence and the government as a whole. This implies that the military never can decide on their own whether military action will be undertaken. As a result, the military is constantly available and waiting for the moment the government gives them an order for military deployment. This order for military deployment is called a mandate. Summarized, the military can only act when the government gives them a mandate, they cannot give a mandate to themselves.

The way mandates are given by the Minister of Defence is elaborated on in article 100 of the Dutch constitution. In the Dutch constitution, article 100 is presented as the following (Ministry of the Interior and Kingdom Relations, 2019, p. 21);

1. *The Government shall inform the States General in advance if the armed forces are to be deployed or made available to maintain or promote the international legal order. This shall include the provision of humanitarian aid in the event of armed conflict.*
2. *The provisions of paragraph 1 shall not apply if compelling reasons exist to prevent the provision of information in advance. In this event, information shall be supplied as soon as possible.*

Article 100.1 states that the Dutch government always has to inform the States General about military missions or actions before this is conduced. Article 100.2 states that an exception on 100.1 can be made, in case of classified or special operations. In this case, informing the States General should be done immediately afterwards (Defensiestaf, 2019).

The presented articles, article 97 and article 100, illustrate that the Dutch armed forces is firmly embedded in national politics and a clear choice has been made the military never can operate without a political mandate.

4.3 Dutch armed forces and international politics

Besides the fact the Dutch military is a politically-governed organisation inside the Netherlands, the Netherlands, and with that the Dutch military, are part of multiple international treaties and alliances. These international treaties and alliances mean that the Netherlands and with this the Dutch armed forces are involved in international politics as well. The North Atlantic Treaty Organization (NATO), the United Nations, and the European Union are well-known examples of this. Being part of these treaties and alliances means that the Netherlands will receive assistance and protection when needed, but has to fulfil duties and help other countries as well (Defensiestaf, 2019).

One of the most important treaties and alliances is NATO. NATO is a transnational political and military organisation with the aim of protecting the freedom and security of its member states. The NATO exists of multiple European states and North America. NATO itself has a limited amount of armed forces and for that reason, has to appeal to the armed forces of its member states when necessary (NATO, n.d.). Article 5 of NATO might be the best known part of the treaty and makes NATO what NATO is about; alliances.

Article 5 of NATO is presented as the following (North Atlantic Treaty Organisation, 2019);

"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

..."

Article 5 as presented above states that when one of the NATO member states is attacked, all of them are attacked. This means they will all stand up, fight, support and defend when one of them is being attacked (NATO, n.d.). In practise this means the Dutch armed forces have to take action and participate in international NATO missions, also when the Netherlands itself is not being threatened or attacked directly.

4.4. Deployment of the Dutch military

There is a difference between what the Dutch military can do on Dutch territory and on international territory. This can be found or be derived from article 97 of the Dutch constitution, presented before. As stated, article 97 of the Dutch constitution presents the tasks of the Dutch armed forces. With presenting the main tasks of the Dutch armed forces, it also indirectly implies what the tasks of the Dutch armed forces are not, since the Dutch armed forces can only do what is stated in the law.

4.4.1 Dutch territory

Despite the fact it is not written down literally, article 97 of the Dutch constitution implies that acting on Dutch territory is not one of the tasks or duties of the Dutch armed forces. Since this is the case, it became a part of common law that the Dutch military will never act on Dutch territory. Besides, it is in line with the Separation of powers and a can be seen as a mechanism to minimize the chance the Dutch armed forces will take over power.

There are some expansions on this law, that can be summarized as that the Dutch armed forces can act on Dutch territory, when they are explicitly asked for support by other civilian authorities as for example the Dutch police. A support request to the Dutch armed forces can for example be done in case of disasters and/or crisis management, for example during the Covid-19 pandemic, or when a civilian authority, as the Dutch police force, needs specific expertise. When the Dutch armed forces accepts the support request, the mandate and rules of the asking actor are the one that counts, what means it cannot actually be seen as a military action. This means that when someone from the Dutch armed forces gets a supportive role at the Dutch police force, he or she has to respect the mandate and rules of the police force instead of those of the Dutch armed forces.

4.4.2 International territory

For acting on international territory, other laws, rules and treaties matter. Two of the most important are the principle of sovereignty and the main UN principle that one State will never attack another State. Both these international laws and rules come down to the fact a State should never (uninvited) interfere with or in another State. Those in power of the concerning State has or have supreme authority and does not have to answer to other States (Defensiestaf, 2019).

There are three potential exceptions that can be made on the earlier presented international laws and rules when interference and/or use of force are approved (Defensiestaf, 2019). Firstly, a State always has the right of self-defence when being attacked (United Nations, 2021). Secondly, a State can interfere in another State when they are asked for help by the government of that State. About a third exception is discussion; a humanitarian intervention. The humanitarian intervention should be seen and used as a last resort and can only be used under strict conditions.

4.5 The Dutch Defence Organisation

The Dutch Defence Organisation consists of different components, departments and units. Figure 1, presented below, provides an organization chart of the structure of the Dutch Defence Organisation.

As presented in figure 1, the Dutch Defence Organisation is a politically-driven organization and with this an extension of Dutch politics. The Minister of Defence, the highest position in figure 1, is part of the Dutch government and is responsible for everything concerning the Defence organisation. The 'Staatssecretratis' [Secretary of State], a political position as well, and 'Secretaris-generaal' [General Secretary] are there to support the Minister of Defence. The 'Bestuursstaf' [Administrative staff] are the people who inform the minister and prepare, develop and carry out decisions concerning the policy that is being pursued by the Dutch military. De Bestuursstaf consists of multiple smaller departments with all a different focus and different tasks.

The 'Commandant der Strijdkrachten' has the highest military function in the chain of command, which means he or she is in charge of the operational commands of the Dutch military; 'de Koninklijke Marine' [the Dutch Navy], 'de Koninklijke Landmacht [the Dutch Land Force] and 'de Koninkijke Luchtmacht' [The Dutch Air Force]. The 'Commandant der Strijdkrachten' works closely with the minister and advises about military choices, issues and dilemma's. The 'Koninklijke Marechausee' is under control of the earlier mentioned General Secretary, could be seen as the Military police and performs tasks such as guarding the Dutch borders. The 'Defensie ondersteuningscommando', [the Defence Support command], on the left in figure 1, is there to arrange all the necessary things and services to make a mission run smoothly. Lastly there is the 'Defensie Materieel Organisatie' unit that organises everything concerning necessary material.

The presented chart in figure 1 shows the structure of the Dutch military organisation. It does not include all the different components, departments and units. The Defence Cyber Command is not shown in this figure, but is placed at the same level/line as the de Koninklijke Marine' [the Dutch Navy], 'de Koninklijke Landmacht [the Dutch Land Force] and 'de Koninkijke Luchtmacht' [The Dutch Air Force], under the direct command of the 'Commandant der Strijdkrachten'.

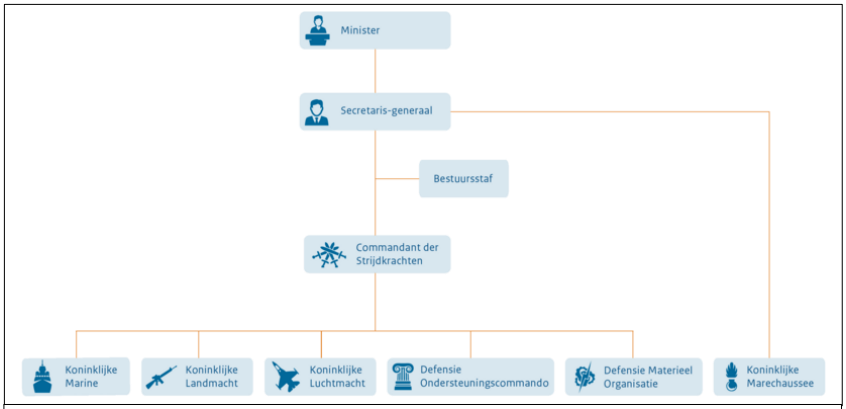

Figure 1: Organization chart Dutch Defence Organisation
Source: Ministerie van Defensie (2021)

4.6 The Defence Cyber Command

The DCC is a special unit of the Dutch Military established in 2014 as a reaction on the worldwide trend of (growing) hybrid- and cyber related threats. Not anticipating on this trend would have created a situation in which the Dutch military would no longer be able to fulfil its role in protecting and keeping the Netherlands safe (Ministerie van Defensie, 2012).

The DCC has multiple tasks, including protecting the Dutch cyber domain and infrastructure, protecting the Dutch Military as an organisation in the cyber domain, supporting Dutch commands with cyber elements when on mission and developing cyber related knowledge to keep up to date (Ministerie van Defensie, 2018c). In order to do this, the DCC can perform offensive- and defensive cyber operations (Ministerie van Defensie, 2020a). Offensive cyber operations are actions in the cyber domain with an offensive character and are performed with the aim to influence the opponent's actions or make it completely impossible for the opponent or enemy to act. Offensive cyber operations include hacking or invading the opponent's computers, networks or weapon systems. By performing offensive cyber operations, a so called deterrence strategy is created. A deterrence strategy arises when your (potential) opponent or enemy knows that you are able to perform cyber operations and are willing to do so and able to influence the opponent performing cyber operations against the Netherlands. This way the Netherlands makes itself less attractive as target of cyber-attacks, since the opponent knows that the Netherlands can and will strike back if they decide to attack (Defensie Cyber Strategie, 2016; Ministerie van Defensie, 2018b). On the other side there are defensive cyber operations. Defensive cyber operations are actions in the cyber domain with a defensive character, which includes monitoring networks and data or defending themselves when an offensive cyber operation of the opponent occurs (Ministerie van Defensie, 2012).

In addition to the cyber operations that the DCC performs, the unit is the centre of expertise on the subject as well. The Cyber Warfare and Training Centre, a section of the DCC, is established to reach this goal. This section is particularly concerned with the development of knowledge and skills in order to develop new capacities and strategies for the DCC in the cyber domain (Ministerie van Defensie, 2018a; Defensie Cyber Commando, n.d.).

Besides, the DCC has a close relation to the Military Intelligence and Security Service, since the DCC does not have a mandate to monitor or collect intel themselves. In the Netherlands, only two intelligence services do have this mandate; the MIVD and the AIVD (Defensiestaf, 2019). To monitor and collect intel, the two intelligences services work under specific legislation, the so called 'Wet op de inlichtingen- en veiligheidsdiensten' [the Intelligence and Security Services Act] (AIVD, n.d.). This law states very strict what these services can do, and with this especially what they cannot do. Both the MIVD and the AIVD make sure relevant and useful intel will be passed on to the right party to assess, process and use this information. For this reason the DCC depends on the intelligence services to stay up to date about what happens in the cyber domain and to prepare cyber operations. The DCC receives most of their intelligence from the MIVD (Ministerie van Defensie, 2018b).

4.6.1 Defence Cyber Command; a developing unit

The DCC is a relative young unit of the Dutch Military. Because of this, the DCC is still developing and exploring, with multiple improvements and implemented changes over the last few years as the result. During the interviews with the DCC staff members, three of these developments and changes were mentioned remarkably often; the change in structure, in its role, and in the position of the unit.

According to the respondents these three developments and changes have improved the DCC and its functioning in particular and will for this reasons be explained here in further detail.

4.6.1.1 Structure of the DCC

Firstly, as they performed their duties, the DCC realised the cyber domain is a much broader and more complex issue than just computers and hackers. According to the DCC respondents, computers and hackers have been the dominant frame of mind for too long, at the expense of other developments. In other words, the insight arose that computers are mainly a means to achieve a certain effect, but there are more mans and other knowledge and skills necessary in order to create the intended effect. Or, as one of the DCC respondents stated during one of the interviews;

"Cyber is about computers as much as air forces about the composition of the air"
(DCC staff member, 2021)

The main message here is that the DCC cannot just focus on computers and hackers alone, but needs a broader view and strategy, and with that a broader variety and diversity of knowledge and skills in order to be successful and complete. These were brought together in the staff, containing among others; the intelligence section, logistics section and finance section. As a result of this, the Cyber Defence Command has grown the past years, not just in the amount of employees but in the field of knowledge, skills and capacities as well.

4.6.1.2 Role

Secondly, the role of the DCC has changed over the years. The interviewed DCC staff members stated that, at first, the DCC mostly played a supporting role in the Dutch Military. This means that the DCC was mostly there to support other departments of the Dutch armed forces during missions or when requested on cyber related questions. Nowadays, the DCC is more active on its own and on a strategic level. This means they are not just depending on requests of other military departments anymore but carry out more commands and tasks themselves.

4.6.1.3 Position of the DCC

The last element of change that is presented here is the position of the DCC; literally as well as figuratively. At the first, the DCC was placed under the Dutch Land Forces. Here the unit did not get the space to develop or to make itself known as much as they needed. Later on, in 2018, the unit was placed under direct control of the Commandant der Strijdkrachten; the senior officer with the highest rank of the Dutch armed forces (Ministerie van Defensie, 2018a). All the interviewed DCC staff members have stated this has been a significant change, which allowed the unit to grow and develop. Figuratively the DCC occupies a new position, since it has been busy putting itself on the map, in the Defence organisation as well as in national politics, and created better understanding of the cyber domain. When the DCC was just established, the rest of the Dutch Military did not really understand what this unit did. They expected the DCC to be helpful if security camera's or infrastructure should be hacked. In reality, the cyber domain is much more than just hacking and nowadays other military units have a much better understanding of the role that cyber could play in their daily work now.

So, since the DCC is a relative new unit of the Dutch military, significant changes and developments have occurred since its establishment. These changes and developments helped the unit develop in a

positive way, made that others got a better understanding of the unit and that the unit got more room to act.

4.7 Conclusion 'Case description'

When necessary, the Dutch government can implement different instruments of power, including the Dutch military. Clear should be that the Dutch armed forces are not deployed very easily. Article 97 of the Dutch constitution presents its tasks, and there cannot be deviated from. Besides, a lot of different laws, rules, (juridical) restrictions, national and international political decisions have to be respected and made before a military action can start. The fact the Dutch armed forces always need a political agreement to get a mandate, shows that the Dutch armed forces is really one of the instruments of power of the government.

The DCC is a relative new unit of the Dutch armed forces. The DCC has multiple tasks in the cyber domain, from protecting the Dutch armed forces from cyber-attacks to be ready to perform cyber-attacks themselves. The DCC is a developing and chancing unit, the last few years, among others, its structure, role and position changed what benefited the unit. Important to realise is that the DCC must abide by the same rules as the Dutch armed forces in general, since it is part of the Dutch Defence Organisation, and for this reason can never act without a mandate.

5. The Defence Cyber Command fighting disinformation

This thesis explores how the DCC staff members perceive their role in the process of detecting and counteracting disinformation and their ability to act when disinformation occurs. This chapter will focus on the first part of this question, how the DCC staff members perceive their role in the process of detecting and counteracting disinformation. In order to present the debate of fighting disinformation as complete as possible, different experts on this topic are being interviewed as well. Their ideas and opinions on a potential role for the DCC in fighting disinformation are presented in the second part of this chapter.

As presented in the hypothesis in chapter 2, I expect the DCC staff members to state that they see detecting and counteracting disinformation as one of their tasks, firstly because spreading disinformation is seen as a strategy in hybrid-warfare and secondly because fighting disinformation would be in line with one of the main tasks of the Dutch military, namely protecting the Kingdom of the Netherlands. Besides, I expect the DCC to look at this differently than the majority of the interviewed experts, since literature research suggested that most scientists and journalists often focus on solutions for problem like theses without government involvement.

However, the interviews made clear that most of the DCC staff members do not see an active or leading role for the DCC in detecting or counteracting disinformation. Most of them state the government should take a leading role in this but should not necessarily deploy the DCC or Dutch armed forces in this process. However, the majority of the DCC respondents state that the DCC could have a supporting role in counteracting disinformation in case disinformation occurs. The following paragraphs will explain these findings in more detail. In paragraph 5.1 the ideas of the DCC staff members will be presented, followed by the ideas of the experts in paragraph 5.2. Paragraph 5.3 will provide an overview of chapter 5.

5.1 Defence Cyber Command staff members

5.1.1 Disinformation as a threat and use of force

Firstly it is important to know how the DCC staff members look at disinformation, if they experience it as a threat and if they see it as an use of force or not. This is important since it already tells a lot about how disinformation is seen and experienced in this military unit. In case disinformation is not experienced as a threat or seen as an use of force, the reasons for the DCC to fight it are hardly, or not at all, present.

It can be stated that all the interviewed DCC staff members see disinformation as a threat to society. They dominantly do so because of the undermining character disinformation has. More concrete, the DCC staff members fear for the effects of disinformation for the democratic rule of law and independent elections. What differs is how the respondents appreciate this threat, some of them just acknowledge the treat where others use strong words to describe it and state disinformation is a;

"… big and worrisome threat"
(DCC staff member, 2021)

In addition, the DCC staff members state they do not see disinformation as a problem for just Dutch society. They state that disinformation is a phenomenon that does not only undermine institutions and trust in the Netherlands, but has an effect on the NATO alliance and missions, as well as on European institutions. In other words, the DCC staff members see disinformation as a cross-border problem. This is in line with the in the Case description presented fact that the Dutch armed forces are part of the NATO alliance and European Union, and for this reason are active in NATO missions in the international context. It shows that the DCC staff members have a broader focus than on Dutch society alone and have to deal with this problem in the NATO context as well.

At the same time, most of the DCC staff members do not see disinformation (campaigns) as a so called use of force. You can speak of an use of force when people get hurt or die, or when physical damage is done (DCC staff member, 2021). The interviews made clear that only three out of eight DCC respondents state you can call targeted disinformation (campaigns) an use of force, but only under certain circumstances. The other five DCC respondents state you cannot call targeted disinformation (campaigns) an use of force. The question whether disinformation can or cannot be seen as an use of force matters, since it has consequences for what is (legally) seen as possible- and appropriate responses.

5.1.2 Fighting disinformation

Since its clear the DCC staff members experience disinformation as threat on the national and international level and some of them state it can be seen as an use of force, this paragraph will elaborate on how the DCC staff members think about fighting this threat, and more concrete if they think there is a role for their unit in this fight.

5.1.2.1 A potential role for the Defence Cyber Command

It could be stated that most of the DCC staff members do not see an active or leading role in the process of detecting and counteracting disinformation for the DCC. As presented in the operationalization in chapter 2, fighting disinformation can be divided in two pillars; detecting disinformation (professionally searching for disinformation and its source) and counteracting disinformation (action taken to end disinformation being spread and present in the Netherlands). Since detecting and counteracting disinformation are very different tasks with different rules and restrictions, these are separated in the presentation of how the DCC respondents perceive their role in this.

5.1.2.1a Detecting disinformation

As stated before, detecting disinformation is defined as professionally searching for disinformation and its source. During the interviews it became clear that all the DCC respondents agreed on the fact detecting disinformation is not a task for the DCC and will probably never be one. This is in line with the (current) laws and rules concerning monitoring and collecting intel, as presented earlier in the Case description of this thesis. The DCC respondents state that detecting disinformation can be seen as collecting intel and should for that reason be a task for intelligence services. In addition, the DCC staff members do not see this change in the (near) future and moreover, do not want it to change. Their common reason for this is that they think it will be at the expense of the democratic values of the Netherlands when an executive unit, as the DCC, will start to perform tasks like collecting intel or detect disinformation, since the necessary checks and balances are not present in those units.

5.1.2.1b Counteracting disinformation

As stated before, counteracting disinformation is defined as action taken to end disinformation being spread and present in the Netherlands. According to the DCC respondents, the DCC could play a supporting role in counteracting disinformation, but think there are more suitable parties and institutions to counteract disinformation.

During the interviews some of the respondents questioned whether the DCC or the Dutch armed forces in general should have a task like this. They acknowledge the fact the Dutch armed forces have much knowledge of and experience with acting in crisis situations and fighting threats, but not specifically on fighting disinformation. These respondents think there are more suitable institutions in the Netherlands, as for example the NCTV.

But, according to a majority of the respondents this does not mean there is not any role for the DCC in counteracting disinformation. When the government decides to take action against the spread of disinformation and states countermeasures are needed, the DCC could act in a supporting role and could perform this action. A potential countermeasure would for example be to hack the disinformation spreading company, group or person. To sketch how this could look like, the case of a provocation video in the Ukraine-European Union referendum is used as an example.

Provocation in the Ukraine-EU Association Agreement referendum

In January 2016, a few months before to the EU-Ukraine *Association Agreement* referendum, a YouTube video was published in which multiple Ukrainian soldiers from the Azov battalion stated they will commit terrorist attacks in the Netherlands in case the Dutch will vote against the EU-Ukraine agreement in this referendum. In order to reinforce their message, they burned the Dutch national flag in the video. However, the Azov battalion and the Ukrainian government immediately denied to have anything to do with the video and stated the video, and with this the threat, was fake and staged by another organisation or group (Smeets, 2016).

Although the threat was fake, the disinformation in the video could have had, or maybe even has had, an influence on how Dutch people look at the referendum. Seen the directness and intensity of the threat, the Dutch government could have decided to react on it by trying to unmask and attack the publisher of the video by hacking them. In order to perform these countermeasures, a mandate to do so could have been provided to the DCC.

Keep in mind that this is just a simple illustration of what the DCC respondents see as example of a situation in which the DCC could provide a potential countermeasure. As explained in the Case description, there are a lot of requirements that must be met before the DCC and Dutch armed forces in general, can carry out an action like this in reality.

Notable to mention is that there is no consensus between the DCC respondents, since not all them agree on the fact the DCC could (just) have a supporting role in counteracting disinformation. Where the majority of the respondents agreed on the fact the DCC could have a supporting role in fighting disinformation, the three other DCC respondents were very outspoken, either positive or negative, about this. One of the DCC respondents really is convinced of a role for the DCC in counteracting disinformation, and not just a supporting one. According to the respondent, counteracting disinformation is in line with the lines of effort of the DCC, and for this reason is their duty. Moreover,

the respondent states that the DCC should want to do it, take responsibility and see it as one of their (basic) tasks.

At the same time, two other DCC respondents call it very unlikely for the DCC to play (any) role in the process of counteracting disinformation. They state it will, from a juridical perspective, be very complicated to do so. According to them, disinformation cannot (judicially) be seen as an use of force, which complicates a legitimate response. This will be explained later on in more detail. In addition, they state it should not be a task for a governmental organisation to interfere in a discussion about what is the truth and what is not, which is according to the respondents what will happen here. In addition, they state it is unlikely for the DCC to counteract disinformation since the societal support of the Dutch Military Organisation is quite low at the moment. They expect that society would not accept measures taken by the Dutch armed forces and DCC to fight disinformation or the fact they will be involved in this, since citizens could get the impression the Dutch armed forces is keeping an eye on its citizens which is, as presented in the Case description, not a task for the DCC or Dutch armed forces in general.

5.1.3 A leading role for the government

Since the majority of the DCC respondents do not see a role for the DCC in the process of detecting and counteracting disinformation, it is interesting to see that most of them do place this responsibility with the Dutch government. Most of the DCC respondents state it is the government's duty to protect Dutch society and its citizens from threats, including disinformation. One of the respondents specifically stated that;

"You could see disinformation as a form of criminal behavior, and since the government is fighting crime because of its negative influence on society, disinformation is something the government could takes measures against as well"
(DCC staff member, 2021)

Despite the fact most of the DCC respondents agree on the fact the government should take a leading role in fighting disinformation, they do not agree on how this should be done or who should be doing it. One of the respondents states it should be a task for the Ministry of General Affairs, where five other respondents state that it should be a task for the Dutch intelligences services.

More specifically does a significant number of the DCC staff members plea for a governmental interdepartmental security council in order to fight disinformation. In this interdepartmental security council different governmental departments should have a seat, as for example the Ministry of the Interior and Kingdom Relations, The Ministry of Foreign Affairs and the Ministry of Justice and Security but also more substantive miniseries as the Ministry of Economic Affairs and Climate Policy and Ministry of Social Affairs and Employment. The idea behind this security council is that; firstly, experts on different themes are present and secondly, everyone's interest can be represented when deciding on how to fight against disinformation. Firstly, it is important to bring experts on different themes from different departments together. The reasons for this is that disinformation is not targeted on just one group, party or department and can be about different themes, which makes there is not one person or department expert on all the disinformation that is being spread. The fact experts on different themes from different departments would all be part of this interdepartmental security council makes that all kinds of disinformation on different themes can be recognized. At the same time, this security council is important since this way everyone's interest can be represented when deciding on how to

fight against the actual occurrence of disinformation. According to one of the DCC respondents (2021) this is important since disinformation is being spread by countries that are our (trading) partners at the same time. An interdepartmental security council would be necessary to determine what the next steps will be, since something has to be done against the spread of disinformation but without hurting the partnership. In other words, this council should be take into account everyone's interest while thinking about a strategy to fight against disinformation.

"… a threat for one can be an opportunity for the other"
(DCC staff member, 2021)

At the same time, one of the other interviewed DCC staff members warns about the often viscous and bureaucratic character of councils like these. The respondent states it is important to limit these effects, since disinformation is an elusive and rapidly spreading threat, that could escape our concentration when reacting to slow or waiting too long.

5.1.4 Summary 'Defence Cyber Command staff members'

The interviews conducted made it clear that the majority of the DCC staff members do not see an active or leading role for the unit in fighting disinformation. Most of the respondents question a role for the Dutch armed forces in this process in general and state there are more suitable institutions in the Netherlands to do this. However, according to the majority of the DCC respondents, the DCC could play a supporting role in fighting disinformation, meaning they could perform countermeasures provided that they get the mandate to do so.

5.2 Experts

In order to include and present the complete societal debate on disinformation in this thesis, different experts on the topic of disinformation and fighting it are interviewed as well. Surprisingly, the interviewed experts are divided on the question if the DCC should play a role in detecting and counteracting disinformation. Literature based research suggested that most scientist and journalists would state a role for an extended part of the government would be in conflict with Dutch democratic values. However, some of the interviewed experts do actually plea for a role for the DCC, or the Dutch armed forces in general, in detecting and counteracting disinformation. This paragraph will present more details on these findings.

The interviewed experts can be divided in two groups. The first group of experts consists of six experts without any connection to the Dutch armed forces or Ministry of Defence in general. The second group of experts consists of four respondents that are related to the Dutch armed forces or Ministry of Defence in one way or another, but not to the DCC. More information on the respondents or the two different groups of respondents can be found in the methodology chapter of this thesis.

5.2.1 Disinformation as a threat

Just like the DCC respondents, the experts were asked about how they look at disinformation and if they experience it as a threat. It became clear that, just like the DCC respondents, all interviewed experts see disinformation as a threat to society. Besides, they all agree with one another by naming the same unwanted effects of disinformation as its undermining character, which causes polarization and lose of trust in society. In addition, they expect disinformation to have or already have had an (unwanted) effect on the democratic rule of law and elections. Besides, in their view, disinformation

can undermine the trust in (democratic) institutions and different groups in society. Long term this could lead to a situation in which people do not know who or what to trust anymore with the result that;

"… Dutch society will transform into a kleptocracy"
(Van der Meer, 2021)

A kleptocracy is a society in which the people in power make themselves powerful and rich at the expense of others, a society led by thieves (Cambridge Dictionary, 2021). When using this concept, Van der Meer refers to a society in which the people in power are not afraid to use for example disinformation to improve their position and with this create a society in which people do not know who to trust and what to believe anymore. The quote shows some of the worries Van der Meer has; the negative and undermining effects disinformation can and will have on our society and the big structures our society is built upon. He states that if nothing is done, in order to fight disinformation, a kleptocracy will be the future of Dutch society.

5.2.2 Experts on a potential role for the Defence Cyber Command in fighting disinformation

Both the groups of experts, related and unrelated to the Dutch armed forces, were asked for their thoughts on a potential role for the DCC in fighting disinformation. Overall it can be stated that both groups of experts are divided on this question, which is interesting since I expected them to be on the same page per group. However, it seems that three of the experts who are not related to the Dutch armed forces, Van der Noorda, De Ridder and Duyvesteyn, and two of the experts who are related to the Dutch armed forces, Heida and Bouwmeester, think there could be a role for the DCC in fighting disinformation. At the same time, there are two experts who are not related to the Dutch armed forces, Jacobs and Van der Meer, and two of the experts who are related to the Dutch armed forces, Ducheine and Pijpers, who do not see a role for the DCC in detecting and counteracting disinformation.

One respondent, Romein, takes a middle position in this debate and states the DCC could possibly play a role in the process of detecting and counteracting disinformation, but not necessarily. Romein questions if the Dutch armed forces and DCC are the most suitable institutions to perform this task because of juridical restrictions. At the same time, the respondent does not exclude the possibility the DCC will, now or in the future, become more suitable to perform this task.

5.2.2.1 Experts who see a potential role for the DCC

As stated, a total of five experts, both related and unrelated to the military, see a potential role for the DCC in fighting disinformation. Their main argument for this is the same; the State has a duty to protect its citizens and can deploy the military to do so. Since disinformation is a threat to Dutch society, the Dutch armed forces and the DCC specifically could and should be deployed in fighting disinformation.

"I think it is important that countries, and especially their military organisations, develop knowledge concerning these threats and monitor these threats as well as the technical developments surrounding it. And organise its defence against this threat."
(De Ridder, 2021)

"I think this should be a task for the Dutch armed forces, especially since it is about hybrid-warfare and international politics"
(Van der Noordaa, 2021)

Duyvesteyn, De Ridder and Van der Noordaa, all non-related to the Dutch armed forces, state there could be a role for the DCC in fighting disinformation. The three experts agree on the fact the most important factor is that the rules and restrictions for tasks as these should be very clear, in order to prevent wrong decisions or judgements for being made, as has happened before in the LIMC case[1]. Where Duyvesteyn and De Ridder think current frameworks should be evaluated, and if necessary, improved in order to fight 'upcoming' hybrid-warfare threats as disinformation, Van der Noorda thinks this should be able to do within the current rules and juridical framework;

"I think it would be a missed opportunity if the Dutch armed forces would not fulfill this task and I even think this could be done within the current juridical framework."
(Van der Noorda, 2021)

Respondents Heida and Bouwmeester, both related to the Dutch armed forces, state there could be a role for the DCC, but make a strict distinction between detecting and counteracting disinformation. They state there is not a role for the DCC in detecting disinformation, since detecting, monitoring and collecting intel, and with this detecting disinformation, is a task for the Dutch intelligences services and should not be performed by an executive unit like the DCC. At the same time, they both do see a role for the DCC in the process of counteracting disinformation. They state the DCC can have the role to counteract disinformation when this appears.

5.2.2.2 Experts who do not see a potential role for the DCC

As stated, there are experts who state there is not a role for the DCC in fighting disinformation as well. Non-military related expert Jacobs states we do not need a governmental organisation to fight disinformation. He states the problem of disinformation could be solved by focussing on the authenticity of information. Van der Meer is not convinced of a role for the DCC in fighting disinformation either. He states this task should belong to the Dutch intelligence services instead of the DCC. He states this because of the fact the intelligence services have a (more suitable) mandate to do so and have the right internal democratic checks and balances. Van der Meer states tasks like these should not be done by executive unites like the DCC, where the democratic checks and balances are not present in order to protect our democratic society.

[1] *In 2021 the Land Information Manoeuvre Centre (LIMC), a relatively new unit of the Dutch land forces, was strongly criticized. The unit its task was to track and analyse prevailing narratives and societal developments, which includes among others the supply and distribution of disinformation on different themes (Ministerie van Defensie, 2020b). However, the LIMC only used open sources to monitor, outline and predict societal developments and wasn't interested in collecting information concerning individuals it became clear that LIMC violated national laws and rules concerning the processing of personal data and operated without the necessary mandate (Rosenberg & Berkhout, 2020).*

"We live in a democratic rule of law, that we must uphold. We should be careful and prevent a situation in which we are using instruments to protect our democratic rule of law against the threat of disinformation and by doing so harming that very democratic rule of law."
(Van der Meer, 2021)

Respondents Ducheine and Pijpers, both related to the Dutch armed forces, do not see a role for the DCC in the process of detecting and counteracting disinformation either. Their main argument is that, from a juridical perspective, it will be very difficult to do so and they question whether you should want to place a task like this with a governmental unit. Moreover, the respondents state, even when it turns out the DCC and Dutch armed forces will receive all the necessary mandate and tools to do so, the DCC will not be the right institution to perform this task. Ducheine states there are more suitable institutions to fight this threat and questions if fighting disinformation should be places by a cyber-related unit, since;

"Disinformation is more than just operating in the cyber domain, so it is not such a logical assumption that the DCC would be concerned with that."
(Ducheine, 2021)

5.2.3 Summary 'Experts'

From the interviews it became clear that the ideas and opinions concerning a role for the DCC in fighting disinformation differ between the interviewed experts. Noteworthy is that these differences run through the two groups alike; both within the armed forces-related and the non-armed forces related expert group there are very different opinions on the desirability of a role for the DCC in fighting disinformation. Apparently the nature of the relation of the expert with the armed forces has no predictive value in this and other factors and/or considerations are more decisive.

Noteworthy is also that, broadly speaking, the Dutch armed forces related experts treat the questions along the same lines as the DCC respondents. Despite the fact these experts have different opinions and ideas about a potential role for the DCC, they do think about and consider the same factors and circumstances, like the juridical restrictions. Even more interesting is the fact this group of experts comes to different conclusions on the question whether the DCC should play a role here.

The non-Dutch armed forces related experts are divided on the question as well. Both the experts in favour of a role for the DCC and the experts against this idea who belong to this group take in consideration existing the juridical restrictions. The non-Dutch armed forces related experts who are in favour of a role for the DCC state the current frameworks might be evaluated and when necessary be adjusted. Other experts in this group are against that because of, in their opinion, the lack of democratic checks and balances in executive institutions like the DCC when they would be performing tasks like these.

5.3 Summary 'The Defence Cyber Command fighting disinformation'

This chapter presented the research outcomes concerning a potential role for the DCC in fighting disinformation. Three groups of respondents were interviewed; DCC staff members, experts who are related to the Dutch armed forces and experts who are not related to the Dutch armed forces.

Summarized it can be stated that all the respondents see disinformation as a serious threat to society because of its undermining character. However, the respondents think differently about a potential role for the DCC in fighting disinformation. There seems to be no connection between their point of view concerning whether or not the DCC should play a role in this and their own organisational backgrounds, since all three groups have respondents who are in favour of a potential role for the DCC as well as respondents who are against a role for the DCC in fighting disinformation. Their individual views and risk assessment with regard to such a role for the DCC seem much more decisive.

6. The ability to act

This thesis explores how the DCC staff members perceive their role in detecting and counteracting disinformation and their ability to act when disinformation occurs. The first part of this question was focussed on in chapter 5 of this thesis. This chapter will focus on the second part of this question, namely the potential ability of the DCC to act in case disinformation occurs.

As presented in the operationalisation in chapter 2 of this thesis, the ability to act for the DCC in occurrence of disinformation is based on two factors: the legal framework and the necessary resources such as knowledge and skills. This chapter is based on the semi-structured interviews conducted with DCC staff members, and mostly on those conducted with the legal advisors of the DCC. Additionally, as presented in chapter 2 as well, I expect the DCC to play an active role in fighting disinformation. In other words, I expect that they are doing this under the current frameworks or, if this is not the case, that they are at least actively thinking about how to create conditions making that possible and work.

However, it can be stated the DCC's ability to act in occurrence of disinformation is very limited because of juridical restrictions. This means the DCC does not play an active role in fighting disinformation at the moment. These findings will be explained in further detail in the three following paragraphs. First, in paragraph 6.1, the legal framework will be explained and applied to disinformation and the DCC. Secondly, in paragraph 6.2, the knowledge and skills the DCC has and/or needs in order to fight against disinformation of will be presented. In the conclusion of this chapter, paragraph 6.3, a summary about the ability of the DCC to act in occurrence of disinformation will be presented.

6.1 Legal Framework

This paragraph will provide insight into how the legal framework can be applied to the fight against disinformation in context of the ability of the Dutch armed forces and the DCC to act. More concrete, will paragraph 6.1.1 describe the legal framework and will the juridical principles be applied to disinformation. In paragraph 6.1.2 these principles will be applied to the DCC specifically.

6.1.1 The juridical principles and disinformation

6.1.1.1 Sovereignty, the use of force and self-defence applied to disinformation

As presented in the Case description, the principle of sovereignty is one of the most important international legal principles. It states that those in power of a State (the government) have supreme authority within that State's territory. This means that States do not have to answer to other States, other States cannot interfere in the State's internal affairs without an invitation and States are not allowed to use force against each other (Defensiestaf, 2019). When a certain State violates this international law and unjustifiably uses force against another State, the 'attacked' State has the right to defend itself with force, called the principle of self-defence.

In the case of targeted disinformation campaigns from one State to another, the principle of sovereignty, and with this international law, may be violated (Legal advisor DCC, 2021). When a state-concerted or -directed disinformation campaign aims to influence, for example, the public debate and stability in the targeted State, this could qualify as an unwanted and uninvited interference in internal political affairs and thus as a violation of the principle of sovereignty.

However, the DCC legal advisor states that, in principle, disinformation and targeted disinformation campaigns cannot be seen or labelled as an use of force in a legal sense and the chance this will change in the future is very small. The reason for this is, according to the DCC legal advisor, that an use of force has to cause injury, death or damage, and disinformation (often) only has an indirect effect, since it is highly unlikely that disinformation would directly cause injury, death or damage. Rather, disinformation is used to manipulate public opinions or incite persons to take certain actions (which might include actions that cause injury, death or damage). Disinformation can in this case potentially be seen as the reason or motivation why something happened, but it is not the disinformation itself that led to this damage. Although it is certainly possible that a disinformation campaign qualifies as a use of force, for example if a State manages to incite mobs to riot, loot and plunder, or even contribute to social unrest that escalates into a civil war, there are two difficulties in planning a suitable response. Firstly, it will be practically very difficult to attribute the acts of the persons to a particular and specially described disinformation campaign, since disinformation often has an indirect effect. Secondly, it will be difficult to attribute the disinformation campaign to a particular State, since disinformation can be spread unobtrusively and anonymously. Operations in the cyber domain, and with this the spread of disinformation, can for example be done over someone else's server(s) or by using fake accounts. According to the DCC legal advisors, these two factors have an influence on performing a suitable response, since it depends firstly on the answer to the question whether the disinformation campaign can be labelled as a use of force and secondly if the responsible State can be identified and hold responsible. This is why it is unlikely, if not impossible, that disinformation in practice will be labelled as a use of force or the principle of self-defence can be applied in a practical situation. Both these issues are not restricted to disinformation but apply to the cyber domain at large, which makes countermeasures and the right of self-defence in the cyber domain very complex.

6.1.1.2 The plea of necessity

The plea of necessity is a customary international law principle that allows a State to take any necessary action, including an use of force, against another State if and insofar this is necessary to avert a threat that is so critical that the victim State has no choice but to act that way. The necessary action must be proportional to the threat and must be ceased as soon as the threat is over. A major difference between the plea of necessity and the earlier presented principle of self-defence is that in the case of the plea of necessity, it is not necessary that a threat is attributed to any particular actor; the plea of necessity is aimed against the threat itself, regardless of the attribution. On the other hand, most States agree that the plea of necessity can only be invoked against threats against their most critical assets the destruction of which could cause partial collapse of society, as for example (critical) national infrastructure.

The DCC legal advisor states that the plea of necessity can be used in the cyber domain as well. The respondent gave the example of when a current threat in the cyber domain comes from servers that are in another State than your own. Because of the principle of sovereignty you cannot just interfere with the serves that are attacking you. In this case you can contact and cooperate with the State in which the respective servers are located, but when there is limited time and/or the only way to mitigate this current threat is by shutting down the servers immediately, this could be done under the plea of necessity if the threat is severe enough. The complex, unobtrusive and anonymous character of the cyber domain is shown here again, since the servers form which the threat originated do not necessarily have to be the servers of the State that is behind the threat.

Theoretically the plea of necessity can be applied to the phenomenon of disinformation as well. A possible limiting factor is that disinformation campaigns are often conducted very scattered and over a longer amount of time, which makes it unlikely that the plea of necessity could be applied at one certain point in time within such a campaign, as it would be difficult to pinpoint the exact origin of the threat. Indeed this is the entire concept of hybrid warfare; States conduct hostile action, using the entire arsenal of State powers, which may be unlawful but remain below the level of seriousness that would justify an armed response. But, as the legal advisor of the DCC predicts, the plea of necessity will, sooner or later, be used to mitigate disinformation campaigns as well.

6.1.2 Juridical principles applied to the Defence Cyber Command

As explained in the Case description, the DCC is an executive unit of the Dutch armed forces, a governmental entity, and for that reason can only do what the government is authorised to do. This means that the DCC needs a mandate before they can act. Moreover, within the Netherlands, the DCC can only be deployed either for national self-defence purposes or in support of civilian authorities if requested.

As stated in the operationalization in chapter 2, there are two pillars in fighting disinformation; detecting disinformation (professionally searching for disinformation and its source) and counteracting disinformation (action taken to end disinformation being spread and present in the Netherlands). In this paragraph these ability to act of the DCC when disinformation occurs will be presented on the basis of these two pillars.

6.1.2.1 Detecting disinformation

As stated, detecting disinformation is professionally searching for disinformation and its source. Based on the national laws and rules concerning the mandate to monitor or collect intel, as presented in the Case description, in combination with the semi-structured interviews with the DCC staff members, it became clear that the DCC has no legal basis to professionally detect disinformation. Intelligence collection is the responsibility of the two Dutch intelligence agencies, the AIVD and the MIVD, since they have the mandate to do so. Since the DCC does not have this mandate, and probably will never get it either, the DCC is not able, in the way that they are not allowed or authorised, to detect disinformation in case disinformation occurs.

6.1.2.2 Counteracting disinformation

As stated, counteracting disinformation is taking action to end disinformation being spread and presented in the Netherlands. Based on the national laws and rules, as presented in the Case description of this thesis, and the for this thesis conducted interviews with the DCC staff members, especially the DCC legal advisors, it became clear that in the current situation, the ability to act for the DCC (on its own) in counteracting disinformation is very limited from a legal perspective.

The ability to act for the DCC to counteract disinformation when it occurs is limited because of the fact the DCC can only perform an action when the disinformation campaign can be labelled as an use of force violating the principle of sovereignty. When this is the case, the DCC could perform an action under the principle of self-defence, but only when the mandate for this is given. However, expectations that this will happen are low, since it seems unlikely that disinformation campaigns will be seen as an use of force. A different situation occurs when, as presented in the Case description, another national civil institution, as for example the Dutch police, asks the DCC for help in order to counteract

disinformation. In this situation the DCC plays a role in counteracting disinformation but by helping a civil institution and under the mandate of that institution. In other words, there are opportunities in which the DCC could play a role in counteracting disinformation, but this will mostly be a supporting role.

6.2 Necessary knowledge and skills

Other elements on which the ability of the DCC to act when disinformation occurs are based on knowledge and skills. With knowledge is meant the technical- and substantive know-how knowledge to set up and to carry out an action, and with skills is meant the ability and dexterity to perform an action. As will become clear in this paragraph, the two mentioned elements knowledge and skills are not the limiting factor in the ability of the DCC to act.

6.2.1 Knowledge

In order to cause effects in the cyber domain, different forms of knowledge are needed. For this reason most of the DCC respondents plea for teams consisting of employees with diverse types of knowledge. Firstly technical knowledge is required, so you need people who understand how different computers work and how you can influence and control them. Besides technical knowledge, substantive knowledge is needed. Substantive knowledge is needed in order to understand and be able to give meaning and direction to concepts as conflict and war, as well as to intended effects of acting. According to the DCC respondents this can be arranged when the organisation recruits more staff members with different (study-)backgrounds as for example an anthropologist, a behavioural scientist or a political scientist, but also people with more specific knowledge as for example an economist or criminologist. Since, as presented in the Case description as well, the focus at the DCC has dominantly been on hacking in the first few years of their existence, technical knowledge is present at the DCC. Despite the fact the DCC is broadening their scope the last few years, more substantive knowledge is wished for.

Specified to detecting and counteracting disinformation it became clear that the DCC does not have the knowledge to detect disinformation. According to the DCC respondents this is because of the fact that detecting disinformation is beyond the scope of the unit and for this reason the DCC did not organise or implement this knowledge. Looking at counteracting disinformation on the other hand, the DCC does have the necessary knowledge. Since the fact counteracting disinformation will mainly be based on technical cyber knowledge, the necessary knowledge to perform these asks and achieve these effects, is present at the DCC.

6.2.2 Skills

The DCC staff members are permanently working on their skills. This consists of practising the current ones and developing new skills in order to create cyber-effects when needed. Despite the fact the DCC respondents state they do have the necessary cyber skills, it is important to keep training, developing and expanding those skills, since the cyber domain is changing very quickly. A complicating element is that the DCC is quite limited in its opportunities to train and test its skills because of juridical restrictions. This element is mentioned by multiple DCC respondents and experts related to the Dutch armed forces. Heida, of the Counter Hybrid Unit, states training cyber skills is complicated since there are no specialized training environments for the DCC as there are for other military units, like shooting ranges or other training grounds. When trying and testing cyber skills you soon end up in the real

world, which is forbidden since it will bring about a real effect. As presented in the Case description, the Dutch armed forces and DCC can only act when a mandate, an political assignment, is given and that is something that is not happening for training purposes. This does not mean the skills of the DCC are not trained at all, but they are limited to in-house exercises or organised training in the NATO context.

Specified to detecting and counteracting disinformation, the DCC respondents stated that the DCC does not have the skills to detect disinformation since this task is beyond their scope. However, with regard to counteracting disinformation, the DCC does have the necessary skills to take countermeasures when disinformation occurs, which means in theory they could.

6.2.3 Cyber Warfare & Training Centre

According to most of the DCC respondents the Cyber Warfare & Training Centre could play a leading role in developing new knowledge and skills. The Cyber Warfare & Training Centre has, as presented in the Case description, expertise on the subject of cyber and is, among other tasks, concerned with the development of knowledge and skills in order to develop new capacities and strategies for the DCC. According to the majority of the DCC respondents the CWTC should for this reason assess which techniques the DCC should invest in and why and thereafter provide the DCC with the necessary knowledge.

6.3 Summary 'Ability to act'

This chapter has made clear that the DCC is very limited in their ability to act when disinformation occurs. This is mostly because of the current juridical framework the DCC, and the Dutch armed forces generally, have to adhere to. Firstly, the DCC cannot play a role in detecting disinformation, since it is juridically determined that this is a task for the Dutch intelligences services only. In addition, the DCC does not have the knowledge and skills for this, these have not been organised simply because of the fact it is beyond the scope of the unit. At the same time, counteracting disinformation could be done by the DCC, but this seems unlikely since it depends on how disinformation campaigns are seen and labelled. The fact disinformation campaigns can, from a juridical perspective, at this point in time not be labelled as an use of force makes that the options to react on it are limited. A possible option for the future, since it has not happened up to now, is responding to disinformation campaigns under the plea of necessity. Whether the DCC has the necessary knowledge and skills to counteract disinformation depends on how counteractions will be shaped and organised, but is seems like they do have the basic facilities. In other words, the fact the DCC is not able to fight against disinformation at this moment in time is due to the current legal framework and not because of a lack of the necessary knowledge and skills.

7. Discussion

The two pervious chapters made it clear that the majority of the DCC respondents does not perceive an active or leading role for the DCC in the process of detecting and counteracting disinformation. However, most of them state the DCC can play a supportive role in this process, meaning they could potentially take the necessary countermeasures when disinformation occurs. In addition, it became clear that the ability to detect and counteract disinformation by the DCC is restricted by the current legal framework, laws and rules and the lack of a mandate to do so. This makes that even when the DCC respondents would have perceived an active role in the process of detecting and counteracting disinformation for the DCC, the opportunity to actually perform that role would be severely limited by the legal restrictions.

In addition, it is noteworthy that the differences in opinion between the DCC respondents on the one hand and the interviewed experts on the other, about a potential role for the DCC were not what I expected them to be. Based on literature research and as presented in the hypothesis in chapter 2, I expected to find that the non-military experts and especially the scientists and journalist among them, would dominantly plea for societal measures without the interference of the government in order to fight disinformation. At the same time, I expected the DCC respondents to plea for a role for a national security institution like the DCC in this fight. However, it turns out the opinions are not divided along the lines I expected them to be. Fact is that both the DCC respondents and the experts are divided among themselves; some of them state fighting disinformation is not a task for the DCC and the government, where others state it is. This outcome shows that the way the respondents look at a potential role for a national security institution like the DCC in the process of detecting and counteracting disinformation, is not so much based on their (scientific- or organisational) background, but in fact dominantly on the way they look at the question which are the most effective ways to fight disinformation on the one hand and what they perceive as the risks and dangers of certain strategies to counteract disinformation on the other. In addition, the way they look at the current (juridical) frameworks also influences their preferences.

As stated, I also expected this research to show that the DCC respondents would see it as their duty to fight disinformation because of two reasons. Firstly, because of the fact disinformation campaigns can be seen as a hybrid- and cyber threat (to the Kingdom of the Netherlands). Secondly, because it is one of the main tasks of the Dutch armed forces, and with this the DCC, to protect the Kingdom of the Netherlands against threats. However, this research had shown this is not the case. As stated, the majority of the DCC respondents does not perceive an active or leading role for the DCC in the process of detecting and counteracting disinformation and state the government and an interdepartmental security council should take this responsibility. Moreover, some of the DCC respondents questioned whether the Dutch armed forces should play a role in fighting disinformation at all, and stated there are more suitable institutions in the Netherlands to do so. I think this outcome is remarkable since it is one of the main tasks of the Dutch armed forces and DCC to be pro-active on fighting threats and protecting the Kingdom of the Netherlands. In addition, all the DCC respondents are of the unanimous opinion the disinformation is such a threat.

Besides the observation in the previous paragraph, I think it is surprising that a majority of the DCC respondents puts the responsibility to fight the threat of disinformation by the government and an

interdepartmental security council. I think this is surprising, since both these entities do not have a specific focus on cyber and cyber-related threats. The fact that the DCC is a specialised cyber unit in combination with the fact that disinformation is dominantly being spread through social media, made me expect that the DCC respondents would perceive fighting disinformation as a suitable task for the DCC. What this seems to show is that there is no consensus on the question whether the threat of disinformation is dominantly to be characterised as a cyber related issue. In the course of my research I realised cyber is not just about hacking, but also on how certain effects in the physical world can be brought on the basis of cyber. However, I think that fighting disinformation, in this moment in time, cannot be seen as a completely separate issue from the developments in the cyber- and social media domain. Understanding and mastering the tactical and technical aspects of this is just as important as understanding and mastering the societal impact aspects, as presented in the literature review. Eventually, when all is said and done, I think a State will always need the tactical and technical capacities to be able to literally defend itself in the cyber domain against cyber-related threats like targeted disinformation campaigns. So, a State always will need a unit that is capable and able of doing just that, within the armed forces or elsewhere.

A possible explanation for why the majority of the DCC staff members do not perceive a role for the DCC in fighting disinformation is the fact that most of them state (targeted) disinformation campaigns cannot be seen as an use of force. One of the most concrete conditions an action should meet before it can (juridical) be called an use of force is that, as a result of this action, people have to get hurt or die, or physical damage has to be done (Interviewed DCC staff member, 2021). As presented in the Case description, International Law and the principle of sovereignty make that a country can only use force in another country when they are asked for help or in the case of self-defence. This makes the question if targeted disinformation campaigns can or cannot be seen as an use of force important, since it has (juridical) consequences for what are seen as (legal) legitimate and appropriate responses or possible countermeasures when disinformation occurs. Since the Dutch armed forces, and with this the DCC, are pro-active on reacting to the use of force, this (indirectly) means that when disinformation is not seen as an use of force, the DCC would not even be able to play a role in fighting it. In other words, if disinformation is not seen as an use of force, the DCC and Dutch armed forces cannot be deployed to fight it, since, in juridical terms, there is nothing to respond to. From the data presented in chapter 5 it became clear that the majority of the DCC respondents state disinformation campaigns cannot be seen as an use of force, which has been confirmed in chapter 6, what makes that the military unit is not able to respond to this threat, with the result the DCC respondents do not perceive a role for their unit in fighting this threat.

The fact there is no consensus between the DCC respondents on a potential role for the DCC in detecting and counteracting disinformation leads to the question if this is because of the current frameworks and discourse they are in, or if they really think this should not be a task for their unit. As presented in the literature review, military organisations often have an organizational culture in which discipline, a professional ethos, tradition and cohesion are central elements, which are function elements in fighting battles but could form obstacles to innovation and change in the organisation (King, 2020; Chinn & Dowdy, 2014; Levesque, 2013). In this case it could be that the DCC staff members do not see fighting disinformation as a task for the DCC since it does not fit the current frameworks and is something they have never done before. In addition, it could be 'difficult' for staff members in this organisation who think about thing differently to speak out, because of the fact this is not in line with the strict military organizational culture. Although this cannot be concluded on the basis of this

thesis, since it is not directly asked to the DCC respondents and in even in case it was, the respondents might answer 'correctly in line with their discourse', not even knowing or realising they might be affected or influenced by it, this is important to think about. Clear is that disinformation is a growing hybrid-threat that affects States all over the world, including the Netherlands. Questioning, critically rethinking and debating the current frameworks is important and more out-of-the-box thinking should be done, within the DCC, the Dutch armed forces in general and beyond, in order to identify, select and/or constitute the most suitable (network of) parties and organisations to fight this threat and limits its influences.

What makes this thesis societal relevant is that it has provided insight into the debate who should play a role in fighting disinformation, and more concrete if the DCC could be the national security institution performing this task. As stated, the DCC does not perceive an active or leading role for themselves in the process of detecting and counteracting disinformation nor do they have a mandate to do so. This creates a follow up question; if it is not the DCC, who is the suitable actor or are the suitable actors in the fight against disinformation? As presented in the introduction, research has shown that most of the Dutch citizens want the big tech companies to take responsibility, but their policy around limiting disinformation and its effects stays unclear (I&O Research, 2017). At the same time, the Dutch government is mainly focussed on raising awareness and resilience towards disinformation in society. I my observation, this situation does not constitute a complete and effective approach in relation to the current and developing threat of disinformation. Fact is that the amount of disinformation campaigns is rising, and forecasts do not expect this to decline in the near future since, as Bader (2019) stated, disinformation is *"a low-cost strategy with a potentially high impact* (Bader, 2019, p. 34). Since I observed no concrete plan of action to organise a comprehensive approach to detect and counteract disinformation in the course of my research, I feel like precious time is being lost and action should be taken now.

8. Conclusion

In the conclusion, the last chapter of this thesis, an answer to the research question will be formulated. In addition, the limitations of this research are presented, further research suggestions are given and recommendations for in praxis are presented.

8.1 An answer to the research question

Disinformation is a growing threat to (democratic) societies all over the world. Its undermining character makes that people lose trust in national institutions, politics and each other, which will or could lead to societal disruption and the lack of overall integrity. In order to protect the Netherlands against this threat, different institutions, both within the government and its executive organisations as well as the in the scientific-community and the private domain, are thinking about the most suitable approach to fight this threat and protect our democratic values at the same time. Because of the fact that not much is known about the potential role of national security institutions in fighting disinformation, this thesis focusses on how the staff members of a specific military unit, the DCC, think about a potential role for them and their unit in this fight. With the aim to bring empirical knowledge and innovative theoretical insights into the debate of fighting disinformation, and especially about the potential role national security institutions could play in this, the following research question was formulated;

> *How does the Defence Cyber Command perceive its role in the process of detecting and counteracting disinformation in the Netherlands, and what is their ability to act in moments of disinformation?*

On concluding remarks it could be stated that the vast majority of the DCC staff members do not perceive an active or leading role for this military unit in the process of detecting and counteracting disinformation. Reason for this is that in their opinion, such a role does not fit the current (legal) frameworks of the DCC and they do not have or expect to receive a mandate to perform an active or leading role in this process either. Most of the DCC staff members state there are more suitable organisations and institutions in the Netherlands than the DCC, and the Dutch armed forces in general, to perform these tasks, like an interdisciplinary security council or the NCTV. However, the DCC staff members state that a supporting role for the DCC in fighting disinformation would potentially be possible. They state that an executive organisation like the DCC should never be involved in detecting disinformation, that being a task of the Dutch intelligences services, but that they could have a supportive role regarding counteracting disinformation, in taking countermeasures against (the senders) of disinformation.

In addition, it can be stated, that at this time, the DCC is limited in its ability to act in moments of disinformation. To be specific, the DCC is technically able to perform countermeasures in moments of disinformation based on their knowledge and skills, but cannot do so because it is restricted by the current (legal) frameworks; laws and rules. In other words, the limited ability of the DCC to act in moments of disinformation is not based on a lack of knowledge and skills, but on the current (legal) frameworks and the absence of the necessary mandate.

There are a number of elements contributing to the current situation concerning the mentioned legal frameworks and absence of a mandate, but the most significant one is the fact that (targeted) disinformation campaigns are legally not seen as an use of force. An action is seen as an use of force when it causes injury, death or damage, what often is not the case with disinformation. As long as this is the case, the possibilities for obtaining (legal) frameworks and a mandate to act, are very limited and as a result of this the DCC, and Dutch armed forces in general, would not be able to perform countermeasures against disinformation in the foreseeable future.

In order to offer a broader context concerning the earlier presented research question, in addition to the DCC staff members, a broadly composed group of military and non-military experts was interviewed about disinformation, it's effects and the need and potential ways to fight it. All interviewed experts see disinformation as a growing threat to (democratic) societies all over the world and are convinced that disinformation needs to be counteracted more effectively. However, when asked what in their opinion the best ways are to do so, the answers differed. It turned out the way the experts look at a potential role for the DCC in the process of fighting disinformation, is not so much based on their (scientific- or organisational) background, but in fact dominantly on the way they look at the question which are the most effective ways to fight disinformation on the one hand and what they perceive as the risks and dangers of certain strategies to counteract disinformation on the other.

8.2 Research limitations

While doing this research, things happened and situations occurred that have had or could have had a limiting effect on the course of this research or the research outcomes. Despite the fact I tried to limit the influence of these things and situations as much as possible, it is important to be aware of them while reading this thesis. The limitations are divided in three categories and presented in more detail in this paragraph.

8.2.1 Research design

This research has been done on the basis of a so called case-study research design. As presented in the methodology chapter, case-study based research provides specific data concerning one or a few cases, which leads to detailed and in-dept data. At the same time, the external validity of a case-study is often limited and the research outcomes are not regularly generalizable because of the context specific data you collected. According to Bryman (2016) this is an often named disadvantage of case-study based research.

Since this research is done by a single case-study research design, the research outcomes are limited generalizable. This limitation is dominantly the case in the international context, and less significant in the Dutch national context. In the international context I expect the research outcomes to be generalizable only very limited, since the armed forces of different countries cannot easily be compared to one another and in other countries other laws and rules apply. In the Dutch context the research outcomes could be generalizable to other military units and probably to other executive extended parts of the government as well, since they have to deal with the same or comparable laws and rules. Since this thesis is focussed on national security institutions, the fact the research outcomes are not or limited generalizable in the international context does not cause serious problems.

8.2.2 The interviews

There are four limitations concerning the interviews. Firstly, all DCC respondents are anonymised and their interviews were not recorded because of privacy- and safety reasons. As a result the interviews with the DCC respondents could not be transcribed and analysed in the same way as the expert interviews, which means the research outcomes are presented in a more general way and the use of quotes and references is limited. A second limitation is the language. Since all the respondents were Dutch and the DCC is a Dutch organisation, all the interviews were conducted in Dutch. As a result of this, the quotes presented and information used from these interviews are translated from Dutch to English by me. Accordingly, there is the possibility that the value or exact meaning of certain words or phrases changed in the process of translation. Thirdly, there has been a limitation due to the Covid-19 pandemic. As a result of the measures during the pandemic, some of the interviews were done online. Despite the fact everyone is used to using online platforms as MS Teams or Skype nowadays, and the conducted interviews proceeded without any technical difficulties, it could be stated that the interviews were impersonal this way. This could have had an effect on how comfortable the respondents felt during their interview and what they did and did not tell me. Lastly, although I am convinced of the fact that seventeen semi-structured interviews is a satisfying number in this field of interest, there are always more and different perspectives, ideas and views on subject. While doing this research and writing this thesis I really tried to include different points of view to cover the whole debate concerning this subject, but it is important to realise there a probably people in this field who cannot relate to the presented research outcomes.

8.2.3 Classified and sensitive information

While writing this thesis for, with and about a military unit, I have been in touch with classified and sensitive information. Since presenting this classified and sensitive information would have led to difficulties with publishing this thesis and presenting it to my supervisor, second reader and the public, I made the decision to exclude all classified or sensitive information from this thesis. The main argument to do so was that I wanted to make sure the thesis could be made publicly accessible. What I realised while doing the research and writing this thesis is that the influence of this decision has sometimes been more challenging than expected. Overall, it was not a problem that occurred while analysing my research outcomes, but rather when sketching the context and case in which this thesis fits. Security institutions often prefer to neither deny nor confirm certain information, for example the way they are structured or how they work. This makes that I cannot describe their structure or tasks precisely. While this challenge does not directly influence the research outcomes or my conclusions, it did pose a challenge when communicating and presenting data.

8.3 Further research suggestions

This thesis showed that the DCC staff members do not perceive an active or leading role for the DCC in the fight against disinformation. Given this fact, further research should be done in order to find the actor who can and wants to play a role in this fight.

Because of the fact the research outcomes of this thesis are not generalizable to all national security institutions in the Netherlands, a similar study aimed to other national security institutions in the Netherlands could be done in order to find out how they perceive a role in fighting disinformation. In addition it is relevant to do further research on how other (European) countries deal with the threat

of disinformation and especially how they fight this threat. Interesting ideas and opportunities for the Dutch approach and the organisations involved may emerge from this. Thirdly, it will be interesting and relevant to dive into the current (juridical) frameworks; are these frameworks still accurate, and if they are not, how can they get upgraded without this being at the coast of our democratic values?

8.4 Recommendations in praxis

The research conducted in the context of this thesis made it clear the DCC does not perceive a role for itself in the process of detecting and counteracting disinformation in the Netherlands. The DCC respondents stated there are more suitable organisations and institutions in the Netherlands than the DCC, and the Dutch armed forces in general, to perform these tasks. The DCC respondents did however see a possible supporting role for the DCC concerning counteracting disinformation, and stated that in their opinion the DCC has the ability to perform this supporting task. While doing my research I encountered a lot of enthusiasm and drive concerning the fight against disinformation, but also a situation in which the various governmental organisations involved are still seeking clarity with regard to the division of tasks and responsibilities. On the one hand that is not necessarily surprising, since the spread of disinformation through cyber and social media is a relatively new phenomenon, and organising the fight against it in an orderly and sensible way is complex and takes time. On the other hand, it is an urgent problem and threat that has to be dealt with. I would therefor recommend speedy clarification of the current framework of assignments of tasks and arrangements concerning the detecting and counteracting disinformation in the Netherlands within the Dutch governmental organisations involved. This clarified framework of assignments of tasks and arrangements should give direction and concretization about which organisations do have a role in fighting disinformation and how these task and responsibilities are to be divided between the organisations involved. It also would clarify how these organisations support and complement each other and how they can work together efficiently. Doing so would give more direction and clarity in general and would also give clarity in relation to the possible supporting role of the DCC, and with that more effectiveness and efficiency in the fight against disinformation.

During this research it became clear that the legal framework within which the DCC operates, does not allow the DCC, or the Dutch armed forces in general, an active or leading role in the process of detecting and counteracting disinformation. There are multiple reasons for this, but a dominant explanation is the fact that, at this moment in time, (targeted) disinformation campaigns cannot be seen as an so called use of force. This matters since the use of force is a condition for what is legally seen as a legitimate and appropriate response or possible countermeasure when disinformation occurs. When disinformation is not seen as an use of force, the DCC is not be able to play a role in fighting it. I recommend an active approach and to investigate whether the current judicial framework is still adequate and sufficiently up-to-date. Taking in account the fact that (targeted) disinformation can cause substantive and intense damage and in an indirect way can contribute to the loss of life, I recommend that the government investigates in particular whether (targeted) disinformation, under certain conditions, can nevertheless be regarded as an use of force.

References

AIVD (n.d.). Wet op inlichtingen- en veiligheidsdiensten. Retrieved from https://www.aivd.nl/onderwerpen/wet-op-de-inlichtingen-en-veiligheidsdiensten [September 29, 2021].

Bader, M. (2019). Disinformation in Elections. *Security and Human Rights* (29): p. 24-35.

Beckett, L. (2021). Facts won't fix this: experts on how to fight America's disinformation crisis. *The Guardian*, 1st of January 2021. Retrieved from https://www.theguardian.com/us-news/2021/jan/01/disinformation-us-election-covid-pandemic-trump-biden

Bellingcat (2021). *The GRU's MH17 Disinformation Operations Part 1: The Bonanza Media Project.* Retrieved from https://www.bellingcat.com/news/uk-and-europe/2020/11/12/the-grus-mh17-disinformation-operations-part-1-the-bonanza-media-project/ [September 29, 2021]

Bradshaw, S. & Howard, P. N. (2019).) *The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation*. Working Paper 2019.2. Oxford, UK: Project on Computational Propaganda.

Brinkel, T. (2017). The Resilient Mind-Set and Deterrence. In: Ducheine & Osinga (red.) *Netherlands Annual Review of Military Studies 2017.* T.M.C. Asser Press: p. 19 t/m 35.

Britannica (n.d.). *Checks and balances*. Retrieved from https://www.britannica.com/topic/checks-and-balances [June 18, 2021].

Bryman, A. (2016). Social Research Methods. Oxford: Oxford University Press.

Cambridge Dictionary. (2021). Kleptocracy. Retrieved from https://dictionary.cambridge.org/dictionary/english/kleptocracy [July 31, 2021]

CBS News (2020). Tackling disinformation is national security issue says former NSA general counsel. *CBS News*, 16th of December 2020. https://www.cbsnews.com/news/tackling-disinformation-is-national-security-issue-says-former-nsa-general-counsel/

Chinn, D. & Dowdy, J. (2014). Five principles to manage change in the military. McKinsey & Company. Retrieved from https://www.mckinsey.com/industries/public-and-social-sector/our-insights/five-principles-to-manage-change-in-the-military

Costa, C.P. & Geltzer, J.A. (2019). To Fight Disinformation, Rethink Counterintelligence. Defence One: 14th of October 2020. Retrieved from https://www.defenseone.com/ideas/2019/10/fight-disinformation-rethink-counterintelligence/160582/

De Ridder, J. (2021). *What's So Bad About Misinformation?*

De Wijk, R., Bekkers, F. & Sweijs, T. (2020). Hybride Dreigingen en Hybride Oorlog: Consequenties voor de Koninklijke Landmacht. Den Haag: HCSS Security.

Debunk.EU (n.d.). *Debunking disinformation together!* Retrieved from https://debunk.eu/ [October 1, 2021].

Defensie Cyber Commando. (n.d.). Defensie Cyber Commando; cyber slagkracht voor de krijgsmacht [Powerpoint]. file:///C:/Users/Charl/Downloads/Presentatie%20Elanor%20Boekholt%20(1).pdf

Defensiestaf. (2019). Nederlandse Defensie Doctrine 2019. Den Haag: Defensiestaf.

Drutman, L. (2021). Trump supporters storm the Capitol to attack democracy. Here's how Congress can save it. Think, January 7th 2021. Retrieved from https://www.nbcnews.com/think/opinion/trump-supporters-storm-capitol-attack-democracy-here-s-how-congress-ncna1253105 [June 18, 2021]

European Commission (2019). *Report on the implementation of the Action Plan Against Disinformation*. Brussels: European Commission.

Fallis, D. (2009). A Conceptual Analysis of Disinformation. ResearchGate. https://www.researchgate.net/publication/42101173_A_Conceptual_Analysis_of_Disinformation

Francart, L. (2010). What does resilience really mean? *La revu géoplitique.*

Gillham, D. (2021*). Fake news can lead to bad investment decisions*. FinFeed, February 12th 2021. Retrieved from https://finfeed.com/features/fake-news-can-lead-bad-investment-decisions/ [June 18, 2021].

Herik, B. van den, Molendrijk, T. & Bouwmeester, H. (2020). Zeg me dat het niet waar is…? Nederlands beleid en de rol van de krijgsmacht tegen desinformatie. Militaire Spectator, 189 (9): p. 418 – 429.

I&O Research (2017). Desinformatie leidt tot verwarring bij Nieuwsconsument. Amsterdam: I&O Research.

Ingram, M. (2018). The media today: Britain sets up a 'fake news' security task force. Columbia Journalism Review, 24th of January 2018. Retrieved from https://www.cjr.org/the_media_today/theresa-may-fake-news-task-force.php

Isa, M. (2017). How misinformation is used to influence markets. *News24*, 25th of August 2017. Retrieved from https://www.news24.com/fin24/finweek/featured/how-misinformation-is-used-to-influence-markets-20170825 [June 18, 2021].

Karlova, N. & Fisher, K. (2012). "Plz RT": A Social Diffusion Model of Misinformation and Disinformation for Understanding Human Information Behaviour. *Information Research*.

King, A. (2020). The Culture of Military Organizations. Washington Headquarters Services. Retrieved from https://www.whs.mil/News/News-Display/Article/2343941/the-culture-of-military-organizations/

Krekó, P. (2020). *The drivers of disinformation in central and eastern Europe and their utilization during the pandemic*. Slovak Republic: Globsec.

Landman, K. (2020). De wettelijke bestrijding van desinformatie: is het middel erger dan de kwaal? *Nederlands Tijdschrift voor de Mensenrechten*, (25) 4: p. 1-16.

Lasonjarias G, Larsen A.J. (2015). Introduction: A New Way of Warfare. In: Lasconjarias G, Larsen JA (eds) Response to Hybrid Threats. *NATO Defence College Forum Papers Series*, pp 1–13.

Levesque, C.J. (2013). Culture, Military. In: Piehler, K.G. (red). *Encyclopedia of Military Science*. Thousand Oaks: Sage Publications.

Levush, R. (2019). *Government Responses to Disinformation on Social Media Platforms: Comparative Summary*. Retrieved from https://www.loc.gov/law/help/social-media-disinformation/compsum.php [September 29, 2021].

Marotta E. & Nunzi, A. (2011). Security Apparatus. In: Badie, B., Berg-Schlosser, D. & Morlino, L. (red). *International Encyclopedia of Political Science*. Thousand Oaks: Sage Publications.

Ministerie van Defensie. (2012). Defensie Cyber Strategie. Kamerstuk 33.321 (nr.1). Retrieved from https://zoek.officielebekendmakingen.nl/kst-33321-1.html [July 30, 2021]

Ministerie van Defensie. (2016). Defensie Cyber Stratgie. Kamerstuk 33.321 (nr.7). Retrieved from https://zoek.officielebekendmakingen.nl/kst-33321-7.html [July 30, 2021].

Ministerie van Defensie. (2018a). *Bauer over cybercommando: militaire capaciteit die aan belang wint.* Retrieved from https://www.defensie.nl/onderwerpen/cyber-security/nieuws/2018/07/05/bauer-over-cybercommando-militaire-capaciteit-die-aan-belang-wint . [July 30, 2021].

Ministerie van Defensie. (2018b). Defensie Cyber Strategie 2018: Investeren in digitale slagkracht Nederland. Den Haag: Ministerie van Defensie.

Ministerie van Defensie. (2018c). Defensienota 2018: Investeren in onze mensen, slagkracht en zichtbaarheid. Den Haag: Ministerie van Defensie.

Ministerie van Defensie. (2020a). Defensievisie 2035: Vechten voor een veilige toekomst. Den Haag: Ministerie van Defensie.

Ministerie van Defensie. (2020b). Land Information Manoeuvre Centre helpt Defensie anticiperen. Retrieved 30 July 2021 from https://www.defensie.nl/actueel/nieuws/2020/11/16/land-information-manoeuvre-centre-helpt-defensie-anticiperen

Ministerie van Defensie. (2021). Defensie.nl. Retrieved from https://www.defensie.nl/ [July 31, 2021].

Ministry of the Interior and Kingdom Relations (2019). The Constitution of the Kingdom of the Netherlands 2018. Den Haag: the Ministry of the Interior and Kingdom Relations.

MIVD. (2017). Hybride Oorlogsvoering. Jaarverslag 2016; Specials 01. Retrieved from https://magazines.defensie.nl/specials/2017/01/05_hybride-oorlogsvoering [July 31, 2021].

NATO (n.d.). *Wat is de NAVO?* Retrieved from https://www.nato.int/nato-welcome/index_nl.html [September 29, 2021].

NCTV (z.j.). *Desinformatie*. Retrieved from https://www.nctv.nl/onderwerpen/desinformatie [September 29, 2021].

Niekerk, B. & Maharaj, M. (2013). Social media and information conflict. *International Journal of Communication*, (7) 1: p. 1162-1184.

North Atlantic Treaty Organisation (2019). *The North Atlantic Treaty.* Retrieved from https://www.nato.int/cps/en/natolive/official_texts_17120.htm [September 29, 2021].

O'Connor, C. (2021). *COVID-19 Vaccine Misinformation Monitor: The Netherlands*. London: Institute for Strategic Dialogue. Retrieved from https://www.isdglobal.org/digital_dispatches/covid-19-vaccine-misinformation-monitor-the-netherlands/ [October 14, 2021].

Rademaker, M., Sweijs, T. & Voorhoeve, J. (2017). *Hoe beschermen wij ons tegen Russische diensten?.* The Hague Centre for Strategic Studies: Den Haag.

Rathenau (2020). *Digitale dreigingen voor de democratie – Over nieuwe technologie en desinformatie*. Den Haag: Rathenau Instituut.

Rijksoverheid.nl (n.d.). *Desinformatie en nepnieuws tegengaan.* Retrieved from https://www.rijksoverheid.nl/onderwerpen/desinformatie-nepnieuws/aanpak-desinformatie-en-nepnieuws [June 18, 2021].

Robbins, J. (2020). Countering Russian Disinformation. *Centre for Strategic & International Studies:* 23th of September 2020. Retrieved from https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation [June 18, 2021].

Rosenberg, E. & Berkhout, K. (2020). Hoe defensie de eigen bevolking in de gaten houdt. *NRC Handelsblad*: 15 november 2020.

Rosenberger, L. (2020). Disinformation Disorientation. *Journal of Democracy*: Vol. 31 (1): p. 203-207.

Schiffrin, A. (2017). Disinformation and Democracy: The Internet Transformed Protest but did not Improve Democracy. Journal of International Affairs (71) *1*: p. 117-125.

Smeets, H. (2016). 'Oekraïners' dreigen met aanslag bij nee in referendum. NRC, January 19th 2016. Retrieved from https://www.nrc.nl/nieuws/2016/01/19/anti-nederlands-dreigfilmpje-is-russische-propag-1582894-a987847 [October 6, 2021].

Sullivan, H. (2021). US Capitol stormed: what we know so far. The Guardian, January 7th 2021. Retrieved from https://www.theguardian.com/us-news/2021/jan/07/us-capitol-stormed-what-we-know-so-far [June 18, 2021].

Takken, W. & van Dijk, W. (2021). Zo worden sociale media weer van ons. *NRC Handelsblad*, 18th of January 2021. Retrieved from https://www.nrc.nl/nieuws/2021/01/18/zo-worden-sociale-media-weer-van-ons-a4028014

Thorson, E. (2016). Belief Echoes: The Persistent Effects of Corrected Misinformation. *Political Communication*, (33) 3: p. 460-480.

United Nations (2021). Chapter VII — Action with respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression; Article 51. Retrieved from https://legal.un.org/repertory/art51.shtml

Vigdor, N. (2020). Twitter flags posts by Trump that made premature claims of victory or baseless ones about election fraud. *The New York Times*, 4th of November 2020. Retrieved from https://www.nytimes.com/2020/11/04/us/politics/trump-twitter-labels.html

Vuković, J., Matika, D. & Barić, S. (2016). Hybrid warfare challenges. *Security & Defence Quarterly*; 3(12).

Waltzman, R. (2017). *The Weaponization of Information: The Need for Cognitive Security*. United States: RAND Corporation.

Wardle, C. & Derakhshan, H. (2018).' Informatie Wanorde: Misinformatie, Desinformatie en Mailinformat. In: Ireton, C. & Posetti, J. (red) Handboek voor Journalistiek Onderwijs. UNESCO: Parijs: p. 60-73.

Williams, S. (2017). MH17 and the international crime court: A suitable venue?. Melbourne Journal of International Law (17) *1*: p. 210-237.

Wong, K. (2020). Organizational Culture: Definition, Importance, and Development. Retrieved from https://www.achievers.com/blog/organizational-culture-definition/ [September 29, 2021].

Appendix

Interview guide DCC medewerkers

Introductie

Ten eerste wil ik u hartelijk danken voor uw tijd en deelname aan mijn onderzoek. Ik zal eerst nog wat meer over het onderzoek en mijzelf vertellen. Mijn naam is Charlie van Delden en op het moment schrijf ik mijn masterscriptie voor de Master Human Geography: Conflict, Identities and Terretories, over de potentiële rol van het DCC in het tegengaan van desinformatie in Nederland. Voor deze scriptie zal ik verschillende mensen interviewen; werknemers van het DCC om te zien hoe zij zelf denken over de potentiële rol van hun organisatie, mensen van het Nederlandse leger die niet verbonden zijn met de cyber afdeling en experts buiten de defensie organisatie om die, naar mijn mening, een interessant perspectief aan deze scriptie kunnen toevoegen.

Eerst drie praktische vragen:

- Wilt u nog steeds deelnemen aan het interview?
- Hebt u er bezwaar tegen dat uw naam in de scriptie genoemd wordt?
  De gespreksverslagen worden niet in de scriptie opgenomen maar kunnen eventueel wel door de universiteit opgevraagd worden. Ik wil wel graag citaten opnemen in mijn scriptie, maar deze kunnen op uw verzoek ook geanonimiseerd worden.
- Geeft u toestemming dat dit interview wordt opgenomen?
  Deze opname is alleen bedoeld voor mijzelf om het interview op een later moment uit te kunnen werken.

Algemeen

- Wilt iets over uzelf en uw functie bij het DCC vertellen?
- Hoe bent u bij het DCC terechtgekomen?
- Hoelang werkt u al bij het DCC? / Hoelang bekleed u deze positie al?

Desinformatie

- Hoe definieert u desinformatie?
- Ziet u desinformatie als een serieuze bedreiging (voor Nederland)?
    - Waarom wel, waarom niet?
    - Voor wat? Maatschappij, democratie, rechtsorde, etc.
- Ziet het DCC desinformatie als een bedreiging?
    - Zo ja, welke bedreigingen en voor wat?
- Wat vindt u van het statement dat desinformatie gezien kan worden als ‘het nieuwe/moderne wapen’?

Desinformatie en DCC

- Valt het bestrijden van desinformatie volgens u onder nr. 97 van de grondwet?
- Valt het bestrijden van desinformatie volgens u onder the lines of effort van het DCC?
    - Zo ja, welke specifiek?

- Speelt desinformatie een rol in uw functie bij het DCC?
  Denk aan twee mogelijkheden; als taak of als bedreiging
    - Waarom wel, waarom niet?
    - Zo ja, in welke vorm?
- Ziet u het tegengaan van desinformatie als onderdeel van uw functie bij het DCC?
    - Waarom wel, waarom niet?
- Vindt u dat het tegengaan van desinformatie een van de taken van het DCC *zou moeten zijn*?
    - Waarom wel, waarom niet?
  - Zo ja:
    - WAT: Wat kan/moet het DCC doen?
      - detecteren en melden, valse content verwijderen, tegenmaatregelen nemen, etc.
    - HOE: Hoe denkt u dat dit gedaan kan worden, of gedaan zou moeten worden?
    - IN STAAT OM: Is het DCC toegerust voor deze taak? Waar blijkt dat uit?
      - welke kwaliteiten, technieken zijn er in huis, wat moet er nog gebeuren
    - Vindt u dat het tegengaan van desinformatie een grotere rol zou moeten hebben binnen het DCC?
  - Zo nee:
    - Waarom niet; principieel niet of praktisch niet (te druk)?
    - Waar hoort deze taak dan wel thuis? (binnen of buiten defensie, landmacht?)
    - Bepaalde onderdelen wel bij DCC (verschil detecteren en …)?
- Ziet u desinformatie als een cyber-aanval?
- Valt het tegengaan van desinformatie volgens u onder offensieve of defensieve cyber?

<u>Desinformatie opsporen en bestrijden</u> (detecting and counteracting)

- Denkt u dat er een verschil is tussen disinformatie opsporen en bestrijden?
- Denkt u dat beide, één of nog andere van deze taken er een voor het DCC zou kunnen zijn?
- Bestrijden: Vraagt dit vraagstuk om hard cyber, soft cyber of geen cyber maatregelen?

<u>Dilemma's</u>

- Ziet u bepaalde dillema's en risico's die het tegengaan van desinformatie met zich meebrengen?
  - 'We moeten iets doen' versus 'vrijheid van meningsuiting en journalistiek'
  - Wat als desinformatie vanuit de overheid zelf komt?
    - Trump situatie: Opdrachtgever is verspreider

<u>Ontwikkelingen</u>

- Heeft u in de afgelopen jaren (de 6 jaar dat het DCC bestaat) veranderingen opgemerkt in de manier waarop het Nederlandse leger, en in het bijzonder het DCC, naar desinformatie kijkt, in algemene zin en als een bedreiging die gemitigeerd zou moeten worden?
    - Zo ja: wat heeft u opgemerkt? En wat vindt u daarvan?

<u>Specifiek per afdeling</u>

Inlichtingen
Kijken jullie naar desinformatie?
Kunnen jullie eventueel detecteren en tegengaan?

- In welke mate kijken jullie nu naar desinformatie?
- Is er specifiek voor de J2 een rol in het detecteren en tegengaan van desinformatie?
- Welke middelen etc. zijn daar voor nodig?
- Hoe zorgen jullie geen LIMC te worden (opgerold te worden)?
- Is dit bijvoorbeeld een wetswijzing waard?

Jurist
Wat kan en mag er volgens de wet en hoever willen we überhaupt gaan?

- In hoeverre is het mogelijk voor het DCC om desinformatie te detecteren en tegengaan?
- Is het mogelijk het DCC meer bevoegdheden, middelen te geven wat betreft het detecteren en tegengaan van desinformatie?
    - Waarom wel of niet?
    - Welke bevoegdheden en middelen zijn er nodig?
    - Welke gevolgen brengt dit met zich mee?
        - Positief en negatief
- Zouden we moeten willen dat het DCC meer ruimte krijgt om deze taak uit te voeren?
    - Welke nadelen brengt dit met zich mee?
    - Is het het waard (de dreiging groot genoeg) om dit door te zetten?

Cyber operations
Wat kan er, welke middelen kunnen er ingezet worden?

- Wat is precies jullie rol bij het DCC?
- Zou het tegengaan van desinformatie een taak zijn voor deze afdeling binnen het DCC?
    - Waarom wel, waarom niet?
    - Zo nee; kan dit niet of wilt men dit niet? Waar dan wel?
- Beschikken jullie over de capaciteiten voor deze taak?

Voormalig LIMC
Wat ging er mis?

- Is LIMC de grens overgegaan; maatschappelijk gezien ja, maar naar de toekomst kijkend…?
- Moet de wetgeving of de manier van werken aangepast worden?

Cyber Warfare & Training Center
Speelt desinformatie een rol hier, krijgt het aandacht/prioriteit?

- Wat is precies de taak van het CWTC?
- Is er plek/aandacht voor desinformatie bij het CTWTC?
    -> Zou dit er meer moeten zijn?
- Hoe is dit de afgelopen jaren veranderd?

<u>Einde</u>

- Heeft nu nog opmerkingen, aanvullingen of vragen aan mij?

Interview guide Militaire experts

Introductie

Ten eerste wil ik u hartelijk danken voor uw tijd en deelname aan mijn onderzoek. Ik zal eerst nog wat meer over het onderzoek en mijzelf vertellen. Mijn naam is Charlie van Delden en op het moment schrijf ik mijn masterscriptie voor de Master Human Geography: Conflict, Identities and Terretories, over de potentiële rol van het DCC in het tegengaan van desinformatie in Nederland. Voor deze scriptie zal ik verschillende mensen interviewen; werknemers van het DCC om te zien hoe zij zelf denken over de potentiële rol van hun organisatie, mensen van het Nederlandse leger die niet verbonden zijn met de cyber afdeling en experts buiten de defensie organisatie om die, naar mijn mening, een interessant perspectief aan deze scriptie kunnen toevoegen.

Eerst drie praktische vragen:

- Wilt u nog steeds deelnemen aan het interview?
- Hebt u er bezwaar tegen dat uw naam in de scriptie genoemd wordt?
  De gespreksverslagen worden niet in de scriptie opgenomen maar kunnen eventueel wel door de universiteit opgevraagd worden. Ik wil wel graag citaten opnemen in mijn scriptie, maar deze kunnen op uw verzoek ook geanonimiseerd worden.
- Geeft u toestemming dat dit interview wordt opgenomen?
  Deze opname is alleen bedoeld voor mijzelf om het interview op een later moment uit te kunnen werken.

Algemeen

- Kunt u mij iets over uzelf en uw functie vertellen?
- Hoe is uw functie gerelateerd aan cyber?
- Hoe is uw functie gerelateerd aan desinformatie?

Desinformatie

- Hoe definieert u desinformatie?
- Waar ziet u desinformatie?
  professioneel of persoonlijk
  - Voorbeelden: de media, platforms, plekken, onderwerpen, landen
- In welke vormen komt u desinformatie tegen?
- Welke rol speelt sociale media in desinformatie volgens u?

Desinformatie als bedreiging

- Welke gevolgen kan desinformatie volgens u voor de Nederlandse maatschappij hebben?
  - Kunt u daar voorbeelden van geven?
- Ziet u desinformatie als een serieuze bedreiging voor de Nederlandse samenleving/democratie?
  - Waarom?
  - Kunt u daar voorbeelden van geven?
- Wat vindt u van het statement dat desinformatie gezien kan worden als ‘het nieuwe/moderne wapen’?
- Ziet u desinformatie als een cyber (gerelateerde) dreiging?

Desinformatie tegengaan: hoe?

- Wat moeten we als samenleving naar uw idee doen om desinformatie tegen te gaan?
- *Overheid*: Denkt u dat de Nederlandse overheid hierin een rol moet spelen?
  - Zo ja, welke rol en op welke manier?
- *Leger*: Denkt u dat het Nederlandse leger een rol *kan* en *zou moeten* spelen in het tegengaan van desinformatie?
  - Zo ja, welke rol en op welke manier?
  - Ziet u een verschil in het opsporen en het tegengaan van desinformatie?

Defensie Cyber Commando

- Bent u bekend met het Defensie Cyber Commando en haar taken?
  zo nee, even kort toelichten
- Denkt u dat het Defensie Cyber Commando een rol *kan* en *zou moeten* spelen in het tegengaan van desinformatie?
    - Waarom wel of niet?
    - Welk organisatieonderdeel kan dat anders doen, landmacht?
- Hoe, op welke manier en met welke middelen, denkt u dat het DCC desinformatie in de Nederlandse samenleving tegen kan gaan?

Dilemma's

- Ziet u bepaalde dillema's en risico's die het tegengaan van desinformatie met zich mee kan brengen?
- Ziet u bepaalde dillema's en risico's die het tegengaan van desinformatie *door de overheid* met zich mee kan brengen?
  - Hoe kijkt u naar het feit dat het DCC een verlengde is van de overheid?
    - De overheid bepaalt wat waarheid is en ingrijpt
  - Vindt u dat dit een inperking is voor de vrijheid van meningsuiting/journalistiek?
    - Waar liggende de grenzen, wat zijn de criteria in deze afweging?

Extra

- De Nederlandse overheid is gefocusseerd op het onderwijzen van haar burgers in het weerbaar maken voor desinformatie, ziet u dit als een mogelijke oplossing?
- Denkt u dat Nederland zich op een andere manier zou moeten verdedigen?
  - Ja en hoe?
- Welke andere organisaties denkt u aan?

Einde

- Heeft nu nog opmerkingen, aanvullingen of vragen aan mij?
- Kent u nog andere mensen die kunnen bijdragen aan mijn scriptie en die ik zou kunnen interviewen?
    - Kunt u mij eventueel introduceren?

Interview guide Non-militaire experts

Introductie

Ten eerste wil ik u hartelijk danken voor uw tijd en deelname aan mijn onderzoek. Ik zal eerst nog wat meer over het onderzoek en mijzelf vertellen. Mijn naam is Charlie van Delden en op het moment schrijf ik mijn masterscriptie voor de Master Human Geography: Conflict, Identities and Terretories, over de potentiële rol van het DCC in het tegengaan van desinformatie in Nederland. Voor deze scriptie zal ik verschillende mensen interviewen; werknemers van het DCC om te zien hoe zij zelf denken over de potentiële rol van hun organisatie, mensen van het Nederlandse leger die niet verbonden zijn met de cyber afdeling en experts buiten de defensie organisatie om die, naar mijn mening, een interessant perspectief aan deze scriptie kunnen toevoegen.

Eerst drie praktische vragen:

- Wilt u nog steeds deelnemen aan het interview?
- Hebt u er bezwaar tegen dat uw naam in de scriptie genoemd wordt?
  De gespreksverslagen worden niet in de scriptie opgenomen maar kunnen eventueel wel door de universiteit opgevraagd worden. Ik wil wel graag citaten opnemen in mijn scriptie, maar deze kunnen op uw verzoek ook geanonimiseerd worden.
- Geeft u toestemming dat dit interview wordt opgenomen?
  Deze opname is alleen bedoeld voor mijzelf om het interview op een later moment uit te kunnen werken.

Algemeen

- Kunt u mij iets over uzelf en uw functie vertellen?
- Hoe is uw functie gerelateerd aan cyber?
- Hoe is uw functie gerelateerd aan desinformatie?

Desinformatie

- Hoe definieert u desinformatie?
- Waar ziet u desinformatie?
  professioneel of persoonlijk
  - Voorbeelden: de media, platforms, plekken, onderwerpen, landen
- In welke vormen komt u desinformatie tegen?
- Wat is de rol van sociale media in de verspreiding van desinformatie volgens u?

Desinformatie als bedreiging

- Welke gevolgen kan desinformatie volgens u voor de Nederlandse maatschappij hebben?
  - Kunt u daar voorbeelden van geven?
- Ziet u desinformatie als een serieuze bedreiging voor de Nederlandse samenleving/democratie?
  - Waarom?
  - Kunt u daar voorbeelden van geven?
- Wat vindt u van het statement dat desinformatie gezien kan worden als ‘het nieuwe/moderne wapen’?
- Ziet u desinformatie als een cyber (gerelateerde) dreiging?

Desinformatie tegengaan: hoe?

- Wat moeten we als samenleving naar uw idee doen om desinformatie tegen te gaan?
- *Overheid*: Denkt u dat de Nederlandse overheid hierin een rol moet spelen?
  - Zo ja, welke rol en op welke manier?
- *Leger*: Denkt u dat het Nederlandse leger een rol *kan* en *zou moeten* spelen in het tegengaan van desinformatie?
  - Zo ja, welke rol en op welke manier?
  - Ziet u een verschil in het opsporen en het tegengaan van desinformatie?

Defensie Cyber Commando

- Bent u bekend met het Defensie Cyber Commando en haar taken?
  zo nee, even kort toelichten
- Denkt u dat het Defensie Cyber Commando een rol *kan* en *zou moeten* spelen in het tegengaan van desinformatie?
    - Waarom wel of niet?
    - Welk organisatieonderdeel kan dat anders doen, landmacht?
- Hoe, op welke manier en met welke middelen, denkt u dat het DCC desinformatie in de Nederlandse samenleving tegen kan gaan?

Dilemma's

- Ziet u bepaalde dillema's en risico's die het tegengaan van desinformatie met zich mee kan brengen?
- Ziet u bepaalde dillema's en risico's die het tegengaan van desinformatie *door de overheid* met zich mee kan brengen?
  - Hoe kijkt u naar het feit dat het DCC een verlengde is van de overheid?
    - De overheid bepaalt wat waarheid is en ingrijpt
  - Vindt u dat dit een inperking is voor de vrijheid van meningsuiting/journalistiek?
    - Waar liggende de grenzen, wat zijn de criteria in deze afweging?

Extra/als er tijd is

- De Nederlandse overheid is gefocusseerd op het onderwijzen van haar burgers in het weerbaar maken voor desinformatie, ziet u dit als een mogelijke oplossing?
- Denkt u dat Nederland zich op een andere manier zou moeten verdedigen?
  - Ja en hoe?
- Welke andere organisaties denkt u aan?

Einde

- Heeft nu nog opmerkingen, aanvullingen of vragen aan mij?
- Kent u nog andere mensen die kunnen bijdragen aan mijn scriptie en die ik zou kunnen interviewen?
    - Kunt u mij eventueel introduceren?