Putin's Pravda

Defensive policies of the Dutch Government against Russian information warfare and influence operations.

Author: Anahita Shekary
Supervisor: Dr. mr. E.E.A. Dijxhoorn
Second Reader: Mr. drs. W.J.M. Aerdts
Master Thesis Crisis and Security Management

Abstract

In the past years, Western democracies have noticed an increase in Russian disinformation campaigns. These campaigns are focused on exploiting vulnerabilities in democratic societies in order to weaken their adversaries internally. Due to the rapid technological developments and the overall use of online platforms, the Russians have found a new enabler for their influence operations. These operations are also targeted at the Netherlands. In this thesis the Dutch governmental policy against Russian information warfare and influence operations will be analysed. This will be done in order to evaluate to what extent the Dutch government is taking defensive measures to protect their society. This thesis will ultimately make recommendations as to what should and can be done to increase the defensive capabilities of the Dutch against Russian information warfare and influence operations.

Master Thesis Crisis and Security Management

Putin's Pravda

Defensive policies of the Dutch Government against Russian information warfare and influence operations.

Word Count: 20994

Anahita Shekary
Student number: s2119153
anahitashekary@gmail.com

Supervisor: Dr. mr. E.E.A. Dijxhoorn
Second Reader: Mr. drs. W.J.M. Aerdts

University of Leiden
Institute Security and Global Affairs.

Table of Contents

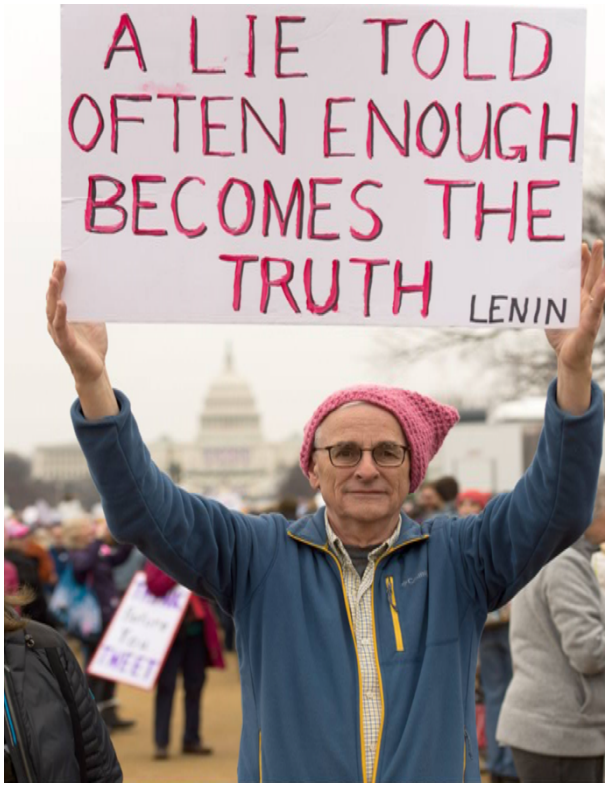
Preface

The Russian language has two words which both mean 'truth', '*istina*' and '*pravda*'. The meaning of the Russian word '*istina*' is the same as the meaning of 'truth'. '*Pravda*', however, has a deeper meaning that well represents the Russian culture. The meaning of the word '*pravda*' can best be understood as a tactical lie. This lie is legitimised by the fact that '*pravda*' serves a higher purpose, namely protecting the Russian state and people (Giles 2019:110).

Due to this reason the West often finds it difficult to understand and judge statements made by Russian leaders or news outlets. 'A statement can be considered 'true in Russia because it is pravda but found to be untrue in the West because it is not istina' (Ibid.). It should, however, be noted that propagating *pravda* is not only legitimised, but also stems from a long Russian tradition. Within this tradition, the truth is not a constant factor but is constantly being reinvented in order to protect the Russian state.

Currently Western democracies are facing Russian disinformation campaigns that are targeting societies in order to influence decision making processes. The Western inability to think from a Russian perspective and to correctly make the distinction between *pravda* and *istina* implies that Western governments lag behind when searching for counter-measures against Russian information warfare and influence operations.

In this thesis the Dutch defensive policy against Russian information warfare and influence operations will be analysed in order to evaluate to what extent the Dutch government is protecting their citizens against Russian interference.



21-01-2017 Washington D.C. United States of America.

List of abbreviations

AIVD - Dutch General Intelligence and Security Service

DNC – Democratic National Committee

EU- European Union

IRA- Internet Research Agency

IWIO – Information Warfare and Influence Operations

JIT- Joint Investigation Team

MIVD – Military Intelligence and Security Service

NATO- North Atlantic Treaty Organization

NCSC - National Cyber Security Centre

NCTV – National Coordinator of Terrorism and Security

RT – Russia Today

STRATCOM – NATO Strategic Communications Centre of Excellence

UN- United Nations

US – United States

I. Introduction

Since the 2016 United States (US) Presidential Elections and the alleged Russian interference in those elections, Russian influence operations have more and more been perceived as a threat to Western Democracies (Shimer, New Yorker 2018). The Russians did not only allegedly try to hack the American Democratic Party (DNC), but it is also suspected that they attempted to interfere in the elections by influencing the public debate (Mueller press conference 2019). The aim of this influence campaign was to change the outcome of the elections and to increase tensions within American society (Idem). Although the Russian influence campaign during the 2016 US elections is seen by many as the starting point of Russian influence operations in the West, the threat of Russian interference in democratic processes started long before 2016 and is not limited to the United States alone (Janda 2018:182). Examples of this are the Brexit referendum, the investigation into the cause of the 2014 Malaysian Airlines (MH17) airplane crash and both the French and German presidential elections in 2017 (Hall 2017: 51). More evidence is being found that the Russians use information warfare as a part of their influence operations for their grand strategy implemented worldwide (Janda 2018:181). In order to protect Dutch society from Russian information warfare, various Dutch governmental agencies have formulated policies on this topic. The suitability of the policies in relation to the existing threat has however not yet been tested. It is therefore important to investigate whether the current approach of the Dutch governmental agencies is suitable to counter the Russian threat. This thesis' research question will thus be:

'To what extent does the Dutch governmental policy to counter Russian information warfare and influence operations match the Russian threat, and take defensive measures to protect Dutch society?'

In order to answer the research question, the second chapter of this thesis will provide a literature review of the current state of the academic literature regarding the use of defensive measures taken by the West. This chapter will also discuss the Russian intelligence services and their practices, goals, methods and aims to influence Western societies, of which the Netherlands is a part. This is done in order to provide a clear view of the existing threat of information warfare within the Russian practice of influence operations (IWIO). Subsequently the Russian use of IWIO will also be elaborated in this literature review chapter. This is important since a better understanding of the Russian use of IWIO will contribute to the analysing whether the Dutch approach matches the nature of the Russian threat.

In the next part of the second chapter, the theoretical framework of this thesis will be discussed. The framework of Herbert Lin on how to develop a response to IWIO will be used to analyse the current Dutch approach on countering Russian IWIO. The substantiation for this will also be given in this theoretical framework.

The third chapter describes the used methodology, it will give insights in how the research was conducted and explain certain methodological decisions about the case and sources on which the analysis was made. In order to make this analysis, the fourth chapter of this thesis will provide additional background information about the Russian threat and the current Dutch approach by answering the following sub questions;

1. What is the nature of the Russian IWIO threat in the Netherlands?
2. What is the current approach of the Dutch governmental agencies against Russian information warfare?

Eventually in the fifth chapter an analysis will be made of the present Dutch defensive policies against Russian IWIO on the basis of the framework of Lin. In order to analyse the current state of the Dutch policy and to examine what the available policy options are and how they can be implemented.

To explain the relevance of this thesis it is important to understand the nature of the Russian IWIO threat. In 2013 the Russian General Gerasimov wrote an article about his ideas on modern warfare. In this article Gerasimov theorized about a new type of warfare that was later labelled by Western countries as 'hybrid warfare'. Gerasimov described how the role of non-military means to achieve political and strategic goals had grown, and, in many cases, had exceeded the power of force of weapons in their effectiveness' (POLITICO 2017; Military Review 2017). These new non-traditional means are being used to disrupt and weaken the adversary's entire society (Monaghan 2016:67). For the Russian Federation, the United States is currently the most significant threat (Giles 2019: 36-37). But due to the cooperation of the United States with its Western allies within NATO, as well as the strategic location of many of the NATO countries on the border of Russia, other Western countries are now also perceived as a threat to Russia's sovereignty (Janda 2018: 181-183). Another international alliance Russia identifies as a threat to their own security is the European Union (Giles 2019: 37).

The importance of discussing the Dutch case lies in the fact that the Netherlands is both a member of NATO as well as of the EU. In addition, the Dutch are currently leading the investigation concerning the MH17 airplane crash, which was allegedly shot out of the sky by a Russian missile. Due to this investigation Russia may consider the Netherlands as part of a larger security threat.

In order to effectively counter this security threat, Russia is trying to actively weaken its Western adversaries by means of influence operations (Benkler et al 2018:235). These operations are aimed at intensifying political division and weakening Western democracies (Ibid). The information warfare Russia is currently practicing in the West is just one of the components of the much larger hybrid threat Russia is posing (Revaitis 2017-2018:272). These and other aspects of IWIO, such as the use of cyber, will be elaborated in the literature review of this thesis.

The Dutch Ministry of Defence, the Ministry of Foreign affairs, the Ministry of Justice and Security, and the Ministry of Interior and Kingdom Relations have alerted Dutch citizens about the possible threat of Russian influence operations. These four ministries created policies in order to counter this threat (Ollongren 2017). While the Dutch Ministry of Defence and the intelligence and security agencies are constantly working on their defensive capacities, the Dutch Ministry of Interior launched a campaign to create awareness about disinformation in the run up to the provincial and European elections which took place in March and May, 2019. The campaign was called ‘’Blijf kritisch’’ which means ‘’Remain Critical’’ (Ministry of Interior and Kingdom Relations 2018).

By analysing both the Russian threat as well as the Dutch policy for countering Russia’s IWIO activities, this research will attempt to contribute to the academic debate regarding Russian influence operations. The research will consist of a policy analysis of four separate Dutch ministries, which will be supported by interviews held with civil servants working for these ministries. Subsequently the policy will be tested by means of Lin’s theory on IWIO. This theory provides a framework which can be used by governments to implement policy measures against Russian IWIO (Lin 2018). This theory, as well as the corresponding framework, will be explained and elaborated in the theoretical framework of this thesis.

The analysis will ultimately test whether there is an imbalance between the Russian IWIO threat and the Dutch approach to countering this threat. Following the results from the analysis, this thesis will make a policy recommendation for the governmental agencies of the Netherlands. By doing so this thesis will contribute to the current governmental approach, since this thesis presents the first research that analyses the current policy against IWIO which focusses on a variety of aspects of the Russian IWIO threat in The Netherlands. Analysing the Dutch approach is of importance since the societal consequences of Russian IWIO can have damaging effects. Therefore, analysing whether the Dutch policy is focussing on the right aspects of the threat is of relevance to the Dutch society.

The way in which Russia and Western democracies differ in types of military strategic thinking and the lack of academic literature that focusses on this difference, makes the scientific relevance of this research abundantly clear (Giles 2016: 13). Additionally, due to the incorporation of an analysis based on Lin’s framework, this thesis will provide an academically supported analysis of the current Dutch policy. An analysis like this has not been done before and will therefore offer a new assessment of the current policy.

A significant part of the academic literature is either about the role of cyber in influence operations, or focuses on countries other than The Netherlands. The threat of Russian influence operations needs to be seen from an international perspective since it is widely spread and does not focuses solely on one country in specific (Hall 2017: 52). But for the Netherlands it is of relevance to also specifically examine the Dutch case.

The aim of this thesis is therefore to give clearer insights into the way the Dutch government is countering Russian IWIO and to analyse whether the current Dutch approach matches the nature of the Russian IWIO threat. Examining the Dutch case is of even greater importance since the MH17 plane crash in which 196 Dutch nationals lost their lives (NOS 2014). And because the Dutch government has played a leading role in the investigation of the crash. Dutch intelligence and security agencies have observed a disinformation campaign**,** by the Russian Internet Research Agency (IRA), which was specifically focussed on getting the general public to question the legitimacy of the investigation (AIVD 2017). This situation makes the Netherlands especially vulnerable when it comes to Russian information warfare. This thesis will therefore solely focus its analysis on the Dutch case starting from July 2014 until spring 2019. Although the research will only consist of an analysis of the Dutch policy on this topic it is important to also take into account examples coming from other Western countries, since the Russian IWIO threat is an international one.

After the analysis of the Dutch approach based on Lin's framework on how to counter Russian IWIO, this thesis concludes that although the Dutch government has definitely taken steps in the right direction, there are still a lot of measures that need to be taken in order to fully protect the Dutch society. The Dutch approach does not only focus on the technological aspect of these operations, but also on the psychosocial aspects of IWIO, this focus matches the Russian threat.

Although the Dutch government has taken measures to detect and reduce the impact of an IWIO large parts of the Dutch society are still unaware of the IWIO threat. This might have consequences for the effect of the measures that are being taken, since awareness about the threat is one of the key aspects of these defensive measures.

In order to increase the results of the current policy this thesis recommends to expand the visibility of the awareness campaign as well as perform plans to increase media literacy and furthermore to create laws that restrict the spread of disinformation online. In addition to this the Dutch government should implement a critical vulnerability analysis which focuses on the Dutch society itself.

II. Literature Review & Theoretical Framework

In this chapter the theoretical basis will be laid for analysing the Dutch governmental approach against Russian IWIO, to emphasize the importance of analysing the Dutch case in specific. In order to do so this chapter will define the different components of this thesis' research question, such as IWIO, Russian IWIO and defensive measures, by the means of a literature review. Thereafter different theories regarding the issue of governmental defensive measures against IWIO will be discussed. Finally this chapter will argue that the framework conceived by Lin is the most suitable for answering the research question.

In order to protect Dutch society against the threat of IWIO the Dutch government has created several policies. These policies and other measures that are being taken by governmental institutions will be emphasized in the fourth chapter of this thesis that answers the question: What is the current approach of the Dutch Governmental agencies against Russian influence operations and information warfare?

Literature Review

When studying Russian IWIO it is important to first define what an influence operation is, and then distinguish the different methods and techniques the Russians use for their operations. Since the Russian IWIO threat can best be defined in light of the broader picture.

Although the concept influence operations is increasingly being used by the wider public the use of influence operations has been used for centuries while conducting war. Because of globalisation and technological innovations the nature of war has changed and has become more complex, this entails that the traditional concept of influence operations does no longer fit the changing times.

This new type of warfare is also often referred to as hybrid warfare. This concept was first published by Simpson. In her definition she mainly focussed on who was fighting wars instead of how wars were fought (Simpson 2005:4-5). She emphasized the importance of also taking into account non-state actors when analysing war. The concept of hybrid warfare has since become more popular and is also being used by states militaries. The definition of hybrid warfare which is currently most referred to is the one by Frank Hoffman. He defines hybrid warfare as 'any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behaviour in the battlespace to obtain their political objectives' (Hoffman 2010: 443). This thesis will use Hoffman's definition since it includes both states and non-state actors and focusses on tactics and combinations of (non)-traditional weapons.

Because definitions of influence operations tend to differ it is important to critically examine which term to use when analysing Russian IWIO. Already thousands of centuries ago the military strategic thinker Sun Tzu introduced the idea of influence operations by writing down ideas on how to fight a war without violence. This idea can be seen as the starting point of what we now call influence operations. 'This is the essence of influence operations' anything intended to sway the body politic of any party involved' (Cohen 2011:2). This is done without getting involved in armed conflict, therefore influence operations take place without kinetic violence (Lin 2018). These definitions do however not take into account one important aspect of influence operations; 'the physical outcome of political decisions' (Hutchinson 2010:14). Which is being accomplished through the most important task of influence operations 'to beneficially change (for the influencer) the emotions, behaviour, knowledge and beliefs of the targeted group' (Ibid). The U.S. Military defined the term influence operations thus follows: 'A deliberately planned and synchronized series of actions designed produce desired behaviours within adversaries and affected populations through the direct or indirect, threat or actual use of all U.S. military power and capabilities in order to achieve a relative advantage or desired end state' (Santa Maria 2013:31).

Another definition of the term influence operations is formulated by RAND:

> 'Influence operations are the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post conflict to foster attitudes, behaviours, or decisions by foreign target audiences' These actions are in the interest of the state which conducts the influence operations (RAND Institute).

This thesis chooses to use this definition formulated by RAND, since this definition includes all different aspects which were mentioned in other literature. The definition does not solely focus on wartime but also includes capabilities used in peacetime. This is of importance since due to the so called 'grey zone' of war, states are now permanently facing threats. This grey zone can best be understood as: 'coercive and aggressive in nature, but that is deliberately designed to remain below the threshold of conventional military conflict and open interstate war' (Brands 2016). Moreover, the definition formulated by RAND focusses both on the societal aspect of influence as well as the physical effect they may have.

Within the practice of influence operations information warfare can currently be seen as one of the most effective components. Information warfare and influence operations are, however, not the same and therefore should not be confused. Information warfare is simply one aspect of influence operations (Lin 2018). Information warfare can best be described as: 'the deliberate use of information by one party on an adversary's population to confuse, mislead and ultimately influence the actions that the targeted population makes' (Lin 2018).

Although this type of warfare is not new technological innovation and globalization surely impacted the use of it. For this reason information warfare is often associated with cyber. In Western media and policy

documents, terms such as ‘cyber warfare’ and ‘information warfare’ are often used interchangeably; this, however, may affect the Western counter approach as Russia has a different view on these tools and strategy (Kramer et al. 2019: 479). ‘Instead of cyberspace Russia refers to “information space,” and includes in this space both computer and human information processing, in effect the cognitive domain.’ (Giles 2016: 9). The decision for a specific operation and tools thus depends on a prior analysis (Thomas 2001: 3). The use of technology is just one of the many resources available that can be used in order to weaponise information. ‘Information weapons’ can be used in many more domains than cyber, crucially including the human cognitive domain’ (Giles 2013:10). Russian information policy makers consider information related operations from a different perspective than the West (Kramer et al 2019: 479). They distinguish information related topics in two different categories: technical information and psychological information (Ibid). This distinction is of significance because Russia sees psycho-physical security as the most crucial threat to a nation’s security (Idem: 480). The intensification of cyber and information technology has unquestionably made it easier for Russian secret services to carry out their operations (Sanger 2018:183). ‘Thanks to the internet and social media the kind of operations Soviet PSYOPs teams once could only fantasize about – upending the domestic affairs of nations with information alone – are now plausible’ (POLITICO 2017). By including the terms ‘cyber’ and ‘information technology’, the reference to and focus on cyber operations is often quickly made. There is, however, a major difference between cyber warfare and cyber-enabled warfare. Cyber warfare can best be described as ‘the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks’ (RAND Institute). Whereas in cyber enabled warfare, cyber is merely the tool used to carry out the operation (Lin 2018). In order to fully capture the nature of the Russian IWIO threat, it is best to separate the aim of the Russian influence operations from the tools they use. Since these tools constantly change, one can only ascertain the most used tool for a certain period. At this time information technology (IT) is the most critical enabler of Russian influence operations (Gianetti 2017: 101). This directly implies that cyber warfare is part of Russia’s toolkit, although it should not be mistaken for the only enabler for their operations.

Cyber operations which involve the use of hacking are, however, the most difficult, dangerous and expensive for a country to execute. In contrast to these types of cyber operations, which may possibly affect the critical infrastructure of a country, disinformation is a relatively inexpensive and easily accessible tool to damage or affect the society of one’s adversary. Because cyber has increasingly become the most critical enabler for IWIO and a different way of thinking was determined between the West and the Russian deployment of cyber. It is important to also take into account IWIO specified from a Russian perspective.

It has been argued that the Kremlin has introduced a new type of warfare, whereby tools such as disinformation and fake news are used to influence electoral processes and the civil society (Allcott & Gentzkow 2017: 212). The use of cyber is specifically pointed out by Western media and policy makers as a dangerous weapon in Russia's hybrid warfare arsenal in order to realize their goals (Giles 2016:13). In their view, social media and hacking activities by groups such as APT28 and 29, also referred to as FancyBear and CozyBear, would make it possible to change, steal and spread information in such a way that it benefits the Russian state (Jensen et al. 2019). In combination with the changing nature of information dissemination, which has created both new opportunities and vulnerabilities in Western societies (Palmertz 2016:1), this has made the use of information technology a perfect tool for the Russian Secret Services (Sanger 2018:183). Although cyber is by some still being viewed as the most important weapon in Russia's arsenal (Cohen & Ofir Bar'el 2017: 53), there is a growing agreement that this is not the case (Hutchinson 2006: 220). In order to have a better understanding of the full nature of the Russian threat, it is important to have a better understanding of Russia's views on the use of cyber during their influence operations, so as to understand that influence operations cannot be considered a new phenomenon.

Although the Russians use cyber as an enabler, it should not be taken as a critical component of Russian influence operations (Kramer et Al 2019: 439). No Russian definition of IWIO utilizes the term cyber (Idem: 479); instead Russia's main focus of their information operations lies in the psychological aspect of these operations (Idem: 480). In order to better comprehend the origin of these Russian operations, one has to take into account their history and development. Since these techniques find their roots in a long history of strategic military thinking, they can therefore only be understood by including a historical component (Hingley 1970: xi). Although the rules of warfare have adapted over the years due to the changing nature of war, IWIO specifically have a long history and have been practiced by the Russian secret services for centuries (Sanger 2018: 183).

These influence operations originate from a long tradition covering a broad spectrum of various types of acts. One aspect the numerous tools and acts all have in common is the psychological component (Bittman 1985:35-69). The Russians have been using psychological operations, also referred to as PSYOPs, in order to effectively carry out their influence operations. Influence operations have been deployed on a large scale both internally as well as externally ever since (Bittman 1985:35-69.). The aim of these influence operations is to negatively affect the state's opponent in order to weaken them and reduce the threat to its own state (Giles 2016:24). Over the past decades the Russian secret services made influence operations by using information warfare and psychological manipulation part of their regular ''playbook'' (Hingley 1970: 265-275). Influence operations are actively being used by the Russian secret services in order to influence policy decisions taken by their opponents (Giles 2016:11). In order to effectively counter these operations, it is important to understand where they come from and

how they have developed over the years. As previously stated, Russia has an extensive history of influence operations and information operations in particular (Bittman 1985: 35-40). Almost every Russian Tsar had his own intelligence service; this tradition stems from a long history of mistrust of the Russian rulers towards their own people as well as others (Idem.). In 1881, the Ochrana was the first Russian secret service which operated according to 'dual system of supervision'. This meant that the Ochrana looked at both internal as well as external threats (Idem: 69-116). The Ochrana can also be seen as the founder of Russian disinformation since it was the first Russian secret service to spread propaganda, scandals and fake news in foreign countries (Idem: 80). The Ochrana did, however, not fully implement the use of IWIO; this did not happen until after the second World War (WWII) with the establishment of the KGB.

Not long after the end of WWII, in 1954, the then leader of the Soviet Union and the communist party, Jozef Stalin, introduced a new Russian secret service: the NKVD of which the KGB (Komiteit Gosoedarstbennoj Bezopasnost) was a part (Idem: 225-264). The KGB was meant to serve as the 'shield and sword' of the communist party, which lead Russia during the Soviet era (Bader & de Jong 2006: 260). During the time of the Soviet Union, the KGB used disinformation both for internal as well as for external purposes (van Herpen 2016:88). The internal KGB propagandistic disinformation was mainly used to portray a horrific image of the West, and strove for internal demoralization (Bittman 1985:55). 'The Soviet bloc was not sustained by fervent belief in the system, but by acquiescence in a common discourse that co-opted the population' (Pomerantsev 2015:42). The practices and goals of the organization were both defensive and offensive in nature. Due to the Cold War and the large external threat the Soviet Union was facing, the KGB had to enlarge its scale and focus on external operations. Therefore, the First Chief Directorate (foreign intelligence) became the most important directorate (Bittman 1985: 39). One of the smaller departments of the First Chief Directorate was 'service A' (active measures). Among other things they were responsible for carrying out the Russian disinformation strategy (Andrew & Gordievsky 1990: 652). Disinformation messages often contained large segments of correct information to inspire confidence (Bittman 1985:56). The KGB labelled disinformation as 'white', 'grey' or 'black' based on the level of accuracy of the message (Benkler et al 2018: 243). Due to the internal and external practices during the Cold War, Russia has become an expert in the use of information warfare and the political manipulation that may follow (Pomerantsev 2015: 42). Already in 1985 the KGB recognized the growing importance of computer technology and the opportunities this may offer for future IWIO (Bittman 1985:66).Current Russian IWIO practices have deep roots in long-standing Soviet practices which emphasizes the importance of studying them, as their methods have not changed, only their tools and enablers did (Giles 2016: 33).

As mentioned above, it is clear that Russian influence operations find their roots in different manipulation and interference tactics, also referred to as 'Soviet Deep Operation Theory', which has

evolved over the years (Shea 2002). Initially the Russians used Maskirovka (маскировка), which literally means 'masking, to mislead the enemy in times of war' (Idem). The Soviet Military Encyclopedia in 1944 referred to Maskirovka as: 'means of securing combat operations and the daily activities of forces; a complexity of measures, directed to mislead the enemy regarding the presence and disposition of forces'. In order to do so, six elements were part of the Russian military strategy; 'surprise, camouflage manoeuvres intended to deceive, concealment, the use of decoys and military dummies and disinformation' (Ash for BBC 2015). Maskirovka was used as both a weapon against Western security and intelligence agencies, and to monitor the United States in the first half or the twentieth century (Shea 2002). During this period strategic political elements were also added to the Maskirovka strategy. The main goal was to manipulate facts in order to alter the perception of the adversary's society (Idem). During the second half of the twentieth century Maskirovka was further developed and became a new Russian military doctrine called Reflexive Control (Idem). Unlike Maskirovka, Reflexive Control does not only include military deception but also embodies a broader understanding of psychological operations and hybrid warfare (Giles 2016: 19-21). Reflexive Control can therefore be seen as a tool to generate a type of behaviour that is desired in a country's adversary (Komov 1997:18-22). Reflexive Control is still being used by Russian military and intelligence agencies, and can be defined as 'The systematic methods of shaping the adversary's perception, thereby decisions, and latently forcing him to act voluntarily in a way that would be favourable to Russia's strategic interests' (Giles 2016:19). In other words, Reflexive Control is being used in order to generate a desired model of behaviour by planting ideas and motives within an adversary's society and political system (Ibid). 'The basic elements of reflexive control include distraction, overload paralysis, exhaustion, deception, division, pacification, deterrence, provocation, suggestion and pressure, all with the intent of manipulation' (Komov 1997:19). The Russian secret services consider an IWIO operation successful whenever the targeted society's decisions are being made that are unconsciously influenced by Russian operations (Giles 2017).

Due to technological innovation and globalisation, the Russians have been re-adjusting the Reflexive Control doctrine over the years, meaning that the tools that enable these operations have changed (Sanger 2018: 183). 'Stalin used Soviet propaganda to sow fear and distrust ... but Facebook and other social media sites gave it the reach Stalin could scarcely have imagined' (Ibid). Not only have the tools the Russians use changed, the opponent's vulnerabilities that could be exploited have also changed over the years. Therefore Russian secret services revise them every few years (Idem). The Russian secret services have a directorate which specialises in dissecting enemy weaknesses, analysing failures and mistake and exploiting them (Bittman 1985: 39) in order to disrupt Western powers internally so chaos will ensue (Giles 2019: 24).

When Russia tries to influence their opponent's society, different aspects are taken into account, such as: economic activities, political tensions, relations: both internationally political and private, cultural

aspects, and both regular and social media (AIVD 2016: 3/7). In order to effectively complete the influence operation, the Russians use elements in the opponent's language, culture, math, philosophy, science and their history (Giles 2016:12). Other aspects that are intensively analysed by the Kremlin are vulnerabilities and tensions within other societies (Bittman 1985: 44). The most important aim of an influence operation is to create a false narrative, a lie that strongly influences the perception of citizens (Giles 2016:12). Russian influence operations are precisely adjusted to the society they are targeting (Pomerantsev 2015:42). Due to this, and in addition to the ever-changing tools the Russians apply, it is vital to realise that influence operations can be difficult to identify (Idem).

There is growing evidence that Russia has been using information warfare against Western countries (Besemeres 2016:37-48). Attention to this form of hybrid warfare has increased over the past years. Not only has it caught the attention of Western media outlets, but also of politicians and the general public (Idem). This is in response to several recent events which occurred; for example the annexation of Crimea in 2014, the MH17 plane crash, the 2016 US presidential elections, and the Brexit referendum. Evidence, however, indicates that information warfare should not be seen as a new phenomenon, particularly when creating policy for a counter strategy. With the advent of modern day technology, information warfare has gradually become more important (Benkler et al. 2018:263-264). Cyber and information technology have become new tools which are being used by the Russians for their influence operations. 'It's not just cyber, not just electronical warfare, it's not just intelligence but it's really effective integration of all these capabilities with kinetic measures to actually create the effect that the commanders want to achieve' (Giles 2017). Information warfare during peacetime is mainly being used to execute strategic tasks such as influencing public opinion, which even eventually may lead to indirectly influencing electoral processes in favour of the Russian Federation (Giles 2016: 10).

Due to the rising significance of social media, interfering online is particularly inexpensive and simple (Lin 2019:11; FireEye 2019). Evidence shows that Russians have been actively using troll factories in order to spread disinformation online (Aro 2016; 123 Gianetti 2017:100-101). Russia's disinformation campaigns should therefore be seen as a public/private partnership since the Russian leadership often outsources the creation of disinformation (Oosterwoud 2019). Among other things, the Russians have set up a propaganda centre called ''The Internet Research Agency'' (IRA) (Sanger 2018:182). 'The Internet Research Agency could actually degrade social media's organizational; power through weaponing it' (Idem:183). The IRA sends out tweets and creates fake stories with the aim of shaping the public debate to eventually create a real life protest (Benkler et al 2018: 263-264). Due to the large amount of variety in online platforms, the Russians can choose which platform fits best; 'Every platform has different advantages from an adversary standpoint' (McNamara 2019).

Fake news and disinformation are not only spread by the use of social media or bots. When taking into account the way in which the Russians understand 'information weapons', it becomes clear that this weapon can be used in many more domains than cyber alone (Giles 2016:10). The Russians have set up their own news channels such as Russia Today (RT), Russia Beyond the Headlines and Sputnik, who now broadcast worldwide and share their version of 'the truth' (van Herpen 2016: 91-95; Hall 2017:53). These mass media channels are a different enabler, but are also part of Russia's information warfare (Giles 2016:46). When it comes to Russian IWIO any type of communication channel can be used (Bittman 1985:56). 'The purpose of the message is to trigger a chain reaction, therefore the choice for best medium is important' (Ibid). Despite using their own channels to broadcast Russia's version of the truth, the Russians are also actively manipulating trust in mainstream Western media. By doing so, Russia is attempting to increase the credibility of their disinformation (Oosterwoud 2019). In addition to the spreading of disinformation, Russia is also trying to directly influence Western politicians who mainly come from specific types of parties. Various right-wing Western politicians have been connected to Russia (Janda 2018; 182). This is not always done directly but often through an intermediary or a donor group (FireEye 2019). This method of influencing is relatively easy and is extremely effective (Giles 2017). Due to this reason, some Russia experts argue that this is why the current Russian President, Vladimir Putin, is focusing on this aspect of warfare. 'Putin is eighty percent propaganda and twenty percent violence' (Pomerantsev 2015: 40). This is in line with the Soviet strategy, where informal techniques such as information warfare are as much instruments of foreign policy as formal ones (Bittman 1985: 43). Another aspect is that different targets, and different threats, ask for different counter measures. In order to determine the focus and specific aspects of their policy, Western governments should carefully analyse their adversary's strategy and playbook.

In order to effectively integrate counter measures that protect Western societies against Russian IWIO, governments should certainly focus on cyber as an enabler for IWIO. Cyber should, however, not be the focus of their counter policy. Both historical as well as theoretical evidence shows that Russian IWIO have both a psychological and a technical component. The psychological part of the operations is especially important to take into account when formulating a long term counter strategy that protects Western societies against IWIO. This is because the psychological component lies at the root of human vulnerabilities, and can therefore always be used by adversaries regardless of the tool they use. These aspects are thus of great importance when answering this thesis' research question, and will consequently be taken into account in the analysis chapter.

With the arrival of hybrid warfare as 'the new normal', countries have to take into account new tactics and threats when formulating their defensive measures. This thesis will focus on defensive measures states can take to protects their societies against IWIO and Russian IWIO in specific.

Theoretical Framework

Over the past decade various scholars have conducted research to determine the optimal ways to counter influence operations from a governmental policy perspective. First, one has to define what these defensive measures are and what they attempt to protect by analysing the focus of these measures. The aim of these Russian IWIO's as mentioned above is to create a false narrative, a lie that strongly influences the perception of citizens (Giles 2016:12). This false narrative will potentially have consequences for the voter's perception on political issues and therefore indirectly influence the outcome of democratic elections and the related political decisions (Pomerantsev & Weiss 2014: 12). Russia is using this tool 'for its own purposes and for achieving its own foreign policy goals' (Cizik 2018:13). For this reason defensive measures against IWIO are of great importance to protect citizens against the impact of disinformation (Samadashvili 2015:43-44). This is done to protect the sovereignty and legitimacy of Western democracies.

These defensive measures have to deal with a difficult paradox due to the way in which Western societies are set up. 'Western liberal democracies cannot restrict the right to free speech and the freedom of information' (Ibid). For this reason Western governments have to take into account these liberal values when formulating their defensive strategy. Although some literature argues that 'The Western response to the Russian challenge should be 'more neutral information, better analysis, more honest and transparent politicians, and wider education about the threat' (Ibid). Others suggest a different defensive approach and recommend that in order to defend ourselves, countries should analyse their own weak spots. 'Our first response should be to look at the weaknesses of the Western system and think about areas for target hardening' (Pomerantsev & Weiss 2014: 34).

Western policy makers and researchers have been analysing numerous approaches in order to find a course of action that is most effective and applicable to the Russian IWIO threat. While President Barack Obama was still in office as President of the United States of America, he initiated an act called the Countering Foreign Propaganda and Disinformation Act (CFPDA), which was part of a lager National Defense Act (Hall 2017:50). The aim of the CFPDA was to collect and analyse the stories produced by foreign governments through the use of a 'Global Engagement Centre' (Idem). However, the USA is not the only country which has to deal with Russian propaganda and disinformation. While Russia has their own television stations RT and Sputnik, which actively broadcast Russia's view on the world on a daily basis, some Russian disinformation is occasionally more targeted at specific situations and audiences. In 2017, both the French presidential elections and the Bundestag elections in Germany were targeted (EUvsDisinfo). The Russians used a combination of cyberattacks, cyber-spying and hacking to gain information (West for Brookings 2017). This information was later used to discredit both French President, Emmanuel Macron, and German Chancellor, Angela Merkel (Idem). The German government decided that the best defensive strategy was to address this issue before the elections were

held by a non-partisan actor, the head of the German intelligence agencies (Brookings 2017). The targeted French presidential candidate, Macron, believed it was best to address the Russian interference as late as possible, and announced the issue just minutes before the end of his campaign (Hall 2017: 53). Hall argues that scholars working at the Atlantic Council, an international relations think tank, argued that the best defensive measure for the EU against Russian IWIO is to begin exposing EU politicians who are supported financially by Russia and who fight propaganda (Idem:54). In their opinion, the EU should follow in the footsteps of CFPDA and create a joint taskforce that would coordinate the counter measures taken against the Russian threat (Ibid).

But countering Russian information warfare does not only happen by taking offensive and defensive measures against cyber-attacks, hacks or cyber espionage. Within virtually every research study on this topic, the importance of societal awareness is mentioned (Hall 2017: 56). Hall argues that: 'Successfully countering any disinformation means there must be an engaged, informed, and media-literate citizenry.' (Ibid). This view is supported by other literature. Currently troll and robot accounts on social media are Russia's main tools to spread disinformation. Fighting these accounts is one aspect of the counter strategy, but creating resilience within the targeted society may even be more important to protect societies (Aro 2016:124). Although some scholars argue for the option of censorship of Russian messages by the EU and the US, or for offensive counter information warfare by the Western alliance, (Thornton 2015:44) the focus of the defensive strategy needs to be found within Western societies themselves (Aro 2016:124). This approach of increasing media literacy and knowledge about disinformation through education seems to be effective in Finland (Mackintosh 2019). The case of Finland is, however, a specific one since the Finish population, in contrast to most EU citizens, is well aware of the Russian threat (Idem).

The focus on education and societal resilience is also emphasized by the Dutch Institute of Information Rights (IViR) of the University of Amsterdam, which conducted a research study commissioned by the Dutch Ministry of Education, Culture and Science. In this research study, an inventory was compiled about possible counter methods (McGonagle et al: 3). In the report various relevant strategies were elaborated on, all of these strategies contained the following objectives: preventive measures, identification and monitoring measures, limitation or correction measures, and law enforcing or not law enforcing measures (Idem:25). Other studies agree on measures to detect and expose Russian IWIO but also underscore the importance of acknowledgement of the Russian IWIO threat by Western political leaders (Janda 2018:186). They argue that aside from exposing and acknowledging the Russian use of IWIO, the political leadership should also confront Russia politically (Idem:187).

Despite the fact that literature concerning defensive measures against IWIO has increased, little has been written about policy measures that governments can take to protect their societies against this threat. In order to find the most suitable framework to analyse the Dutch approach against IWIO available

literature was consulted. The framework of Lin was the only framework that combined recommendations which recurred in almost all the available literature.

In his article 'Developing responses to cyber-enabled information warfare and influence operations' (Lin 2018), which elaborates on a larger research study: 'On cyber enabled information/influence warfare and manipulation' (Lin & Kerr 2017), Lin describes both the detection of IWIO as defensive measures that can be taken against them. This framework was also used for Lin's article: 'On the organization of the U.S. government for responding to adversarial information warfare and influence operations' (2019), this article focussed on USA governmental response to IWIO. Lin's theory uses a variety of criteria of IWIO, such as psychological and technological elements to develop a response to IWIO that is based on empowering and increasing resilience in Western societies. Lin combines numerous components of previously mentioned methods while focusing on the actual nature of the Russian threat, as elaborated in this theoretical framework. He describes that in order to sufficiently respond to an adversary's IWIO, it is important to ascertain that the adversary is actually conducting such a campaign. The importance of recognizing the threat is also acknowledged by Samadashvili and Janda. This can be difficult because a successful cyber-enabled IWIO campaign may not be noticeable if it was intended to be kept a secret (Ibid). 'An adversary's IWIO campaign – if successful- is likely to be invisible because the primary goal of IWIO is to persuade the target's population that its desires and preferences are well aligned with those of the adversary' (Ibid). Nevertheless, the identification of a foreign state being responsible for these handlings is a central aspect of detecting an ongoing IWIO (Ibid). Lin describes three elements of detection that can be used by governments:

1. Recognizing parties that might have something to gain from conducting such campaigns.
2. Detection and identification of automated IWIO weapons in use.
3. Detecting efforts to undermine the legitimacy of institutions that provide societal stability and continuity.

After establishing evidence of an adversary's IWIO campaign, defensive measures must be taken. Within the defensive measures, a distinction can be made between two different categories:

1. 'Measures to help people resist the operation of the IWIO weapon targeted at them.' (Lin 2018)
2. 'Measures to degrade, disrupt or expose an adversary's arsenal of IWIO weapons as they are being used against a target population.' (Idem)

The first category: 'Measures to help people resist the operation of the IWIO weapon targeted at them.' Is supported by almost all of the available literature concerning defensive measures against IWIO. Since the importance of focussing on societal resilience is almost everywhere being emphasized (Aro 2016:124; McGonagle et al: 3). Within this category three possible measures can be taken:

- The first measure is helping people to become more resilient against the effects of IWIO by making it easier for them to engage their rational thought capabilities. Here Lin refers to the use of ‘’debiasing’’.
- The second measure within the first category is using these human biases to find ways to counteract the effects of an adversary’s IWIO. It is important to keep in mind the psychological effects of ‘’affect heuristic’’. This effect implies that the way people feel about a certain situation influences their decision making processes and the conclusions that they draw.
- The third measure Lin mentions is concerning education. By educating the general population to think, look, and reflect critically on the information they consume, people will be less likely to believe everything that they see and read.

The second category: ‘measures to degrade, disrupt or expose an adversary’s arsenal of IWIO weapons as they are being used against a target population’ consists of five possible measures to degrade, disrupt or expose the adversary’s IWIO:

- The first measure is the use of fact checkers in order to counter disinformation.
- The second measure is to disrupt the financial incentives for providing fake news.
- The third option that Lin addresses is to bring reduce the amount of automated amplifiers of a disinformation campaign.
- The fourth measure is to create more transparency with regard to the political traffic that is displayed on social media.
- The fifth and final measure focuses on future defensive strategies.

As mentioned previously in this theoretical framework, all of these five suggested measures were suggested not only Lin but also other research.

What separates Lin’s ideas from other theories, is the framework Lin offers that can help guide Western governments. Lin makes a clear distinction between the psychological and technological aspect of IWIO. By doing so, Western governmental agencies can more easily divide responsibilities and tasks so that the various Ministries can focus on the aspects of the threat they have capabilities in. Another facet which makes Lin’s framework very interesting and helpful is the broad applicableness of the framework. Lin does not propose fixed measures that only offer one option, but rather offers options which governments can adapt at their own discretion. Due to this and because almost every measure Lin suggests is substantiated by other literature. This thesis will use Lin’s framework to analyse Dutch policy.

This thesis' literature review has shown that the main aim of Russian IWIO is to achieve political goals which benefit Russian leadership by weaponizing information to exploit societal vulnerabilities in the West. The main target for these operations is the general public, because their opinion ultimately influences the democratic decision making process. In order to do so the Russian use both technological as well as psychological elements for their IWIO.

In the past years different Dutch governmental agencies have developed policy in order to protect their society against the Russian threat. When looking at the current policies and protocols adopted by Western governments one can observe a specific focus on the cyber aspect of these operations (Giles 2016:13). This focus on cyber is supported by the findings in the theoretical framework of this thesis. When taking into account the use of IWIO by Russia, one can observe a focus on the psychological and societal aspects of these operations, and not as much on cyber itself. The focus on cyber by the Government of the Netherlands might therefore have security consequences for both the Dutch government as well as the Dutch population. Because of the current state of both the academic literature and the current Dutch governmental policy, this thesis will not focus specifically on the cyber aspect of IWIO, but instead focus on defensive measures taken by the Dutch government to protect the Dutch society from a broader perspective. In order to answer this research-question, the following hypothesis will be tested:

H1: 'The Dutch government's defensive policy on Russian IWIO does not fit the actual IWIO threat because the Dutch counter strategy focuses too much on the cyber aspect of these influence operations'.

Although different theories have been written about governmental approaches against Russian IWIO, the framework offered by Lin is found to be the most suitable in order to answer the research question. This framework matches the current threat of IWIO to Western societies, since the recommended measures do not solely focus on technical enablers of IWIO but also on other aspects of the threat. Lin's framework offers detecting measures for an IWIO in progress, as well as measures to reduce the impact of IWIO. Most importantly the measures described in Lin's framework are supported by findings coming from other literature and for that reason do not stand alone.
By making an analysis based on the collected information by the use of Lin's framework this thesis aims to contribute to the gap in the academic literature concerning defensive measures against Russian IWIO and the policy options Western governments have in order to protect their societies. This research will use both academic literature and interviews with experts in the field (see methodology chapter). The goal of this thesis is to provide clarity and insight into the current situation regarding Russian IWIO in The Netherlands in order to ultimately answer the research question.

III. Methodology

In this chapter the methodology that was used to answer this thesis' research question, the case selection and the theoretical basis of the analysis will be explained. In order to answer the aforementioned research question this thesis focused upon the strategy of the different governmental agencies of The Netherlands. By choosing the case of IWIO carried out by Russia within The Netherlands this thesis focused solely on the complexity of one specific case (Bryman 2012). Despite the specific focus on Dutch policy, information from other countries was also included in the analysis. This is due to the fact that it is crucial to analyse Russian influence operations from a broader perspective. Since Russia's hostile attitude is no longer specified on the US, but has become an anti-globalization attitude, their main aim is to disrupt and cause chaos in order to weaken their opponents (Giles 2019: 24). When doing so, the Russians use the same techniques in different countries (Ibid). This emphasizes the importance of not only looking at examples of Russian IWIO for the Dutch case but also taking into account the international examples.
By using qualitative research, this thesis tried to gain a better understanding of the topic of Russian information warfare as a part of influence operations. The qualitative research method is suitable to this thesis' topic due to the specific nature of the case and the lack of quantitative data regarding the topic of IWIO. Due to this, and because of the way in which this type of research is conducted, qualitative research sees phenomena as constructions rather than unchangeable facts. When analysing Russian influence operations, it is important to take into account different aspects of the case in order to portray a full image. However, one has to keep in mind that this thesis was written from a Dutch perspective. This directly implies that this research will always include subjectivity (Bryman 2012) and that the external validity of this research is low since it cannot be generalized to other countries.

This methodology chapter strives to set forth the qualitative research methods used to look into the defensive measures of the Dutch government against Russian IWIO and clarify the decisions that were made in order to answer the research question. The aim of this thesis was to evaluate the current Dutch approach against Russian IWIO and to question to what extend the current defensive measures match the Russian IWIO threat in order to protect Dutch society. This thesis will thus serve as a case study specified to the Netherlands. The decision to focus on the Dutch governmental policy had several reasons. Although Russian interference was noticed in a variety of countries, the case of The Netherlands is an interesting one due to one specific incident: the plane crash of Malaysian Airlines, MH17. The plane, which was allegedly shot down by a Russian missile, caused the death of 196 Dutch citizens. This event will further be discussed in the next chapter of this thesis and is seen as the starting point of this thesis' analysis. By researching the period from July 2014 until spring 2019, this research both analysed the period in which IWIO were not a regularly discussed topic among the general population, as well as a period in which they were. This is because the crash of flight MH17 took place prior to the media and social scientist started to demonstrate massive interest in the use of disinformation to influence democratic processes.

In order to answer the research question this thesis first gives more background information about the Russian IWIO threat specified toward the Netherlands. Thereafter an evaluation was given of the current Dutch policy concerning the topic of IWIO. Finally, an analysis of the Dutch governmental policy was made by the use of Lin's framework for developing a response to IWIO. This is validated by the theoretical framework and literature review of this thesis, which were both based on a broad literature study. Both the evaluation of the current Dutch policy as well as an explanation of the Russian IWIO threat specified on the Dutch case are of importance in order to formulate an answer to the research question.

In the analysis chapter, Lin's framework for developing a response to IWIO was used to analyse the collected data coming from the policy documents. As described in the theoretical framework in chapter II, Lin's framework consists of detection measures and defensive measures which can both be taken by governments in order to protect their society against IWIO. These measures were applied to the analysed policy documents.

Due to the available data concerning the topic of IWIO, the decision was made to focus on four of the Ministries: The Ministry of Interior and Kingdom Relations, The Ministry of Justice and Security, The Ministry of Defense, and the Ministry of Foreign Affairs. These four ministries were the only four who formulated policy on the issue of disinformation. The different Ministries each have their own ideas and interests regarding the topic. Although the analysis chapter primarily looked at the interviews and corresponding policy documents drawn by the Ministries individually, the interdepartmental working group, initiated by the Ministry of Interior and Kingdom Relations, the EU Action Plan Against Disinformation, and the NATO Stratcom initiative will also be taken into account.

To answer the research question, first relevant policy documents, and press releases by the Dutch government were gathered. Thereafter, data was collected by conducting semi structured in-depth interviews with experts from the field. This data is complementary to the data coming from the policy documents. At this moment, the data that was collected is the best available data, one always has to keep in mind that new data may become available.
The Interviewees came from different sectors such as: The Ministry of Defence, The Ministry of Foreign Affairs, Think Thanks, working groups and other events related to the topic. In order to portray a complete overview of the Russian threat, interviews were also held with Russia experts. Some of these interviews were held confidentially. For this reason all interviews will be anonymized. Interviewee profiles that are available in this thesis' Appendix on page 58. In order to select the interviewees the following criteria were applied: all interviewees have either knowledge about disinformation or Russian warfare, have been working on this topic for a longer period of time and are participating in the interdisciplinary working group on disinformation. In order to increase objectivity, at least two experts per Ministry were asked to participate. Unfortunately it was not possible to interview experts from the

Ministry of Foreign Affairs. The Dutch security services will be disregarded because of the difficulties related to the accessing of information and the focus of this thesis on the policy aspect of the defensive measures.

Using semi-structured interviews was helpful when gathering more (background) information (Bryman 2012). When analysing in-depth interviews, it is important to realise that language plays a key role, and the meaning of words can be multi interpretable (Idem: 472). Therefore the interviews that were used were recorded if permission was granted by the interviewee. The interviews were held on the basis of a semi-structured topic list which entails a deductive approach via a funnel model (Ibid). Topics which were discussed were the extension of the issue of IWIO and Dutch policy regarding this matter. The semi-structured topic on which the questions were based list is included in the Appendix of this thesis on page 57. All interviewees stemming from a similar position or background will be questioned based on the same topic list. The decision to use a semi structured topic list was made because it is likely that this will generate more information than when using a structured/closed topic list (Ibid). This is beneficial for the outcome of the research. The topic list used to question the interviewees is based on the theoretical framework and a funnel model (see Appendix).

The aim of this thesis was to evaluate the current policy of the Dutch governmental agencies regarding Russian IWIO, and to question whether or not this policy is focussing on the correct aspects of the Russian threat. Thus, this thesis served as a case study on Russian IWIO in the Netherlands after the crash of Malaysian Airlines flight MH17. The analysis was based on policy documents coming from Dutch governmental agencies and interviews. The collected data was analysed by the use of Lin's framework on how states can develop a response to IWIO. In the next chapter more background information is given about the Russian IWIO threat in the Netherlands, as well as about the current Dutch policy.

IV. Context and Background

In this chapter the context and background will be outlined of both the Russian IWIO threat in The Netherlands as well as the current state of the policy regarding the topic of IWIO by the Dutch government. In part I of this chapter the Russian IWIO threat will be specified on the Dutch case in order to get a better understanding of the present- day risks. In part II the Dutch policy against IWIO and Russian IWIO in specific will be elaborated. The aim of this chapter is to create a better understanding about the current state of the threat and what the Dutch approach is to counter this threat. This will help contribute to answering the research question since the context and background information which is given in this chapter is of great importance for the analysis made in the next chapter of this thesis. The first part of this chapter will conclude that although there is only one large example of Russian IWIO in the Netherlands; the IWIO campaign surrounding the cash investigation of flight MH17. One should not forget to put this example in the international context. For this reason Dutch governmental institutions are taking the threat of Russian IWIO to influence political and democratic processes very seriously. The second part of this chapter does not so much draw conclusions but shows to what extend the Dutch government has taken measures to protect Dutch society against Russian IWIO. An analysis of the current state of these measures will be given in the next chapter.

Part I: What is the nature of the Russian IWIO threat in the Netherlands?

To understand the nature of the Russian IWIO threat in the Netherlands, one must take into account international political dynamics and incidents. This is due to the fact that the methods and tactics used by the Russians during their influence operations are being used all around the globe to weaken their adversaries (Janda 2018:182-183). When preparing and organizing an IWIO, the Russians intensively study their adversaries and the social relationships within their societies (Bittman 1985: 39). This is done to create an IWIO campaign that perfectly matches the vulnerabilities of their adversary's society, in order to exploit those vulnerabilities and to benefit the interests of the Russian state (Palmertz 2016: 31-32).

In order to give a clear view of the nature of the Russian IWIO threat in the Netherlands, it is important to indicate that the Netherlands is a member state of several international organizations which currently have complicated diplomatic relations with Russia (Giles 2019: 24). Russia's aim is to weaken their adversaries so they become stronger themselves (Ibid). Organizations like NATO and the EU have both acknowledged the possibility of Russian IWIO attempting to interfere in the societies and democratic systems of their member states (EUvsDisinfo; NATO Stratcom). It is therefore conceivable that Russia

is trying to conduct an IWIO campaign in the Netherlands, with the aim of creating division about these international organizations or the political system within Dutch society (AIVD 2016; MIVD 2017). This is further acknowledged by Ronald Prins, cyber security specialist: 'Dividing the European countries against each other is of value to them, and we are the first country with elections in 2017. As Germany and France's elections will follow soon, it is not crazy to think they will test their abilities in The Netherlands.' (Data News 2017).

The most serious evidence of Russian IWIO in the Netherlands was after the 2014 airplane crash of flight MH17. Since the crash, Russia has been trying to interfere with the crash investigation and subsequent debate surrounding culpability (Bijleveld 2018; Shuster for Time magazine 2016). Due to the important role the Dutch currently play in the crash investigation, and because the Dutch Prime Minister has openly acknowledged and accused Russia as the perpetrator, The Netherlands is seen as a plausible victim for Russian IWIO (Press Conference Prime-Minister Mark Rutte 2018). Within hours after the crash, thousands of tweets and fake messages were being scattered with the purpose of framing the Ukraine for the plane to crash (Kist & Wassens 2019). These fake tweets and messages were designed and sent from a Russian propaganda company based in Moscow. This company, called 'The Internet Research Agency' (IRA), actively tried to create a false narrative concerning the events that occurred before, during, and after the plane crashed (Idem). Besides tweets and messages the Russians also tried to falsify evidence to undermine conclusions drawn by the JIT (Clingendael 2019). Still today, the Russian trolls are trying to illegitimize the outcome of the JIT report and make the general public question the report's findings (Bijleveld 2018; Kist & Wassens in NRC 2019).

Another example that may point to support the theory of Russian interference was the deep division surrounding the referendum held in 2016 with regard to the association treaty with the Ukraine, as well as the political debate that preceded it (Elsevier 2016; NOS 2016). Clear evidence was found that Russia exploits fragmentation within states in order to destabilize its enemies, and this referendum can be taken as a prime example of how democracy can divide a nation (EUvsDisinfo; Giles 2015). During the political campaign that preceded the referendum, diverse international and Dutch media outlets reported fake news that was later found to be spread by pro-Russian sources (Elsevier 2018). This evidently shows the importance for Russia to help undermine these elections, or at least to polarize the debate

One can state that the presented evidence highlights that the Netherlands is indeed a probable target for Russian IWIO. This is due to the Dutch membership in both NATO and the EU, which are both seen by Russia as security threats (Giles 2019: 24). Therefore, creating division between countries within these international organizations or within the member states internally will reduce the security threat for Russia. But even more than the Dutch membership of NATO and EU the Netherlands is a likely target for Russia's IWIO as a result of the plane crash of MH17 and the subsequent leading role of the Dutch

in the crash investigation. It has been established that, both after the crash, and during the crash investigation, Russian IWIO were actually targeting the public's opinion about the events that occurred in order to make them question the authorities (Bijleveld 2018). The existence of the Russian threat has been acknowledged by multiple Dutch governmental agencies, such as the Dutch General Intelligence and Security Services, the Minister of Defense, and the Prime Minister. The biggest threat of these IWIO is, however, not being Russia's target, but rather the way in which these operations are conducted. The methods Russia uses exploit critical vulnerabilities within societies. Since these issues are already existing topics that only need to be exploited, people who are affected by disinformation themselves become the biggest problem as they are the ones who believe the story and will start to spread it (Mcnamara 2019). This is how a fake story finds its way into actual human networks and is spread within groups of like-minded citizens (Idem; Mo Jang et Al. 2017:104). Due to this tactic, countries' inhabitants can actually become a countries' largest threat (Mcnamara 2019). This is because when being spread by real citizens instead of fake accounts and bots the information will faster be transmitted to other real citizens who have indirect political influence. The decision on which is based on the information they gather, that potentially can be part of an IWIO.

In the following section of this context and background chapter, the Dutch governmental policy regarding the topic of IWIO will be further elaborated upon.

Part II: What is the current approach of the Dutch governmental agencies against Russian influence operations and information warfare?

As explained in the introduction and theoretical framework of this thesis, Western democracies have been facing the threat of Russian information warfare as a part of Russia's larger influence operations. The threat of Russian IWIO askes for defensive policy measures taken by the Dutch government in order to protect the Dutch society. As shown by the theoretical framework, it is believed that when specific policy measures are taken by Western governmental agencies, this can help reduce the impact of these operations on Western civilians and on societies as a whole (Lin 2018). In order to analyse whether or not the Dutch governmental agencies are taking measures that match the nature of the Russian threat, one first needs to outline the current Dutch approach. In this chapter the policy approach of four Dutch governmental agencies will be elaborated upon. Thereafter in the analysis chapter, the existing policies will be analysed by the use of Lin's framework, which was explained previously in this thesis' theoretical framework. The structure of the following analysis will be based on the concepts which were provided in the literature review.

For this thesis four of the Dutch governmental agencies' policies will be analysed. This, however, does not mean that these governmental agencies are solely involved in this issue. Other Ministries and international organizations also play a significant role in current policy strategies. Because of this reason an analysis will first be given of the four most relevant Ministries for this topic, these being:

1. Ministry of Interior and Kingdom Relations
2. Ministry of Justice and Security
3. Ministry of Defense
4. Ministry of Foreign Affairs

Second, an interdepartmental and European approach will be set forth. These approaches may include cooperation with Ministries which were not analysed among the four most relevant Ministries because they never developed policy on this topic themselves, but whose involvement is, nevertheless, of importance for the interdepartmental approach such as; the Ministry of Education, Culture and Science. The first time the term 'disinformation' was referred to in governmental policy was in the 2016 governmental budget of the Ministry of Foreign Affairs. Disinformation was then placed under the subchapter: 'policy regarding Russia' (Rijksbegroting Ministerie van Buitenlandse Zaken 2015-2016: 14). This thesis will first begin with the evaluation of the Ministry of Interior and Kingdom Relations, as this Ministry is in the lead on the current campaign against fake news.

Ministry of Interior and Kingdom Relations

The Ministry of Interior and Kingdom Relations is the first to be evaluated. This is due to the fact that the Ministry has officially taken the lead in countering disinformation and managing the

interdepartmental cooperation among the Ministries, as well as in the international context (Interviewee #3). In several reports of the Dutch General Intelligence and Security Service (AIVD), it was emphasized that the Netherlands is a target of the Russian intelligence agencies who are using known tactics of influence operations that are focused on influencing decision-making processes (AIVD Jaarverslag 2016:7). Minister Ollongren first wrote a note concerning this issue to the Dutch parliament in November, 2017 (Ollongren 2017). In this note concerns were expressed, and it was confirmed that the Dutch Cabinet recognized the findings of the AIVD. The Cabinet stated that they found interference by other states completely undesirable and therefore recognized the need for measures (Idem). As a result, Cabinet instructed several measures to be implemented and informed political parties and organizations who are involved in the Dutch electoral processes, about digital resilience (Idem).
Thereby the Cabinet underscored the importance of societal awareness for the manifestation of the digital threat, and therefore continued to make efforts to create awareness among the Dutch population. The Cabinet simultaneously consulted about the issue with private partners such as technological companies (Idem).

At the end of 2018, the Ministry of Interior and Kingdom Relations announced their approach to create awareness among the Dutch population for the first time. This was done within the estimated budget plan for the year 2019, and by the State Secretary of this Ministry in his note to Parliament regarding digital inclusion (Knops 2018). Their approach was later further explained by Minister Ollongren in a note to Parliament about 'the threat of disinformation and influencing of the elections' (Ollongren 2018). This note was also signed by the Minister of Foreign Affairs and the Minister of Education, Culture and Science. In this note the threat assessment of the Cabinet was outlined, which was formulated as follows; the threat of spreading disinformation by other states in order to undermine and destabilize the democratic legal order has to be recognized as a real threat (Idem). The Cabinet acknowledges that spreading disinformation is a threat for Dutch society as a whole, and therefore calls for a multidimensional approach in which multiple stakeholders take their responsibility (Idem). The focus of the approach against the disinformation threat lays in counteracting the influence on public opinion. The Dutch Cabinet is aware of the fact that the threat especially manoeuvres itself online (Idem). Minister Ollongren also mentioned the US 2016 presidential elections, the Brexit referendum, and the elections in France, Germany and Sweden as examples of democratic processes in which evidence was found of trollfactories and disinformation campaigns which were used to influence public opinion (Idem).

Academic research by the Rathenau Institute about the topic of disinformation, for the Netherlands specifically, shows that until 2018 the spread of online disinformation had not had a large negative impact on Dutch society. One of the reasons for this is the way in which the Dutch media is organized. Due to the great diversity in media outlets coupled with the pluralism of opinions and views, the Dutch

society has a strong level of trust in the media (Idem). In order to maintain this strength of media pluralism and the level of media literacy of society, the coalition agreement of Rutte III agreed on investing in strengthening investigative journalism (Idem).

The campaign against disinformation and influence of public opinion has formulated the principles of the policy as follows (Idem):

- Values and norms according to the constitution, such as Freedom of Speech are of great importance when formulating an approach.
- The significance of an independent, strong and diverse media landscape is acknowledged in order to create and maintain a strong democracy.
- Trust will be placed in technological companies that they will take their responsibility through self-regulation.
- Media and digital literacy are seen as two key aspects of countering the impact of disinformation
- Stimulating academic research concerning disinformation
- Coordination must exist, not only with partners within the Netherlands but also with European allies, as disinformation does not stop at the border. This will be initiated in the European working group 'Action Plan Against Disinformation'.

The focus of the policy lies within the two elections that both took place in the spring of 2019: the Provincial state elections, and the European elections. In the run-up to these elections, the Cabinet prepared an awareness campaign in order to create consciousness among Dutch society with regard to the risk of disinformation and how to detect it. Civil servants were also trained on how to become aware by the means of a game about disinformation, which is currently being developed (Interviewee #1). Another feature of the policy was to actively develop more knowledge about the issue of disinformation(Idem).

The Ministry of Interior and Kingdom Relations launched their awareness campaign: 'Blijf Kritisch' ('Remain Critical'), in March of 2019, only two weeks prior to the first Dutch elections of that year (Rijksoverheid 2019). The campaign contained a video that was broadcasted both online as well as on television, which offered an explanation as to why fake news is being spread on social media, and a checklist on how to detect fake news (Idem).

In addition to this campaign, the Ministry also initiated a working group on how to counter disinformation. This working group is interdepartmental and is held every few weeks. It will be further addressed at the end of the first part of this analysis (Interviewee #5).

Ministry of Justice and Security

Whereas the Dutch Ministry of Interior and Kingdom Relations focuses on maintaining safety for both elections and society by creating awareness, the Ministry of Justice and Security's main task lies at the other side of the security spectrum. The Ministry has two departments that are principally involved when policy on this subject is formulated and executed. These are the National Coordinator of Terrorism and Security (NCTV), and the National Cyber Security Centre (NCSC). Due to the nature of their work, some information and activities are classified and can therefore not be included in the research data for this thesis (Interviewee #3). In his letter to Parliament in April of 2019, Minister Grapperhaus of Justice and Security advised the members of Parliament about opposing unwanted foreign state influencing threats (Grapperhaus 2019). The approach the Ministry of Justice and Security uses consists of the following measures that are specifically focused on the topic of disinformation (Idem):

- Improving the spread and access of information both nationally and internationally. To accomplish this the Netherlands will participate in the EU initiative of a Rapid Alert System. This will further be expanded upon later in this thesis.
- Enhancing awareness in order to create resilience. As well as the awareness campaign, which is coordinated by the Ministry of Interior and Kingdom Relations, training will be offered in both the national and the international context so that countries can learn to both identify and respond to state threats. This will be carried out by NATO as well as by the EU.
- Implementing measures both for defence and deterrence on several levels. For example, by registering lobbyists, protecting political civil servants, ensuring that elections are held safely, and acknowledging signals of influence operations and disinformation. This is done by both the NCTV and the Ministry of Defense, which will be further discussed later in this thesis.
- Cooperating internationally. EU agencies need to improve their co-operation methods, especially regarding topics such as disinformation, elections and cybersecurity. These issues do not stop at borders, and it is therefore of crucial importance to address their cohesion.

As the Ministry of Interior and Kingdom Relations is the lead of both the awareness campaign as well as the interdepartmental working group, the Ministry of Justice and Security is primarily focused on the security concern regarding information warfare (Interviewee #3). Despite the importance of societal awareness, which is recognized by the Ministry of Justice and Security, their job 'can more be seen as the job of a firefighter' (Interviewee #2). One of the interviewee's stated that:

> 'We are here to extinguish a fire, we need to know how to extinguish, sometimes help by doing it and to make sure the impact of the fire remains as small as possible. It is not our task to investigate who started the fire. That responsibility lies with the Intelligence and Security services.' (Interviewee #2).

The work of the NCTV and the NCSC within the Ministry should, however, not be viewed separately.

> 'Where cyber is nowadays mainly seen as an enabler to spread disinformation, it should also be seen the other way around. Direct cyber-attacks, such as hacks or even the idea that a hack, which can affect the critical infrastructure of a nation such as banks, water and electricity networks, has or will take place, is enough to eventually lead to lack of trust and create chaos. When this happens, cyber used in a completely different way but for the same purpose, namely influencing public opinion at its weakest spot' (Interviewee #2).

It is precisely this societal turmoil which can eventually create security concerns. The corresponding security task is reserved for the Ministry of Justice and Security. Because of this, the responsibility of recognizing and detecting disinformation, indicating what the aim of this disinformation is, and formulating a proportional response which eventually might be used is reserved for the Ministry of Justice and Security (Attachments note to Parliament Grapperhaus 2019).

Ministry of Defense

Although the Ministry of Defense is part of the interdepartmental working group, their policy regarding countering disinformation generally has another focus. The main concern of the Ministry, as it pertains to disinformation, is focused on Dutch soldiers deployed abroad (Interviewee #4).

In their multi-year development plan, which the Ministry presented in February of 2017, disinformation was initially suggested as a topic attention 'should be paid to' (Meerjarig Perspectief Defensie 2017). Listed under the heading 'Hybrid Warfare', disinformation was described as being part of an asymmetrical way of warfare (Idem). Minister of Defense, Bijleveld, along with her colleagues from the Ministry of Foreign Affairs, specifically condemned Russia in 2018 for conducting information warfare regarding the topic of battling ISIS in a United Nations context (Blok note to Parliament 2018 about ISIS). Later that year, in the Ministry's Mission Evaluation Report, the Minister again emphasized the threat of Russian information warfare, this time focused on undermining NATO's presence in Lithuania (Bijleveld 2018). Russia was actively spreading disinformation in order to influence the public's opinion with the aim of reducing support for NATO's involvement (Idem). This example of information warfare within EU/NATO/UN missions does not solely focus on undermining the mission's legitimacy among the civil population'; in addition to information warfare to discredit the mission as a whole, information warfare is also being used to destabilize soldiers in particular (Interviewee #4). Evidence was found that Russia has been spreading disinformation targeted at soldiers or their family and friends at home in order to make them more vulnerable (Idem). The Ministry of Defense therefore now actively informs their personnel and those at home that this could happen, in anticipation of this potential eventuality (Idem).

When it comes to disinformation and information warfare, open source policy documents and interviews only provide insight into the way in which the Ministry participates in the interdepartmental working group. This is coupled with the fact that information warfare is being used against missions and soldiers in operations which the Dutch are participating in. As well as cooperation on the EU level, the Ministry of Defense is also cooperating with their NATO allies to counteract disinformation and influence operations. Due to the sensitivity of the topic, this research is unable to analyse the full policy as the Dutch Military Intelligence and Security Service has not been taken into account.

Ministry of Foreign Affairs

The policy of the Ministry of Foreign Affairs regarding Russia's disinformation campaign started in 2015-2016 when the Ministry of Foreign Affairs stated that Russia is actively trying to destabilize countries that are part of the EU. The Ministry of Foreign Affairs believes that the Netherlands should support initiatives that counterbalance Russian disinformation (Rijksbegroting Ministerie van Buitenlandse Zaken 2015-2016: 14). One important subject on which Russia is focusing with the spread of disinformation in the Netherlands, is the case of the MH17 airplane crash (Blok 2018 about MH17). The Ministry of Foreign Affairs, therefore, stressed this topic when visiting Moscow in April, 2018 (Idem). While addressing the topic when speaking to their Russian counterparts, the Ministry of Foreign Affairs also discussed the topic in their 'Integrated Foreign Affairs and Security Strategy for 2018-2022'. The Ministry referred to the awareness campaign and to intensifying cyber deterrence (Ministry of Foreign Affairs 2018). Other policy they created and implemented was written in the European context, and will therefore be discussed later.

Interdepartmental Working Group

As stated previously in this chapter, the different Ministries have a partially joint approach when it comes to counteracting information warfare. By emphasizing the problem regarding disinformation, not only by the Minister but by the entire Cabinet, the Dutch state is sending a clear signal that the threat of information warfare does not belong to one Ministry, but instead requires a multidimensional effort. The participating Ministries in this working group are: The Ministry of Interior and Kingdom Relations, The Ministry of Justice and Security, The Ministry of Defense, The Ministry of Foreign Affairs, The Ministry of Education, Science and Culture, The Ministry of Economic Affairs and Climate Policy, and the Intelligence and Security Services (Interviewee #1). At the very outset of the awareness campaign, which was led by the Ministry of Interior and Kingdom Relations, one other Ministry was asked to participate – and actually became very much involved, as its contribution was critical to the result of the campaign (Interviewee #1). The Ministry of Education, Culture and Science played a key role in implementing the awareness campaign. Their role was to help improve media literacy within Dutch society in order to teach them how disinformation works, and also how to detect it (Idem). This was partially done with the help of the company DROG, which created a disinformation game for children

(Interviewee #1). It was not the first time a Dutch governmental agency worked with this company. DROG already created a game for the Dutch Armed Forces. In this game the participants had to destroy NATO by the use of disinformation in order to become familiar with how it works (Interviewee # 5). The aim of these games is to create knowledge of what fake news is, and how easily it can be used (Oosterwoud 2019). The interdepartmental working group is currently awaiting the results of research conducted by the University of Amsterdam which will help to determine the direction of the new policy (Interviewee #1). These results are expected to be available by September 2019 (Idem).

European Coordination and NATO

On a European level the main approach, which is also being implemented in Dutch governmental policy, is the Action Plan Against Disinformation (Interviewee #1). This plan consists of four pillars (European Commission 2018):

I. Improving the capabilities of Union institutions to detect, analyse, and expose disinformation.
II. Strengthening coordinated and joint responses to disinformation.
III. Mobilising the private sector to tackle disinformation.
IV. Raising awareness and improving societal resilience.

The first pillar: improving the capabilities of Union institutions to detect, analyse, and expose disinformation has the aim of effectively addressing the threat of disinformation. In order to do so, reinforcement of the European Strategic Communication Taskforce, The European External Action Service, and the EU Fusion Cell is necessary (Idem:5-6). This can be done by providing them with an extra number of specialised staff to process relevant data (Ibid). In order to detect, analyse, and expose disinformation, one needs to develop a threat analysis. This forms the basis of counteracting disinformation (Ibid). EU member states can contribute to this by increasing their national capabilities and increasing the necessary resources to support the work of the EU (Ibid).

The second pillar: strengthening coordinated and joint responses to disinformation includes the creation of a Rapid Alert System (RAS), which is meant to trace real-time disinformation campaigns (Idem: 7). Within RAS the EU is cooperating with NATO (EU commission 2018). The aim of RAS is to improve the situational awareness of the EU member states which can, in turn, help the effectiveness of the response (Ibid). Member states are each asked to deliver a point of contact who can closely cooperate with, and be the link to, the other member states and RAS (Interviewee #5). The RAS has must be closely linked to existing 24/7 capabilities in order to deliver a prompt reaction. This reaction must be both fact-based and spread through effective communication channels. Both are vital to counter and deter disinformation (Ibid). In order to let RAS operate to its fullest capacity, the cooperation between

EU member states and the EU institutions have to be further strengthened, especially when it concerns the sharing of information, learning, and creating awareness (Idem:8).

The third pillar: mobilising private sector to tackle disinformation emphasizes the importance of the participation of the private sector in addition to the work that governments of member states already do. The role of online platforms and advertisers is crucial when it comes to counteracting disinformation, as the problem of disinformation is directly linked to them (Ibid). Also citizens are increasingly asking for initiatives to counter disinformation and are now, in some cases, even taking the lead by creating their own fact checking websites such as the website nieuwscheckers.nl (Universiteit Leiden).

The fourth and final pillar: raising awareness and improving societal resilience. Societal awareness of the threat of disinformation is seen by the EU as a topic of great importance (Idem:9). This is because increasing societal resilience against the effects of disinformation will be the best counter strategy against disinformation. 'A comprehensive response to disinformation requires active participation by civil society.' (Idem). This can be achieved by creating a better understanding of the sources and tools used, as well as of the intentions why disinformation is being spread (Ibid). Another important component of improving societal resilience is by being aware of one's own vulnerabilities. The EU and its member states should therefore learn to quickly identify key vulnerabilities among the member states (Idem:9-10). In addition to research to identify these key vulnerabilities, independent fact checkers and researchers should be employed to investigate the structures and mechanisms of disinformation in order to better understand the threat (Idem:10). This should be done in both the member states individually but also in an EU network of fact checkers (Ibid). The final important action which must be implemented to increase public awareness and resilience, is to empower EU citizens when it comes to media literacy in order to better recognize and deal with disinformation (Ibid). The EU, therefore, will invest in both media literacy and in the work of the independent media, since/as this is essential for the functioning of democracies (idem:11).

In her note to Parliament, Minister Ollongren of Interior and Kingdom Relations previously stated that the Dutch Cabinet will start implementing the actions that have been formulated in the EU Action Plan Against Disinformation. She also declared that Dutch governmental agencies will therefore not only create their own policy based on interdepartmental consultation, but also in a broader European context. However, when analysing the policy that the various Dutch Ministries have implemented, it is clear that not all of the European policy recommendations from the action plan have been implemented thus far.

This chapter's aim is to discuss the current policy of the Dutch governmental agencies against the threat of Russian information warfare. Several conclusions can be drawn based on this policy analysis. The Dutch approach against Russian information warfare mainly focuses on the spread of disinformation online, which is primarily enabled by social media and other online platforms. The current implemented

policy is based on two separate initiatives: the awareness campaign led by the Ministry of Interior and Kingdom Relations, and the participation in the RAS system which is led by the EU. By doing so, current Dutch policy is mainly focused on the 2019 spring elections in order to ensure that no disinformation is being spread to influence the outcome of these elections.

Although the Dutch military on a large scale depends on international cooperation with their NATO partners, NATO is not often mentioned in the current Dutch policy. The Dutch ministry of Defense is participating in working groups organized by NATO's Stratcom initiative. And although the topic of disinformation is being discussed during NATO summits the Dutch governmental agencies do not have policy guide lines coming from NATO that can be implemented. Dutch Minister Ollongren has argued for better cooperation between NATO and the EU on the issue.

When analysing the notes to Parliament written by different Dutch Ministers, it appears that the Cabinet has focused their policy on an approach of creating awareness and debate surrounding the topic of disinformation. The aim of this approach is to counteract the impact of disinformation. This is only possible when creating a resilient society. The purpose of the formulated policy is to help improve societal resilience in order to reduce the threat of Russian information warfare.

A difficulty that arise and that must be taken into consideration when creating policy regarding the topic of countering disinformation, is the issue of restriction. There is a fine line between counteracting and putting restrictions on basic human rights such as freedom of speech which also includes freedom of media and press (Interviewee #1; #3). 'Since we, luckily, do not know a Ministry of Information in The Netherlands, it is very difficult for a governmental agency to decide whether something is disinformation or just some one's opinion' (Interviewee #1).

In the analysis chapter, the current Dutch policy, as described above, will be analysed by the use of Lin's Framework. By doing so, the current policy will be tested in order to determine whether or not the policy adequately matches the current Russian threat of information warfare as a part of their larger influence operations.

V. Analysis

In this chapter an analysis will be made of the current Dutch policy to counter Russian IWIO, this is done by applying the framework by Lin (2018) which describes policy measures to protect a nation against cyber enabled information warfare and influence operations (IWIO). Lin's framework will be used to test the current Dutch policy measures which are described within the context and background chapter of this thesis. The purpose is to determine whether or not the current policy matches the actual Russian threat.

Defending the Netherlands against IWIO by Russia is of critical importance as Russia has been actively trying to influence Western societies as described in the theoretical framework. This attempt to influence is being carried out by the use of cyber-attacks and disinformation campaigns. These are designed to create a false narrative in order to undermine trust in their democratic institutions and governments, and in democratic processes by targeting a specific audience within societies (Janda 2018:182). Societies 'serve the adversary's interests but do not know that they are being duped' (Lin 2018). Russia believes that the insecurity of other states will eventually increase Russia's security (Giles 2019:23). This principle does not only count for Russia in times of conflict; Russia will therefore always try to weaken others in order to become stronger themselves (Vendil Pallin 2017:255-278).

Lin's theory is based on the assumption that in order to defend a nation against cyber enabled IWIO**,** there are three focus areas one needs to pay attention to: detecting an IWIO in progress, reducing the impact of an IWIO, and developing offensive IWIO strategies and capabilities (Lin 2018). This analysis will focus on measures for detecting and reducing the impact of an IWIO.
Since the detection of an IWIO campaign is crucial for ultimately reducing the impact of it on a society, it is important to investigate what the Dutch government is doing in regard to this aspect of fighting IWIO. The detection measures that can be taken by governments are as follows:

1. Recognizing parties that may have something to gain from conducting such campaigns.
2. Detecting and identifying automated IWIO weapons in use.
3. Detecting efforts to undermine the legitimacy of institutions that provide societal stability and continuity.

Detection of IWIO

The first step in the detection of a possible IWIO campaign lies in recognizing parties for whom it might be beneficial to conduct these types of campaigns. Due to the specific nature of this thesis this first step was already taken when formulating the research question. But IWIO are useful instruments for many

different types of adversary's (Lin & Kerr 2017:18). The Netherlands could be an interesting target for Russian IWIO campaigns for several reasons. As the Netherlands is both part of the EU and of NATO, it is important to not only take into account the bilateral relationship but also to analyse the current situation from a multilateral perspective. Since the Cold War ended there has been optimism that the hostile relationship between Russia and the West would change and good diplomatic relations could be built (Gower & Timmins 2007: XXII). After the Soviet Union fell apart and more of Russia's neighbouring countries started to become members of the EU and/or NATO, Russia felt more and more isolated (Ibid). The enlargement and expanding defensive capabilities of the EU and of NATO made Russia feel increasingly marginalized (Ibid). This is still the case today. With the annexation of Crimea, Russia sent out a clear signal to both the EU and NATO. In response to the annexation, NATO decided to send an enhanced forward presence (Rijksjaarverslag Ministerie van Defensie 2018:27). This means that NATO troops will be present in both the Baltic States and in Poland as part of a reassuring measure to help these countries deter Russia (Ibid). The presence of NATO troops in these former Soviet countries, and the unified EU front, which covers their entire left border threatens Russia. Russia's perception of being under constant external threat does, however, not solely stem from NATO's presence, but is internally consistent (Giles 2019:37)

Part of Russia's current strategy against these Western alliances lies in weakening them internally; in that case, Russia does not have to become stronger itself (Idem: 23). Since the Netherlands is both part of the EU as well as of NATO, weakening the Dutch society internally or influencing their views on EU or NATO membership could be beneficial to Russia. When the EU is internally fragmented and increasingly polarised, it will be less likely to provide a united front against Russia, which will then decrease the security risks for the Russian Federation (Giles 2019:24). A high ranking general in the Dutch military described it as follows: 'Russia is currently fighting an 'opportunity war, they are not creating problems within societies but they observe vulnerabilities which they can exploit. A little push through information warfare can be enough to be the tipping point' (Interviewee #4). A prime example of this is the Dutch referendum regarding the association treaty with the Ukraine. The referendum was already polarising the Dutch society, but several efforts to spread disinformation to further intensify the discussion were detected (Interviewee #5). The Dutch Ministry of Foreign Affairs stated in their 2018 Annual Report that 'Russia has increasingly become assertive when it comes to international relations, specifically towards the EU' (Rijksjaarverslag Ministerie van Buitenlandse Zaken 2018:11). The Ministry also addressed the fact that the diplomatic relationship between Russia and the Netherlands has come under pressure due to several events [1](Idem:12).

[1] Such as small diplomatic incidents like the mistreatment of Dutch diplomat Onno Elderenbosch and the arrest of former Russian Ambassador to the Netherlands Dmitri Borodin or the Russian attempt cyber operation which was disrupted by the Dutch Military Intelligence and Security Service.

One of these events was the airplane crash of flight MH17. This flight is presumed to have been shot down by a Russian BUK rocket in the July of 2014. The airplane crash was investigated by a Joint Investigation Team (JIT) in which authorities of the Netherlands, Australia, Belgium, Malaysia and the Ukraine co-operated to establish facts about the crash, and to identify those responsible in order to ultimately deliver evidence which could lead to prosecution of those responsible (Openbaar Ministerie 2019). Since the investigation by the JIT was led by the Dutch, and all evidence pointed toward Russia as being the most likely perpetrator, Russia had a clear and vested interest in either influencing the outcome of the report or making people question the reports results. 'When it comes to the spread of Russian disinformation, MH17 can be seen as the largest disinformation subject' (Interviewee #5). When analysing whether or not Russia may have something to gain from conducting an IWIO campaign in the Netherlands, it is clear that due to the EU and NATO membership, as well as the plane crash of MH17, the Netherlands is a likely target.

Another step to detecting a possible Russian IWIO campaign lies in the detection and identification of automated IWIO weapons that are being used. The Dutch government has taken the first steps towards improving the detection of IWIO by participating in the EU Rapid Alert System (RAS). The main aim of the RAS is to provide real time alerts on disinformation campaigns (EU Action Plan against Disinformation 2018: 7). The importance of rapid emergence is also emphasized by Lin & Kerr (Lin & Kerr 2017:19). This is done by sharing instances of disinformation campaigns, regular sharing of analysis, trends and reports EU-wide, and formulating a coordinated response. While doing so, the EU is ensuring that the detection, identification and potential responses are time and resource efficient (EUvsDisinfo 2019). Although the European External Action Service, in close cooperation with the EU Commission, will act as the facilitators of the RAS, there still lies a great responsibility with the member states as need to provide information and knowledge to the RAS (Ibid). The Dutch agencies share this information in two phases: first the information is shared with their member states and, second, when an IWIO is detected, the information is shared with the Dutch Crisis Centre (NCC) (Interviewee #5). By participating in the RAS, the Dutch governmental agencies are making the important step of detecting IWIO campaigns. When it comes to detecting possible Russian IWIO campaigns in the Netherlands, the University of Amsterdam has found evidence of automated IWIO weapons in use during the aftermath of the plane crash of MH17 in 2014 (NRC 2019). In the first two days following the crash, the IRA sent over 66.000 tweets aiming to frame Kiev as the perpetrator of the crash (Idem). Due to the evidence of fake tweets scattered by the IRA aiming to create a false narrative about events regarding the MH17 crash, one may conclude that a Russian IWIO campaign was detected to influence the public's opinion about the events that took place.

The third and final detecting measure Lin mentions is the detection of efforts to undermine the legitimacy of institutions which provide societal stability and continuity. This measure is very difficult

to implement since determining whether the spread information is part of a Russian strategy or the mind-set of a part of the Dutch society is difficult to ascertain. The Dutch government does not want to interfere with basic human rights such as freedom of speech. Therefore, the detection of this measure cannot be further established (Interviewee #1). There is, nevertheless, growing evidence about Russian IWIO targeting the JIT's report about the MH17 airplane crash (Minister Grapperhaus 2019; NRC 2019). The danger of IWIO is that 'citizens do not even agree on the events that have happened – each side has its own version of facts to drive their own narratives' (Lin & Kerr 2017:19). The aim of targeting the JIT's report with an IWIO weapon is to compel the general public to question the legitimacy and independency of the report's conclusions (Minister Grapperhaus 2019; NRC 2019). By doing so, the Russians are trying to undermine the credibility of institutions. Minister Grapperhaus said in his speech to parliament on June 20th that the Ministry of Justice and Security is monitoring this possible threat (Minister Grapperhaus 2019).

Reducing the impact of IWIO

After the detection of an IWIO campaign, policy implementations are needed in order to reduce its impact. When formulating policy to reduce the effect of IWIO on Western societies, it is important to be aware that although the means of the operations may have changed due to technological innovation, the human mind has not changed (Lin 2018). Defensive measures, therefore, need to be consistent with this notion. Lin has divided defensive measures that have the aim to reduce the impact of IWIO into two categories:

Category I: Measures to help people resist the operation of the IWIO weapon targeted at them.
Category II: Measures to degrade, disrupt, or expose an adversary's arsenal of IWIO weapons as they are being used against a target population.

As the responsibility of the second category of measures mainly lies with technological companies and online platforms, or as Lin describes it, infrastructural entities in the information environment, the main focus of this analysis is on the first category.

Category I consists of three possible measures that Western governments can take, and is focused on reducing the impact of an IWIO by creating resilience within their societies. The first measure to cause the population to become more resilient against the effects of IWIO is by making it easier for people to engage their rational thought capabilities. In order to do so, one needs to begin by understanding the root of human vulnerabilities. It has been argued that human biases are the cause of these vulnerabilities since they often distort the ability to think rationally and clearly (Lin & Kerr 2019:8). If this is the case, this could be remedied by restoring such biases and helping people find ways to use their capabilities for rational thought to the fullest. This phenomenon is called 'debiasing' (Lin 2018). Due to the false

narrative that is created by IWIO, the process of debiasing becomes very important. One method describes that in order to debias people, they must be ‘’vaccinated’’ against fake news (Lin & Kerr 2017:20). Since different Dutch governmental agencies have been cooperating with the company known as DROG, the Dutch have been trying to inoculate their population against fake news (Interviewee #1; #5; Oosterwoud 2019). The contrast between the Dutch approach and Lin’s framework lays in the method that is being used to do so. Lin describes how, by pre-emptively flagging false claims and simultaneously delivering the first message about those claims, combined with an immediate explicit refutation of potential responses, people will become more aware (Lin 2018). DROG, however, uses another technique. In their game, which is called ‘Bad News’, the participant becomes the one who is spreading fake news (Oosterwoud 2019). The goal of this game is individual resilience. DROG tries to achieve this by teaching people on an individual level to understand what disinformation is and how it is being used (Idem). One of the focus points when doing so is to not be reactive but rather to pre-bunk citizens. This idea of not subsequently having to respond to disinformation, but instead to anticipate on it, is also described by Lin (Lin 2018).

Another important factor of debiasing is in the way in which messages are refuted. When presenting a new message with the aim of refuting the one that is part of an IWIO, the new message must contain more than simply factually accurate information (Idem). It is important for the new message to present information which does not conflict with the core believes and values of the targeted audience. In order to do so, the new information still needs to be presented in a way that people will consider compatible with their views on the issue (Idem). This aspect of debiasing is much more difficult to implement in governmental policy as Dutch policy makers continue to struggle with the thin line between information which is actively being used for an IWIO campaign or the views or beliefs of some citizens (Interviewee #1; #3). By presenting new information that is specifically chosen in order to minimize interference with peoples’ beliefs and values, information may be politicized (Idem).

Lin also describes the implementation and use of fact checking tools to help determine whether the information that is being shared online is accurate or false (Lin 2018). Although Dutch governmental agencies do not have a fact checking tool themselves, the EU RAS offers such an option (EUvsDisinfo). Due to the fact that the RAS has a 24/7 capability, a prompt reaction to disinformation can be delivered. The reaction, which must be fact-based and spread through effective communication, can help citizens to quickly asses the accuracy of doubtful claims. The Dutch government may not have their own fact-checking facility, but on the ‘’Blijf Kritisch’’ campaign website the government does refer to the website: nieuwscheckers.nl. On this website, which was developed by the University of Leiden, facts that are mentioned in, for instance the news, are being verified (Rijksoverheid 2019).

The second measure to make the population more resilient against the effects of IWIO is by using human biases to counteract the effects of an adversary’s IWIO weapon. Whereas IWIO take advantage of the

way the human mind works, this measure also has a psychological element. When trying to use biases to counter IWIO, human decision and conclusion making, also called intuitive reasoning strategies or heuristics, need to be taken into account (Lin & Kerr 2019:8). These 'affect heuristics' substitute simple human judgement to execute the process of estimating. This process can result in cognitive biases which may lead to flawed conclusions and decisions (Ibid). Therefore, IWIO use this phenomenon, whereby people make decisions based on how they feel about a certain topic or situation, in order to influence people's judgment (Ibid). When taking this into consideration Lin suggests using biases when formulating a response strategy (Lin 2018). One important result of the affect heuristics is the effect of repeated false statements. Repeating false claims or statements will most in all probability result in an increase of belief in those untruths (Idem). This phenomenon is also acknowledged by Dutch policy makers. The NCTV has as their main task to first detect disinformation, then interpret the underlying message and finally to create perspective for action (Interviewee #3). 'When formulating a response, we always take into account that to deny is to strengthen'(Idem). The Dutch government will therefore always endeavour to demonstrate another perspective or view on 'the truth' when communicating a response (Idem).

The third and final measure to make the population more resilient against the effects of IWIO is by educating the general population. These educational efforts are focused on improving the ability of citizens to think critically about the media they consume (Lin 2018). When doing so the focus of the governmental policy should concentrate on teaching its people to think, look and reflect critically on the information they are offered and consume. The aim of this approach is to create resilience, as people will become less likely to be influenced by all that they read and see (Idem; Aro 2016:124). The Dutch government is actively working on this topic by the use of several means. The first way in which the government is trying to achieve resilience against disinformation is through the 'Blijf Kritisch' campaign, which was initiated by the Ministry of Interior and Kingdom Relations. The campaign focuses on creating awareness surrounding the existence of disinformation, and offers a checklist to teach citizens how to investigate whether or not information is fake (Rijksoverheid 2019). The checklist explains the distinction between qualitative investigative journalism and online platforms on which everybody can post messages and express themselves. The checklist also briefly explains how fake news is being spread, as well as the methods and techniques fake news creators use to make it appear real (Idem). Additionally, the website teaches the user how to consult several sources in order to verify the spread message.

Another way in which the Dutch government is trying to educate Dutch citizens is by increasing media literacy from an early age, the importance of this measure is emphasized in many literature and has also proven to be effective in Finland (Hall 2017:56; Mackintosh 2019). Although the Ministry of Interior and Kingdom Relations is in the lead, there is close and intensive cooperation with the Ministry of

Education, Culture and Science (Interviewee #1). In addition to supporting the 'Blijf Kritisch' campaign the Ministry of Education, Culture and Science also founded the website 'mediawijsheid.nl' which offers teaching materials for both parents as well as teachers on how to use and interpret information coming from all the different media sources that are currently available (mediawijsheid.nl 2019). Both the Ministry of Interior and Kingdom Relations and the Ministry of Education, Culture and Science are also currently working with the company, DROG, to create a game to increase media literacy at/in schools throughout the country (Interviewee #1).

The second category of measures have a different focus compared to the first category. Whereas the first category was about the targeted audience and creating resilience, the second category is more focused on the technological aspect of IWIO. As stated above, category II measures will only be briefly discussed in this analysis.

Category II consists of five types of measures that can be taken in order to degrade, disrupt or expose an IWIO operation. Because the enablers for IWIO nowadays are mainly online platforms, the responsibility of these measures generally lies with the involved technological companies (Lin 2018).

The first measure is employing fact checkers in order to counter disinformation. Although this measure has already been discussed, and the fact checking capability of the RAS is part of both the Dutch and the EU policy, technological companies and social media platforms also share a responsibility here. Online platforms increasingly use fact checkers in order to eliminate fake news (Facebook.nl 2019). A hard intervention of governments in these companies is, however, not yet possible or is deemed unnecessary. Minister Ollongren commented in February 2019 that she is currently not about to formulate a law against fake news. In the Minister's opinion, the main responsibility of monitoring the content of the information that is spread on online platforms still lies with the platform itself (Ollongren 2019).

The second measure which has been suggested is to disrupt the financial means for providing fake news. The creation of fake news and disinformation is often outsourced by the Russian government to private companies, removing the financial incentive to create fake news can diminish the production of it (Oosterwoud 2019). Social media platforms such as Facebook and Instagram are currently working on discovering ways to disrupt the economic incentives of disinformation, 'since most fake news is financially motivated' (Facebook 2017). Information concerning methods to disrupting financial measures to create fake news are not mentioned in Dutch policy.

The third measure is to reduce the number of automated amplifiers of disinformation. By reducing the volume of automated amplifiers, the actual size and range of disinformation that is being spread will eventually also shrink (Lin 2018). Varying social media platforms such as Facebook and Twitter are currently working on deleting spam-accounts that are being used to spread disinformation (NOS 2018).

Details regarding the current state of reducing the number of automated amplifiers is not mentioned in Dutch policy.

The fourth measure is to create more transparency in the political traffic displayed on social media. The term political traffic includes both political ads as well as political campaigns targeted at people through algorithms (Lin 2018). In a letter to Parliament, the Dutch Cabinet endorsed the importance of free information gathering in order to have a legitimate and fair democratic electoral process (Ollongren 2019). The Cabinet acknowledges the significant role that technological companies play and has therefore agreed with the EU to draw a code of conduct for these companies (Idem). The EU Code of Conduct for dealing with disinformation secures measures which must be adopted by tech-companies to increase transparency regarding political advertisement (Idem). Currently this code of conduct is being implemented by self-regulation of these companies, although it is also intensively being monitored on a EU level.

The fifth and final measure is one that focuses on future defensive strategies. This measure puts in implements forensics to detect information operations and disinformation. When focusing on future events, it is of importance to concentrate on information that could have a damaging effect in the future, such as forged e-mails, videos, audio, etc. (Lin 2018; Lin 2019: 12-17). The reason why forging information can be an effective and fast tactic for IWIO is because they work more rapidly than the news cycle. 'While legitimate investigators, analysts and journalists pored over the documents, the adversary would be able to point directly to the falsely incriminating information' (Lin 2018). This threat is also being acknowledged by the NCSC. 'A false online message about a technological vulnerability can have large societal consequences. It is therefore enough to spread the message; even if the event never occurred, this can lead to instability' (Interviewee #2). The Ministry of Defense is currently working on this fifth measure as they have a department which tries to predict global events and changes in order to remain ahead of possible future security threats (Interviewee #5).

In this analysis the current Dutch approach and policy measures have been tested by the use of Lin's framework for developing a response to IWIO. Various Dutch governmental agencies have taken steps to protect the society of the Netherlands against Russian IWIO, and additional policy is being developed to improve the current approach. The Dutch governmental agencies both formulate policy themselves as well as participate in the joint European effort to counter disinformation. The EU approach, which partly consists of the work of the department EU vs Disinfo, faced difficulties and criticism after this department claimed several Dutch articles were fake news, while in reality they were not (Interviewee #1). This event clearly emphasizes the challenges of dealing with the topic of disinformation (Idem). Due to the fine line between human rights and freedom of speech, and identifying the /issue of fake news, the Dutch government operates very carefully. This may eventually lead to less policy on this topic than is desirable, in order to make sure these basic human rights are always well respected (Idem).

VI. Conclusion

‘All warfare is based on deception –

To subdue the enemy without fighting is the acme of skill.’

Sun Tzu – The Art of War.

The aim of this thesis was to evaluate the current Dutch defensive policy measures concerning Russian IWIO in the Netherlands. This was done through an analysis of the current policy measures based on the theory of Lin (2018), which offers a framework for developing a response to IWIO. Whereas the previous research primarily focused on technological counter-measures against Russian IWIO, this thesis aims to answer the research question from a multi-dimensional perspective. This thesis has examined Dutch policy regarding Russian IWIO in order to answer the research question:

To what extent does the Dutch governmental policy to counter Russian information warfare and influence operations match the Russian threat and take defensive measures to protect Dutch society?

The nature of the Russian IWIO threat can best be described as an effort to achieve political goals which benefit Russian leadership by weaponizing information and exploiting societal vulnerabilities. Russian IWIO use both technological as well as psychological components. The main target for these operations is the general public, as their opinion ultimately influences the democratic decision making process. Until now the main focus of Russian IWIO in the Netherlands has been on influencing the public’s opinion regarding the MH17 airplane crash and the outcome of the JIT report.

The framework for developing a response to IWIO offered by Lin is based on the current threat of IWIO to Western societies. The recommended measures described in the framework do not solely focus on the technical enablers of IWIO but also take into account other aspects of the threat. Lin’s framework offers detecting measures for an IWIO in progress, as well as measures to reduce the impact of IWIO. The measures offered in his framework are supported by findings coming from other literature, as described in the theoretical framework.

When analysing the Dutch defensive policy by the use of Lin’s framework, the following conclusions can be drawn: The Netherlands is likely an interesting target for Russian IWIO for multiple reasons. The Dutch Ministry of Foreign Affairs has acknowledged this increased Russian interest and aggression. One of the reasons for Russia’s interest in the Netherlands is because the Netherlands participates in multilateral organizations and partnerships such as NATO and the EU. Another reason is the JIT’s investigation of the 2014 MH17 airplane crash which The Netherlands is currently leading. Since the

JIT's evidence is pointing at Russia for being the perpetrator of this incident, Russia has a clear interest in influencing the outcome or the legitimacy of the JIT's report. In order to identify automated IWIO weapons in use, the Dutch governmental agencies are participating in the European led RAS, which is part of a larger European effort to counter disinformation. The Dutch government concluded that when it comes to the Russian IWIO threat in the Netherlands, the main focus lies on spreading disinformation about the airplane crash of flight MH17. The detection of the IRA's efforts show that Russia indeed used automated IWIO weapons targeted at Dutch society to influence public opinion. A final point to detect a Russian IWIO are measures to undermine the legitimacy of institutions that provide societal stability and continuity. Although the Dutch government finds it difficult to interfere in these types of matters, as it is their top priority not to infringe on human rights like freedom of speech or press, it may still be necessary to formulate a policy on this topic. The Russian attempt to discredit the JIT's report by the use of IWIO campaigns, may lead to a decrease in the perceived legitimacy of institutions for the general population.

After the detection of Russian IWIO, governments need to take measures to reduce the impact of IWIO on society. The first category of measures the Dutch government is currently taking focuses on the psychological element of these operations. This consists of measures to tackle cognitive human vulnerabilities by cooperating with the company DROG, which developed a program to 'vaccinate' people against disinformation. Other approaches the Dutch government has taken are the way in which fake messages are being refuted as well as the use of fact checking tools such as the 24/7 capability to deliver a prompt reaction to disinformation by RAS. Another measure to help citizens grow more resilient against the effects of IWIO is by using human cognitive biases to counter the effects of IWIO. The Dutch government is well aware of these psychological effects and therefore tries to show another view of 'the truth' when communicating a response, instead of denying it. The final measure to help people resist an operation of an IWIO weapon is by educating them. Educating people to think critically about the media they consume will create a more resilient society. This will be beneficial in the long term. In order to help increase societal resilience the Dutch government has created an awareness campaign called 'Blijf Kritisch'. Another aspect of societal resilience, on which the Dutch government is actively working, is increasing media literacy by offering teaching materials to both parents and teachers to educate children about how to consult different sources and how to verify their legitimacy.

The second category of measures to reduce the impact of IWIO on society consists of measures which are more focused on the technological aspect of these operations. This involves the use and implementation of fact-checkers. The Dutch government believes that the main responsibility to check whether a message is real or fake lies with online platforms. The Dutch government does, however, contribute to the fact-checking capability of the RAS. Another measure is to disrupt financial incentives to spread fake news. This is possible due to the fact that fake news is often outsourced by governments

to private actors. The Dutch government has not yet created policy in order to counteract these financial incentives. Social media platforms such as Facebook and Twitter have acknowledged that part of the problem regarding fake news is the financial motivation. Therefore Facebook has indicated an intention to formulate a strategy to counter this. Another measure the Dutch government has not yet created policy on is to reduce the number of automated amplifiers to diminish the size and range of disinformation. The Dutch government however does take measures to create more transparency with regard to political traffic such as political campaigns and ads which are displayed on social media. They do so through following the EU Code of Conduct on emphasizing the importance of free information gathering to increase transparency of political traffic online, in order to have fair and legitimate democratic elections.

The final measure is to implement a future defensive strategy. Although policy has been created on actual threats, an actual future Dutch strategy about countering disinformation has not yet been developed. While the Ministry of Interior and Kingdom Relations is currently waiting for the results of the research conducted by the University of Amsterdam, the Ministry of Defence does have a department that tries to increase the predictive power of the Dutch Military, in order to be able to anticipate future threat.

This thesis has discussed the defensive policies of the Dutch governmental agencies against Russian IWIO. When analysing the Dutch approach by the use of Lin's framework, the analysis has shown that although the Netherlands has only quite recently implemented measures to increase their capabilities for influence operation detection by joining the EU RAS, Russian information warfare targeted at the Netherlands has started long before. In the aftermath of the airplane crash of flight MH17, Russia initiated a disinformation campaign with the aim of misleading the public's opinion about the cause and the perpetrator of the crash. During the investigation into Russia's IWIO campaign targeted at MH17, automatic amplifiers were found to spread disinformation on online platforms. General detective measures, such as detection and identification of automated IWIO weapons not targeted at MH17, however, still need to be contrived. As it has been determined that Russia has actively been trying to undermine the legitimacy of the JIT report, the third detective measure; detecting efforts to undermine the legitimacy of institutions, has also been used by the Dutch government.

It should be noted that all of the current detecting measures are focused on the MH17 airplane crash. In order to consistently protect Dutch society against IWIO, the Dutch government should establish a detection capability which focuses on various societal vulnerabilities in order to immediately counter the future spread of disinformation during events.

By introducing the 'Blijf Kritisch' campaign, the plan to invest more in media literacy, and the cooperation with the company, DROG, in order to ''vaccinate'' people against fake news, the Dutch government is taking their first steps in creating long term resilience among the Dutch population. In

order to successfully ensure the results of the campaign and the plan to increase media literacy, the government still needs to take steps. Both the campaign and the teaching materials are not widely known and large parts of the Dutch population remain unaware of the threat of Russian IWIO. When improving Dutch governmental policy, the Ministry of Education, Culture and Science should be more involved, especially when it comes to the process of implementing teaching materials about media literacy and fake news in the regular curriculum for schools. By doing so, the Dutch population will be educated from a very young age concerning the dangers and consequences of disinformation, which will in turn increase their awareness and resilience.

Due to the nature of measures with a more technical nature, the responsibility for some of these measures lies only partially with the Dutch government. This subsequently makes it challenging for the government to create policy on this subject. Future research should look deeper into the defensive measures online platforms can take to counter the threat of IWIO. Only by including these platforms and fully implementing Lin's framework, can the entire nature of the Russian threat be countered.

One can conclude that the Dutch government has taken defensive measures that correspond to the nature of the Russian threat. The Dutch approach does not only focus on the technological aspect of the operations but also on the psychosocial part of IWIO. It can also be concluded that the Netherlands is making progress in creating a resilient society against Russian IWIO. In order to increase the results of the current policy, it is recommended to expand the visibility of both the awareness campaign as well as plans to increase media literacy. It is also recommended to create laws to restrict the spread of disinformation online. In addition to this the Dutch government should implement a critical vulnerability analysis which focuses on Dutch society itself. Only when Dutch policy makers are aware of these internal vulnerabilities, will it be possible to take counter-measures which fully protect the Dutch society against the Russian IWIO threat. Only then the Netherlands can be rest assured that Putin's Pravda does not become reality.

Bibliography

AIVD (Algemene Inlichtingen en Veiligheidsdienst) (2015). *'Jaarverslag'*. Ministerie van Binnenlandse Zaken en Koningsrijks Relaties.

AIVD (Algemene Inlichtingen en Veiligheidsdienst) (2016). *'Jaarverslag'*. Ministerie van Binnenlandse Zaken en Koningsrijks Relaties.

AIVD (Algemene Inlichtingen en Veiligheidsdienst) (2017). *'Jaarverslag'*. Ministerie van Binnenlandse Zaken en Koningsrijks Relaties.

AIVD (Algemene Inlichtingen en Veiligheidsdienst) (2018). *'Jaarverslag'*. Ministerie van Binnenlandse Zaken en Koningsrijks Relaties.

Allcott, H. & Gentzkow, M. (2017). *Social media and Fake News in the 2016 Elections.* Journal of Economic Perspectives. Standford University.

Andrew, C. & Gordievsky, O. (1990). *KGB The Inside Story*. New York: Harper Collins

Aro, J. (2016). *The cyberspace war: propaganda and trolling as warfare tools*. European view (2016), 15:121-132.

Ash, L. (2015). ''How Russia outfoxes its enemies'', *BBC:. http://www.bbc.com/news/magazine-31020283.* Conducted on 19 april 2017.

Bader, M. & de Jong, B. (2006). *Geheime diensten in Rusland: schild en zwaard van het regime-Poetin.* Internationale Spectator. Jaargang 60 – nummer 5. Instituut Clingendael.

BBC (2018). ''Russian spy: Theresa May condemns 'despicable act''. https://www.bbc.com/news/av/uk-43419433/russian-spy-theresa-may-condemns-despicable-act

Besemeres, J. (2016). *A difficult neighbourhood: Essays on Russia and East-Central Europe since World War II*. ANU Press.

Bittman, L. (1985). *The KGB and Soviet Disinformation*. New York: Pergamon-Brassey's – International Defense Publishers.

Bogdan, R., Taylor, S.J. (1990). *Looking at the Bright Side: A Positive Approach to Qualitative Policy and Evaluation Research*, Qualitative Sociology, 13(2), 183- 192.

Brands, H. (2016). *Paradoxes of the Gray zone.* Foreign policy Research Institute.

Bryman, A. (2012). *Social Research Methods*. Oxford: Oxford University Press.

Budget Ministry of Interior and Kingdom Relations 2018

Cizik, T. (2018). *Russian Information Warfare in Central Europe.* Information Warfare: New Security Challenges in Europe. Centre for European and North Atlantic Affairs. Bratislava.

Clingendeal Instituut (2019). *Analyse- Conflict en fragiele staten: De bellngcat- blik op Russische desinformatie rondom MH17.*

Cohen, F. (2011). *Influence operations.* Fred Cohen & Associates.

Cohen, D. & Bar'el, O. (2017). *The use of Cyberwarfare in influence operations*. Tel Aviv University, Israel.

Colonel Eikmeier, D.C. (2004). *Centre of Gravity Analysis*. Military Review. National Defense University Press.

Dhanapala, J. (2018). Soft Power, *Hard Challenges and the Disarmament Operative.* The Journal of International Communication

Elsevier Weekblad (2016). ''Dit is waarom kiezers tegen Oekraine-verdrag stemden.'' https://www.elsevierweekblad.nl/nederland/achtergrond/2016/11/dit-is-waarom-kiezers-tegen-oekraine-verdrag-stemden-402736/

Elsevier Weekblad (2018). ''EU-strijd tegen nepnieuws wakkert angst voor censuur en willekeur aan.'' *https://www.elsevierweekblad.nl/buitenland/achtergrond/2018/01/eu-nepnieuws-577605/*

EUvsDisinfo spreadsheet on RAS. March 2019.

European Commission (2018). *Action Plan against Disinformation*. European Commission contribution to the European Council. Brussels.

Facebook FAQ (2019): https://www.facebook.com/help/publisher/182222309230722
https://www.facebook.com/facebookmedia/blog/working-to-stop-misinformation-and-false-news

Farrell, H. & Schneier, B. (2018). ‘’Information attacks on Democracies’’, *Lawfare Blog:* https://www.lawfareblog.com/information-attacks-democracies

FireEye (2019). ‘’Threat Research: framing the problem cyber threats and elections.’’ https://www.fireeye.com/blog/threat-research/2019/05/framing-the-problem-cyber-threats-and-elections.html

FoxIT (2017). ‘‘Why wouldn’t Russia also interfere with the Dutch elections?’’. https://www.fox-it.com/en/insights/media/wouldnt-russians-also-interfere-dutch-elections/

Gianetti, W. (2017). *A Duty to Warn: How to help America fight back against Russian disinformation*. Air & Space power Journal.

Giles, K. (2013). *Divided by a Common Language: Cyber Definitions in Chinese, Russian and English.* International Conference on Cyber Conflict. NATO CCD COE Publications Tallinn.

Giles, K. (2016). *Handbook of Russian Information Warfare*. NATO Defense College. Rome, Italy.

Giles, K. (2019). *Moscow Rules: what drives Russia to confront the west*. Chatham House Insights Series, Londen & Brookings Institution Press, Washington D.C.

Governmental budget Ministry of Foreign Affairs 2015-2016

Gower, J. & Timmins, G. (2007): *Russia and Europe in the Twenty-First Century An Uneasy Partnership*. London: Anthem Press.

Hall, H.K. (2017). *The new voice of America: countering foreign propaganda and disinformation act.* First Amendment Studies 51:2, 49-61.

Hingley, R. (1970). *The Russian Secret Police*. London: Hutchinson & Co

Hoffman, F. (2010). *Hybrid Threats: neither omnipotent nor unbeatable.* Orbis 53 (3), 441-455.

Hutchinson, W. (2006). *Information Warfare and Deception.* Edith Cowan University. Perth, Australia. Informing Science Volume 9.

Hutchinson, W. (2010). *Influence Operations: Action and Attitude*. Edith Cowan University.

Janda, J. (2018). *How to boost the Western response to Russian hostile influence operations*. Wilfried-Martens Centre for European Studies. Vol. 17 (2) 181-188.

Jensen,B. & Valeriano, B. & Maness, R. (2019): *Fancy bears and digital trolls: Cyber strategy with a Russian twist,* Journal of Strategic Studies, DOI: 10.1080/01402390.2018.1559152

Kist, R. & Wassens, R. (2019). ‘’Hoe de Petersburgse trollenfabriek te werk ging na de MH17-ramp’’. https://www.nrc.nl/nieuws/2019/05/13/russische-trollen-verspreidden-mh17-fabels-a3960029

Komov, S.A. (1997). *About Methods and Forms of Conducting Information Warfare, Military Thought.* Journal of Slavic Military Studies. Taylor & Francis.

Lin, H. & Kerr, J. (2017). *On Cyber-enabled information warfare and information operations.* Oxford Handbook of Cybersecurity.

Lin, H. (2018). ‘’Developing Responses to Cyber-Enabled Information Warfare and Influence Operations’’, *Lawfare Blog: https://www.lawfareblog.com/developing-responses-cyber-enabled-information-warfare-and-influence-operations*

Lin, H. (2019). ‘*’On the organization of the U.S. Government for Responding to Adversarial Information Warfare and Influence Operations’’*. Journal of Law and Policy for the Information Society. Stanford University. United States.

Mackintosh, E. (2019). ‘’Finland is winning the war on fake news. What it’s learned may be crucial to Western democracy.’’ https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/

McNamara, L. (2019). During Meeting on Election Security at the American Embassy in Wassenaar.

McGonagle, T. & Coche, E. & Plaizier, C. & Klus, M. (2018). *Inventarisatie methods om ‘’nepnieuws’’ tegen te gaan.* Inistutuut voor Informatierecht, Universiteit van Amsterdam.

Orenstein, H. (2017). *Contemporary Warfare and Current Issues for the Defense of the Country.* Military Review November-December 2017.

Minister Blok (2018). Note to parliament about Dutch battle against ISIS. - - https://www.rijksoverheid.nl/documenten/kamerstukken/2018/04/13/kamerbrief-met-voortgangsrapportage-nederlandse-bijdrage-in-strijd-tegen-isis

Minister Blok (2018). Note to parliament about visit Moscow. https://www.rijksoverheid.nl/documenten/kamerstukken/2018/04/26/kamerbrief-met-terugblik-op-bezoek-aan-moskou

Ministry of Foreign Affairs (2018-2022). ‘‘Geintegreerde Veiligheidsstrategie’’.

Minister Grapperhaus (2019). Speech to parliament June 20th 2019.

Minister Grapperhaus (2019). ‘’Combat threats of Foreign States’’.

Minister Grapperhaus (2019). ‘’Attachments: Combat threats of Foreign States’’.

Ministry of Defense (2017). Meerjarig Perspectief Defensie: Houvast in een onzekere wereld: lijnen van ontwikkeling in het meerjarig perspectief voor een duurzaam gerede en snel inzetbare krijgsmacht.
Ministry of Defence (2018). ‘’MIVD verstoord Russische Cyberoperatie bij de organisatie voor het verbod op chemische wapens’’. 04-10-2018. https://www.defensie.nl/actueel/nieuws/2018/10/04/mivd-verstoort-russische-cyberoperatie-bij-de-organisatie-voor-het-verbod-op-chemische-wapens

Minister Ollongren (2017): Note to parliament about influencing public opinion by other foreign states.

Minister Ollongren (2018): Note to parliament about threat disinformation and influencing elections.

Minister Ollongren (2019): Note to parliament about transparency about political advertisement on Facebook.

Mo Jang et Al. (2017). *A computational approach for examining the roots and spreading patterns of fake news: Evolution tree analysis.* Computers in Human Behavior 84 (2018) 103-113. Elsevier.

MIVD (Militaire Inlichtingen en Veiligheidsdienst) (2016). *'Jaarverslag'*. Ministerie van Defensie.

MIVD (Militaire Inlichtingen en Veiligheidsdienst) (2017). *'Jaarverslag'*. Ministerie van Defensie.

MIVD (Militaire Inlichtingen en Veiligheidsdienst) (2018). *'Jaarverslag'*. Ministerie van Defensie.

Monaghan, A. (2016). *Putin's Way of War: The 'War' in Russia's 'Hybrid Warfare'.* Chatham House. Londen.

Mueller R. (2019). Ministry of Justice United States of America Press Conference on the 29th of May 2019.

NOS (2016). ''Initiatiefnemers referendum: Oekraïne kan ons niets schelen''. 31-03-2016. https://nos.nl/artikel/2096268-initiatiefnemers-referendum-oekraine-kan-ons-niets-schelen.html

NOS (2018). ''Al duurt het Jaren, veroordeling van Rusland is zeker niet onmogelijk''. 25-05-2018. https://nos.nl/nieuwsuur/artikel/2233514-al-duurt-het-jaren-veroordeling-van-rusland-is-zeker-niet-onmogelijk.html

NOS (2018). Twitter sluit miljoenen accounts in hoop bots te weren. https://nos.nl/artikel/2240265-twitter-sluit-miljoenen-accounts-in-hoop-bots-te-weren.html

NRC Handelsblad (2017). *Nabestaande MH17 veelvuldig lastiggevallen met desinformatie.* Consulted on April 12th 2019.

Oosterwoud, R. (2019). During Meeting on Election Security at the American Embassy in Wassenaar.

Palmertz, B. (2016). *Theoretical foundations of influence operations: a review of relevant psychological research.* Centre for Asymmetric Threat Studies Swedish Defense University.

POLITICO (2017). ''The Gerasimov Doctrine: It's Russia's new chaos theory of political warfare. And it's probably being used on you.'' September/October 2017. https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538.

Pomerantsev, P. (2015). *Authoritarianism Goes Global (II): The Kremlin's Information War.* Journal of Democracy, Volume 26, Number 4. John Hopkins University Press.

Prime-Minister Mark Rutte (2018). Press Conference May 25th.
https://www.youtube.com/watch?v=H97uqanW0Ik . Minute 1:10.

RAND Institute (2009). *Foundations of Effective Influence Operations: A framework for enhancing Army capabilities*. RAND Corporation. United States.

Rijksjaarverslag Ministerie van Defensie (2017).

Rijksjaarverslag Ministerie van Defensie (2018).

Rijksjaarverslag Ministerie van Buitenlandse Zaken 2018

Samadashvili, S. (2015). *Muzzling the Bear: Strategic Defence for Russia's Undeclared Information War on Europe.* Wilfried Martens Centre for European Studies. Brussel, Belgium.

Santa Maria, S.D. (2013). *Improving influence operations by defining influence and influence operations.* School of Advanced Military Studies. United States Army Command.

Secretary of state Knops (2018). Note to parliament about accessibility of digital communication for everybody.

Shea, T.C. (2002). *Post-Soviet Maskirovka, Cold War Nostalgia, and peacetime engagement.* Military Review Vol 82, No. 3.

Shimer, D. (2018*).* ''Smaller Democracies grapple with the threat of Russian interference.'' *The New Yorker. 08-12-2018*: https://www.newyorker.com/news/news-desk/smaller-democracies-grapple-with-the-threat-of-russian-interference

Shuster, S. (2016). How Russia has obscured the fact in the MH17 investigation. *Time Magazine:* http://time.com/4512834/mh17-russia-buk-ukraine-evidence-putin/

Simpson, E. (2005). *Thinking about Modern Conflict: Hybrid Wars, Strategy and War Aims.* Midwest Political Science Association.

Thomas, T.L. (2001). *Information Security Thinking: A Comparison of U.S., Russian, And Chinese Concepts.* Journal of Slavic Military Studies. Taylor & Francis.

Thomas, T.L. (2004). *Russia's Reflexive Control Theory and the Military.* Journal of Slavic Military

Studies. Taylor & Francis.

Thornton, R. (2015). *The changing nature of Modern Warfare*. The RUSI journal 160:4, 40-48.

West, D.M. (2017). ‘’How to combat fake news and disinformation.’’
https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/

Appendix

Semi structured Topic Lists

1. How would you describe the threat of Russian information warfare?

2. What role do you see for cyber when analysing this threat?

3. What type of policy regarding this subject does your department have? (What measures are being taken?)

4. How do the different governmental agencies cooperate on this subject?

5. Where do you see room for improvement?

Profile Interviewees

Some of the interviews have to remain confidential and for that reason a description of the interviewees is given below.

Interviewee 1: A senior policy adviser at the Ministry of Interior and Kingdom Relations who has been involved in the process of countering disinformation from the beginning.

Interviewee 2: A high ranked Military officer who is currently at the head of the NCSC at the Ministry of Justice and Security.

Interviewee 3: A senior policy officer at the Ministry of Justice and Security specialist on foreign threats and interference.

Interviewee 4: A General of the Dutch Army, who worked on the topic of foreign interference and influence operations for several years.

Interviewee 5: A policy adviser working at the Ministry of Defense on countering Hybrid Warfare.