Master thesis

Cooperating to counter hybrid threats?

The relative lack of responsiveness of the Netherlands to hybrid threats between 2014 and 2019.

Universiteit Leiden
The Netherlands

Leiden University	Faculty of Governance and Global Affairs
Program:	Master Crisis & Security Management
Student:	Julia de Hoop, BSc
Student number:	S2344963
Date of admission:	08-06-2019
Word count:	22230 words (Excluding References)
	24273 words (Including References)
Thesis Supervisor:	Dr. E. Dijxhoorn
Second Reader:	Mr.drs. W.J.M. Aerdts

Abstract

The purpose of this thesis is to study the security policy decision-making process of the relevant Dutch ministries and security agencies, including their responsible intelligence agencies, in order to explain the lack of responsiveness by these ministries and security agencies to hybrid threats facing the Netherlands. The method of this research is a case study. The responsiveness of the relevant Dutch ministries to hybrid threats between 2014 and 2019 is reconstructed by process tracing the security decision-making process regarding hybrid threats of the relevant ministries and security agencies through public official reports and notes. This thesis concludes that the variety of definitions for hybrid threats by all relevant ministries and security agencies and the absence of a legitimate leading Dutch ministry in realizing an integrated strategic response to hybrid threats lead to a relative lack of responsiveness to hybrid threats in the Netherlands. Furthermore, the extensive amount of hybrid threats presented in the literature review on hybrid warfare and the changing character of hybrid threats make it difficult for relevant Dutch ministries and security agencies to address all these threats simultaneously. This thesis therefore recommends that relevant Dutch ministries and security agencies must create a common definition for hybrid threats facing the Netherlands in order to realize an interdepartmental strategy to counter hybrid threats. Furthermore, one Dutch ministry must obtain the legitimate power to lead all relevant ministries and security agencies, including their responsible intelligence agencies, in order to counter hybrid threats collectively.

Table of Contents

List of Abbreviations

AIV	Advisory Council on International Affairs
AIVD	General Intelligence and Security Service
ARV	General Safety Council
ASIFU	All Source Intelligence Fusion Unit
AZ	Ministry of General Affairs
BENELUX	Belgium, the Netherlands and Luxembourg
BIV	International Security Budget
BuZa	Ministry of Foreign Affairs
DCC	Defense Cyber Command
DefCERT	Defense Computer Emergency Response Team
EU	European Union
IVS	International Security Strategy
JSCU	Joint Sigint Cyber Unit
J&V	Ministry of Justice and Security
KMar	Royal Netherlands Marechaussee
MIVD	Dutch Military Intelligence and Security Service
MINUSMA	United Nations Multidimensional Integrated Stabilization Mission Mali
NATO	North Atlantic Treaty Organization
NBV	National Signals Security Bureau
NCTV	National Coordinator for Security and Counterterrorism
NCSC	National Cyber Security Center
OVV	Dutch Safety Board
OSCE	Organization for Security and Co-operation in Europe
SOPs	Standard Operating Procedures
Wiv 2002	Intelligence and Security Services Act 2002
WRR	Netherlands Scientific Council for Government Policy
Wvo	Security Investigations Act

1. Introduction

1.1 Problem and research question

During conflicts and crises, the awareness of a need for an integrated approach to the protection of vital interests in the Netherlands exists, but a proactive and institutionalized application of an integrated approach to counter hybrid threats is not yet established in the Netherlands (BuZa, 2018, p. 24). The proactive and institutionalized application of an integrated approach to counter hybrid threats is also known as a grand strategy (Ducheine, 2016, p.9). According to Ducheine (2016, p7), hybrid threats emanate from the integrated use of a combination of all available power tools to influence the behavior of others. The Russian takeover of Crimea and the downing of flight MH-17 completely surprised the Netherlands, which resulted in a situation where the Netherlands seemed unsure on how to respond (Treisman, 2016, p. 54). This confusion was a direct result of the successful application of hybrid threats by the Russian Federation (Ducheine, 2016, p.10). These hybrid threats do not have to be primarily present during officially declared conventional conflicts but can also be present even before a conventional armed conflict emerges (ibid, p.8.). The annexation of Crimea and the downing of flight MH-17 in 2014 were therefore a wakeup call for the Netherlands to start paying more attention to hybrid threats and especially those emanating from Russia. However, five years later in 2019, at the time of writing, the Netherlands still lacks a grand strategy regarding both defensive and offensive hybrid threats (BuZa, 2018, p. 24).

Having a grand strategy regarding hybrid threats instead of separate reactive crisis teams will increase the response to hybrid threats (Ducheine, 2016, p.9). The better different instruments of power are coordinated, the more synergy is achieved in order to provide security, which is one of the tasks of the Dutch government (ibid, p.9). The Dutch government is responsible for the response to threats that are facing the Netherlands and the protection of the Netherlands (Dutch Consitution, 2019, art. 97). Since there is no grand strategy regarding hybrid threats in the Netherlands, it is necessary to research what can explain this relative lack of responsiveness of the relevant Dutch ministries and security agencies to hybrid threats between 2014 and 2019. Therefore, the following main research question is formulated:

What can explain the relative lack of responsiveness of the relevant Dutch ministries and security agencies, including their responsible intelligence agencies, to hybrid threats between 2014 and 2019?

The security policy decision-making process of relevant Dutch ministries and security agencies resulted in a relative lack of responsiveness to hybrid threats. For that reason, an explanation for the relative lack of responsiveness to hybrid threats can be found in the security policy decision-making process of relevant Dutch ministries and security agencies. This research will focus on the structures

and the security policy decision-making process of relevant Dutch ministries and security agencies, including their responsible intelligence agencies. By analyzing the security policy decision-making process on the actual response to hybrid threats of relevant Dutch ministries from 2014 until 2019, the answer to what can explain the relative lack of responsiveness to hybrid threats between 2014 and 2019 can be found.

1.2 Background

The Russian takeover of Crimea and the downing of flight MH-17 completely surprised the Netherlands, and were a direct result of the successful application of hybrid threats by the Russian Federation (Treisman, 2016). The following section explains how hybrid threats in the Netherlands can also be present even before a conflict emerges and why the annexation of Crimea and the downing of flight MH-17 in 2014 were a wakeup call for the Netherlands to start paying more attention to hybrid threats and especially those emanating from Russia.

On 27 February 2014, unidentified individuals in unmarked uniforms also known as "little green men" entered Ukraine and occupied the main governmental buildings of Crimea (Galeotti, 2016, p. 284). At that moment, the international community including the Netherlands was still in the aftermath of the 2014 Winter Olympics that were held in the neighboring state Russia between 7 February and 23 February (ibid.). On 4 March 2014, Russian President Putin made an official statement and stated that the "little green men" in Crimea were local self-defense units of pro-Russian separatists that were striving for a Russian identity (Kremlin, 2014). According to Putin, these pro-Russian separatists would not have been able to occupy the governmental buildings in Crimea if the Ukrainian government was a stable system (ibid.). Putin also did not acknowledge the authorities in Ukraine, because these authorities came to power through what he considered "an anti-constitutional takeover" (ibid.). Russia suggested a referendum so that all citizens of Crimea could legitimately vote to whether or not secede from Ukraine. Furthermore, Putin stated that the intentions of Russian troops in Crimea were nothing more than self-protection. Subsequently on March 16, an announced referendum was organized under the supervision of Russian soldiers (Galeotti, 2016, p. 284). This referendum resulted in the annexation of Crimea and its integration into the Russian Federation on March 18 (Ramicone, 2014, p 6). Despite the fact that the Netherlands regarded the referendum as illegitimate and illegal because of the low turnout and the influence of Russia on the results, the annexation of Crimea occurred (ibid., p.6). Although the Russian government initially denied its direct military intervention in Crimea, it later turned out to be that the "little green men" were actually Russian military units operating along with separatist armed units in Crimea (Galeotti, 2016, p. 86). Hybrid threats such as the denial of Russian influence on the annexation of Crimea were implemented even before the Netherlands noticed it and showed the effectiveness of hybrid threats. As a result, the Netherlands was

not able to respond on time to the situation in Crimea. The inability to respond to these hybrid threats were therefore a wake up call for the Netherlands to start paying more attention to hybrid threats.

The conflict between Ukraine and Russia also directly affected the Netherlands on 18 July 2014, by taking down Malaysian Airlines flight MH-17 by a then unknown force killing all 298 people aboard, including 173 Dutch citizens in eastern Ukraine (Gibney, 2015, p. 169). In the days after downing flight MH-17 and during the presentation of the investigations of the Dutch Safety Board (OVV), multiple contradictory versions about the causes of the MH-17 plain crash were spread by the Russian Federation (AIV, 2017, p.10). Also, before and after the presentation of the investigation report by the OVV on 13 October 2015, Russian intelligence services attempted to hack the OVV systems with cyber attacks (ibid., p.10). On 24 May 2018, a joint investigation team announced that the unknown force that brought down flight MH-17 was a Buk missile installation that belonged to the Russian army (Government, n.d.). While the Russian Federation is morally and politically to blame for the downing of MH-17, it remains less clear how to define the Russian responsibility under international human rights law (Gibney, 2015, p. 169).

The denial of Russian military involvement, the Russian maneuvers in the gray zone of international law and the offensive cyber actions against Dutch targets during the described events in Crimea are examples of hybrid threats facing the Netherlands. The means that are used to target the Netherlands, characterize a conflict in the absence of a conventional armed conflict. Therefore, the two described events show the consequences of hybrid threats that are facing the Netherlands.

1.3 Grand strategy and responsiveness

The motivation for this research is the absence of a grand strategy regarding hybrid threats by the relevant Dutch ministries. In order to emphasize the relevance of a grand strategy to hybrid threats, the concept grand strategy must be explained. A grand strategy is a method and a level of decision-making to determine how war and operations are used to achieve the goals of a state (Amersfoort, 2016, p. 219). A grand strategy therefore is the calculated relationship of means to large ends (Gaddis, 2002, p.7). It is about what means and how these means are deployed in order to achieve the determined goals of a state. The fighting of wars and the management of states therefore demand the calculation of relationships between means and ends for a longer stretch of time (ibid, p.7). Furthermore, a grand strategy exists separately of a political security administration on the side of (military) operations and of an operational and tactical level (Amersfoort, 2016, p. 219). In recent years, Dutch ministries involved in the response to hybrid threats, such as the ministry of defense, are entangled in business operations, efficiency issues and bureaucratic concerns (ibid., p. 221). As a result, there is a lack of strategists with predictive capacity who focus on safety situations in the Netherlands. In this case, a grand strategy to counter hybrid threats would imply a proactive and institutionalized application of an

integrated approach to counter hybrid threats (BuZa, 2018, p. The Dutch government is responsible for realizing an integrated approach to counter hybrid threats, which implies the collaboration of all relevant Dutch ministries and security agencies. Therefore, the absence of a grand strategy regarding hybrid threats resembles the relative lack of responsiveness of relevant Dutch ministries and security agencies to hybrid threats facing the Netherlands.

Moreover, the concept responsiveness is relevant to explain in order to understand the research question. Bernardes and Hanna (2009) define responsiveness as "the ability of an organization to respond quickly and flexibly to its environment and meet the emerging challenges with innovative responses" (p. 34). Responsiveness therefore is the capacity to gain advantage by intelligently, rapidly and proactively seizing opportunities and reacting to threats (ibid.p. 34). A responsive organization adopts an after-the-fact behavior once a triggering episode has occurred (ibid., p. 45). The relevant and increasingly important triggering episode in this case is the wakeup call for the Netherlands to start paying more attention to hybrid threats and especially those emanating from Russia. A grand strategy in order to counter these hybrid threats would increase the responsiveness of relevant Dutch ministries and security agencies.

1.3 Sub questions

Some of the threats the Netherlands is currently facing can be defined as hybrid threats (Ducheine, 2016, p.10). In order to research possible explanations of the relative lack of responsiveness by the relevant Dutch ministries to hybrid threats between 2014 and 2019, first the hybrid threats the Netherlands is facing must be determined. Therefore the first sub question is formulated:

What are hybrid threats and what hybrid threats is the Netherlands facing?

According to article 97 of the Dutch constitution, the Dutch government is responsible for the defense and protection of the interests of the Kingdom as well as for the maintenance and promotion of the international legal order (Dutch Consitution, 2019, art. 97). The relevant Dutch ministries, including their responsible intelligence agencies, and security agencies, are therefore also accountable for the response to hybrid threats the Netherlands is facing. Therefore, the causal factors that can explain the lack of responsiveness to hybrid threats must be found in the actions of these Dutch ministries and security agencies. The hybrid threats the Netherlands is facing and the different ministries that are accountable for the response to those hybrid threats must be researched and defined. Therefore, the following second sub question is formulated:

Which Dutch ministries and security agencies, including their responsible intelligence agencies, are involved in response to the hybrid threats the Netherlands is facing?

The answer to the main question can be found in the structures and the decision-making process of the involved Dutch ministries by analyzing the political decision-making process on the actual response to hybrid threats from 2014 until 2019. The three models for policy decision-making known as the rational actor model, the organizational process model, and the bureaucratic politics model from Graham Allison (1969) will be used to explain the lack of responsiveness of the involved Dutch ministries and agencies since these models provide three levels of analysis for policy decision-making. Allison for example explains that different ministries frame an issue differently, which results in irrational policy decisions. In order to research the models of Allison, the manner how relevant Dutch ministries frame hybrid threats must be researched. The third sub question therefore is:

How have hybrid threats been framed by the relevant Dutch ministries and security agencies, including their responsible intelligence agencies, *between 2014 and 2019?*

Both scholars and professionals consider a grand strategy for the response to hybrid threats favorable (NCTV, 2016, p.7; WRR, 2011, p. 8; van Amersfoort, 2016, p.217). The Netherlands still lacks a grand strategy to response to hybrid threats. The actual response of the relevant Dutch ministries and security agencies to hybrid threats between 2014 and 2019 must be examined in order to determine if the policy decision-making variables from Allison lead to the actual relative lacking responsiveness to hybrid threats. By analyzing the actual response in the chosen time period, the causal mechanisms explained by Allison can be compared with the empirical evidence. Hence, the last sub question is formulated:

What has been the actual response of the relevant Dutch ministries and security agencies, including their responsible intelligence agencies, to hybrid threats in terms of a grand strategy between 2014 and 2019?

The last sub-question also answers how the actual response to hybrid threats by the relevant Dutch ministries contributes to a grand strategy or how the actual response contributes to the lack of responsiveness.

1.4 Academic relevance

One of the main tasks of the Dutch government is to protect Dutch citizens from threats by creating and adhering to policies that are aimed to become resilient to these threats. Policies that provide resilience for threats include a grand strategy for countering threats and the creation of response

mechanisms for threats. Currently, the Netherlands is facing hybrid threats that are potentially affecting the security of Dutch citizens but a strategy about why and how to counter hybrid threats is missing (van Amersfoort, 2016, p. 219). Since a wide range of hybrid threats is facing the Netherlands, it is unclear how the current response of Dutch Ministries to hybrid threats is protecting Dutch citizens. Therefore, this research aims to determine how the gap between hybrid threats and the safety of Dutch citizens can be closed by researching the policy decision-making process on the response to hybrid threats in the Netherlands. By not just analyzing the output, but also the input of the involved actors through the three conceptual models of Allison, this research contributes to give a theoretical based insight into the current lack of responsiveness by the Dutch government. By applying the theory, it can be determined how the Netherlands currently develops its national security strategy.

1.5 Societal relevance

Even after five years since the presence of hybrid threats became apparent, the Netherlands still lacks a grand strategy to counter hybrid threats. Therefore, it is relevant to research what causes this lack of responsiveness by analyzing the security policy decision-making process of the relevant Dutch ministries regarding hybrid threats. By researching what causes the relative lack of responsiveness, this research is relevant for the ability of the Netherlands to overcome the obstacles that cause the relative lack of responsiveness to hybrid threats.

1.6 Overview

In the following chapter, a literature review on hybrid warfare and a theoretical framework for the three policy decision-making models from Allison are presented and explained. Based on the literature review and the theoretical framework, the indicators that can explain the lack of responsiveness to hybrid threats by relevant Dutch ministries and security agencies are presented in an analytical framework. In the third chapter, the relevant Dutch ministries and security agencies are operationalized and the case study design and methodology are explained. Chapter four presents an empirical description of the response to hybrid threats by the relevant Dutch Ministries between 2014 and 2019, followed by an analysis. The empirical timeline is based on public reports from relevant Dutch ministries, which were published and operational between 2014 and 2019. The indicators for the policy decision-making models that can explain the relative lack of responsiveness to hybrid threats are found in the empirical timeline. The final chapter answers the main question and concludes that the framing of hybrid threats by relevant Dutch ministries and the absence of a legitimate leading Dutch ministry, or their responsible intelligence and security agencies, explain the relative lack of responsiveness to hybrid threats facing the Netherlands. Also, the extensive amount of hybrid threats presented in the literature review on hybrid threats and the unnoticeable character of hybrid threats make it difficult for relevant Dutch ministries to address all these threats simultaneously with one grand strategy. Finally, recommendations for future research are given and a discussion is presented.

2. Theoretical framework

Hybrid threats are relative new forms of threats described by academia. In order to answer the main research question, it is important to position the relative lack of responsiveness to hybrid threats by relevant Dutch ministries and security agencies, including their responsible intelligence agencies, in the standing theory on hybrid threats. This chapter answers the first sub-question based on the literature review on hybrid warfare. First a literature review on the concept hybrid threats and hybrid warfare is presented. The policy decision-making models of Allison (1969) are a theoretical framework to analyze the relative lack of responsiveness to hybrid threats by involved Dutch ministries and organizations. The theoretical framework from Allison is explained and presented and the theory on hybrid threats and three policy decision-making models are translated into an analytical framework. This analytical framework forms together with the operationalized research variables from chapter three the basis for the collection of empirical data.

2.1 Literature review Hybrid Warfare

Throughout history, many wars have been characterized by both regular and irregular warfare (Gray, 2007). Especially in 1989, scholars introduced theories about new forms of warfare characterized by non-state actors that accomplish their goals by conventional military capabilities and information technology thus influencing the enemy's conceptions (Lind, Schmitt, Sutton, Wilson and Nightengale, 1989). Analysts introduced new concepts like 'new wars', 'fourth-generation warfare' and 'asymmetric warfare' in an effort to conceptualize changes in contemporary warfare based on the idea that warfare differed strongly from older patterns of armed conflict (Renz, 2016; Kaldor, 2013; van Creveld, 2004). All of these concepts struggled to provide historical context for portraying a clear division between this new warfare and the traditional conflicts fought by conventional means (Gray, 2007).

A common aspect of these new forms of warfare is that direct military confrontations would only benefit the stronger opponent (Lanoszka, 2016, p.177). Therefore, the weaker combatants are using more incremental, subtler and indirect tactics such as the use of propaganda as well as attacking the weak points of opposing militaries (ibid., p.177). Liang and Xiangsui concluded in 1999 that the United States (US) could only be conquered by its weaker opponents by applying alternative capabilities in the economic, legal and information domain (Liang and Xiangsui, 1999, pp. 34-59). The scholars argued that a distinction between physical military power and other forms of non-physical power enable a blurry approach of defeating a physical stronger force (ibid.). Eventually, scholars acknowledged this blurring of warfare categories and introduced the concept of hybrid warfare (Hoffman, 2009).

The concept of hybrid warfare first emerged in 2005 in an article by the scholar Erin Simpson who stressed the importance of which actors are fighting instead of how actors were fighting using the Vietnam and Iraq war as cases (Simpson, 2005). Then, Marine Corps Combat Development Commander Lieutenant General Mattis, later United States Secretary of Defence and the scholar Frank Hoffman explained hybrid warfare as a blend of traditional, irregular, catastrophic, and disruptive modes of warfare (Mattis and Hoffman, 2005). Thereafter, Frank Hoffman (2007) has been a leading proponent of the concept hybrid threats and introduced this concept in his work "The rise of Hybrid Wars". He defines a hybrid threat as:

> "Any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the battle space to obtain their political objectives" (Hoffman, 2010, p. 443).

This definition includes both states and non-state actors. Hoffman is followed by other scholars, including Gray, Boot, and McCuen, who agree with Hoffman's definition and conceptualization of hybrid warfare (Hoffman, 2014). Hybrid warfare involves the complementary use of conventional and unconventional military means. Besides hybrid warfare, also other types of warfare such as "new total war, ambiguous warfare and non-obvious warfare are used to describe the current definition of hybrid warfare" (Connel and Evans, p. 3). However, Connel and Evans note that the conceptual domain of these other types of warfare is broad and often vague (ibid., p.3). Also, these other types of warfare resemble the definition of hybrid warfare such as "ambiguous warfare" and are often loaded with ambiguous concepts and definitions and sometimes even lack a proper definition (ibid., p.3). The fragmentation of warfare types that attempt to define the same warfare situation makes it difficult to research this mode of warfare and threats. Therefore, it is important to converge the types of warfare that describe the same threats into one type of warfare and one definition in order to research warfare and the different threats present in the contemporary world. Despite literature on concepts such as "new total war" and "non-obvious warfare", hybrid warfare remains the leading concept to describe the blurred and complementary use of conventional and unconventional means in order to obtain political objectives (ibid., p.3).

In hybrid warfare, unconventional warfare is used to expose and exploit the vulnerabilities of the opponent without having a direct kinetic confrontation between militaries (Lanoszka, 2016, p. 176). Paradoxically, conventional warfare is used as minimally as possible in hybrid warfare but rather used as a threat to change the behavior of its opponent (ibid., p176). However, it is often forgotten that central to understanding hybrid warfare is that both conventional and unconventional warfare tactics are used. Hybrid warfare thus requires credible conventional and unconventional powers that are able to engage and defeat their target at different levels of military escalation (ibid., p.176). In hybrid

warfare, an actor is actively striving to undermine a state's territorial integrity, undermine the political cohesion and disrupt the economy (ibid, p. 178). Hybrid warfare can serve goals such as territorial expansion or indirectly influence the behavior of other sovereign states. By influencing the behavior of another sovereign state by an enemy state, the influenced state behaves more favorable for this enemy state (ibid. p. 186).

Other scholars argue that hybrid warfare is not new but just an evolving form of old warfare (Mosquesra and Bachman, 2016). Hybrid warfare as a concept only highlights the tools that Russia uses to pursue its foreign policy ambitions that were not studied before the Crimea crisis (Renz, 2016). Therefore, hybrid warfare has become a misguided attempt to group every action Russia does, which makes the concept not generalizable for other analyses (ibid.). Russell Glenn (2009) also argues that hybrid warfare fails to explain the current modes of warfare and the application of military capabilities because the definition of hybrid warfare is too vague and comprehensive. The broadness and vagueness of hybrid warfare thus does not always contribute to the useful concept-building of contemporary conflicts and threats. For that reason, it is important to keep in mind that there might be new forms of contemporary conflicts and threats emerging, and that these conflicts and treats cannot all be brought easily under the concepts of hybrid warfare. If hybrid warfare indeed is a well-defined and researched concept, then it would be possible for states to adopt a general framework in how to counter hybrid threats. Hoffman acknowledges that his comprehensive approach to define hybrid warfare cannot explain all forms of emerging contemporary conflicts and threats and consequently emphasizes that his definition is not binding and the hybrid element only indicates the existence of multiple changing (military) capabilities and actors that are merging into a changing method of warfare (Hoffman, 2007).

Despite the difficulty to define the concept hybrid warfare, organizations such as the North Atlantic Treaty Organization (NATO) started to use hybrid warfare in 2014 to describe Russia's military activities during the occupation of the Crimea and eastern Ukraine (NATO, 2015a). Also, future predictions about contemporary warfare and threats by scientists include the concept of 'hybrid' elements such as cyber-attacks or bio hacking (Bachmann, 2015, p. 80). Patrick Cullen (2018) for example concluded in a report for the European Centre of Excellence for Countering Hybrid Threats that one of the key insights from studies on hybrid threats is that states are less likely to correctly understand the mysteries and puzzles of hybrid threats until the effects are already underway (Cullen, 2018, p. 5). Although hybrid threats have the same strategic characteristics as conventional threats, the diversity of individual hybrid threats against a specific weakness of a targeted society can result in each individual hybrid threat having its unique purpose. An important aspect of hybrid warfare is that hybrid threats are relatively likely to manifest as unknown threats while a state is not even aware of these threats (ibid., p. 4). Therefore, Cullen, Bachman and NATO agree with Hoffman that the hybrid

element of hybrid warfare and hybrid threats only indicate the existence of multiple changing (military) capabilities and actors that are merged into a changing method of warfare.

Multiple hybrid threats can be found in the academic literature. Multiple scholars stress cyber attacks, the spreading of disinformation, propaganda and empowering local non-state actors as hybrid threats (Hoffman, 2009; Lanoszka, 2016; Bell, 2012; Popescu, 2015; Mosquera and Bachmann, 2016). Now hybrid warfare and the existence of hybrid threats are explained, the following figure presents the actual threats the Netherlands is facing according to these scholars.

Author	**Hybrid Threats**
Hoffman (2009)	• Antisatellite weapons.
Hoffman (2009)	• Small unit leaders with decision-making skills. • Encrypted command systems. • Cyber warfare directed against financial targets.
Lanoszka, (2016).	• Propaganda. • Agitation. • Border skirmishes. • Insert unmarked soldiers. • Espionage. • Fomented local demonstrations. • Insert unmarked militia groups to occupy official government buildings. • Facilitate local referenda to lend an air of legitimacy. • Provide rebels with diplomatic cover • Cyber attacks. • Sabotage.
Bachman (2015)	• Cyber-attacks • Bio hacking
Bell (2012)	• Cultural and political diplomats. • Linguists. • Intelligence personnel trained to ascertain open-source intelligence • Civilians trained in stabilization and reconstruction. • Information operations and efforts to resolve ‘‘legitimate’’ grievances

Popescu, N. (2015)	• Functioning border management systems
Popescu, N. (2015)	• Spreading Disinformation • Exert Economic Pressure • Empowering Proxy insurgent groups • Effective anticorruption agencies • Hacking
Mosquera and Bachmann (2016)	• Malicious use of Lawfare • Media • Information operations • Strategic Communication
Munich Security Conference (2015)	• Cyber attacks • Economic Warfare • Regular Military Forces • Special Forces • Irregular Forces • Support of local unrest • Information Warfare and Propaganda • Diplomacy

Figure 1. Hybrid Threats

The first sub question is: What are hybrid threats and what hybrid threats is the Netherlands facing? The answer to this sub-question is that the definition of hybrid threats as a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the battle space by both state actors and non-state actors results in an extensive range of appearances as shown in figure 1. As a result of the extensive range of hybrid threats, all states, including the Netherlands, can be targeted by hybrid threats even while these states are not aware of those threats. Some intelligence agencies are experimenting with new methods and practices to develop a hybrid threat situational awareness (Cullen, 2018, p. 5). A part of this process involves new ways to search for signals and facts that manifest as anomalies or patterns that indicate a possible hybrid threat to a society. However, the literature review on hybrid warfare also provides information about the difficulty to identify hybrid threats a state is facing. Besides the wide range of appearances, hybrid threats are not always noticeable until the goal of hybrid threats are already achieved by the opponent. Therefore, it is difficult for a state to increase the responsiveness to hybrid threats that can vary in several forms and are often not even noticeable.

2.2 Theoretical framework policy decision-making

The answer to the main question can be found in the security policy-decision making process of the relevant Dutch ministries and security agencies. There are several approaches for analyzing security a policy decision-making process. Neoliberalism for example, explains that states are unitary and rational actors who make decisions based on self-interest and cost-to-benefit analyses (Sterling-Folker, p.115). With Neoliberalism, the rationality of not having a grand strategy to counter hybrid threats is analyzed. Another theory to analyze the security policy decision-making process is the theory of bounded rationality from Herbert Simon (1971, p. 170- 172). Bounded rationality counters the rational choice theory and states that individuals and organizations as unitary actors are not value maximizing from a particular course of action because these individuals are not able to assimilate and process all the information that would be needed to make a decision that maximizes all benefits (ibid., p. 171). Individuals and organizations cannot get access to all the information required, and even if this would be possible, their minds are unable to process the information properly because the human mind is bounded by cognitive limits. Therefore, the results of policy-decision making are “satisficing”, a combination of the words “satisfy” and “suffice” which imply that situations are simplified by the action taker to a certain level which makes the choice sufficient and satisfying to make and understand (ibid., p.172).

In order to deepen the analysis of the security policy decision-making process regarding hybrid threats, a theory is needed that analyzes both the rational choice and the information input of the relevant Dutch ministries and security agencies. A theoretical framework analyzing both rational choice and the information input of relevant ministries and security agencies is the policy decision-making theory of Graham Allison (1969). Allison (1969) formulated three models for policy decision-making known as the Rational Model, the Organizational Model, and the Bureaucratic Politics Model, labeled I, II, and III. The works "Conceptual Models and the Cuban Missile Crisis" (1969) and the Essence of Decision: Explaining the Cuban Missile Crisis (1971) from Allison are milestones in the analysis of the bureaucratic role in policy decision-making (Smith, 1980). By applying the three conceptual models, Allison scientifically demonstrated the influence of organizational bureaucracy on policy decision-making (Bendor and Hammond, 1992, p. 301). Allison also presented evidence that organizational and bureaucratic political factors significantly influence the policy decision-making process (Argyris, 1976). In this case, the foreign policy decision-making models of Allison can also be applied to the security policy decision-making process of the relevant Dutch ministries and security agencies because policies and measures to counter hybrid threats also concern foreign policies and international relations. Therefore, a security policy decision-making process has the same organizational structures as a foreign policy decision-making process. Allison provides a unique framework to research security policy decision-making in three different angles. After fifty years, the models of Allison are still applied to similar political science cases (Bendor and Hammond, 1992, p.

301). The extensive conceptual models and the leading role in researching policy decision-making are therefore the justification to use the work of Allison.

Model I: Rational Actor Model

Allison's first conceptual model is known as the Rational Actor Model (Model I) and was the main conceptual model to research organizational behavior in foreign policy making before the additional models II and III (Allison, 1969). The rational actor model explains how a nation or government could have chosen an action or policy, given the strategic problem that it faced (ibid.,p. 688). For example, in confronting the hybrid threats posed by international actors, a rational policy analysis shows how this confrontation is a reasonable act from the point of view of the involved Dutch ministries and security agencies, given their strategic objectives.

The actor is the national government that is seen as a rational, unitary decision maker. This actor has specific goals, different options to act and an estimation of the consequences that follow from each alternative (ibid., p. 693). The actions are the response to the strategic problem, which the unitary actor faces. Threats and opportunities determine the actions of the state. The sum of activity by actors within the state determines what the state has chosen as its solution. Thus the action is a unitary choice together with the consequences (ibid., p.693). Rational choice is value maximizing where the rational actor selects the action were the benefits outweigh the costs in terms of its goals and objectives. The rational policy model is applied by revealing the pattern towards a value-maximizing action.

In creating foreign policy, the main assumption of value-maximizing behavior is that all states seek security and strive for survival (ibid., p. 694). Therefore, security policy actions of a state are the result of a combination of national values and objectives, the perceived alternative courses of action, the estimates of various sets of consequences and the valuation of each set of consequences (ibid., p. 694). Multiple courses of action relevant to a strategic problem provide the spectrum of options. In the rational policy model, the strategic characteristics of the problem are researched (ibid., p.694). Empirical evidence about the details of behavior is used to present a clear vision of the purposive choice from the point of view of the action nation.

Allison argues that Model I is useful but that it must be supplemented by additional models that also focus on the organizations and the political actors involved in the policy decision making process. A shortcoming of model I is the fact that governments perform large actions for many reasons. States are black boxes covering a highly differentiated decision-making structure and policy outcomes are the consequences of multiple smaller actions by individuals at various levels within bureaucratic organizations (ibid., p. 690). These individual actions are often only partially compatible with the conceptions of national goals, organizational goals, and political objectives. Therefore, the additional

Organizational Process Model (Model II) and the Bureaucratic Politics Model (Model III) improve the explanation and prediction of security policy decision-making.

Model II: Organizational Process Model

Model II identifies the relevant organizations and displays the patterns of organizational behavior that anticipated a chosen action (ibid., p. 690). Model I explains governmental behavior as the choice of a unitary, rational decision-maker that is centrally controlled, completely informed, and value maximizing (ibid. p. 693). However, governmental structures consist of loosely allied organizations with each having their own perceptions. For that reason, governmental action consists of the acts of these organizations. How a government deals with a problem can therefore be understood according to a second conceptual model, not as deliberate choice but rather as outputs of large organizations functioning according to standard patterns of behavior (ibid., p. 690).

To govern a broad spectrum of problem areas, governments consist of large organizations with each its own responsibility for a particular area. Each organization manages its own set of problems and acts in quasi-independence concerning these problems. Because problems often do not fall within the domain of a single organization, governmental behavior reflects the independent output of several organizations (ibid., p. 698). Each organization addresses its own set of problems, processes information, prepares and performs a range of actions. To coordinate and perform these tasks, standard operating procedures are required (ibid., p. 698). Accordingly, a government consists of organizations with their own fixed set of standard operating procedures. The behavior of these organizations and therefore the government is determined by routines established in these organizations.

Although government leaders can influence this output, the behavior of loosely organizations is determined by standard rules of operation. Only existing means and capabilities make actions and options possible for leaders (ibid., p.699). The available means, capabilities and routines determine the range of options for these leaders. Organizational outputs structure the situation concerning an issue where leaders base their decision upon. Outputs frame the problem, provide information, and make the initial moves which frame the issue that is presented to the leaders (ibid., p. 699). Subsequently, the actions to tackle a problem are determined by the outputs of separate involved organizations instead of by one unitary formal leader.

Actions according to standard operating procedures do not enable a flexible adaptation to a problem. Detail and nuance of actions by loose organizations are determined predominantly by organizational routines and not the formal leaders direction (ibid., p. 702). Organizational priorities, perceptions, and issues are stable and new activities consist of small adaptations of existing activities. An action is not stopped when the costs outweigh the benefits (ibid., p. 702). Organizational stakes in actions carry loose organizations beyond the loss point.

In the analysis with model II, all loosely allied organizations are the actors instead of one unitary state (ibid., p. 690). The units of analysis are consequently the involved ministries or agencies in a state. Because all these organizations are permitted to act, most actions will be determined within these organizations. Each loose organization frames problems, processes information, and performs some actions in quasi-independence. These fractionated powers determine ultimately what different options are presented to the state leader in order to address a problem (ibid., p. 703).

Model III: Bureaucratic Politics Model

The third model focuses on the internal politics of a government. Events in security policy affairs are understood as outcomes of various overlapping bargaining games among players positioned in the national government (ibid., p. 690). The perceptions, motivations, positions, power, and maneuvers of these players result in governmental actions.

The main conception of the bureaucratic politics model is that the "leaders" who represent the top of organizations are not a unitary group (ibid., p.690). Each individual in this group is a player in a central competitive game called bureaucratic politics. Governmental behavior can thus not be understood as organizational output but as outcomes of bargaining games. In contrast with Model I, the bureaucratic politics model has no unitary actor but rather many actors as players, who focus not on one specific set of strategic goals and objectives but rather various conceptions of national, organizational, and personal goals, making governmental decisions not by rational choice but by bargaining outcomes (ibid., p. 707). The decisions and actions of governments are therefore outcomes that are not chosen as a solution to a problem but are the result of compromise, coalition, competition, and confusion by government officials. Many players are bargaining along structured circuits among individual members of the government. Time pressure created by deadlines forces issues to the attention of busy leaders. Examples of bureaucratic and political factors among ministries and individuals are competitive games, the usage of power and the exclusion of other players.

Individual ministries and prominent leaders in the ministries become players in the national security policy game by occupying a critical position in the decision-making arena. If a state performs an action, that action is partially the outcome of bargaining games among different ministries within the government (ibid., p. 708). Model III analyzes the various players, with different perceptions and priorities, focusing on separate problems, and influence the outcomes that constitute the governmental action. The independent variables that lead to bureaucratic politics are therefore the exclusion of relevant ministries and security agencies, including their responsible intelligence agencies in the policy decision-making process and prominent individuals within these ministries and security agencies involved in the decision-making process. This means that if a case provides the evidence that the activities of a prominent individual lead to a policy in favor of this prominent individual,

bureaucratic politics are an independent variable that leads to the eventual policy decision. Correspondingly, if relevant ministries or security agencies in the policy are excluded from the policy decision-making process, bureaucratic politics are an independent variable that leads to the eventual policy decision.

2.3 Analytical framework

The analytical framework merges the security policy decision-making models from Allison with the relative lack of responsiveness to hybrid threats by relevant Dutch ministries and security agencies that serve as the basis for the empirical description. Therefore, the policy decision-making models are translated to the lack of responsiveness to hybrid threats by the involved Dutch ministries and security agencies between 2014 and 2019. After explaining the different theories, the research variables from the analytical framework will be further operationalized in chapter three. According to the policy decision-making theory, the following causal mechanisms lead the current Dutch responsiveness to hybrid threats:

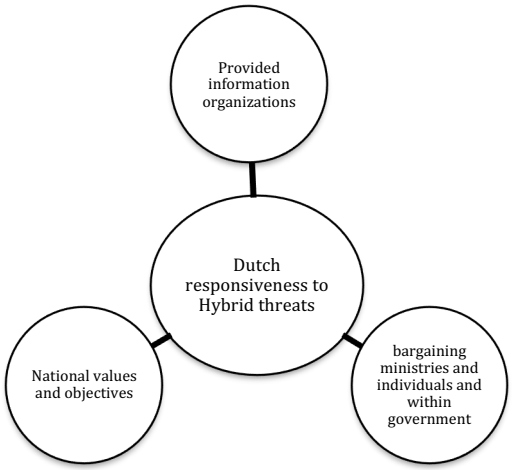

Figure 2. Analytical framework for the Dutch response to hybrid threats according to three policy decision-making models (Allison, 1969).

The analytical framework from figure 2 is based on the three conceptual models from Allison (1969). Based on the rational choice model, the national values and objectives towards hybrid threats must be researched. The provided information by organizations represents the organizational process model. Finally, the bargaining game by relevant ministries and security agencies within government represent the bureaucratic politics model. In order to research the empirical evidence thoroughly, two additional frameworks zoom in on the organizational process model and the bureaucratic politics model from figure 2.

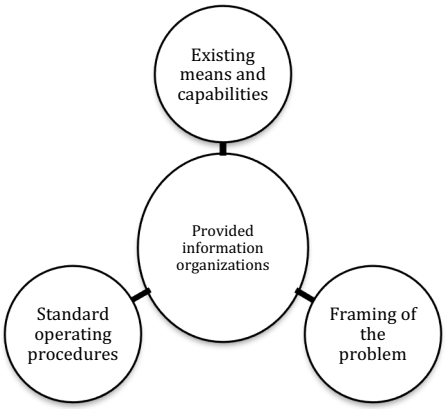

Figure 3. Analytical framework for policy decision-making model II (Allison, 1969).

Currently, the Netherlands has no integrated strategic approach to counter hybrid threats and therefore a relative lack of response to hybrid threats. For analyzing the empirical evidence, the relevant Dutch ministries and security agencies must be researched in order to find their objectives and means for not having an integrated and strategic response to hybrid warfare. In order to analyze model 2 from Allison, the framing of the problem of hybrid threats by relevant Dutch ministries and security agencies must be researched. Also, the SOP's and the existing means and capabilities of each relevant ministry and security agencies must be researched.

Figure 4. Analytical framework for policy decision-making model III (Allison, 1969).

In order to analyze policy decision-making model III from Allison, the bargaining games during the policy decision-making process of the responsiveness to hybrid threats in the Netherlands must be researched. The exclusion of other relevant ministries and security agencies are an indicator for bureaucratic politics according to the theory. Also, the influence of prominent individuals during the security policy decision-making process must be researched.

3. Methodology

Chapter one introduced the absence of a grand strategy regarding hybrid threats in the Netherlands while a grand strategy is recommended by multiple organizations (NCTV, 2016, p.7; WRR, 2011, p. 8). The absence of a grand strategy indicates the relative lack of responsiveness of relevant Dutch ministries and security agencies to hybrid threats. The main research is formulated: What can explain the relative lack of responsiveness of the relevant Dutch ministries and security agencies, including their responsible intelligence agencies, to hybrid threats between 2014 and 2019? The answer to this question should be sought in the security policy decision-making process regarding hybrid threats by the relevant Dutch ministries and security agencies. In chapter two, a few theoretical approaches were set out to look at the problem in such a way that ultimately the analysis framework could be developed. By using the analysis framework of Allison, it is possible to research the lack of responsiveness of the involved Dutch ministries and security agencies to hybrid threats by analyzing the security policy decision-making process regarding hybrid threats by these Dutch ministries and security agencies between 2014 and 2019. In this chapter, the methodological framework and case study design are explained. Thereafter, the data collection of this research is explained and justified. Furthermore, the second sub-question is answered by defining the relevant Dutch ministries and security agencies, including their responsible intelligence and security agencies. Finally, the validity and reliability of this research are discussed.

3.1 Research design

In order to answer the main research question, this research uses a literature review and a document study. This research uses a process tracing method, which systematically examines empirical evidence in the light of the research question and hypothesis posed by the researcher (Collier, 2011). This case study first explains the theoretical perspective on the lack of responsiveness of the relevant Dutch ministries and security agencies to hybrid threats. Based on a literature review on hybrid threats and a theoretical framework on policy decision-making from Allison, the phenomenon hybrid warfare and the variables that can lead to a security policy decision are explained. Thereafter, the variables that lead to a security policy decision are translated to the relative lack of responsiveness of the relevant Dutch ministries and security agencies to hybrid threats between 2014 and 2019. Subsequently, the responsiveness of the involved Dutch ministries and security agencies to hybrid threats between 2014 and 2019 are reconstructed according to the empirical evidence. A timeline is created by process tracing the national decision-making process of the involved ministries and security agencies through public official reports and notes. Finally, the analysis determines what independent variables from the analysis framework from Allison lead to the causal mechanism resulting in the relative lack of responsiveness by the relevant Dutch ministries and security agencies.

3.2 Relevant Dutch ministries and security agencies

In this section the second sub-question of this study is answered by defining the relevant Dutch ministries and security agencies, including their responsible intelligence agencies, to hybrid threats between 2014 and 2019. The answer to the sub-question is relevant for this research because it determines which Dutch ministries and security agencies including their responsible intelligence agencies are included in this research and why.

Based on the existing literature on hybrid threats, multiple hybrid threats and target areas of these hybrid threats can be defined. Because hybrid threats can occur in a wide range of target areas in the Netherlands, every Dutch ministry or security agency can be affected by hybrid threats. For the feasibility of this research, only the ministries and security agencies, including their responsible intelligence agencies that are primarily responsible for the safety and security of the Netherlands are researched. For example, the Dutch ministry of Finance is unmistakably affected by hybrid threats and involved in responding to hybrid threats, but is situated in the periphery of the policy decision-making arena about strategically responding to hybrid threats. Of course, outliers such as the ministry of Finance and the ministry of Education, Culture and Science are important and involved in the decision making-process, but providing security is not their primarily task. However, the scope of this research does not take away that according to the existing literature on hybrid threats, outliers such as the ministry of Finance and the ministry of Education, Culture and Science should be involved in the security policy decision-making process in order to counter hybrid treats.

The ministries that are the units of analysis in this research are the ministry of Defense, the ministry of Justice and Security (J&V), the ministry of Foreign Affairs and the ministry of General Affairs (AZ). According to article 97 of the Dutch constitution, the task of the Dutch Armed Forces is to defend and protect the national interests (Dutch constitution, 2018). The Dutch ministry of Defense is an actor in the realization of a response to hybrid threats and therefore involved in the decision-making process of realizing a strategic integrated approach to counter hybrid threats. Also, the ministry of J&V works in the same manner towards realizing a safer and more just society. Also, the Ministry of AZ is responsible for coordinating overall government policy. The Prime Minister is also the Minister of AZ and his tasks consist of the coordination of government policy and communications (Government, 2018). The ministry of Foreign Affairs works with other actors to combat foreign threats (Ministry of Foreign Affairs, 2018). Therefore the ministry of Foreign Affairs is also involved in the policy decision-making on countering hybrid threats in the Netherlands.

The security agencies contemplated in this research are units of analysis such as the Dutch Military Intelligence and Security Service (MIVD), the General Intelligence and Security Service (AIVD) and the National Coordinator for Security and Counterterrorism (NCTV). The MIVD provides intelligence

and security information for the Dutch Armed Forces. The Ministry of Defense is responsible for the actions of the MIVD (MIVD, n.d.). The MIVD is a unit of analysis because it provides information about possible military threats to relevant Dutch ministries and other security agencies. Also the AIVD provides intelligence and security information about threats that are facing the Netherlands to the relevant ministries and security agencies. The ministry of the Interior and Kingdom Relations is responsible for the AIVD (AIVD, 2015, p1). Both the MIVD and the AIVD have the best insight into threats that are facing the Netherlands and are capable of responding to several hybrid threats. Therefore, the MIVD and the AIVD both play an advisory role and an executive role in the policy decision-making process in order to counter hybrid threats that are facing the Netherlands. The ministry of J&V is responsible for the NCTV. The NCTV is the executive element protecting the Netherlands from threats that could disrupt Dutch society (NCTV, n.d.). Therefore, the NCTV is a relevant security agency that is involved in the security policy decision-making process in order to counter hybrid threats faced by Netherlands.

Besides the Dutch ministries and their involved agencies, also scientific advisory agencies are involved in the decision-making process on countering hybrid threats. The most important advisory agency is the Netherlands Scientific Council for Government Policy (WRR), which is an independent advisory body for government policy. The task of the WRR is to advise the Dutch government on strategic issues. However, the WRR is not responsible for the eventual security policy decisions that are made by the involved ministries (WRR, 2018). Also, the Advisory Council on International Affairs (AIV) of the Netherlands is an independent advisory agency advising the Dutch government and parliament on foreign policy issues among which peace and security (AIV, 2018). Therefore, the AIV is involved in the security policy decision-making process on countering hybrid threats in the Netherlands by advising the relevant Dutch ministries without being responsible for the eventual security policies. Finally, the WRR and the AIV are units of analysis in this research because these security advisory agencies provide prominent advisory input for relevant Dutch ministries and security agencies. Figure 5. presents an overview of the relevant ministries, security advisory agencies and security agencies responsible for the current response to hybrid threats.

Relevant Dutch ministries	**Relevant Security agencies**	**Relevant Security advisory agencies**
Ministry of airs		WRR
Ministry of Defense	MIVD	AIV
Ministry of Justice and Security	NCTV	
Ministry of Foreign Affairs		
Ministry of General Affairs	AIVD	

Figure 5. Relevant Dutch ministries and security agencies on responsiveness to hybrid threats.

Now that the units of analysis are explained and presented, an analysis scheme can be made of the different policy decision models from Allison and the units of analysis. For each model, multiple indicators are presented that translating the theory of Allison into measurable indicators. By searching for the indicators of the policy decision-making models in the empirical evidence, an explanation for the relative lack of responsiveness to hybrid threats by the Netherlands could be found.

Concept	Indicators	Ministry of General Affairs	Ministry of Defense	Ministry of Justice and Security	Ministry of Foreign affairs	AIVD	MIVD	NCTV	WRR	AIV
Model 1	National Objectives									
	National Means									
Model 2	Framing Problem									
	SOP's									
	Means and Capabilities									
Model 3	Prominent individuals									
	Excluding relevant ministries and security agencies									

Figure 6. Analysis scheme.

3.3 Data collection

For this single case study a combination of a desk study and a document analysis is used for the empirical data. The chronological empirical timeline is based on reports from the relevant Dutch ministries and security agencies. The collected data on the actual response to hybrid threats by the involved Dutch ministries and security agencies is based on primary sources in the form of official reports and documents published on the Internet by the involved ministries and security agencies. These reports and archive documents are reliable because they concern information about the responsiveness to hybrid threats published by the involved ministries and security agencies themselves. First, all national annual reports from the relevant ministries between 2014 and 2019 are used. Secondly, based on the theory on hybrid warfare and the definition of relevant ministries and security agencies that are involved with the responsiveness to hybrid threats, published reports

informing about hybrid threats or strategies to counter hybrid threats between 2014 and 2019 on the websites from the ministries and security agencies are used for the document study. In order to include or exclude official reports and documents from the involved ministries and security agencies, the following criteria are used:

- The reports were published or operative between 2014 and 2019.
- The reports inform about the presence of hybrid threats.
- The reports inform about the current response to hybrid threats.

For the feasibility of this research, all official reports and documents published after April 2019 are not included in this research. The following figures show the timelines with official publications of each relevant Dutch ministry and security agency providing information about the response to hybrid threats.

Ministry of Foreign Affairs

Date	**Report**
June 2013	International Safety Strategy
May 2015	Rijksjaarverslag Buitenlandse Zaken 2014
May 2016	Rijksjaarverslag Buitenlandse Zaken 2015
May 2017	Rijksjaarverslag Buitenlandse Zaken 2016
March 2018	Integrated foreign and safety strategy
May 2018	Rijksjaarverslag Buitenlandse Zaken 2017

Figure 7. Timeline published reports Foreign Affairs 2014-2019.

Ministry of Justice and Security

Date	**Report**
May 2015	Rijksjaarverslag Justitie en Veiligheid 2014
September 2015	Cybersecuritybeeld Nederland csbn 2015
May 2016	Rijksjaarverslag Justitie en Veiligheid 2015
September 2016	Cybersecuritybeeld Nederland csbn 2016
May 2017	Rijksjaarverslag Justitie en Veiligheid 2016
June 2017	Cybersecuritybeeld Nederland csbn 2017
May 2018	Rijksjaarverslag Justitie en Veiligheid 2017
June 2018	Cybersecuritybeeld Nederland csbn 2018
March 2019	Informatiestrategie 2017-2022

Figure 8. Timeline published reports Justice and Security 2014-2019.

Ministry of Defence

Date	Report
May 2015	Rijksjaarverslag Defensie 2014
May 2016	Rijksjaarverslag Defensie 2015
May 2017	Rijksjaarverslag Defensie 2016
May 2018	Rijksjaarverslag Defensie 2017
December 2017	Beleidsdoorlichting Nationale Veiligheid

Figure 9. Timeline published reports Ministry of Defence 2014-2019.

Ministry of General Affairs

Date	Report
May 2015	Rijksjaarverslag Algemene Zaken 2014
May 2016	Rijksjaarverslag Algemene Zaken 2015
May 2017	Rijksjaarverslag Algemene Zaken 2016
May 2018	Rijksjaarverslag Algemene Zaken 2017

Figure 10. Timeline published reports Ministry of General Affairs 2014-2019.

NCTV

Date	Report
December 2016	Nationaal Veiligheidsprofiel 2016
July 2017	Chimaera (departmental confidential) (not researched)
November 2018	Horizonscan Nationale Veiligheid 2018

Figure 11. Timeline published reports NCTV 2014-2019.

MIVD

Date	Report
January 2014	Digital Espionage
January 2014	Espionage Abroad
January 2014	Espionage in the Netherlands
April 2015	Year report MIVD 2014
April 2016	Year report MIVD 2015
April 2017	Year report MIVD 2016
October 2017	AIVD and MIVD Cyber espionage
April 2018	Year report MIVD 2017

Figure 12. Timeline published reports MIVD 2014-2019.

AIVD

Date	Report
April 2015	AIVD year report 2014
April 2016	AIVD year report 2015
April 2017	AIVD year report 2016
October 2017	AIVD and MIVD Cyber espionage
March 2018	AIVD year report 2017
April 2019	AIVD year report 2018

Figure 13. Timeline published reports AIVD 2014-2019.

WRR

Date	Report
May 2017	Veiligheid in een wereld van verbindingen. Een strategische visie op het defensiebeleid

Figure 14. Timeline published reports WRR 2014-2019.

AIV

Date	Report
October 2015	Deployment of Rapid-Reaction Forces
April 2015	Instability around Europe
November 2017	The future of NATO and European Security

Figure 15. Timeline published reports AIV 2014-2019.

3.4 Data Analysis

Based on the literature review on hybrid warfare and the theoretical framework of the policy decision-making models from Allison, an analytical framework has been developed in section 2.3. The indicators for the research variables from the analytical framework are also summarized in figure 6. For the analysis, first the reports are systematically assessed in order to extract the policy decision-making indicators from figure 6 from the documents. For assessing the reports, the indicators for the policy decision-making models from Allison are translated to questions that can be answered by the text in the reports. The following questions are answered for each report or document in order to find the policy decision-making indicators of the relevant ministries and security agencies:

1. How is the problem of 'hybrid threats' framed?
2. What are the means and capabilities to counter hybrid threats?
3. What are the standard operating procedures of the organization regarding hybrid threats?

4. Are there prominent individuals involved in the policy decision-making?
5. Are other relevant ministries and security agencies involved in the response?
6. Is there an overlap between the tasks of the relevant ministries and security agencies?

The exclusion of other relevant ministries and security agencies and the influence of prominent individuals during the security policy decision-making process are indicators for the presence of bureaucratic politics, which is the third policy decision-making model from Allison. It is not possible to find a direct answer to the question whether or not relevant ministries are excluded in the policy decision-making process in the empirical evidence. Therefore, question five and six are used to create a security policy decision-making network regarding hybrid threats according to each individual relevant ministry or security agencies. As a result, the collaborations or isolation of relevant ministries or security agencies will become visible and the exclusion of relevant ministries and security agencies can be found.

A chronological timeline is made with the relevant ministry or security agency and the answers to the questions that relate to the indicators of the three policy decision-making models from Allison. Then, the reports are analyzed by comparing the three policy decision-making models with the empirical evidence. The independent variables that are responsible for the lack of responsiveness by the Dutch involved ministries and security agencies to hybrid threats will become visible in the empirical timeline. The process tracing analysis will show which independent variables from the theory correspond to the empirical data. Eventually, the corresponding independent variables which resemble the organizational obstacles in the decision making process are identified.

3.5 Validity and Reliability

Qualitative research is used because the objective of this research is to gain in-depth insight into the lack of responsiveness of the Netherlands to hybrid threats with the help of theoretical approaches and practical research. The findings of this research are based on subjective, interpretive and contextual data. In order to be trustworthy, the findings of the research must meet some quality criteria by way of credibility (Lincoln & Guba, 1985). In this study, the research approach, data collection and analysis are constituently documented. Also, multiple research questions are formulated and answered. Furthermore, indicators for the policy decision models are defined in order to guide the collection and process of data that show the relation between organizational decision-making structures and the relative lack of responsiveness to hybrid threats. In order to increase the reliability and validity, this research combines a literature review and a document analysis.

In addition, only primary sources are used to increase the reliability. As a consequence, a similar research will not have different results. The internal validity of this research is realized trough the extensive amount of used empirical evidence in order to analyze the independent variables that lead to the relative lack of responsiveness by the involved Dutch ministries and security agencies. By researching all relevant Dutch ministries and security agencies, including their responsible intelligence, the external validity of this research is increased.

4. Analysis

In this chapter, the theory on hybrid threats, policy decision-making and the developed analysis framework are linked to the obtained empirical data. Each section is concluded with a sub-conclusion, which also gives an answer to the concerned sub-questions. All sub-conclusions together form the basis for answering the central research question at the end of this chapter. First, a chronological timeline is created for every indicator for the policy decision-making models from Allison based on the published reports from the relevant Dutch ministries and security agencies, including their responsible intelligence agencies. Thereafter, the empirical timeline of all present indicators is analyzed for each policy decision-making model in order to answer the main question.

4.1 Empirical timeline

In this section, the third sub-question is answered by the empirical timeline of the indicators for the three policy decision-making models from Allison: How have hybrid threats been framed by the relevant Dutch ministries and security agencies, including their responsible intelligence and security agencies between 2014 and 2019? Thereafter, the final sub-question is answered: What has been the actual response of the relevant Dutch ministries to hybrid threats in terms of a grand strategy between 2014 and 2019?

Framing of Hybrid Threats

The first indicator for the Policy Process model is the framing of hybrid threats by relevant Dutch ministries and security agencies. In 2014, the ministry of Foreign Affairs did not particularly frame the problem of hybrid threats but noted that the crisis in Ukraine led to many additional unforeseen tasks and commitments and tolerated that safety policies focused more on the instability around Europe (BuZa, 2015, p. 34). J&V framed hybrid threats that year as cyber crime and digital espionage. The potential impact of cyber attacks and disruptions was also increasing due to rapid digitization (J&V, 2015, p. 88). Both the ministry of defense and the ministry of AZ did not frame the problem of hybrid threats al all.

The MIVD stated that by the annexation of Crimea in March 2014, the Russian support for the pro-Russian separatists and the large-scale, threatening arms race on the Ukrainian border, the more assertive role of the Russian Federation in the region became clearly visible (MIVD, 2015, p. 12). Besides Ukraine there was also an increased Russian military display of power and strategic messaging with military means, such as the deployment of the Russian strategic bomber fleet and the Russian navy in the immediate vicinity of NATO territory (MIVD, 2015, p. 13). Digital espionage was also increasingly becoming a part of unwanted activities of foreign intelligence services (MIVD Digitale Spionage, 2014, p. 1.). Foreign intelligence services were involved in manipulation,

influencing and controlling migrant groups in the Netherlands. Digital espionage was used to obtain data from organizations concerned with the interests of migrant groups (MIVD Digitale Spionage, 2014, p. 1.). The AIVD also stated that digital espionage was a hybrid threat. For the implementation of digital espionage, states used the available knowledge, capacity and resources of hacker groups and private organizations, such as IT companies and universities (AIVD, 2015, p. 24). The structural presence and activities of the Russian intelligence and security services in the Netherlands, combined with worldwide Russian operations against the West, affected the political, military and economic position of the Netherlands and its allies (AIVD, 2015, p. 30). The AIVD also found in 2014 that Chinese intelligence activities were taking place on Dutch territory. These activities related to both recruitment and the collection of specific information on topics such as economic and political issues (AIVD, 2015, p. 30).

In 2015, the ministry of Foreign Affairs defined the problem of hybrid threats as the illegal annexation of Crimea and destabilizing actions in Eastern Ukraine that led to concern about instability on the Eastern side of Europe (BuZa, 2016, p. 12). The cross-border threats to the Netherlands were of such a size and complexity that an international approach was required. (BuZa, 2016, p. 27). J&V framed the problem of hybrid threats as a growing number of cyber operations and digital attacks with political-military purposes that were part of hybrid warfare (CSBN, 2015, p. 22). A combination of all possible means including political, economic and military resources was used. According to J&V, political leaders secretly deployed hybrid threats and the responsibilities for these activities barely became visible or were denied by these leaders (CSBN, 2015, p. 22). The Netherlands was vulnerable for these hybrid threats due to the increasing dependence on IT (J&V, 2016, p. 20). There were no acute problems, but there were conceivable risks on the longer term by for example the possible gradual build-up of undesirable strategic dependencies of players from other states for certain vital goods or services (J&V, 2016, p.21). The ministry of Defence and AZ still did not frame the problem of hybrid threats in 2015.

The MIVD stated that in addition to digital espionage, the MIVD also investigated offensive cyber capabilities of foreign powers. The most common hybrid threats were information operations, which have the goal of influencing the public opinion. This type of activity was increasingly used as a supplement to classical military operations and conventional military means. Non-state actors often did this through the digital domain. The MIVD noted that these groups were often supported and directed by foreign intelligence services (MIVD, 2016, p. 38). The most important targets that the MIVD recognized were the ministries of Foreign Affairs and the ministry of Defense. Also, defense suppliers were target of espionage from non-Western states with military ambitions (MIVD, 2016, p. 35). The AIVD was also focused on cyber threats such as digital espionage. China, Russia and Iran were the biggest cyber threat to the national security. (AIVD, 2016, p. 21). Espionage was also

mentioned as a hybrid threat by the AIVD (AIVD, 2016, p. 25). The AIV framed the problem of hybrid threats as a wide range of methods of warfare. Russia used for example cyber and information operations (AIV instability, 2015, p. 8).

In 2016, the ministry of Foreign Affairs explicitly included new hybrid threats such as cyber threats (BuZa, 2017, p. 11). The ministry of J&V, the ministry of Defence and the ministry of AZ did not frame the problem of hybrid threats in 2016. The MIVD argued that hybrid tactics were used by the Russian Federation to create uncertainty and affect the public opinion in third party states. Influencing and information operations supported the strategic goals of Russia. Russia presented its own acts as humanitarian, reasonable and de-escalating and portrayed Western actions as hysterical, hypocritical, anti-Russian and escalating (MIVD, 2017, p. 12). A hybrid warfare campaign was usually lengthy by nature and had an up scaled violence structure with varying visibility and physical intensity. Hybrid warfare was therefore both a goal and a mean. (MIVD, 2017, p. 23). The AIVD stated that Russia was gathering information in Dutch target areas such as the economy, science, politics and defense. In 2016, most attention was drawn towards Russian cyber attacks, but the Russians also used intelligence officers to recruit human sources (AIVD, 2017, p. 6). Russia's espionage activities were aimed at influencing the decision-making processes, perceptions and public opinion in the Netherlands. The dissemination of disinformation and propaganda also played an important role. The rise of the Internet made it easier for Russia to extend their reach and the impact of hybrid threats. (AIVD, 2017, p. 7). The AIVD also identified several state actors abusing facilities in the Netherlands to target third states. As a result, the Netherlands became an unwilling conduit for hostile activities to violate the economic, military and political interests of other nations (AIVD, 2017, p. 6).

The Ministry of Foreign Affairs mentioned that in 2017, the actions of Russia, in the region east of the European Union, and especially in Ukraine, had a destabilizing effect. Hardly any progress had been made in the past year in implementing the Minsk agreements to end fighting in eastern Ukraine in the fight against terrorism (BuZa, 2018, p. 18). J&V argued that in previous years, the digital resilience of individuals and organizations lagged behind in the development digital threats. (J&V, 2018, p. 16).
The ministry of Defence claimed that hostage software caused systems in the energy and transport sector, hospitals, government agencies and other vital sectors to fail (Defense, 2018, p. 15). For the first time, the ministry of AZ framed the problem of hybrid threats. The security situation changed due to the instability in the east caused by the annexation of Crimea by Russia and the downing of flight MH17. The security situation was also changing due to the interdependence of international production and transport chains and the significance of international infrastructures for, for example, the Internet and energy. (AZ, 2018, p. 17).

The MIVD stated that the modernization of the Russian armed forces continued in 2017. The Russian possibilities for waging a large-scale conflict increased. Moreover, the hybrid threats that were coming from the Russian Federation were the interplay of misleading, undermining and openly disruptive activities. In addition, there was more Russian involvement in conflicts in 2017 outside the traditional Russian focus areas. (MIVD, 2018, p.9). Espionage, influencing and sabotage in the digital domain were a serious and growing threat to the Netherlands. Also hacking was used to sabotage or hacking information to influence decision making or public opinion. Digital espionage was also increasingly being used to support traditional espionage operations and vice versa. The Netherlands was vulnerable for digital espionage. (MIVD, 2018, p.9). A military conflict between the Russian Federation and NATO was on the short term very unlikely, but unlike in the recent past, conceivable. This was a so-called low probability, very high impact scenario. Because Russia is a nuclear superpower, a conflict with Russia always had a potential nuclear dimension. (MIVD, 2018, p. 18).

The AIVD argued that through digitization and globalization, the external safety and internal safety tasks were increasingly intertwined. (AIVD, 2018, p. 3). Russia used the vulnerabilities of open and democratic societies for their hybrid tactics. Russia was trying to take a role in geopolitics stage in the Middle East, where Russia wanted to direct a peace solution in Syria. (AIVD, 2018, p. 4). In addition to digital espionage, Russian officials gathered information in the field of economics, science, politics and defense through espionage. There were also attempts at the recruitment and targeted collection of specific information about economic and political topics determined by China. (AIVD, 2018, p. 8). The WRR framed the problem of hybrid threats in 2017 as using unannounced, large-scale military exercises and rapid movements, secret support for separatist groups, but also economic pressure. (WRR, 2017, p. 71).

In 2018, the ministry of Foreign Affairs framed the problem of hybrid threats as the use of a hybrid mix of conventional weapons and modern methods of exerting influence. “States employ a combination of military, diplomatic and economic resources and media influence to achieve strategic objectives” (International integrated security strategy, 2018). Increasingly, hostile states tried to influence democratic processes and spread disinformation in other countries, engage in espionage and cyber attacks, take economic measures and create strategic dependency.
Because deception, ambiguity and denial were key to state actors engaging in hybrid conflict, they often used proxies who appeared not to be associated with the state. At the same time, inadequate regulation in the digital and information sectors presented opportunities for ill-intentioned parties, who caused damage without crossing a clear line (International integrated security strategy, 2018).
J&V defined disruption, information manipulation, information theft, espionage, system manipulation, and hacking as hybrid threats in 2018 (CSBN, 2018, p.14). The AIVD mentioned that the tension between Russia and the West remained high. President Putin was trying to position Russia as a world

power and to strengthen his position in his own country. He tried to weaken his opponents and acted aggressively towards the Baltic states. The attempts by the Russian military intelligence service GROe to poison a former intelligence officer in the UK and to hack into the network of the Organization for the Prohibition of Chemical Weapons in The Hague were examples of these operations (AIVD, 2019, p.7). Finally, more states were focusing on political and economic espionage. China, Iran and Russia were the biggest threats. (AIVD, 2019, p. 8).

The sub-conclusion and answer to the third sub-question is that J&V, the MIVD and the AIVD were the first ministry and intelligence agencies that framed hybrid threats as cyber crime and digital espionage in 2014. Later, in 2018, J&V extended its definition for hybrid treats with disruption, information manipulation, information theft, espionage, system manipulation, and hacking as hybrid threats in 2018 (CSBN, 2018, p.14). The ministry of Foreign Affairs first framed hybrid threats as the illegal annexation of Crimea and destabilizing actions in Eastern Ukraine. Later, in 2018, the ministry of Foreign Affairs framed hybrid threats as a combination of military, diplomatic and economic resources and media influence to achieve strategic objectives (International integrated security strategy, 2018). The ministry of Defence did not frame the problem of hybrid threats until 2017, where the ministry used cyber threats as hybrid threats that were facing the Netherlands. While the Ministry of Foreign Affairs gradually proceeded to frame hybrid threats more globally, the MIVD and the AIVD proceeded to frame hybrid threats more towards the Russian Federation and China (AIVD, 2018, p. 3). The AIV framed the problem of hybrid threats as a wide range of methods of warfare. Russia used for example cyber and information operations (AIV instability, 2015, p. 8). The WRR framed the problem of hybrid threats in 2017 as using unannounced, large-scale military exercises and rapid movements, secret support for separatist groups, but also economic pressure. (WRR, 2017, p. 71). The ministry of AZ, only framed the problem of hybrid threats in the Netherlands from 2017 as the instability in the East and the interdependence of international production and transport chains and the significance of international infrastructures for the Internet and energy (AZ, 2018, p. 17). It can therefore be concluded that almost every relevant ministry and security agency frames the problem of hybrid threats differently and that the amount of hybrid threats is endless.

Means and capabilities

The second indicator for the Policy Process model is the sum of means and capabilities of relevant Dutch ministries and security agencies to counter hybrid threats. In 2014, the ministry of Foreign Affairs made contributions to reassure NATO measures. The increase in international security threats demanded much of the relatively limited and reduced capacity of Foreign Affairs in recent years. As a result in 2014, the International Security Budget turned out not to be sufficient to finance a major new mission in addition to the ongoing missions. (BUZA, 2015, p. 34). J&V strengthened the cooperation

between government and corporate businesses to increase the resilience to IT disruptions and cyber attacks. In addition, the Cyber Security Assessment Netherlands (CSBN) was published in 2014 (J&V, 2015, p. 86).

The same year, the ministry of Defence prepared units for a NATO Response Force (NRF). Also, the Defense Cyber Strategy (DCS) was implemented (Defense, 2015, p. 15). The Defense Computer Emergency Response Team (DefCERT) was reinforced with additional personnel and supports the security of the most critical networks and systems of Defense. The Defense organization also took a first step in the development of offensive cyber capabilities by launching the Defense Cyber Command (DCC) (Defense, 2015, p. 17). Finally, the Defense organization worked closely with public and private partners in the cyber domain and contributed to cyber programs from NATO and the EU. The capabilities of the ministry of AZ were doing in-depth investigations on foreign policies (General Affairs, 2015, p. 22). The MIVD worked with teams consisting of analysts and specialists for the collection of information. The reports of the service were all-source products based on intelligence and cyber information from the intelligence and security network of defense and information from partner services. (MIVD, 2015, p. 10). The main capability of the MIVD was informing the public (MIVD Digitale Spionage, 2014, p. 1). (MIVD Spionage in Nederland, 2014, p. 1). (MIVD Espionage abroad, 2014, p. 7). The AIVD investigated digital attacks which posed a threat to national security such as espionage, sabotage or attacks causing social unrest or disruption (AIVD, 2014, p. 26).

In 2015, the ministry of Foreign Affairs stationed diplomats in Belarus and Moldova and the support for independent Russian-language media was intensified (BuZa, 2016, p. 12). The ministry of Foreign Affairs also supported the use of the OSCE as an instrument of comprehensive security and stability in Europe. This also applied to the OSCE activities with regard to the conflict in Ukraine, such as the direction of the Minsk process and the Special Monitoring Mission. The Netherlands contributed with personnel and material to this mission (BuZa, 2016, p. 12). The ministry of Foreign Affairs also made further agreements with Germany on military cooperation between the Dutch 43rd Mechanized Brigade and the First German Panzer Division. The Netherlands, Belgium and Luxembourg also agreed that from the end of 2016 the Belgian and Dutch air forces would jointly monitor the BENELUX airspace (BuZa, 2016, p. 14). The ministry of Foreign Affairs presented initiatives for international law and cyber standards, digital rights and capacity building in the newly established "Cyber Taskforce", a collaboration between two Ministry of Foreign Affairs policy departments, which must ensure the continuation of the policies set out at the Global Conference on Cyber Space (BuZa, 2016, p. 16). J&V strengthened the National Cyber Security Center and public-private partnerships were further developed through the development of the National Detection and Response Network (J&V, 2016, p.20). Also, the intelligence capacity was expanded in order to monitor objects (J&V, 2016, p.81).

The ministry of Defense concluded that during a simultaneous deployment on land, the sea and in the air, the armed forces could not fully provide their own combat support unless it concerned the same mission in the same operating area. Fire support, medical support and transport capacities were the limiting factor. For a second operation, the Ministry of Defense would rely on its allies. If deployment was expected within a higher threat scenario, a longer preparation time was required. Material limitations and a lack of specialized personnel also had a negative impact on the operational readiness of the armed forces in 2015 (Defensie, 2016, p. 135).

Access to the cable, in combination with knowledge about the modus operandi of state actors, enabled the MIVD to take action in order to prevent damage from threats (MIVD, 2016, p. 40). In addition, the MIVD actively contributed to the concept knowledge sharing from the Defense cyber strategy. The DCC also further employed employees at the MIVD (MIVD, 2016, p. 38). In 2015, the AIVD issued two threat assessments for all sectors. (AIVD, 2016, p. 31). The AIV played an advising role based on the findings of its research.

In 2016, the ministry of Foreign Affairs continued the robust and unified EU response to the aggressive Russian actions in Ukraine. Partly due to the intercession of the Netherlands, economic sanctions against Russia were extended twice, thereby maintaining pressure on Moscow to implement the Minsk agreements. (BuZa, 2017, p. 13). The ministry strengthened attention to the increasing threats regarding the IT domain; for example an awareness campaign and a phishing campaign were carried out (BuZa, 2017, p. 63). J&V contributed to a safe and stable Netherlands by preventing and limiting social disruption by recognizing threats, increasing the resilience of citizens, business and government bodies and strengthening the protection of vital interests. (J&V, 2017, p. 87). Also further investments were made this year in digital resilience and intelligence in the digital domain. Moreover, the capacity of the Royal Netherlands Marechaussee (KMar) was increased together with the ability to deploy cyber assets as an integral part of the military performance. To make this possible, efforts were made to recruit cyber professionals in order to broaden the possibilities for rapid innovation and to intensify the cooperation with other actors (Defensie, 2017, p. 17-18).

The Prime Minister submitted an act to the Lower House of Parliament in the second half of 2016, together with the Ministers of Defense, Internal Affairs and Kingdom Relations and J&V, which replaced the Intelligence and Security Services Act 2002 (Wiv 2002). From now on, the Dutch intelligence and security services were authorized to investigate cable-bound telecommunications (AZ, 2017, p. 8). The AIVD investigated clandestine Russian influence activities against the Netherlands and Dutch interests, keeping the government fully informed so it could take appropriate action. (AIVD, 2017, p.7). The AIVD's National Signals Security Bureau (NBV) undertook numerous

activities in 2016 to better safeguard confidential and sensitive Dutch government information. These included the expansion and professionalization of the National Detection Network, improving its ability to identify cyber attacks and to compile accurate analyses of the threat they pose. The service also completed several evaluations of information-security products, including the Tiger S mobile telephone (with NATO certification) and hard-disk encrypter Hiddn. (AIVD, 2017, p. 6).

Whilst the ministry of Foreign Affairs continued to focus on “pressure and dialogue” the sanctions against Russia's actions in both Eastern Ukraine and Crimea were extended in 2017 by the same ministry. They also strengthened diplomatic capacity in the region east of the European Union with the opening of embassy offices in Minsk and Chisinau (BuZa, 2018, p.19). The ministry also incorporated the international efforts in the digital domain into a strategic framework, the International Cyber Strategy "Building Digital Bridges". (BuZa, 2018, p. 21). For J&V, extra funds were included in the J&V budget to invest in the National Detection Network. By sharing information, digital threats were recognized as early as possible, which resulted in the strengthening of Dutch cyber security. Additional investments were also announced in 2017 for the coming years. Together with the Ministry of Economic Affairs, J&V started the construction of a Digital Trust Center. Finally, the Cyber Security Data Processing and Reporting Obligation Act came into force on 1 October 2017, which was the first Dutch law specifically dealing with cyber security. (J&V, 2018, p. 16).

The ministry of Defence, strengthened the DCC to meet the high demand for support of operational commands in the cyber field (Defensie, 2018, p. 15). Attacks with so-called hostage software caused worldwide failure of systems in the energy and transport sector, hospitals, government agencies and other vital sectors. In this context, the Defense organization further strengthened its own cyber capabilities. For the protection of the Dutch defense networks, the use of cyber assets in military operations or the gathering of intelligence, the same knowledge, skills, techniques and equipment were used. The MIVD was strengthened in order to optimally deploy intelligence resources to support the military performance of tasks in the cyber domain and to further develop active defense measures. Activities also continued on closer cooperation between the DCC and the MIVD, which is in line with the Defense Cyber Strategy (Defensie, 2018, p. 15). In 2017, the Defense organization also further deepened international military cooperation, especially with the strategic partners Belgium and Luxembourg, Germany, France, Norway, the United Kingdom and the United States. Close cooperation between Belgium, Luxembourg and the Netherlands continued over the past year. The 13 Light Brigade, the Belgian Mediane Brigade and the Luxembourg Military Center prepared themselves in 2017 for contributions to the EU Battle Group in 2018. In 2017, Belgium and the Netherlands also decided on closer cooperation between the Marine Corps and the Belgian Light Brigade. (Defensie, 2018, p. 15-16).

In addition to the traditional scenarios, such as large-scale flooding and natural disasters, new threats such as terror, hybrid threats became increasingly important. This is reflected in safety analyzes such as the International Security Strategy (IVS) 'Safe World, Safe Netherlands' (Beleidsdoorlichting Nationale Veiligheid, 2017, p. 33). The ministry of AZ mentioned that the new Intelligence and Security Services Act enabled to act more effectively regardless of further technological developments. For the implementation of the new Intelligence and Security Services Act, the government made 20 million euros available for the coming years. (AZ, 2018, p. 7). With regard to internal safety awareness, the AIVD carried out over 200 presentations, briefings and workshops for government organizations, civil aviation and other vital providers. The AIVD also made three threat assessments and one risk analysis. (AIVD, 2018, p. 10). The WRR advised to develop the future of the armed forces from an integrated security strategy that includes internal and external security. For the purpose of this strategy, the WRR advised the establishment of a General Safety Council (ARV) and a Planning Office for Safety. (WRR, 2017, p. 1).

In 2018, the Ministry of Foreign Affairs focused on cooperation with EU member states. The cooperation included sanctions, development cooperation, EU missions and operations, capability development, information exchanges, joint responses to hybrid threats and external aspects of counterterrorism and cyber security cooperation. (BuZa, 2018, p. 32). The Dutch intelligence and security services were investigating state actors that may pose a threat to the Netherlands' security and interests. This investigation helped to provide greater insight into undesirable foreign interference. (BuZa, 2018, p.32). The AIVD was able to provide insight into the risks of espionage and foreign interference for the Netherlands and for Dutch companies in 2018. Therefore, the AIVD visited various authorities, gave hundreds of awareness presentations for government partners such as the National Counterterrorism and Security Coordinator. The AIVD, finally informed the NCTV and several ministries about their findings. The account managers of the intelligence services at the police also played an important role. The AIVD issued around 40 intelligence reports on espionage and unwanted foreign interference in 2018. (AIVD, 2019, p. 11). J&V developed an information strategy for the ministry of J&V. As a result, employees were guided to work smarter and safer in their working space (Information strategy J&V, 2019, p. 1-2).

The sub-conclusion and answer to the fourth sub-question is that the actual response of the relevant Dutch ministries and security agencies to hybrid threats in terms of a grand strategy between 2014 and 2019 remained limited to creating more cooperation with EU member states by the ministry of foreign affairs. Also, the ministry of Defence further deepened international military cooperation, especially with the strategic NATO partners (Defensie, 2018, p. 15-16). The AIVD and the MIVD both performed executive tasks, but did not propose a grand strategy to counter hybrid threats that are facing the Netherlands. The WRR advised the establishment of a General Safety Council and a

Planning Office for Safety in the Netherlands, which would represent a grand strategy to counter hybrid threats (WRR, 2017, p. 1). However, A General Safety Council or Planning Office for Safety was never created. Also, AZ did not provide any empirical evidence of a response to hybrid threats in terms of a grand strategy. It can therefore be concluded that each relevant Dutch ministry or security agency is focusing on its own capabilities in order to counter hybrid threats instead of working together with a grand strategy. The WRR, which is a security advisory agency drew the attention of creating a grand strategy, but did not have the executive power or responsibility to establish a grand strategy to counter hybrid threats that the Netherlands are facing.

Standard operating procedures

The last indicator for the Policy Process model is the total of SOPs for each relevant Dutch ministry or security agency. The ministry of Foreign Affairs made a new analysis of the international security environment to update the International Security Strategy of 2013 (BUZA, 2015, p. 34). J&V researched and made the public aware of hybrid threats (J&V, 2015). The ministry of Defence deployed intelligence, surveillance and reconnaissance units, a helicopter detachment and special units in Mali (Defense, 2015, p. 15). The ministry of AZ delegated investigations on relevant threats and reported the findings to the relevant ministers (AZ, 2015, p. 20). The MIVD informed the public about cyber threats (MIVD Digitale Spionage, 2014, p. 1). (MIVD Spionage in Nederland, 2014, p. 1). The MIVD also made strategic analysis, which give insight into the security situation and stability from a region or country. Secondly, the MIVD made operational analysis, which focussed on capacities, activities and intentions of opposing military forces. Finally, the MIVD made tactical analyses that support the patrols and operations in the broadcast area (MIVD, 2016, p. 7). The MIVD was also actively investigating threats of state actors in the digital domain (MIVD, 2016, p. 36).

The AIVD shared its findings on a large scale based on the investigation into digital threats with victims, governments and other stakeholders. This was done by direct briefings and presentations, and several information messages and analysis (AIVD, 2016, p. 23). The AIVD also advised multiple ministries, including the ministries of Foreign Affairs and Defense on security issues related to the design and organization of digital information architectures and the security of classified information (AIVD, 2016, p. 33).

The sub-conclusion is that the tasks of the MIVD are, conducting safety investigations, doing research necessary for taking measures, promoting measures to protect the interests, conducting research in other countries on subjects with military relevance and the preparation of threat analysis for tasks related to the monitoring and protection of persons. (MIVD, 2017, p. 7). The SOPs for the ministry of Defense were employing units and researching cyber threats. The ministry of AZ only focused on

delegating investigations on relevant threats and reporting the findings to the relevant ministers. The ministry of J&V focused on informing the public about hybrid threats in order to increase the resilience against hybrid threats. The SOP's for the AIVD and the MIVD did not change throughout the years and consisted of doing research, conducting safety investigations and informing the public about the findings and hybrid threats. (MIVD, 2017, p. 7). Finally, the AIV also conducted research and presented the finding to the public en government.

Involvement of other relevant ministries and agencies

The first indicator for the bureaucratic politics model is the involvement of other relevant ministries and security agencies, including their intelligence agencies, in order to counter hybrid threats according to a specific relevant Dutch ministry of security agency.

In 2014, the ministry of Defense, the Ministry of Foreign Trade and Development Cooperation, and the ministry of J&V worked together in order to realize new policies for the ministry of Foreign Affairs (BuZa, 2015, p. 33). According to J&V, the Ministry of Defense made a contribution by connecting the use of the network by the Royal Netherlands Military Police, Ambulance Care and Customs (J&V, 2015, p. 36). The Ministries of Defense, the ministry of J&V and the Ministry of the Interior and Kingdom Relations started reviewing a covenant with the aim to bring the budget back in line with the actual costs (Defense, 2015, p. 15). In addition, the intelligence capacity in the digital domain of the MIVD was intensified through the expansion of staff and investments in equipment. Part of this capacity concerned the establishment of the Joint Sigint Cyber Unit (JSCU) of the AIVD and the MIVD in the summer of 2014 (ibid., p. 17). The ministry of AZ mentioned the collaboration with the MIVD and the AIVD (General Affairs, 2015 p. 22). The AIVD participated with the MIVD and the National Cyber Security Center (NCSC) in the National Detection Network (NDN) under the coordination of the Ministry of J&V. Together with the NCSC, the AIVD worked on various products, including the factsheet about the Heartbleed bug and the Cyber Security Image of the Netherlands. Together with the ministry of Defence, several security products were developed (AIVD, 2015, p. 36).

In 2015, the ministry of Foreign Affairs collaborated in the areas of defence, diplomacy, economy and development cooperation, which extended to other budgets from the ministries of Defense, and J&V, (BuZa, 2016, p. 27). J&V stressed the cooperation with the AIVD and the MIVD (J&V, 2016, p. 19). The ministry of Defence argued the shared position of the KMar. The Minister of Defence was responsible for the management and the size, composition and required degree of readiness of the KMar.. Several ministries shared the authority over the KMar depending on the task. These are the ministries of J&V including the NCTV, the ministry of Foreign Affairs and the ministry of Defense (Defensie, 2016, p. 54). The NCTV incorporated security measures based on information provided by

the MIVD (MIVD, 2016, p. 61). In 2015, the MIVD intensified the cooperation with the AIVD on counterintelligence (MIVD, 2016, p. 46). The AIVD also mentioned the collaboration with the MIVD and the Ministry of Defence in 2015.

In 2016, the ministry of Foreign Affairs mentioned the collaboration with the ministries of Defense and J&V and Economic Affairs. (BuZa, 2017, p.33). The NCTV worked with the ministries of Foreign Affairs and Defense. (J&V, 2017, p. 88). The AIVD and MIVD had joint teams such as the Unit Counter-proliferation, the Caribbean Team, JSCU and a joint department for Signals Intelligence and Cyber (MIVD, 2017, p. 46). The NCTV took security measures based on information that was provided by the MIVD. The MIVD worked together on cyber security with the National Cyber Security Center, that was part of the NCTV (MIVD, 2017, p. 46). All intelligence and security staff members from the ministry of Defense worked closely together with the MIVD. The Defense Intelligence and Security Network enabled this cooperation (MIVD, 2017, p. 47).

In 2017, a start was made on new policy notes on Foreign Affairs. In the context of an integrated foreign policy, these notes were closely coordinated with the notes of the ministry of Defence. (BuZa, 2018, p. 23). In order to guarantee its integrated nature, decision-making on the International Security Budget (BIV) was prepared and implemented interdepartmentally with the Ministries of Defence, and Foreign Affairs (Defensie, 2018, p. 25). In 2018, according to the ministry of AZ, various policymakers, forums and organizations were involved in the national security sector, including the NCTV and representatives of the ministries of Foreign Affairs and Defense (AZ, 2018, p. 17). In addition, the AIVD and MIVD had a joint Security Investigations Unit. Another important national partner for the MIVD was the NCTV. Based on information supplied by the MIVD, the NCTV took security measures. The AIVD also mentioned to work closely with the MIVD and government partners such as the National Cyber Security Center (NCSC) in order to recognize and contain threats (AIVD, 2018, p. 8).

The sub-conclusion is that the MIVD claims to work closely together with the ministry of Defence, NCTV, J&V and the AIVD. The AIVD also states to work closely with the NCTV, J&V, the MIVD and the ministry of Defence. The cooperation network of the Ministry of Defence matches with the MIVD and the AIVD but also cooperates with the ministry of Foreign Affairs. The NCTV stated to work also with the Ministry of Defence, the ministry of Foreign Affairs, the AIVD and the MIVD. J&V claims to work with the NCTV, the ministry of Defence and the ministry of Foreign affairs. The ministry of Foreign affairs claims to work with J&V, AZ and the ministry of Defence. Both sides thus far mention all the mentioned cooperation between the ministries and security agencies. Both the WRR and the AIV can be seen as isolated security advisory agencies that do not work together with other relevant ministries and security agencies. The WRR and the AIV are also not mentioned by the

other ministries and security agencies. Finally, AZ claims to cooperate with the ministries of Defence and Foreign Affairs, the NCTV, the MIVD and the AIVD. As no other ministry or security agency mentions the cooperation with AZ, the cooperation with the ministry of AZ seems one-sided.

Overlap in the tasks of relevant ministries and security agencies

The second indicator for the bureaucratic politics model is the overlap in the tasks of relevant ministries and security agencies. After comparing the involvement of relevant ministries and security agencies with the overlap in the tasks of these ministries and security agencies, the areas of competition and the exclusion of relevant ministries and security agencies can be found.

In 2014, the coherent efforts covering defence, diplomacy, economics and development cooperation extended to other departments besides the ministry of Foreign Affairs (BuZa, 2015, p. 33). The starting point was to promote the Foreign Affairs security interests through joint efforts in cooperation with other ministries, social organizations and the business community. The JSCU of the AIVD and the MIVD in the summer of 2014 became a cyber unit with overlapping tasks for both the MIVD and the AIVD in order to share knowledge and information. The Ministry of Defense shared tasks during mission MINUSMA with other ministries and security agencies by employing a civilian component during MINUSMA with officials from the Ministries of Foreign Affairs and of J&V. The ministry of AZ did not compete or collaborate with other ministries and security agencies in 2014 (General Affairs, 2015).

The MIVD informed the public together with the AIVD (MIVD Digitale Spionage, 2014, p. 1). (MIVD Spionage in Nederland, 2014, p. 1). (MIVD Espionage abroad, 2014, p. 7). The AIVD also shared multiple teams with the AIVD such as the Unit Contraproliferation Caribbean team, the Project team Syria / Lebanon and the Joint SIGINT-Cyber Unit (MIVD, 2015, p. 45). The activities of the AIVD and the MIVD touched each other in many areas. The AIVD and MIVD coordinate operational activities as much as possible (AIVD, 2015, p. 39). Just like the MIVD and the National Police, the AIVD submits information and intelligence to the NCTV so this organization can perform its duties. The NCTV uses this information to fulfill its coordinating role in the fight against threats facing the Netherlands (AIVD, 2015, p. 40).

The coherent effort covering defense, diplomacy, economy and development cooperation extended also to the budgets from other ministries, such as the ministry of Defence, Foreign Trade & Development Cooperation, J&V and Economic Affairs (BuZa, 2016, p. 27). The KMar is a mean with overlapping authority. The Minister is responsible for management and for determining the size, composition and required degree of readiness of the KMar. The authority over the KMar rests with

several Ministries. Depending on the task, these are the Ministries of J&V (including the Public Prosecution Service and the NCTV, the ministry of Foreign Affairs and the ministry of Defence (Defensie, 2016, p. 54).

On October 2015, the AIVD and MIVD moved to one common building. The new accommodation is responsibility of the Central Government Real Estate Agency. The cooperation with the AIVD is close and intensive. The MIVD and AIVD have a number joint teams (MIVD, 2016, p. 59). The AIVD participates with MIVD and the National Cyber Security Center (NCSC) in the National Detection Network (NDN) under the coordination of the Ministry of J&V. (AIVD, 2016, p. 33). Article 100 procedures for preparing decisions regarding the worldwide deployment of the armed forces in crisis management operations take place in close coordination with the Ministers of Defence and J&V. The application of sanction regulations as part of a sanction policy, are implemented in accordance with the Ministers of Finance and J&V. (BuZa, 2017, p. 33).

Contributions to promote international security, stability and the rule of law from the International Security Budget are determined in consultation with the Minister of Defense (BuZa, 2018, p. 33). In order to carry out its duties, the CTIVD carries out investigations about which it reports to the relevant ministers. In 2017, the CTIVD advised on nine complaints concerning the AIVD and on one complaint concerning the MIVD. The ministers were both advised on one complaint that concerned both the AIVD and the MIVD. (AZ, 2018, p. 24-25).

The final sub-conclusion is that the AIVD, the MIVD, the NCTV, J&V and the ministry of Defence form a joint network that shares tasks and provides information in order to respond to hybrid threats that the Netherlands is facing. The ministry of Foreign Affairs and the ministry of Defence both coordinate resources to counter hybrid threats (BuZa, 2017, p. 33). The ministry of AZ does not compete or collaborate with other ministries and security agencies at all (General Affairs, 2015). Despite the responsibility to ensure national security, the ministry of AZ and the prime minister are not actively involved in coordinating the countering of hybrid threats in the Netherlands. The WWR and the AIV are not part of the shared network to counter hybrid threat with other relevant ministries or security agencies because of their advisory role and isolated position.

Influence Prominent Individuals

The last indicator for the bureaucratic politics model is the influence of prominent individuals within the relevant ministries and security agencies that are involved in the decision-making process. However, the empirical evidence does not provide information about the influence of prominent

individuals. Therefore, no conclusions can be drawn for the influence of prominent individuals within the relevant ministries and security agencies that are involved in the decision-making process.

4.2 Analysis

Section 4.1 presented an empirical timeline of all indicators for the three policy decision-making models of Allison. This section analyzes the relative lack of responsiveness by relevant Dutch ministries and security agencies, including their intelligence agencies, to hybrid threats facing the Netherlands between 2014 and 2019 on the basis of the three policy decision-making models. First, the Rational Policy Model from Allison about national objectives and national means is analyzed. Afterwards, the Organizational Process model and the Bureaucratic Politics model are analyzed. Finally, the main research question is answered and a final conclusion is given.

Model I Rational Policy Model

The rational policy model explains that the Dutch government chooses a rational action or policy, given the strategic problem that it faces (Allison, p. 693). For countering hybrid threats posed by international actors, a rational policy analysis shows that the current status quo is a reasonable act from the point of view of the Dutch government. The Dutch government is seen as the rational, unitary decision maker. The Dutch government has the specific goal to provide security for its Dutch citizens. In this case, hybrid threats and countering opportunities determine the actions of the Dutch government. Based on the information available to the Dutch government, the current status quo considering countering hybrid threats is created where the benefits outweigh the costs in terms of its goals and objectives.

In this case, the Dutch government strives for survival and its primary objective is to provide security for its citizens. According to the empirical data, the most value-maximizing action according to the Dutch government in order to accomplish this objective is to have different relevant ministries and security agencies dealing separately with hybrid threats (BuZa, 2018, p. 24). As a result, all relevant ministries and security agencies stick to their own area of expertise and maximize their value by countering hybrid threats in their own department. The Dutch government did not create an integrated strategy to respond to hybrid threats based on the available information presented to the Dutch government. The relevant ministries and security agencies, including their intelligence agencies, provide the information about the actual hybrid threats and the available means to counter these treats to the government. Therefore, it is possible that the Dutch government made the decision to counter hybrid threats without having an interdepartmental strategy while this decision is not rational because not all information about hybrid threats facing the Netherlands and the available means is available to the Dutch government. Another explanation for not having an integrated strategy to counter hybrid

threats is that the Dutch government did not realize a grand strategy because they did not want take the lead and responsibility to facilitate this grand strategy. The empirical timeline shows that the ministry of AZ including the prime minister is not involved in the policy decision-making process on countering hybrid threats (AZ, 2015, p. 20). Consequently, the absence of a leading government contributed to the lack of responsiveness to hybrid threats in the Netherlands by relevant ministries and security agencies.

Finally, the first explanation of the rational policy model for not realizing an integrated strategy to counter hybrid threats in the Netherlands is that this security policy decision is rationally made in the absence of relevant available information about hybrid threats provided by the relevant ministries and security agencies, including their intelligence agencies. Based on the rational policy model, a second explanation for the current policy decision regarding the response to hybrid threats in the Netherlands is the absence of a leader in the security policy decision-making process. There is no legitimate leading ministry or minister that resembles the unitary rational actor in the policy decision-making process. The ministry of AZ and the Prime Minister are in the position to take the legitimate lead in the integrated response to hybrid threats, but the empirical timeline shows the absence of this ministry and Prime Minister in the decision making process. This rational policy model provides the first global explanation of the relative lack of responsiveness to hybrid threats in the Netherlands. In order to explain why not all relevant information is available to the Dutch government to make a rational decision considering the responsiveness to hybrid threats, the organizational process model must be analyzed.

Model II Organizational Process Model

Between 2014 and 2019, all relevant ministries and security agencies came up with a definition for hybrid threats in the Netherlands. The second sub-question was: How have hybrid threats been framed by the relevant Dutch ministries and security agencies between 2014 and 2019? While J&V, the MIVD and AIVD were leading in framing the problem of hybrid threats in the Netherlands, the ministry of AZ, which includes the Prime Minister, only framed the problem of hybrid threats in the Netherlands from 2017 (AZ, 2018, p. 17). It can therefore be stated that not all relevant ministries and security agencies experienced hybrid threats as a problem in the time period between 2014 and 2019. Also, the ministries of J&V and Defence together with the MIVD and the AIVD defined hybrid threats as cyber operations including cyber attacks, digital espionage and cyber crime (AIVD, 2015, p. 24). From 2016, this definition of hybrid threats was extended with information operations and espionage by the MIVD and AIVD (MIVD, 2018, p.9). The ministry of AZ only defined hybrid threats as the interdependence of international production and transport chains and the significance of international infrastructures for the Internet and energy (AZ, 2018, p. 17). The ministry of Foreign Affairs also used

the most extensive definition for hybrid threats from 2018 by stressing influencing democratic processes and spreading disinformation, engaging in espionage and cyber attacks, taking economic measures and creating strategic dependency. As a result, all ministries frame the problem of hybrid threats differently. Despite the different definitions affecting each other, the different ministries and security agencies all have a different focus on the problem of hybrid threats.

The means and capabilities of the Ministry of AZ remained limited to realizing a new Intelligence and Security Services Act, which enabled the secret services to research the cable in the future (AZ, 2017, p. 8). The ministry of Foreign Affairs mainly focused on international collaboration in order to counter hybrid threats (BuZa, 2017, p. 13). All means and capabilities were therefore focused on realizing international collaboration. The ministry of J&V increased the resilience of Dutch citizens by creating more awareness for hybrid threats. The means to do so were publishing public national threat assessments and informing citizens on how to recognize threats (J&V, 2017, p. 87). The ministry of Defence strengthened both the international military cooperation with NATO and the Defence cyber strategy with the realization of the DCC (Defense, 2015, p. 15). The MIVD investigated hybrid threats and prevented multiple hybrid tactics targeting the Netherlands. Also knowledge sharing was used by the MIVD with the AIVD and the Ministry of Defence in order to create more resilience to hybrid threats. The NCTV researched hybrid threats and informed the public about possible hybrid threats (Beleidsdoorlichting Nationale Veiligheid, 2017, p. 33). Also, the NCTV advised the ministry of J&V and the ministry of Foreign Affairs (J&V, 2018, p. 16). The WRR also researched and published reports on hybrid threats in the Netherlands. Thereafter, the WRR informed the Ministry of AZ to come up with a grand strategy to counter hybrid threats (WRR, 2017, p. 1).

Because the ministries all have their own distinctive focus and capabilities for countering hybrid threats, the only interdepartmental approach to counter hybrid threats is knowledge sharing between the ministry of Defence, the AIVD and the MIVD. The logical reason for this is because these three actors all employ capabilities that focus on cyber threats and digital espionage. As a result, all ministries perform their own tasks in order to counter hybrid warfare through their own approach.

The SOP's of most ministries and security agencies are researching hybrid threats and present the findings to the public and the government. The only executive ministry with regards to hybrid threats is the ministry of Defence because it is able to deploy units. The ministry of Foreign Affairs is also able to deploy sanctions and rules but is limited by its international character of execution. Therefore, the SOPs of the ministry of Foreign Affairs do not correspond to the SOP's of for example the ministry of J&V and the MIVD. Providing information to the public and the Dutch government is one of the SOPs of the relevant ministries and security agencies. Because the first global explanation for the relative lack of responsiveness to hybrid threats is the absence of relevant information for the

Dutch government, the information provided trough the SOPs of the relevant ministries and security agencies is not sufficient for the Dutch government to create an integrated strategic response to hybrid threats in the Netherlands. The explanation for why the provided information by the relevant ministries and security agencies is not sufficient is that each ministry and security agency frames the problem of hybrid threats differently. Because each relevant ministry and security agency focuses on its own area of expertise, the hybrid threats are framed and defined specifically for each ministry or security agency.

In order to get more insight into the origin of the different framing and definitions of hybrid threats by the relevant ministries and security agencies, the bureaucratic politics model must be analyzed.
As a result, the patterns of organizational behavior that anticipated the framing of hybrid threats and the information input by relevant ministries and security agencies are displayed.

Model III Bureaucratic Politics model

The first indicator for the Bureaucratic Politics model is the exclusion of other relevant ministries and security agencies. After analyzing the involvement of relevant ministries and security agencies in the decision making process and the overlap in the tasks of these ministries and security agencies, the areas of competition and the exclusion of relevant ministries and security agencies are found. Based on the question if there are other relevant ministries and security agencies involved in the response, multiple collaborations between the ministries and security agencies can be found. Figure 16 presents a graph about the current interdepartmental connections and collaborations in countering hybrid threats by the relevant ministries and security agencies in the Netherlands.

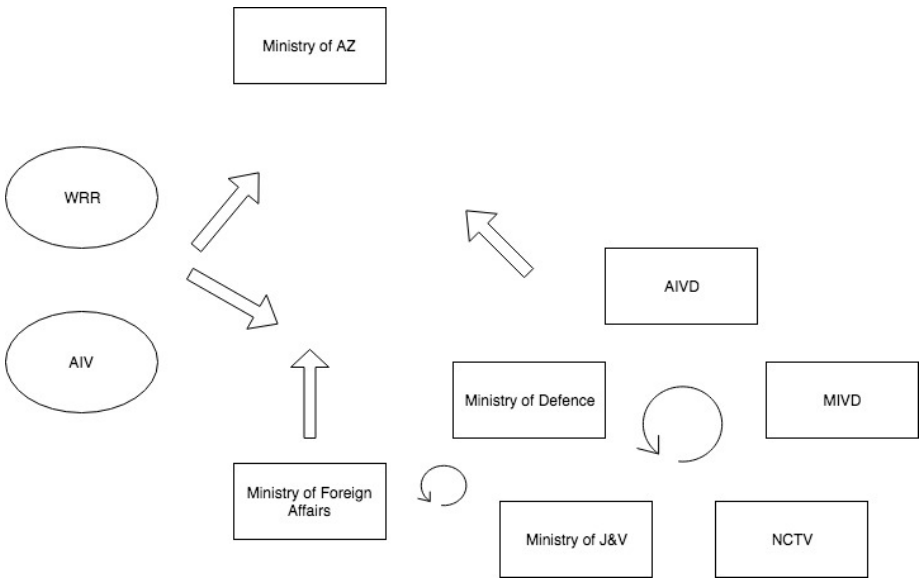

Figure 16. Current interdepartmental connections and collaborations in countering hybrid threats by relevant ministries and security agencies in the Netherlands.

According to the empirical evidence, The AIVD, the MIVD, the NCTV, J&V and the ministry of defence form a joint network that shares tasks and provides information in order to respond to hybrid threats. The ministry of Foreign Affairs and the ministry of Defence also both coordinate resources to counter hybrid threats (BuZa, 2017, p. 33). More specifically, the NCTV, the MIVD and the AIVD collaborate on cyber threats and espionage. The National Cyber Security Centre of the NCTV, the MIVD and the AIVD provides knowledge, information and a collective reaction to cyber threats by these security agencies. The NCTV, MIVD and AIVD share this information with their aligned ministries resulting in the collaboration between the AIVD, the MIVD, the NCTV, J&V and the ministry of Defence. However, cyber threats are only one side of hybrid threats, which makes the collaboration between the security agencies not representative for countering all hybrid threats.

The ministry of Foreign Affairs developed a note for an integrated approach regarding hybrid threats that involved actions from the ministry of Defence (BuZa, 2017, p. 33). Subsequently, the ministry of Defence is mentioned in the response to threats facing the Netherlands. However, the note from the Ministry of Foreign Affairs is primarily made by the ministry of Foreign Affairs and directs the ministry of Defence to follow the note. It can therefore be stated that the collaboration between the ministry of Foreign Affairs and the ministry of Defence is rather one sided. The ministry of Defence collaborates with the ministry of J&V, the ministry of Foreign Affairs and the NCTV by sharing the Royal Military Police since its mandate to use is based on the threat and purpose. This interdepartmental collaboration can therefore not be seen as an integrated approach to counter hybrid threats.

Figure 16 also shows that the ministry of AZ is involved in the policy making process on countering hybrid threats. Altough the Ministry of AZ mentions the information input from the ministry of Defence, the Ministry of Foreign Affairs, the NCTV, the WRR, the MIVD and the AIVD, none of the mentioned ministries and security agencies stress the involvement of the ministry of AZ (General Affairs, 2015). The ministry of AZ is not excluded from the policy decision-making process because the relevant ministries and security agencies provide information about hybrid threats to the ministry of AZ. But, besides the information input, the ministry of AZ is not involved in the response to hybrid threats by the Netherlands except for realizing a new law for the MIVD and AIVD that enables legal access to the cable.

In the empirical timeline, the ministry of AZ mentions the WRR as an information provider. Other relevant ministries and security agencies do not mention the WRR. Therefore, the WRR can be seen as an independent island that only provides information to the relevant ministries and security agencies and is not further involved in the policy decision-making process. This also applies to the AIV and the ministry of AZ. The ministry of AZ also is not further involved in the decision making process on the response to hybrid threats. The information of the WRR and the AIV therefore do not meet the policy

decision-making process of other relevant ministries and security agencies. As a result, the WRR and the AIV are excluded from the policy decision-making process with other relevant ministries and security agencies in the Netherlands.

From a first point of view, no relevant ministry or security agency seems to be excluded from the policy decision-making process on the response to hybrid threats. However, the ministry of AZ does not give information output or collaborates with other relevant ministries and security agencies while the ministry of AZ is able to do so. This makes that the ministry of AZ by definition is not excluded from the policy decision-making process, but that the ministry of AZ does not seek the involvement in the policy decision-making process on the response to hybrid threats. As a consequence, the WRR is excluded because the information exchange does only occur between the WRR and the Ministry of AZ. Also, the ministry of Foreign Affairs took the lead in creating a more integrated response to hybrid threats in the Netherlands. But, because the ministry of Foreign Affairs created the note, this does not directly imply that the other relevant ministries and security agencies accept this lead and collaborate with the ministry of Foreign Affairs. As a result, the triangle between the NCTV, the MIVD and the AIVD in countering hybrid threats remains the only response to hybrid threats while other involved ministries and security agencies maintain their own status quo by focussing on their own domain in stead of collaborating. Exclusion of relevant ministries and security agencies is therefore not the case, but deliberately aiming to be involved in a collaborative response definitely is.

Since the MIVD and the AIVD share a building, operational units and multiple tasks together, competition in order to get the lead in tasks and operations considering hybrid threats cannot be excluded. In order to both remain relevant, the MIVD and the AIVD must compete with each other because otherwise, the MIVD and the AIVD become one national intelligence service. Because hybrid threats and specifically cyber threats are not always aimed at only the military aspect of a state, the MIVD cannot use military relevance in order to claim the lead in countering hybrid threats. As a result, both intelligence services are capable to counter the same threats but besides the joint units, further cooperation stays off. The ministry of Foreign Affairs changed its strategy to counter hybrid threats by involving the ministry of Defence. However, the involvement only implied the contribution to promote the security interests of the ministry of Foreign Affairs. Since it can be stated that each relevant ministry and security agency frames hybrid threats differently, the approach from the ministry of Foreign Affairs does not meet the desired approach of the ministry of Defence and the ministry of J&V. Other ministries and security agencies do not seek to be commanded and involved in a strategy and cooperation that is primarily aimed at meeting the security interests of the Ministry of Foreign Affairs. As a result, other relevant ministries and security agencies do not support the interdepartmental note and the sudden leading role from the Ministry of Foreign Affairs as much as desired. The top down approach in order to interdepartmentally counter hybrid threats comes from a

ministry that is situated at an equal level with the other ministries and security agencies. Therefore, the leading role is not supported enough and a legitimate interdepartmental strategy remains absent.

The absence of the Ministry of AZ with the prime minister in the policy decision-making process results in a struggle for leading an integrated approach to counter hybrid threats by equal ministries. This results in all relevant ministries and security agencies acknowledging the importance of an integrated approach to counter hybrid threats in the Netherlands, but not managing to accomplish this in the absence of a legitimate leader and a general definition of the problem.

The last indicator for the bureaucratic politics model is the influence of prominent individuals within the relevant ministries and security agencies that are involved in the decision making process. However, the empirical evidence does not provide concrete information about the influence of prominent individuals and it cannot be scientifically proven that the prominent individuals exerted enough influence in order to have the Dutch responsiveness to hybrid threats in their favor. Despite the fact that the influence of prominent individuals might be present in this case, this research cannot conclude these findings. However, enough empirical evidence is found for the exclusion of relevant ministries and security agencies in the decision making-process and the competition between relevant ministries and security agencies. As a result of the bargaining games between relevant ministries and security agencies, the Dutch government is unable to collaborate and realize a grand strategy regarding hybrid threats.

Based on the sub-conclusion of the analysis with the policy decision-making models, the main research question can be answered:

What can explain the relative lack of responsiveness of the relevant Dutch ministries and security agencies, including their responsible intelligence agencies, to hybrid threats between 2014 and 2019?

The factors leading to the relative lack of responsiveness of the relevant Dutch ministries and security agencies, including their intelligence agencies, to hybrid threats can be explained by the empirical analysis and the literature review on hybrid threats. First, the analysis of the organizational process model concludes that each relevant ministry and security agency focuses on different hybrid threats. Therefore, the problem of hybrid threats that the Netherlands is facing is framed and defined differently by these relevant ministries and security agencies. Logically, all relevant ministries and security agencies provide capabilities that are aimed at their specific definition of hybrid threats. All the different frames, definitions, SOP's and capabilities for hybrid threats come together at the Dutch government. As a result, the Dutch government is not able to create an integrated strategy because there is no converging information about hybrid threats in the Netherlands available. It is possible that

the Dutch government rationally has not created a grand strategy to counter hybrid threats that are facing the Netherlands because a clear converged frame of hybrid threats is missing.

Secondly, according to the bureaucratic politics model, the different relevant ministries and security agencies share overlapping tasks and units regarding the response to hybrid threats. In order to ensure that the responsibility and the tasks remain within one ministry or security agency, a limited request for an integrated approach to counter hybrid threats is made by these ministries and security agencies. Furthermore, the most relevant ministry of AZ excludes itself from the policy decision-making process. As a result, the competition between other relevant ministries and security agencies such as the ministry of Foreign Affairs are are not able to take the legitimate lead in the response to hybrid threats facing the Netherlands because other relevant ministries and security agencies are considered equal.

Finally, the literature study on hybrid threats stresses the difficulty to clearly identify hybrid threats a state is facing. Besides the wide range of appearances, hybrid threats are not always noticeable until the goal of hybrid tactics are already achieved by the opponent. Therefore, it is difficult for a state to increase the responsiveness to hybrid threats that vary in several forms and are often not even noticeable. The analysis of the organizational process model confirms this difficulty to frame hybrid threats by the Dutch government. The wide range of appearances, the changing character and the low noticeability of hybrid threats explain the different definitions of hybrid threats by relevant Dutch ministries and security agencies. As a result, the different definitions of hybrid threats result in a default to respond to all hybrid threats simultaneously with one grand strategy. The absence of an interdepartmental grand strategy for countering hybrid threats is therefore more the result of default than of purpose by the Dutch government. The self-exclusion of the most relevant ministry of AZ from the policy decision-making process also partially explains the relative lack of responsiveness to hybrid threats. As a result, the competition between other relevant Dutch ministries and security agencies unables these ministries and security agencies to take the legitimate lead in the response to hybrid threats.

This analysis concludes that the different framing of hybrid threats by relevant Dutch ministries and security agencies and the absence of a legitimate leading Dutch ministry or security agency explain the relative lack of responsiveness to hybrid threats facing the Netherlands. Also, the extensive amount of hybrid threats presented in the literature review on hybrid warfare and the changing character of hybrid threats make it difficult for relevant Dutch ministries and security agencies to address all these hybrid threats simultaneously and establish a grand strategy to counter hybrid threats.

5. Conclusions and Recommendations

The purpose of this thesis was to explain the lack of responsiveness of relevant Dutch ministries and security agencies to hybrid threats by researching the security policy decision-making process of the relevant Dutch ministries and security agencies. This chapter concludes the findings of this research. First, the main research question is answered by the conclusions of the analysis. Next, the used theories, the contribution of this research to the academic knowledge of hybrid threats and the research limitations are discussed. Finally, this thesis will conclude with research recommendations.

5.1 Conclusions

The annexation of Crimea and the downing of flight MH-17 in 2014 were a wake up call for the Netherlands to start paying more attention to hybrid threats and especially those emanating from Russia. However, five years later in 2019, at the time of writing, the Netherlands still lacks a grand strategy regarding both defensive and offensive hybrid threats (Amersfoort, 2016, p. 219). Despite several reports and recommendations from organizations such as the National Coordinator for Security and Counterterrorism (NCTV) and the Netherlands Scientific Council for Government Policy (WRR) and the increasing number of hybrid threats, a grand strategy in order to respond to hybrid threats is missing and the responsiveness of the Netherlands to hybrid threats remains limited to the operational level in crisis situations (NCTV, 2016, p.7 ; WRR, 2011, p. 8). From a rational point of view, the absence of a political and military strategy regarding hybrid treats is undesirable (Amersfoort, 2016, p. 217). The Dutch government is responsible for the response to threats that are facing the Netherlands and the protection of the Netherlands (Dutch Consitution, 2018, art. 97). The purpose of this research was to find an explanation for the relative lack of responsiveness and the lack of adaptability by the Dutch government with respect to hybrid threats between 2014 and 2019. As a result, the following main research was formulated:

What can explain the relative lack of responsiveness of the relevant Dutch ministries and security agencies, including their responsible intelligence agencies, to hybrid threats between 2014 and 2019?

This research focused on the structures and the security policy decision-making process of relevant Dutch ministries and security agencies, including their responsible intelligence agencies. By analyzing the security policy decision-making process on the actual response to hybrid threats of relevant Dutch ministries from 2014 until 2019, an answer to what can explain the relative lack of responsiveness to hybrid threats between 2014 and 2019 was found. First, a literature review on hybrid warfare and a theoretical framework for the three policy decision-making models from Allison was presented and explained. Based on the literature review and the theoretical framework, the indicators explaining the

lack of responsiveness to hybrid threats by relevant Dutch ministries and security agencies were presented in the analytical framework. Next, the relevant Dutch ministries and security agencies were operationalized and the case study design and methodology were explained. Chapter four presented an empirical description of the response to hybrid threats by the relevant Dutch Ministries and security agencies between 2014 and 2019, followed by an analysis. The empirical timeline was based on public reports from relevant Dutch ministries and security agencies that were published and operational between 2014 and 2019. The analysis of the empirical timeline with the three policy decision-making models partially explained the relative lack of responsiveness to hybrid threats in the Netherlands.

Based on the literature review on hybrid threats, an important remark can be made about the difficulty to respond to hybrid threats by relevant Dutch ministries and security agencies. The definition of hybrid threats as a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the battle space by both state actors and non-state actors results in an extensive range of appearances. Besides the wide range of appearances, hybrid threats are not always noticeable until the goal of hybrid threats are already achieved by the opponent. Consequently, it is difficult for a state to increase the responsiveness to hybrid threats that vary in several forms and are often not even noticeable. It can therefore be stated that a response to counter all hybrid threats is not realistic and reachable for the relevant Dutch ministries and security agencies. Although it is not realistic and desirable for the relevant Dutch ministries and security agencies to address all hybrid threats the Netherlands is facing, the analysis with the policy decision-making models of Allison shows multiple organizational structures that also partially explain the current lack of responsiveness to hybrid threats by relevant ministries and security agencies.

The policy process model explains that each relevant Dutch ministry and security agency focuses on different hybrid threats. Therefore, the problem of hybrid threats is framed and defined differently by all relevant Dutch ministries and security agencies. All relevant ministries and security agencies provide capabilities that are aimed at their specific definition of hybrid threats. All the different frames, definitions, SOPs and capabilities for hybrid threats come together at the Dutch government. As a result, the Dutch government is not able to create an integrated strategy because there is no converging information about hybrid threats in the Netherlands available. As a result, the Dutch government rationally decided that the current non-integrated response to hybrid threats facing the Netherlands is the most value maximizing in the absence of a clear converged frame and definition of hybrid threats facing the Netherlands.

According to the bureaucratic politics model, the different relevant ministries and security agencies share overlapping tasks and units regarding responding to hybrid threats. The limited request for an integrated approach to counter hybrid threats by the relevant ministries and security agencies and the

self-exclusion of the most relevant ministry of AZ from the policy decision-making process also partially explain the relative lack of responsiveness to hybrid threats. The existing competition between other relevant Dutch ministries and security agencies makes hierarchically equal ministries and security agencies unable to take the legitimate lead in the response to hybrid threats facing the Netherlands.

Concluding this research, there are three explanations for the relative lack of responsiveness of the relevant Dutch ministries and security agencies, including their intelligence agencies, to hybrid threats between 2014 and 2019. The biggest problem is that the relevant Dutch ministries and security agencies frame the problem of hybrid threats facing the Netherlands differently. Also, the absence of a legitimate leading ministry or security agency to establish a grand strategy to counter hybrid threats contributes to the lack of responsiveness to hybrid threats. Furthermore, the extensive amount of hybrid threats presented in the literature review on hybrid threats and the changing character of hybrid threats make it difficult for relevant Dutch ministries and security agencies to address all these hybrid threats simultaneously and establish a grand strategy to counter hybrid threats. The analysis presented in this thesis demonstrated considerable problem framing differences between the relevant ministries and security agencies at countering hybrid threats in the Netherlands. A valuable conclusion that can be drawn from this study is the importance of problem framing and information input by relevant ministries and security agencies in creating a desired integrated strategic approach to counter hybrid threats. Another important conclusion is the importance of a legitimate leading ministry or security agency that ensures all frames and definitions of hybrid threats are converged in order to increase the responsiveness to hybrid threats facing the Netherlands.

5.2 Discussion

This research can serve as a stepping-stone towards fostering an integrated strategy for countering hybrid threats by relevant Dutch ministries and security agencies. When hybrid threats appeared in the last decade of the twentieth century, the relationship between relevant ministries and security agencies was one of information asymmetry and in some respects, competition. Currently, hybrid threats have gradually become a known threat to the Dutch society. Therefore, it is time to reevaluate the relationship between the relevant ministries and security agencies in the Netherlands in order to counter these hybrid threats effectively. Eventually, one of the tasks of the Dutch government is to provide security for its citizens with all means possible.

However, the theory on hybrid warfare shows that hybrid threats can be anything. The different concepts and definitions surrounding hybrid threats make it difficult to research hybrid threats or, in this case, a grand strategy for countering hybrid threats. The broadness and vagueness of hybrid threats makes it worth considering if a grand strategy to counter hybrid threats is able to address all

potential threats. Instead of creating and researching the same approach to constantly different and changing threats, the different conflicts and threats can be researched and defined by concepts that actually can be used to base both research and policies on.

5.3 Recommendations

A recommendation is that future efforts at creating a desired integrated strategy to counter hybrid threats would benefit from a form of collaboration between the relevant ministries and security agencies. This form of collaboration can be realized by converging all definitions of hybrid threats from the relevant ministries and security agencies into one definition of the problem of hybrid threats. Thereafter, the information input from all relevant ministries and security agencies must come together at one central point in order to have the most information available in order to make policy decisions concerning hybrid threats. A recommendation for future research would be to get more in depth insight into the influence of prominent individuals in the policy decision making-process on the response the hybrid threats in the Netherlands. Furthermore, according to the theory on hybrid threats, all Dutch ministries and security agencies can become targets of hybrid tactics. Therefore, a recommendation for future research would be to also include other Dutch ministries such as the ministry of Finance and the ministry of Agriculture, Nature and Food Quality.

5.4 Reflection

A limitation of this research could be the process tracing method and the use of a case study. The research findings of this case study have a limited generalizability for other states with a relative lack of responsiveness to hybrid threats. Another limitation of this research can be the reliability of the empirical timeline. Remarkable in this research was the impressive amount official reports from Dutch ministries and security agencies, which all emphasized their own role in countering hybrid threats. Official reports often only reflect one point of view and despite the fact that reports can be used to find details and facts related to a specific case, the security policy decision-making processes inside Dutch ministries or security agencies are difficult to find. Another limitation of the data collection is the lack of empirical evidence for the influence of individuals for the bureaucratic politics model. Therefore, this research is not able to conclude whether or not prominent individuals influenced the policy decision-making process on the response to hybrid threats in the Netherlands. Finally, to repeat the conclusion of this research, there is no absolute way to research what can explain the relative lack of responsiveness of the relevant Dutch ministries and security agencies to hybrid threats between 2014 and 2019. Multiple reasons lead to the relative lack of responsiveness to hybrid threats and events during the Dutch security policy decision-making process are just one item.

References

Advisory Council on International Affairs. (2018). Retrieved on March 1 from: https://aiv-advies.nl/63v/about-the-aiv

Advisory Counsil on International Affairs. (2017). Retrieved on April 12 from: https://aiv-advies.nl/download/076a0fe9-ef0f-471a-8481-453fcbbe9bb5.pdf

AIV. (2015). *Deployment of Rapid-Reaction Forces.*

AIV. (2015). *Instability around Europe.*

AIVD. (2017). *The future of NATO and European Security.*

AIVD. (2015). *2014 Annual Report General Intelligence and Security Service.*

AIVD. (2016). *2015 Annual Report General Intelligence and Security Service.*

AIVD. (2017). *2016 Annual Report General Intelligence and Security Service.*

AIVD. (2017). *AIVD and MIVD Cyber espionage.*

AIVD. (2018). *2017 Annual Report General Intelligence and Security Service.*

AIVD. (2019). *2018 Annual Report General Intelligence and Security Service.*

Algemene Zaken. (2015). *Rijksjaarverslag Algemene Zaken 2014.*

Algemene Zaken. (2016). *Rijksjaarverslag Algemene Zaken 2015.*

Algemene Zaken. (2017). *Rijksjaarverslag Algemene Zaken 2016.*

Algemene Zaken. (2018). *Rijksjaarverslag Algemene Zaken 2017.*

Allison, G. T. (1969). Conceptual models and the Cuban missile crisis. American political science review, 63(3), 689-718.

Amersfoort. H. (2016) Nederland, de weg kwijt. Over de teloorgang van de militaire strategie en de noodzaak van geschiedenis. Militaire Spectator, 185 (5), 217-231.

Argyris, C. (1976). Single-loop and double-loop models in research on decision making. Administrative science quarterly, 363-375.

Baarda, D.B., Goede, de M.P.M., & Teunissen, J. (2009). Basisboek kwalitatief onderzoek. Groningen/Houten: Noordhoff Uitgevers b.v., 2e geheel herziene druk

Bachmann, S. (2015). Hybrid Wars: The 21 st-Century's New Threats to Global Peace and Security. Scientia Militaria: South African Journal of Military Studies, 43(1), 77-98.

Bell, C. (2012). Hybrid warfare and its metaphors. Humanity: An International Journal of Human Rights, Humanitarianism, and Development, 3(2), 225-247.

Bendor, J., & Hammond, T. H. (1992). Rethinking Allison's models. *American Political Science Review*, *86*(2), 301-322.

Buitenlandse zaken. (2013). *International Safety Strategy.*

Buitenlandse zaken. (2015). *Rijksjaarverslag Buitenlandse Zaken 2014*

Buitenlandse zaken. (2016). *Rijksjaarverslag Buitenlandse Zaken 2015*

Buitenlandse zaken. (2017). *Rijksjaarverslag Buitenlandse Zaken 2016*

Buitenlandse zaken. (2018). *Rijksjaarverslag Buitenlandse Zaken 2017*

Buitenlandse zaken. (2018). *Integrated foreign and safety strategy*

Bunde, T., & Oroz, A. (2015). Munich security report 2015: collapsing order, reluctant guardians?. Munich Security Conference Foundation.

Bernardes, E. S., & Hanna, M. D. (2009). A theoretical review of flexibility, agility and responsiveness in the operations management literature: Toward a conceptual definition of customer responsiveness. International Journal of Operations & Production Management, 29(1), 30-53.

Buitenlandse Zaken (2018). Geïntegreerde Buitenland en Veiligheids-strategie. Retrieved on March 1 from:https://www.rijksoverheid.nl/documenten/rapporten/2013/06/21/veilige-wereld-veilig-nederland-internationale-veiligheidsstrategie

Business Ukraine (2016). Russion Hybrid War in Ukraine. Retrieved on 14 feb 2019 from: http://bunews.com.ua/component/zoo/item/debunking-putins-crimea-claims

Clayton, M. (2016). Allison's Slow "Waltz" with Structure in Foreign Policy Analysis. Retrieved on 12 may 2019 from: https://www.e-ir.info/2016/04/17/allisons-slow-waltz-with-structure-in-foreign-policy-analysis/

Collier, D. (2011). Understanding Proces Tracing. Political Science and Politics, 44, 4, pp. 823-830.

Cullen, P. (2018). Strategic Analysis May 2018. Hybrid threats as a new 'wicked problem' for early warning. The European Centre of Excellence for Countering Hybrid Threats.

Creveld, M. (2004, May). Modern conventional warfare: An overview. In National Intelligence Council Workshop.

Defensie. (2015). *Rijksjaarverslag Defensie 2014.*

Defensie. (2016). *Rijksjaarverslag Defensie 2015.*

Defensie. (2017). *Rijksjaarverslag Defensie 2016.*

Defensie. (2018). *Rijksjaarverslag Defensie 2017.*

Defensie. (2017). *Beleidsdoorlichting Nationale Veiligheid.*

Ducheine, P. (2016). Nationale veiligheid en hybride dreiging: twee kanten van dezelfde medaille. Magazine Nationale Veiligheid en Crisisbeheersing, 14(5/6), 7-10.

Ducheine, P. (2013). Effectiviteit, legitimiteit en verantwoordelijkheid. A. Wagemaker & F. van Nijnatten, Minuutschoten–Liber Amicorum voor Hans Bosch, 25-28.

Dutch Constitution (2018). Artikel 97: Krijgsmacht. *Retrieved at march 2* 2019.

Freier N. (2007). Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional and Hybrid Challenges in Context. Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute.

Freier, N. (2009). The defense identity crisis: it's a hybrid world. Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute.

Gaddis, J. L. (2002). A grand strategy. Foreign Policy, 133(S 50), 57.

Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?. Small Wars & Insurgencies, 27(2), 282-301.

Gibney, M. (2015). The downing of MH17: Russian responsibility?. Human Rights Law Review, 15(1), 169-178.

Government. (2018). Retrieved on march 1 from: https://www.government.nl/ministries/ministry-of-general-affairs

Government. (n.d.). MH-17 Incident. Retrieved on March 7 from: https://www.government.nl/topics/mh17-incident/achieving-justice/the-criminal-investigation

Glenn, R. W. (2009). Thoughts on hybrid conflict. Small Wars Journal, 13.

Gray, C. S. (2007). Irregular warfare: One nature, many characters. Strategic Studies Quarterly, 1(2), 35-57.

Grondwet (2019). *Artikel 97: Krijgsmacht.*

Hoogerwerf, A. & M. Herweijer (2003) Overheidsbeleid: Een inleiding in de beleids- wetenschap. Alphen aan de Rijn: Kluwer.

Hoffman, F.G. (2007). 'Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies'. Retrieved on 12 december from: https//www.potomacinstitute.org/publications/Potomac_HybridWar_0108.pdf

Hoffman, F. G. (2009). Hybrid warfare and challenges. National Defense university Washington DC institution for national strategic studies.

Hoffman, F. (2010). *'Hybrid Threats': Neither Omnipotent Nor Unbeatable*. Orbis, 54 (3), 441-455.

Hoffman, F. (2011). "Future Threats and Strategic Thinking," Infinity Journal, 4, 17.

Hoffman, F. (2014). Hybrid Warfare and Challenges. Strategic studies. pp. 339-348.

Justitie en Veiligheid. (2015). *Rijksjaarverslag Justitie en Veiligheid 2014*

Justitie en Veiligheid. (2015). *Cybersecuritybeeld Nederland csbn 2015*

Justitie en Veiligheid. (2016). *Rijksjaarverslag Justitie en Veiligheid 2015*

Justitie en Veiligheid. (2017). *Rijksjaarverslag Justitie en Veiligheid 2016*

Justitie en Veiligheid. (2016). *Cybersecuritybeeld Nederland csbn 2016*

Justitie en Veiligheid. (2018). *Rijksjaarverslag Justitie en Veiligheid 2017*

Justitie en Veiligheid. (2018). *Cybersecuritybeeld Nederland csbn 2018*

Justitie en Veiligheid. (2019). *Informatiestrategie 2017-2022*

Kaldor, M. (2013). New and old wars: Organised violence in a global era. John Wiley & Sons.

Kremlin. (2014). Vladimir Putin answered journalists' questions on the situation in Ukraine. Retrieved on 13 februari 2019 from: http://en.kremlin.ru/events/president/news/20366

Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. International affairs, 92(1), 175-195.

Liang, Q and Xiangsui, W. (1999). Unrestricted Warfare, PLA Literature and Arts Publishing House, Beijing, pp. 34-59.

Lincoln, Y. S., & Guba, E. G. (1985). Establishing trustworthiness. Naturalistic inquiry, 289, 331.

Lind, Schmitt, Sutton, Wilson and Nightengale (1989). The Changing Face of War: Into the Fourth Generation Marine Corps Gazette. 73, 10, pp. 22-26.

Mahoney, James. (2003). 'Strategies of Causal Assessment in Comparative Historical Analysis', in Mahoney andRueschemeyer (eds.), pp. 337–72.

Mattis, J. and Hoffman, F. (2005). *Future Warfare: The Rise of Hybrid Wars*. U.S. Naval Institute: Proceedings Magazine, 132 (11), pp. 18 – 19.

Maso, I. (1987). Kwalitatief onderzoek. Meppel: Boom

McCuen, J. (2008). "Hybrid Wars," Military Review, 88, 107.

Ministry of Foreign Affairs. (2018). Retrieved on March 1 from: https://www.government.nl/ministries/ministry-of-foreign-affairs

MIVD. (2014). *Digitale Spionage.*

MIVD. (2014). *Espionage Abroad.*

MIVD. (2014). *Espionage in the Netherlands.*

MIVD. (2015). *2014 Annual Report Netherlands Defence Intelligence and Security Service.*

MIVD. (2016). *2015 Annual Report Netherlands Defence Intelligence and Security Service.*

MIVD. (2017). *2016 Annual Report Netherlands Defence Intelligence and Security Service.*

MIVD. (2018). *2017 Annual Report Netherlands Defence Intelligence and Security Service.*

MIVD. (2017). *AIVD and MIVD Cyber espionage.*

MIVD. (n.d.). MIVD. Retrieved on 3 May 2019 from: https://www.defensie.nl/organisatie/bestuursstaf/eenheden/mivd

Mosquera, A. B. M., & Bachmann, S. D. (2016). Lawfare in hybrid wars: the 21st century warfare. Journal of International Humanitarian Legal Studies, 7(1), 63-87.

NCTV. (2016). *Nationaal Veiligheidsprofiel 2016.*

NCTV. (2018). *Horizonscan Nationale Veiligheid 2018.*

Nato (2015a). *Wales Summit Declaration*. (2015). Retrieved at 12 December 2018 from: https://www.nato.int/cps/fr/natohq/official_texts_112964.htm?selectedLocale=en.

Nato (2015b). Supreme Allied Commander Transformation Headquarters, 'Military Contribution to Countering Hybrid Threats Capstone Concept'. Retrieved at 12 december 2018 from: www.act.nato.int/the-countering-hybrid-threats-concept-development-experiment.

NCTV(n.d.). Organization. Retrieved on 3 may from: https://english.nctv.nl/organisation/

Odell, J. S. (2001). Case study methods in international political economy. International Studies Perspectives, 2(2), 161-176.

Popescu, N. (2015). Hybrid tactics: neither new nor only Russian. EUISS Issue Alert, 4.

Ramicone, A. (2014). The Ukrainian Crisis: A Dispute Past and Present. Harvard: Institute of Politics of Harvard.

Renz, B. (2016). Russia and 'hybrid warfare'. Contemporary Politics, 22(3), 283-300.

Schroefl, J., & Kaufman, S. J. (2014). Hybrid actors, tactical variety: Rethinking asymmetric and hybrid war. Studies in Conflict & Terrorism, 37(10), 862-880.

Simon, H. A. (1972). Theories of bounded rationality. Decision and organization, 1(1), 161-176.

Simpson, E. (2005). *Thinking about Modern Conflict: Hybrid Wars, Strategy and War Aims*. Midwest Political Science Association. Retrieved on 21 Februari 2019 from:

Smith, S. (1980). Allison and the Cuban Missile Crisis: a review of the bureaucratic politics model of foreign policy decision-making. Millennium, 9(1), 21-40.

Sterling-Folker, J. (2013). Neoliberalism. in T. Dunne, M. Kurki en S. Smith (Red.), International Relations Theories. Discipline and Diversity (pp. 59 – 76) (3e druk). Oxford: Oxford University Press.

Treisman, D. (2016). Why Putin Took Crimea. Foreign Affairs, 95(3), 8.

Verschuren, P., & Doorewaard, H. (2007). Het ontwerpen van een onderzoek. Amsterdam: Boom

Wetenschappelijke Raad voor het Regeringsbeleid. (2018). Retrieved on 1 March from: https://english.wrr.nl

WRR. (2017). *Veiligheid in een wereld van verbindingen. Een strategische visie op het defensiebeleid.*