Deterrence and Resilience: Two Sides of the Same Coin

The Ability of Dutch Resilience Policy to Deter Hybrid Threats

Jeroen van den Berg

S1501828

Thesis – Crisis & Security Management (MSc)
Supervisor: Dr. E.E.A. Dijxhoorn
2nd reader: Dr. J. Melissen
June 9, 2019
Word Count: 18.715

Table of Content

Introduction

The apparent success of Russian strategy that led to the annexation of Crimea in 2014 has resurfaced the term "hybrid warfare", placing it at the top of governmental agendas. Especially the non-military side of hybrid warfare has prompted national governments all over Europe, including the Netherlands, to generate a better understanding of the phenomenon. Adversaries that use hybrid warfare are "adversar[ies] that simultaneously and adaptively employ a fused mix of conventional weapons, irregular tactics, terrorism and criminal behaviour in the battle space to obtain their political objectives" (Hoffman, 2009). Hybrid strategies are characterised by a high degree of complexity and a lack of transparency, which makes it particularly challenging to construct effective counterstrategies. In response, two potential strategies have been explored: deterrence and resilience. For many decades, military strategy has been dominated by deterrence and it should come as no surprise that it has also been used to make sense of countermeasures against hybrid warfare. Significantly more novel, and less military, is the second strategy of resilience. It has surfaced as a way of countering hybrid operations occurring in the grey zone below the official threshold of war. However, the most novel counterstrategy that has appeared in some academic literature combines the two, creating a "deterrence-by-resilience" strategy in which the likelihood of an attack is limited by a reduction of societal vulnerability, which in turn reinforces deterrence (Lasconjarias, 2017, p. 1). The ability of resilience to deter hybrid threats is mostly dependent on the strength of resilience in national policies (Prior, 2018). Because of the novelty of the term deterrence-by-resilience, it has not yet made its entry into national policies. The opposite holds true for resilience. The main security strategy of the Netherlands, the Integrated Foreign and Security Strategy 2018-2022 (IFSS), not only focusses on the hybrid threats that the Netherlands is facing, but also contributes great value to the potential of resilience as a countermeasure. In order to assess the strength of that resilience in light of its ability to deter, this thesis sets out to answer the following question:

To what extent is deterrence-by-resilience an achievable counterstrategy against the hybrid threats that the Netherlands is facing?

The starting point of this thesis lies in resilience. The Dutch government has published a few strategic documents in which the phenomenon of hybrid warfare in general is assessed, combined with a focus on resilience as a counterstrategy in particular. Those documents show that the Netherlands attributes value to resilience as a potential countermeasure against hybrid threats. At the same time, however, while the academic literature has expanded significantly on the concept and method of resilience, the Dutch hybrid warfare strategy does not provide that conceptual or methodological depth. This lack of analytical strength becomes a problem once deterrence is taken into consideration. In order for resilience to have the ability to deter hybrid adversaries, mere incidental mentioning of resilience in strategic documents is not sufficient. Instead, resilience has to be embedded in counterstrategies, creating a coherent and government-wide response to hybrid threats. Indeed, the academic literature points to the importance of whole-of-government approaches in both resilience building efforts and strategies to counter hybrid threats. This thesis will be exploring the government-wide avenue as well. The IFSS suggests that resilience is also addressed in other government publications outside the security domain. Now, knowing that resilience as a counterstrategy against hybrid threats is very promising, the suggestion that Dutch resilience strategy is significantly broader than the documents on hybrid warfare alone requires further analysis. Namely, if the analysis of government-wide Dutch strategy shows that resilience is widely used and resilience building efforts are well on their way, it would greatly contribute to the achievability of deterrence-by-resilience. To clarify, the analysis is not about the extent to which resilience policy can be executed. Instead, the achievability of deterrence-by-resilience looks at the prominence of resilience in the policy input, which determines of deterrence can realistically be achieved in a relatively short period of time.

The Dutch Context

Over the last couple of years, cooperation at the international level within the NATO alliance and within the European Union (EU) has become increasingly challenging. Both organisations are strained by power politics and political disagreement, undermining their respective decisiveness (Drent & Meijnders, 2018, p. 29). As a result, the presence of the Netherlands on the international stage has grown. In 2018, the Netherlands has been a member of the UN Security Council, including a one-month period in which it held the chairmanship. Additionally, the government has been credited for its leading role in the investigation into the downing of flight MH17 and the active membership of global anti-

terrorism coalitions. In the EU, the relative stability of the Dutch government gives it significant credibility at a time when political unrest dominates the Union. All in all, this growing prominence and visibility at the international stage makes the Netherlands increasingly susceptible to hybrid threats, which also makes an analysis of Dutch countermeasures relevant.

In order to understand the threats the Netherlands is facing, three documents are particularly relevant: the "Integrated Foreign and Security Strategy" (IFSS), published by the ministry of foreign affairs, the "Horizonscan Nationale Veiligheid 2018", published by the National Coordinator for Security and Counterterrorism, and the yearly report of 2017 by the Dutch intelligence service (Ministerie van Buitenlandse Zaken, 2018; Drent & Meijnders, 2018; AIVD, 2018). The novelty of hybrid warfare as a distinct concept in the official publications clearly shows from these documents. The report by the intelligence service, which looks back at the previous year, has no mentioning of the term hybrid warfare, while the IFSS and the "Horizonscan", which both look forward, explicitly use the concept. Also remarkable, the threats discussed in the context of hybrid warfare are largely similar in all documents. The Netherlands places much emphasis on the role of new technologies and swift digitisation. Direct cyberattacks could disrupt vital infrastructure and disinformation campaigns could undermine national politics and cause social disruption. More indirectly, the agencies warn for espionage and the risk of vital information falling in the hands of malign adversaries. Secondly, the growing assertiveness of Russia is seen as a direct military threat. This threat, however, is mostly a matter of collective defence at the alliance level. Yet, responsibility and accountability for defence against the non-military side of hybrid threats lies at the national level (Pulkkinen, 2016, p. 6). Thus, in order for the Netherlands to effectively counter hybrid threats, most change has to happen at that level (Pulkkinen, 2016, p. 6).

Societal Relevance

Where the broad and ambiguous notions of hybrid warfare and hybrid threats prove problematic for analytical purposes, this characteristic is exactly what makes it socially relevant. Of course, regular warfare greatly impacts society as well, but its relative transparency facilitates the construction of effective countermeasures. Hybrid attacks, on the other hand, are often conducted more secretly. Take for example the recently attempted hacks of the OPCW headquarters in The Hague. While eventually discovered, the operation was

surrounded by a cloak of secrecy, supported by the Russian intelligence services. Disinformation campaigns by adversaries are present in several domains. In the political domain, for example, disinformation serves to steer the public opinion towards favourable political parties that advocate beneficial policies. According to a report published by the Dutch intelligence service (AIVD) in the summer of 2017, the same holds true for the Netherlands. One of the core findings suggests that digital attacks are being used to influence democratic processes (AIVD, 2017). In the civil domain, one can see the use of so-called fake news campaigns to influence the public (ibid). In the end, an intense and successful campaign could polarise opinions and cause public unrest. When, for example, such social unrest spreads into the political or economic domain, hybrid activities can be highly efficient. Acknowledging these developments, the literature has started considering the role of society in countering hybrid threats (Pynnöniemi & Saari, 2018; Van der Putten, Meijnders, Van der Meer, & Van der Togt, 2018). Solutions like strengthening resilience are presented as alternatives to traditional means of fighting warfare. To conclude, the growing influence of hybrid warfare beyond the military domain and the increased involvement of civil society in countering the threats make the following analysis socially relevant.

Academic Relevance

It should come as no surprise that the wide range of literature on hybrid warfare has also generated interest from different angles. Those different interpretations have led to a very broad discussion that touches upon very distinct elements of the topic. The same can be observed from the counter-strategy perspective. Resilience strategy has been widely studied, but different interpretations of resilience, as well as the threats it should counter, have generated widely different arguments. Most recently, “deterrence-by-resilience” has manifested itself as the “new kid on the block” (Lasconjarias, 2017). At the same time, however, certain elements seem to reoccur regardless of the chosen perspective. Since the novelty of hybrid warfare has been contested, one might think that traditional tactics could be sufficient to deal with it. Instead, consensus exists on the importance of dealing with hybrid threats at a strategic level. Additionally, many believe this strategy should be designed at a national level. This holds particularly true for resilience, which is widely acknowledged as being contextually dependent. Thus, the literature tells us that hybrid threats require resilience strategy designed by national governments. For the Netherlands in particular, we know that most studies have been done by think tanks in request of the governments. The main aim of

these works has been exploring the threat environment and providing some initial recommendations. Moreover, it is known that the Dutch government has a security strategy in place for the period 2018 – 2020. What the literature does not tell us, however, is anything about how it matches the broader literature. More precisely, the Dutch strategy has not been assessed in terms of its adequacy, it's strengths and weaknesses in relation to deterrence-by-resilience

Reading Guide

In order to answer the question to what extent the Netherlands can achieve a deterrence-by-resilience strategy, this thesis will first review the existing academic literature on hybrid warfare. First, the origin of the concept hybrid warfare will be traced, followed by an analysis of the post-2014 surge in academic literature about the Russian use of hybrid warfare. However, the review of literature on countering hybrid threats will be given most attention. There, the relevance of the strategic level will be emphasised, with a differentiation between military and non-military threats. The most prominent counterstrategy that will be reviewed is resilience. After a more general review of the literature on resilience as a counterstrategy against hybrid threats, the methodological challenge of resilience will be reiterated. In order to make sense of the link between deterrence and resilience, the review will continue by analysing the literature on hybrid warfare that has linked both concepts. By clarifying deterrence as deterrence-by-denial, resilience will be framed within the context of deterrence and the meaning of deterrence-by-resilience will be established. It is in that niche subject of deterrence-by-resilience that the analysis of this thesis can be placed. However, unlike the rather theoretical exploration of the ability of resilience to deter, this thesis will add to the literature by taking a more practical turn and applying the concept to Dutch policy.

After the literature review, a brief reflection on the concepts of hybrid warfare and resilience will be presented. The complexity of both terms requires further clarification that goes beyond the scope of the literature review. Different elements of hybrid warfare will be elaborated upon and resilience will be divided into three distinct types. That distinction, in turn, will help guiding the analysis, contributing to the relevance of that conceptualisation. Most of the analysis, however, will be guided by the theoretical framework. That framework will be divided into two categories. First, it will elaborate on what areas have to be made resilient against hybrid threats. The second category will elaborate on the elements important for any

resilience building effort. The relevance of social capital, cooperation and identifying one's vulnerabilities will be established there. For the analysis, this thesis will draw on two categories of documents. On the one hand, the analysis will start by considering the Dutch strategy against hybrid threats. The number of documents is limited to only three, of which only one not just mentions resilience, but also expands on its strategic relevance. Moreover, that document, the IFSS, suggests that Dutch resilience strategy is a government-wide effort. In order to explore that suggestion and draw any conclusions on the ability of resilience in the Netherlands to deter, the second part of the analysis will include documents outside the context of hybrid warfare as well. It will become clear that numerous Dutch ministries and agencies have resilience prominently embedded in a wide range of policies, by which a wide range of issues is addressed. The Dutch government can draw on that existing policy input to create a coherent response based on resilience that can counter the hybrid threats that it is facing. As it stands, however, that government-wide coherence is lacking, which significantly undermines the ability of resilience in the Netherlands to deter hybrid threats.

Literature Review

Broadly speaking, this review can be divided into two categories. The first category concerns the topic of hybrid warfare in general, reviewing how the academic literature has generally approached the matter. The second category will further explore the literature on countering hybrid threats in particular. The most widely studied perspective that can be observed in the literature on hybrid warfare is the Russian one. It is one of the most widely cited adversaries credited for the use of hybrid warfare. The Russian perspective has generated much academic interest, particularly focussed on analysing Russian hybrid strategies and the elements or forces that have driven the state to adopt these strategies (Chivvis, 2017; Cordesman, 2015; Giles, 2016; Lanoszka, 2016; Monaghan, 2016; Renz & Smith, 2016; Schwartz, 2015). The literature emphasises that countering Russia requires a better understanding of Russian hybrid strategy (Kasapoglu, 2015; Neneth, 2015). The key to understanding Russian strategy predominantly lies with an article written by the chief of the Russian General Staff: Valery Gerasimov. By now, this document has become known as the "Gerasimov doctrine" (Lanoszka, 2016; Monaghan, 2016, p. 65). It was Gerasimov's strategy that has guided the Russian involvement in Ukraine. The Russian success in Ukraine not only testifies to the strength of Russian hybrid strategy, it has undermined NATO's resolve on the international stage and caused the West to be "out-strategised" (Michta, 2014; Hersman, et al., 2017; Weitz, 2014). Generally speaking, there is one dominant reason for Moscow's supposed change in strategy that has undermined the West. Assuming that Russia would be unable to win a conventional war against NATO, the asymmetry and ambiguity of hybrid attacks could undermine Western dominance in the traditional domain, while still allowing Russia to achieve its strategic goals (Monaghan, 2016, p. 66).

The interest in the Russian perspective has made the term hybrid warfare real fashionable in the post-2014 era, representing the period after the Russian annexation of Crimea. Not only in academia, as Andrew Monaghan (ibid) observes, but also in the "wider public policy and media debate about Russian actions" the term formed the bedrock of analysis. As a result, many new disciplines joined the debate, widening the range of perspectives on the topic and allowing new counterstrategies to be considered as well. The term itself, however, was first introduced almost a decade earlier. In the beginning of 2006, Frank Hoffman (2006a) advised the United States' government on the potential upcoming characteristics of conflict. He cautioned the government that, in future conflicts, they would "face hybrid forms purpose build to exploit U.S. vulnerabilities" (ibid, n.p.). Here, the first steps towards a new distinct

concept in the security literature were made. Indeed, later that year, Hoffman (2006b) introduced the term "hybrid warfare" to make sense of the 2006 Lebanon War. In the following years, the term, along with its wide range of synonyms, came to be used to describe other conflicts as well. It has proven to be a useful concept to study the war on terror in Afghanistan and Iraq, as well as the Russia-Georgia war of 2008 and the history of threats coming from Iran (Shirreff, 2010; Cordesman, 2010a; Cordesman, 2010c). Despite these studies, it were the characteristics of the crisis in Ukraine that seemingly motivated academia to pursue this line of hybrid warfare more profoundly. This observation has led some scholars to question the novelty of the term. According to them, the notion of hybrid warfare merely represents "old wine in new bottles" (Ullman, 2015). Williamson Murray and Peter Mansoor (2012) are widely cited for their study of historical conflicts, going back "at least as far as the Peloponnesian War in the fifth century BC" (p. 3). All of these conflicts, they argue, have had characteristics of hybridity (ibid). Yet, it is emphasised that hybrid warfare is a "useful means of thinking about war's past, present, and future" (ibid, p. 1). The following paragraphs set out to review the core of the post-2014 debate on hybrid warfare, working towards deterrence-by-resilience as a counterstrategy.

Level of analysis

Throughout the literature, several levels of analysis have been applied to study hybrid warfare. From a national perspective, for example, the United States has generated particular interest. (Cordesman, 2010b; Hamre, 2016; Murdock, 2010). Above the national level, some scholars have taken a more regional approach, of which the Baltic states, due to their proximity to Russia, are the prime example. Nevertheless, the analytical level that has by far been studied the most is the international level, of which NATO and the EU have been the prime cases studied. The literature on NATO predominantly questions the changing nature of threats and the implications these have on the military alliance (McInnis, 2014; Michta, 2014). Collective defence against the Russian adversary forms the bedrock of the alliance. At the end of the Cold War, however, the military strength of NATO had significantly outgrown the strength of its Russian counterpart. Nevertheless, now that the dominance of the US is no longer self-evident and the Russian threat has manifested itself again, the alliance is under pressure. NATO's credibility is stressed and first and foremost it should get its traditional military might and willingness in order (Niblett, 2014). At the same time, however, the literature points out that it is not all so black and white. It is acknowledged that the alliance

has to reconsider its role in light of new threats, including hybrid ones, but this can only be done effectively if its military strength is beyond all doubt (Lasconjarias, 2017). In part because of this growing pressure on NATO, attention has turned to the potential role of the EU. This literature is mostly interested in the role the organisation could play in countering non-military threats and building resilience (Pronk, 2018; Pulkkinen, 2016, p. 6). Additionally, one can identify literature that looks at both organisations and aims to explore the possibility of closer NATO-EU cooperation and its potential in countering hybrid threats (Drent & Zandee, 2016, Mattiisen, 2016). Mostly cited as a crucial domain of cooperation is the information domain. Both organisations could benefit from a better situational awareness. (Major & Mölling, 2015; Shea, 2016). Information sharing would also have the benefit of improving some much-needed political unity (Major & Mölling, 2015).

Counterstrategies

The complexity and ambiguity surrounding the notion of hybrid warfare is widely accepted throughout the academic debate. Realising the urgency of the matter has led many authors to ask the question how to deal with such complex and ambiguous threats. Effective counter-strategies appear to be as necessary as they are challenging to design. At the same time, consensus exists in the academic community that hybrid threats require addressing at the strategic level. In order to understand what the strategic level is, this thesis will use the definition used by the renowned scholar Lawrence Freedman (2013, p. XI), who clarified that a strategy is about "maintaining a balance between ends, ways, and means". More precisely, it is "about identifying objectives; and about [allocating] the resources and methods available for meeting such objectives" (ibid). Within the context of this research, the method used for achieving objectives is resilience. Strong strategies look at the larger picture, without allowing short-term distractions to cloud the long-term objectives (P. IX-X). Moreover, that means looking at the essentials. There should be an ability to adjust ends to make them better achievable given available means and capacity (ibid). On the relevance of looking at the strategic level for measures countering hybrid threats, the literature writes that governments should urgently provide more strategic clarity (Shirreff, 2010, p. 3). The uncertainty that hybrid threats bring along requires governments to agree on, and articulate, the desired political end state (ibid; Johnson, 2018, p. 158). In particular, Robert Johnson (ibid) emphasises that new strategies should shift their focus more to the non-military side of hybrid threats.

Besides the non-military side of hybrid threats, however, it should be noted that the military side has also been discussed in the literature on counter-strategies. More precisely, a wide range of literature suggests that existing military strategies and planning schemes no longer fit the challenges at hand. In order for national militaries to be more effective, some scholars propose to improve education and learning capacity, which ultimately serves to create a better understanding of hybrid threats and their amorphous character (Hajduk, 2017; Hoffman, 2009; Hoffman, 2007; Kasapoglu, 2015). When strategists better understand where those hybrid threats are coming from, they can act accordingly, instead of constantly responding to hybrid threats after their manifestation (Neneth, 2015). Nevertheless, Piret Pernik and Eve Hunter (2015) warn that none of the above would be possible without first changing the legal and political means available to implement the required changes. This particularly relates to the secrecy surrounding hybrid threats and the relatively new domain in which a lot takes place: the cyber domain.

On the non-military side of hybrid threats, the need for strategic change is equally emphasised. The authors are largely on the same page when it comes to the strength of existing strategies. These are simply insufficient. As early as 2007, Hoffman warned that hybrid warfare requires us to "change how we think about strategy" (p. 51; Hoffman, 2009). Especially at alliance level, there is much concern about the adequacy of existing strategies, which are undermined by recent hybrid threats (Hartmann, 2017, p. 2). Broadly speaking, new NATO strategy has to be more flexible (Michta, 2014). To achieve greater flexibility in terms of the available means, NATO should cooperate with the EU on a strategic level (Hamilton, 2017). In doing so, it would broaden the scope of tools available to the organisation and having more tools ultimately creates strategic flexibility (ibid). Indeed, those elements or strategic principles of flexibility and cooperation have been identified as critical elements of any strategy countering non-military threats. From an international perspective, it has been observed that global interconnectedness allows the effect of an event to easily cross borders. As such, a vulnerability in a relatively distant state could become a vulnerability for the entire international system. Consequently, governments should cooperate and assist each other by providing preventive assistance when needed (Dalton & Shah, 2017; Cordesman, 2010b). At the lower national level, different departments and agencies should actively share information and construct comprehensive counter-strategies (Shirreff, 2010; Giles, 2014; Weitz, 2014). Such an approach, in which all available means aligned, is described as a whole-of-

government approach (Ducheine, 2016, p. 9). According to some scholars, those strategic principles are currently lacking in Dutch policy. Paul Ducheine (2016) warns that the Netherlands does not yet have a sufficiently coherent and integrated security strategy to deal with hybrid threats (p. 7). Van der Putten et al. (2018) elaborate and write that the strategic scope should widen and integrate other domains, for example the economic one, as well (p. 13).

On top of the elements of flexibility and cooperation, the literature on countering hybrid warfare has added one more feature that should be incorporated: communication. This particularly holds true for secrecy and disinformation campaigns, which form an integral part of hybrid threats. In response, communication has been put forward as a crucial element of counter-strategies. Giles et al. (2015) argue that more time and money should be invested in strategic communication. Hybrid warfare could be seen as a battle for the hearts and minds of people, which can only be accomplished by transparent and unambiguous communication (ibid). A very concrete example of better communication is discussed by Anton Shekhovtsov (2015), who argues in favour of an EU-based Russian language TV channel. As the previous paragraphs have already hinted at, the key to accomplishing the ambitious strategic goals and strategic communication lies in cooperation. This is true for both the national and international level.

Resilience

Arguably the main strategy to counter hybrid threats that has been explored throughout the academic literature centres around resilience. Many authors believe that resilience could be a very promising counterstrategy, especially at the national level (Brinkel, 2017; Bilban, 2016; Lasconjarias, 2017). This means that research and the designing of strategy and policy has to be contextually dependent (Cavelty & Prior, 2013; Hanisch, 2016; Svitková, 2017). Different states have different strategic cultures, which makes it imperative to keep the designing of new strategies at the national level (Major & Von Voß, 2016, p. 5). One of the core reasons cited for this focus on the national context relates to the differences in national vulnerabilities. National differences in political, social and cultural characteristics influence resiliency policy, thus making a national lens even more important (Dunn-Cavelty, 2013, p. 2). Matti Pulkkinen (2016) adds that national vulnerabilities are a national responsibility. States can attempt to identify and resolve vulnerabilities at, for example, European or alliance level, but as long as

national vulnerabilities are not resolved, they will continue to pose a threat for the entire Union (ibid; de Graaf, 2016). At a conference about deterrence and resilience, several U.S. government officials emphasised that the resilience of partner states against grey zone operations is of crucial importance to the national security of the U.S. (Connable, 2018, p. 5).

When zooming in on hybrid threats and resilience at the national level, it becomes clear that the political system of different states has been identified as a factor influencing the importance of resilience. When it comes to hybrid threats, the openness of democratic societies is seen as a liability, which makes states with such political systems particularly vulnerable compared to their non-democratic counterparts (Major & Mölling, 2015; Van der Putten et al., 2018). The Baltic states, for example, which house a large Russian population, are particularly concerned about the potential of Russian interference (Major & Mölling, 2015). Thus, the democratic system, characterised by open societies, makes a state vulnerable to hybrid threats, while at the same time limiting the number of countermeasures possible. As Van der Putten et al. (2018) argue, "addressing threats from hybrid conflict and political influencing involves fundamental dilemmas that relate to the balance between openness and security" (p. 3). To mitigate this threat, prevention is crucial. In other words, trying to prevent political influencing requires building resilience (Major & Mölling, 2015, p. 3).

On top of the literature that has looked more at the relevance of resilience, others have studied the conceptual and methodological challenge of the term. While resilience is widely used in national and international strategies, those studies have found that the use is rather superficial, without much conceptual and methodological depth. A study by Katarina Svitková in 2017 has shown that international organisations like the EU and NATO, just like the national governments of the US and the UK, have all significantly increased their use of the term resilience. By analysing official government discourses in the form of policies and official communications, however, the author has found that they use the term "to make sense of the complex security environment" (ibid, n.p.). In other words, there is a new challenge, the hybrid challenge, but its complexity has prevented profound and detailed application of resilience. The review has shown that academia has observed that as well, which has encouraged some scholars to explore that methodological challenge. In order for researchers to deal with the contextual challenge, and make the "ambitious discourse of resilience" translatable, several authors propose a framework of questions to guide policy makers towards actionable policies (ibid). Consensus exists on the first two questions to be asked:

who or what needs resilience and how to build it (Cavelty & Prior, 2018, p. 2; Hanisch, 2016, p. 3). To add to these questions, Michael Hanisch (ibid) proposes to look at the actors responsible for the building of resilience and to ask why resilience is necessary. Myriam Cavelty and Tim Prior (2018, p. 2), on the other hand, assume this actor to be known, but suggest to first analyse how resilience is expressed by the responsible actor, and then to establish ways to measure and monitor resilience. Approaching resilience in such a structured way allows for greater contextual flexibility in the process of designing counterstrategies of resilience (Bilban, 2016).

Deterrence-by-resilience

As the role of resilience in the literature on hybrid warfare became increasingly prominent, a growing number of scholars started to connect it with the more traditional domain of deterrence. In this thesis, deterrence will be understood as a strategy that tries "to prevent a conflict by convincing a potential adversary that the consequences of its actions … will outweigh the potential gains" (Takacs, 2017, p. 1). In other words, deterrence is a cost-benefit analysis conducted by one's adversaries to determine the consequences of an attack. Since complete resilience would never be possible, the idea that negative effects of a hybrid attack may already be mitigated by high levels of resilience has appealed to academia as well. Hence, the question arises if resilience could serve as a deterrent against hybrid threats. Indeed, it should be noted that many scholars agree there exists a link between deterrence and resilience, particularly because high levels of resilience are seen to deny potential adversaries any gains from their attacks (Brinkel, 2017; Cullen & Reichborn-Kjennerud, 2017; *Deterrence by Resilience*, 2018; Giegerich, 2016, Meyer-Minneman, 2017; Pernik & Jermalavičius, 2016; Radin, 2017; Shea, 2016; Takacs, 2017). This kind of deterrence, where an adversary is not deterred based on the risk of high costs, but because of the denial of any gains, is known as deterrence-by-denial.

While the concept of deterrence is widely used, it is in fact an aggregate term used to describe two distinct ways to deter: deterrence-by-denial and deterrence-by-punishment. The former means to manipulate the calculation of prospective gains, while the latter is about the prospective costs (Freedman, 2018). The term "deterrence-by-denial" was first used in 1960, when it was described as "the capability to deny the other party any gains from the move which is to be deterred" (Snyder, 1960, p. 163). Today, the same definition, though

sometimes in slightly different wording, is still being used (Knopf, 2010; Rühle, n.d.; Pernik & Jermalavičius, 2016). Resilience becomes part of the equation when the how-question is discussed. Because resilience is not an act that inflicts costs on an adversary, but rather an internal ability to deal with certain shocks, it can best be placed under the heading of "deterrence-by-denial". Indeed, Pernik and Jermalavičius (2016, p. 3), note that "resilience can be seen as an ingredient of deterrence by denial".

Throughout the literature that has considered resilience as a counterstrategy against hybrid threats, resilience and deterrence have been linked by several authors, each highlighting a different perspective of that link. First, Theo Brinkel (2018), looks at moral as an important element of resilience. Seen from this perspective, the willingness to deter, and therefore the credibility of the deterrence as well, are higher when there is a high moral level (ibid). Secondly, Guillaume Lasconjarias (2017), observes that traditional deterrence still lies in the hands of national militaries, but as a result of the civilianisation of military assets over the last couple of decades, civil resilience has become a crucial element of traditional deterrence (p. 4). Finally, Christoph Bilban (2016) brings slight nuance to the link between resilience and deterrence. He notes that "resilience at least promises to lower the effects of hybrid attacks" in the cyber and information domain, but is not sufficient of its own to deter an adversary (ibid, p. 12). To this end, traditional hard power is still indispensable (ibid).

To clarify the relation between deterrence and resilience, Prior (2018) considers resilience as the "fifth wave" of deterrence. In response to the growing unpredictability and uncertainty of the post-Cold War strategic landscape, a new, fourth wave, of deterrence emerged that started looking at deterrence from the perspective of denial. However, while placing the first steps towards a better understanding of deterrence, the continued uncertainty of the post-Cold War order caused a failure to understand the threats, making it difficult to determine what to deter (ibid). Not only is this the point where resilience comes in, Prior (ibid) even goes as far as arguing that its dominance creates a new, fifth wave, understanding of deterrence. Thus, says Prior (ibid), the uncertainty of achieving one's goals that is created by resilience is exactly what gives it its deterrent capacity (p. 68).

It is in the context of that fifth wave that scholars have taken resilience beyond the context of deterrence-by-denial and consider it as a deterrent of its own. They have introduced the term "deterrence-by-resilience" as a way of understanding counter-strategies against hybrid threats

(Lasconjarias, 2017; Rühle, 2016; Shea, 2016). While no concrete definition of "deterrence-by-resilience" exists yet, one might wonder if a definition of this type of deterrence is necessary. Irrespective of the different types of resilience, all types ultimately prevent an adversary from reaching its intended goals. Thus, linking the existing knowledge on deterrence-by-denial with new observations on resilience and its applicability to the topic of hybrid warfare, has led some scholars to create deterrence-by-resilience as a distinct concept in the security literature (Lasconjaris, 2017; Rühle, 2016; Shea, 2016).

Conceptual framework

Hybrid Warfare

Not only is the practice of hybrid warfare highly complex and difficult to summarise in one definition, the proposed counterstrategy of resilience is conceptually an equal challenge. Providing some conceptual clarity is therefore crucially important. First to be defined is "hybrid warfare". Throughout the literature, the concepts of "hybrid warfare", "hybrid conflict" and "hybrid threats" are used intertwined. Nevertheless, all touch upon largely the same elements. All those relevant elements will be individually discussed below. Based on these elements, the definition by Hoffman (2009) comes closest to a coherent and all-encompassing conceptualisation:

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

When structured in order of appearance, the combined use of military and non-military means is the most widely agreed upon element of the definition. On some occasions, no further differentiation beyond the lines of military and non-military is made (Mattiisen, 2016; Metrick & Hicks, 2018, p. 5; Van der Putten, Meijnders, Van der Meer, & Van der Togt, 2018, p. 1). Most, however, have further specified the meaning of military means. Here, many refer to the difference between conventional and unconventional (McCulloh, 2012, p. 24). Here, it should be noted that unconventional is not always the chosen word. Terms like "irregular", "asymmetric" and "insurgency" are used intertwined, predominantly to emphasise the importance of non-state actors in fighting hybrid warfare (Shirreff, 2010, p. 2; Golovchenko, Hartmann, & Adler-Nissen, 2018, p. 980; Glenn, 2009; *The European Centre of Excellence for Countering Hybrid Threats*, n.d.). When it comes to the non-military side of the hybrid coin, two observations stand out. First, some have placed particular emphasis on the importance of criminal activity (Shirreff, 2010, p.2; Glenn, 2009; Hoffman, 2009). Most, however, view the non-military means as multimodal, including the domains of information, political, economic and civil (Golovchenko, Hartmann, & Adler-Nissen, 2018, p. 980; Glenn, 2009; *The European Centre of Excellence for Countering Hybrid Threats*, n.d.).

The use of non-military means alone, however, does not create the degree of hybridity that gives hybrid warfare its name. Instead, one should also look at the way in which the two

means are used. Adversaries who conduct hybrid warfare use several different means in a simultaneous way. The *European Centre of Excellence for Countering Hybrid Threats* (n.d.) emphasises that hybrid attacks are centrally coordinated and the resources deployed in the attack are used in a synchronised fashion. Van der Putten et al. (2018) define the simultaneity of hybrid warfare along similar lines, but name at an "integrated use of means and actors" (p. 1). According to Lanoszka (2016), more importance should be given to the role of military instruments. This means that non-military tools are only suitable when they are simultaneously backed by hard power deterrence of military attacks (p. 178). Earlier, it has become clear that context plays an important role, not just for resilience, but also for hybrid warfare. As a result, the means deployed by an adversary are not only used simultaneously, but adaptively as well (Glenn, 2009; Hoffman, 2009). It is the context in which an hybrid attack is conducted that determines which combination of means is used. Finally, Shirreff (2010) believes that the right use of different means in a dynamic combination is what gives hybrid warfare its strength (p. 2). This dynamism provides a first step towards understanding hybrid warfare as capable of creating synergetic effects. Indeed, McCulloh (2012) points out that the unique cultural contexts in which hybrid attacks take place, provide the opportunity to optimally combine military and non-military means (p. 24). Thus, when coming together at the right time and on the right moment, synergy is created (ibid). This, in turn, particularly holds true when one takes into account your target's vulnerabilities and takes advantage of them (Mattiisen, 2016).

The final element to clarify has arguably generated most discussion. This has to do with the word "warfare". When considering war as the result of horizontally escalating different means beyond the threshold of war, hybrid warfare is conducted in the grey zone between war and peace. That the zone between war and peace is a grey one is widely agreed upon. Metrick and Hicks (2018) write that hybrid activities "fall in the miasma between clear war and certain peace" (p. 5). Additionally, Van der Putten et al. (2018) point out that clear war is established by a legal threshold of open armed conflict (p. 1). Nevertheless, it is named a grey zone for a reason. Adversaries make clever use of the ambiguities in this area. As Schaus, Matlaga, Hicks & Conley (2018) observe, hybrid attacks make use of military force, but refrain from using "sizeable" force in order to achieve their intended goals (p. 1). Thus, hybrid warfare is said to "exploit the thresholds of detection and attribution" that surround the threshold of war (*The European Centre of Excellence for Countering Hybrid Threats*, n.d.).

Resilience

The notion of resilience has a long history of use in many different domains. As a result, different conceptualisations exist. Within the domain of security studies, the concept is often used without much conceptual consideration. Nevertheless, as Brinkel (2018) observes, resilience is highly complex and can be understood from three distinct perspectives: engineering, adaptive and transformative resilience (p. 374-376). Throughout the literature, some authors have adopted a more exhaustive understanding of resilience, combining all three elements in one definition, while others use a more restricted definition based on one, or perhaps two, elements. According to Lasconjarias (2017, p. 2), resilience is generally understood as "the ability of the community, services, area or infrastructure to detect, prevent, and, if necessary, to withstand, handle and recover from disruptive challenges". While it might seem as a complete definition that combines the engineering and adaptive types of engineering, it makes no reference to the transformative type. A more comprehensive and exhaustive definition comes from the domain of psychology. An often cited definition was presented by psychologist Rodin (Brinkel, 2018, p. 374), who defined resilience as the ability of a unit to prepare for shocks, to recover from shocks, and to adapt and grow after a shock or attack. Predominantly because of the complexity of both hybrid warfare and resilience, it is important to shed light on all the different types that have been used as a conceptual lens to study hybrid warfare.

Without a doubt the most often cited type of resilience is also the most traditional view of it: "engineering resilience". The most important characteristic of this type is its focus on the actual shock or attack. According to this view, a unit is resilient when it has the ability to both maintain status quo or to recover quickly and move back towards status quo as quickly as possible after having endured an attack (Brinkel, 2018, p. 375). Indeed, the ability to recover or "bounce back" is often cited as a core element of resilience (Giegerich, 2016, p. 69; Major & Mölling, 2015, p. 3; Balzacq, 2014, p. 170; Fjäder, 2014, p. 115; Lasconjarias, 2017, p. 2). While a crucial element, the ability to bounce back alone is not a sufficient condition of engineering resilience. The second element is about what has to recover from an attack. In this light, several scholars point to the role of continuity. If one is not able to maintain the provision of basic functions, an actor has to be able to re-establish this ability as quickly as possible (Giegerich, 2016, p. 69; Balzacq, 2014, p. 170; Cavelty & Prior, 2013, p. 1; Resilience, n.d.).

In contrast to the attack-driven concept of engineering resilience, the adaptive view looks more at the situation before an attack, where hostilities and threats manifest themselves. Brinkel (2018, p. 375) defines adaptive resilience as the ability to adapt the current threats and to prepare for future, possibly unknown, attacks. The literature does not add much to this view. In sum, it is about first detecting threats, followed by the ability to manage those threats by adapting, which ultimately serves to anticipate or even prevent an attack (Giegerich, 2016, p. 69; Lasconjarias, 2017, p. 2; Prior, 2018, p. 64).

While most of the definitions are limited to the elements discussed so far, some take it one step further and look at resilience as the ability to transform. In a more abstract sense, transformative resilience should not be seen as the ability to respond to new threats, as was the case with the previous forms, but instead as transforming beyond those threats and elevate above the threat environment (Brinkel, 2018). In other words, it moves beyond the status quo and should be seen as the ability to transform when new threats have rendered existing structures untenable (ibid, p. 376). While adhering to a different concept, "resilience as renewal", Bourbeau (2017) further clarifies our understanding of transformative resilience. According to him, it "means that disturbances would play a triggering role in a sustained and systematic effort to change profoundly a given policy or how a society understands and interprets a particular set of issues (p. 30). Finally, it should be noted that learning capacity is considered a crucial element of the ability to transform or change profoundly (Prior, 2018, p. 64).

Theoretical framework

In February 2016, NATO defence ministers met to discuss the role of resilience in future NATO strategy. In line with the guiding questions by Cavelty & Prior and Hanisch, they came up with seven areas, systems or capabilities that have to be made resilient (Meyer-Minnemann, 2017, n.p.). These areas are as follows:

- Continuity of Government;
- Resilient Energy Supplies;
- Resilient Civil Communications Services;
- Resilient Food and Water Supplies;
- Ability to Deal with Large Scale Population Movements;
- Ability to Deal with Mass Casualties;
- Resilient Civilian Transportation Systems.

Throughout the literature on resilience, the question of who or what should be made resilient has returned on numerous occasions. Most of the time, one area was singled out and further elaborated on. Out of NATO's seven domains, four require further review. Broadly speaking, one can categorise energy supplies, civil communications services and food and water supplies under the heading of critical infrastructure. According to Christian Fjäder (2014), the prominence of critical infrastructure comes as no surprise, as it should be regarded as a result of a process of securitisation. New challenges, characterised by complexity and uncertainty, have emerged as a result of globalisation and critical infrastructure has been part of this process as well. Consequently, resilience has become increasingly regarded as a new strategy to meet these challenges (ibid). In fact, he even argues that the securitisation of critical infrastructure has facilitated a paradigm shift from a traditional national security approach to a resilience approach (ibid, p. 128). The urgency of improving critical infrastructure resilience seems to resonate through the US government as well. In an interview with representatives of different departments conducted by the Center for Strategic and International Studies (Responding to Russia, 2018), its importance was stressed on numerous occasions.

Continuity of government, which constitutes the first area of attention, deserves some consideration of its own, particularly because it seems to touch on different elements or topics discussed throughout the literature. First of all, there is the element of communication. In 2018, Van der Putten et al. published a report to advice the Dutch government on possible measures to take against hybrid threats. When it comes to communication, they advised to ensure the ability of the government to "talk to its own people despite interference measures seeking to prevent it from doing so" (p. 7). In other words, a resilience of communications is

advocated, which is in line with what the “continuity of government”-principle stands for. On the other hand, a continuity of government could also be linked with the resilience of the political spectrum. In particular, this has to do with political influencing, of which we have seen the effects in the 2016 US’ presidential campaign. Keir Giles (2016) phrases this nicely: “Sub Article 5 interventions need resilience, not troops” (p. 55). By the sub article 5 interventions he was referring to Russian political influencing, particularly in the Baltic States, but to a lesser degree in Russia’s entire near abroad as well. The more influence an adversary has on national politics, the more it can influence the government, which will ultimately threaten the continuity of government as well (ibid; Radin, 2017).

By now it is clear that a wide range of actors, systems or domains are advised to be made resilient. Next, the question arises how to do so. From the literature, one can distil two frameworks between which significant overlap exists. Uwe Hartmann (2017) proposes seven principles in strategy-making that could help building and strengthening resilience. The list is as follows:

- Being self-critical;
- Understanding strategy-making as a permanent process;
- Respecting all stakeholders involved;
- Involving societies;
- Arguing about the truth instead of pursuing national interests;
  (“the best way to enhance support of the people” p. 5)
- Educating and selecting the right personnel and emphasizing mission command;
- Revitalizing the comprehensive approach.

Secondly, Liliana Filip (2017) proposes six elements that are important when countering hybrid war strategy. In essence, she argues that the presence of these elements, which are considered building blocks of resilience, could serve as a deterrent against aggressors:

- High level of critical thinking;
- Strong sense of belonging;
- High level of civic participation;
- High levels of economic development;
- The ability of critical infrastructure to absorb the impact of sabotage or attacks;
- Sufficient and quickly accessible financial capital, basic needs and technical resources.

Before addressing the similarities, some remarks are in order. The fifth principle in Hartmann's framework on "arguing about the truth" carries less significance at the national level, since it relates to cooperation at NATO alliance level. Turning to Filip's framework, the final three stand out. The element on economic development tells us that the economic domain is important to be considered, something that was briefly touched upon in the literature review, but a thorough analysis of Dutch economic strategy goes beyond the scope of this thesis. Secondly, the fifth element on critical infrastructure is important, but it relates back to the earlier question on what has to be made resilient. The final element is slightly trickier to position. It can best be regarded as another confirmation that critical infrastructure, in a broader sense of the word, has to be made resilient.

As was the same with the NATO framework on what has to be made resilient, Hartmann's principles and Filip's elements have been discussed throughout the resilience literature as well. Understandably, semantics might differ, but the bullet points that have not been discussed in the previous paragraph, have all been given significant attention in other works. Broadly speaking, the principles can be divided among three categories: social capital, vulnerabilities and cooperation. The first one, social capital, has been linked with resilience by several authors. Amongst others, it features prominently in the work of Dutch scholar Brinkel. According to him, resilience is partly about sharing universal values that give the moral strength necessary to defend ourselves (Brinkel, 2018). In an earlier article, he dives further into this connection between resilience and the culture of society by introducing the work of Bourbeau. What Bourbeau calls the "cultural regime" of a society, the mind-set and morale, influences the expectations people have of a certain emergency (Brinkel, 2017, p. 30). Consequently, when an event actually unfolds, it are those expectations that determine the societal response (ibid).

When it comes to the question how to construct societal values, at first sight a daunting task, the literature points towards the role of politics. If a government wishes to implicate society in new policies, an idea of which the importance has been established before in the context of hybrid warfare, it is also up to the government to bring society on board (Durodié, 2004, p. 14). More specifically, it would require a "political debate over societal values … to re-engage the public" (ibid). In the end, such debate serves the purpose of giving society a direction, instead of allowing it to be directed by opponents (Durodié, 2007, n.p.). Crucial in this regard is to constantly uphold the highest levels of transparency possible (Chivvis, 2017,

p. 9). With that addition, it directly links with the fourth principle of involving society, but also with the third on involving all stakeholders. The idea is that all actors, including private actors and civil society, should be granted a seat at the table to enhance mutual trust (Hartmann, 2017, p. 4). In an open society, many ethnicities and religions often live side by side, without much physical separation, and the openness provided by democracies allows for each and every group to express their opinions. It is important for these minorities to be included at all times, in order to prevent them from being driven into the hand of the opponent (Major & Mölling, 2015, p. 3). Additionally, the literature on social capital could also be seen as support for the Filip's second and third element on a sense of belonging and civic participation.

In the literature, resilience and weaknesses, or vulnerabilities, are widely discussed and often considered as closely intertwined. The position of "being self-critical" at the top of Hartmann's list thus comes as no surprise. Moreover, observing that "critical thinking" is at the top of Filip's list testifies to its relevance as well. Here, intelligence plays a crucial role. In order to be critical, it is important to constantly gather and critically analyse intelligence (Chivvis, 2019, p. 9). In line with Hartmann's recommendation to identify the internal weaknesses, Giegerich (2016) proposes to prioritise a process of systematically identifying vulnerabilities and connects this process with stronger resilience (p. 70). Indeed, Hanisch (2016) argues that resilience is about acknowledging vulnerabilities. Thus, when a crisis occurs that targets a vulnerability, people are prepared and can more easily mitigate the negative effects (ibid, p. 3).

When it comes to countering hybrid threats, cooperation is often cited as a crucial part of any strategy. Hartmann as well does not shy away from recommending cooperation on numerous occasions. Though in slightly distinct forms, a total of three principles relate to cooperation: understanding strategy-making as a permanent process, educating and selecting the right personnel and emphasising mission command, and revitalising the comprehensive approach. The first one about the permanent process highlights the need for constant sharing of information, the second requires selecting personnel from different domains and disciplines which would normally not work together, and the last serves to achieve better cooperation (Hartmann, 2017, p. 5-6). Considering all three as examples of increased cooperation might seem to stretch the concept, but it does represent the broader literature. For example, Jeffrey Rathke (2016) has written about Germany's new security strategy, with a focus on the internal

dimension. Germany has emphasised “statewide security and national resilience” as the core pillars of its new strategy that deals with, amongst others, hybrid threats (ibid, n.p.). As part of this strategy, the Bundeswehr has to cooperate more with internal law enforcement and other civil partners (ibid). Similar efforts of interagency cooperation are advised by Christopher Chivvis (2017, p. 8) to the U.S.’ government. On the other hand, the Russian hybrid threat has forced Finland to invest significantly in international cooperation, not national (Pynnöniemi & Saari, 2018). In a conference organised by the Center for Strategic and International Studies in the summer of 2018, participants agreed that states should operate more in concert with their allies, in order to enhance the effectiveness of individual efforts (Schaus, Matlaga, Hicks & Conley, 2018, p. 1). Moreover, at a national level states are advised to include all societal actors and approach hybrid threats from a concerted whole-of-society angle (ibid, p. 3). Indeed, Prior (2017, p. 4) adds that years of privatisation have made militaries increasingly dependent on civil society, and for them to defend national territory they have to cooperate with each other.

So far, the what and how of resilience has been discussed, but to what extent does this inform about the relation between deterrence and resilience? Do the principles of resilience strategy relate to deterrence strategy? According to the conclusions of a deterrence conference (Connable, 2018) attended by representatives of the U.S. Department of State and Department of Defense, it does. These conclusions include but are not limited to: a whole-of-government approach, better intelligence, good governance and understanding the human domain (ibid, p. 6). Combined, these conclusions form a “comprehensive” deterrence strategy. Remember the elements of social capital, cooperation and vulnerabilities that made up the core of resilience strategy. The whole-of-government approach relates to the element of cooperation, the need for better intelligence relates to the element of vulnerabilities and good governance and understanding the human domain relate to the element of social capital, be it in a slightly indirect manner. Building on the link between deterrence and resilience which was introduced in the literature review, this overlap once again shows the potential of a deterrence-by-resilience strategy. One final remark is in order here. The “comprehensive” deterrence strategy discussed above particularly addresses non-military threats. The success of this strategy remains contingent upon the strength of conventional deterrence. This should be upheld at all times (ibid; Bilban, 2016; Major & Mölling, 2015).

Analysis

Hybrid Warfare Documents

So far, this thesis has provided the theoretical background relevant for understanding deterrence-by-resilience as a strategy against hybrid threats in The Netherlands. This chapter will use that theoretical framework and apply it to existing Dutch counterstrategy against hybrid threats. In particular, an interest in the prominence and use of resilience as a strategic principle will guide the analysis. In order to conduct it, attention will first be paid to government documents particularly addressing countermeasures against hybrid threats. It should be noted here that the government publications on hybrid warfare used for this analysis will be limited to those specifically addressing countermeasures. While more documents exist, they merely mention or analyse the actual threat, without elaborating on possible countermeasures.

As the study of hybrid warfare strategy will show, attention will also be paid to government-wide documents addressing resilience. Already from the theoretical background, it became clear that a whole-of-government perspective to both hybrid threats in general, and resilience as a countermeasure in particular, would improve strategy. Additionally, it will become clear in the following paragraphs that Dutch hybrid warfare strategy also suggests that resilience is also being used beyond the context of hybrid threats. Thus, broadly speaking, the analysis will consist of two categories: documents on hybrid warfare and government-wide documents. The nature of the documents will differ. Most documents are long-term agendas, policies, and strategies of different Dutch ministries and agencies, others are parliamentary letters that clarify a certain policy, and a few can best be characterised as information leaflets. While some concepts may be used intertwined, they all have in common that they are documents written by the Dutch government and either relate to the topic of countering hybrid threats, or to the topic of resilience. In both the categories of hybrid warfare and government-wide, the documents will be analysed for their understanding of the term resilience, as well as the prominence of resilience as a strategic element in those documents. Lastly, for reasons of accessibility, it should be stated here that this thesis will only work with public documents. Especially strategies on hybrid threats are likely to be undisclosed for reasons of national security. The same holds true for strategic documents on resilience that might exist within that context of hybrid threats.

An analysis of the databases of ministries and agencies concerned with Dutch national security policy, reveals only a limited number of policies and strategies on countering hybrid threats. Only three documents specifically elaborate on the different countermeasures that are possible against the hybrid threats that the Netherlands are facing. The first one is the Integrated Foreign and Security Strategy 2018-2022 (IFSS) published by the Ministry of Foreign Affairs. The second document comes from the Ministry of Defence, which published its strategic plans in the Defence Note of 2018. Third, and most recently, the NCTV published an information leaflet on what they call the "phenomenon" of hybrid threats, which also includes a list of possible ways to defend against them. The analysis will start with a brief description of how hybrid threats are understood in the documents, along with an overview of the main challenges to counter hybrid threats. After that, the analysis will turn to resilience, describing the contexts in which the hybrid warfare documents mention resilience. Furthermore, it will be followed by an analysis of how the different hybrid warfare documents look at the ability of resilience to counter hybrid threats. Finally, after a brief analysis of how resilience is understood, it will become clear that each of the documents introduced above mentions resilience as a countermeasure against hybrid threats, but especially the IFSS also contains elements that suggest one should look beyond the context of hybrid threats to understand the role of resilience in Dutch policy making.

Before expanding upon the use of resilience throughout the hybrid warfare documentation, this paragraph will first provide a brief introduction of how the IFSS, the Defence Note and the NCTV leaflet understand hybrid threats and some general strategic principles addressed within them. The IFSS states that technological developments and growing connectivity have made technology more easily accessible and cheaper, which has made it easier to simultaneously deploy different instruments in a concerted fashion (p. 16). Similar observations are made in the NCTV leaflet, which complements with the comment that actors are increasingly agile in their concerted use of a wide range of instruments. (p. 6). The IFSS then proceeds to acknowledge that existing regulation in the digital and information domain is insufficient (ibid). Specifically, it proposes to invest in cyber, intelligence, strategic communication, maritime security and counterterrorism (p. 30). Moreover, political unrest and divide, of which Brexit is cited as a key example, are seen as a threat to international cooperation, which also undermines cooperation on the topic of hybrid warfare (p. 32). If the Netherlands would fail to effectively address hybrid threats, it could lead to a vertical escalation of conflict (p. 20). This is where the Defence note comes on. Broadly speaking, the

note emphasises the need to develop the armed forces into an organisation driven by information, capable of fighting high-tech adversaries (p. 7). In this regard, three specific countermeasures are proposed. First of all, deployment of the armed forces has to be versatile and capable of responding to threats of different intensity (p. 14). Related to this goal is the objective of modernising the range of weapon systems, but also the organisational technology, think of IT-infrastructures, is cited a countermeasure (ibid).

Resilience

On top of some of the countermeasures discussed above, the IFSS, the Defence Note and the NCTV leaflet also specifically mention resilience as an element of their counterstrategies. In fact, resilience is even stressed as one of the core elements of the IFSS (p. 10). However, of those three documents, the Defence Note and some parts of the IFSS also discuss resilience outside of the context of hybrid warfare. First, resilience within the context of hybrid warfare will be discussed. The IFSS significantly expands on the growing activity of foreign actors, who are seeking to influence internal processes from abroad. More than anything, the strategy places great emphasis on the importance of resilience to counter such foreign influencing (p. 34-35). Additionally, the IFSS mentions resilience as an element of countering the proliferation of new high-tech weapons, including nuclear and biological weapons (p. 28-29). Furthermore, the NCTV leaflet, which is completely dedicated to hybrid warfare, mentions resilience on a few occasions and all of them are in the context of countermeasures. This will be elaborated upon in the following paragraph, which analyses how resilience should be build according to these three documents. Beyond the context of hybrid warfare, however, resilience also plays a role in the Defence Note and parts of the IFSS. The Defence Note touches upon it once. It emphasises the intention of the department of defence to reassess the civil-military cooperation with the department of justice and security. It cites a desire to increase resilience of society and vital infrastructure as core reason for this cooperation (p. 15). The context in which this measure is proposed is not exclusively linked to hybrid warfare. Instead, it is a response to the changing threat environment, of which hybrid threats are just one element. In the IFSS, resilience is mentioned without even an indirect link to hybrid threats. Instead, it is discussed as a measure to protect against different threats. First, resilience is mentioned in the context of terrorism and radicalisation. Here, it is pointed out that vulnerable youth has to be made resilient against jihadi influencing (p. 27). Finally, while only marginally touching upon this, the IFSS proposes resilience building to protect the rule

of law, but specifically ascribes this to developing states. Particularly, resilience could serve as a countermeasure against violence, corruption and undermining efforts (p. 39). In general, the analysis presented above suggests that an analysis of the state of resilience in The Netherlands as a deterrent against hybrid threats should look beyond just the context of hybrid warfare.

Next, the hybrid warfare documents propose several practices that could serve to build resilience. Since these practices often cross the boundaries of individual threats, they will be described irrespective of their context, unless specifically relevant. Moreover, they do not explicitly respond to hybrid threats, but the individual threats are often part of how this thesis understands hybrid warfare. First and foremost, in the IFSS cooperation is put forward as a key element to build resilience. This cooperation is not just whole-of-government, it should include private and civil actors as well (p. 29). In particular, it is important that all these actors actively share information (p. 34). While the content of this information can be rather broad, the strategy stresses that a continuous effort is needed to map vulnerabilities and analyse the threat at hand (ibid). Moreover, if the coordinating parties themselves have created a better understanding of the threat, it is crucial they share this information both internally and externally, thereby increasing awareness (p. 35). On top of that, the NCTV adds that exchanging information about possible instruments between states could enhance resilience building efforts (p. 34). Elaborating on this, the document recommends an effort to improve strategic communication, particularly in response to disinformation campaigns of adversaries that serve to undermine internal processes (ibid). The NCTV recommends that the Dutch government constructs its own narrative and express this structurally and credibly (p. 33). Finally, although rather specific, the IFSS proposes to increase protection of local politicians to make them more resilient against foreign efforts to undermine them (ibid).

As described in the conceptual framework, one can distinguish between three types of resilience: engineering, adaptive and transformative. The former is the most straightforward perspective, which assumes an ability to bounce back from a shock or disruption. As the name already suggests, the second type assumes an ability to adapt. Not just to adapt after a shock, but also the ability to change certain tactics or approaches when a new threat requires so. Thirdly, the latter type of resilience is most abstract. It takes it a step further than the second type and prescribes an ability to renew existing practices beyond the status quo, often accompanied by a new understanding of the threat environment. Surprisingly, the Dutch

documents on hybrid warfare provide no definition of resilience. This paragraph will attempt to clarify the definition of resilience as understood by the Dutch government. While it has proven challenging to infer a category of resilience from the documents, it has become clear that most of the proposed changes are adaptive, meaning they occur within the given structures. Transformative resilience, in contrast, assumes those structures to have been rendered untenable. Since that is not the case in the hybrid warfare documents, one can conclude that transformative resilience requires no further analysis. Thus, the adaptive and engineering types of resilience remain to be analysed. Overall, both types of resilience can be identified in the IFSS. For example, the previous paragraphs have shown that the Dutch government uses resilience to protect the rule of law, social stability, governance and independence. In other words, it seeks to use resilience to maintain a status quo, which links it with the engineering view of resilience. On the other hand, the proposition of strengthening resilience by focussing on cooperation and information gathering suggests an intention to adapt to the changing threat environment. Moreover, it suggests that the Dutch government acknowledges that future attacks are possibly unknown, which links it with the definition of adaptive resilience. In the end, however, the rather limited use of resilience in the three documents on hybrid warfare undermines efforts to distil a meaning from them. The next section will attempt to resolve that issue by looking beyond the context of hybrid warfare.

Government-wide Documents

The IFSS emphasises that the Dutch approach to security issues requires coherent policy choices in which a wide range of instruments is combined in a concerted effort (p. 7). As a result, the content of the IFSS is partly based on choices made by other ministries and government agencies (ibid). In other words, a broader perspective is needed to study resilience in Dutch policy. The previous paragraphs have already shown that even the hybrid warfare strategy acknowledges the relevance of resilience beyond that specific context. Moreover, those strategic documents have proven insufficient to concretely and definitively draw conclusions on how the Dutch government understands resilience and its strategic role as a countermeasure against hybrid threats. Furthermore, a government wide analysis of resilience will allow for a certain degree of measurement of resilience in Dutch security policy and strategy, which in turn allows for conclusions to be drawn on the capacity of resilience to deter hybrid threats in The Netherlands.

Method

In order to analyse the extent to which resilience is prioritised throughout Dutch policy, this thesis will draw on the documents published by the national government. It has become clear that resilience requires one to look beyond Dutch hybrid warfare strategy alone. There is no one coherent strategy by one actor, nor a coherent strategy by a several actors. Instead, the starting point of this analysis is that resilience is an element of different strategies by distinct ministries. As the theoretical framework has shown, building resilience potentially requires input from seemingly irrelevant ministries. As a result, the analysis will be government wide, drawing on relevant input from all ministries. This analysis has been limited to the time period between October 2017 and present. In that month, the new and current Dutch cabinet was installed. In order to aid new cabinet members to acquaint themselves with the core tasks and operations of their ministries, each department publishes an introductory file. Generally speaking, this is a summary of what the department has been doing for the past couple years, as well as an overview of ongoing affairs. As a result, if resilience has been part of those affairs, it is likely to be discussed in these files. Furthermore, new cabinets often present strategies for the duration of their period in office, which is typically four years. These documents thus provide the most recent and relevant information to analyse. Finally, it offers the practical advantage of limiting the number of documents requiring analysis. Otherwise, that amount would exceed the scope of this thesis. To filter the vast number of documents within that time period, the analysis has been limited to documents containing the word "resilience", which has been entered as a keyword in the search engine to yield the results. After that selection, the actual content of the documents became relevant. In order for the contents to be analysed, the three central elements of resilience building in the context of hybrid threats, as identified in the theoretical framework, were used: social capital, vulnerabilities and cooperation.

Definition

Before turning to the content analysis on resilience, a brief side note on the definition of resilience is required. While resilience is widely used throughout the selected documents, only a few actually provide a definition. In fact, some documents merely use the concept rather loosely, without much clarification in the surrounding text. It is likely that resilience in those cases is understood from a dictionary definition, which would be as an "ability to resist"

(VanDale, n.d.). On the other hand, other documents use resilience very consciously, providing a lot of context from which a meaning can be distilled. From those documents, the most significant finding regarding the meaning of resilience is that resilience translates into two Dutch concepts: "weerbaarheid" and "veerkracht". The former can be defined as an ability to resist, while the latter is more an ability to bounce back (Grapperhaus, 2018; Ministry of Justice & Security, 2017). An overlapping understanding of resilience comes from the "Agenda Financial Sector" (Ministerie van Financiën, 2018), which equates resilience with the ability to mitigate and absorb shocks, thereby minimising the negative effects of disruptions (p. 3). Another important element of how resilience is understood takes a more societal perspective. The Ministries of Social Affairs & Employment, Infrastructure & Environment, and Justice & Security, all stress the importance of social cohesion (Ministerie van Sociale Zaken & Werkgelegenheid, 2017). The socio-psychological reality, or the societal perception, determines the strength resilience, which is often equated with high levels of trust (Boogers, Van Gaalen & Mintzis, 2017).

In the end, however, there is only one concrete and official definition, provided by the Ministry of Justice and Security. A report, "On route to a resilient open society: building blocks for a vision for the future" (Noordegraaf, Schiffelers, Geuijen, De Morree & Pekelder, 2018, p. 31), commissioned by that Ministry, defined resilience as:

> *The ability of an individual, community or system to resist, bounce back and adapt if a disruption of the normal state of affairs occurs*.

Here, the ability to resist is used to describe the ability to provide certain services, or maintain the function of a certain system, in light of a disturbance, without the system being significantly changed because of it. Secondly, the ability to bounce back is relevant when such a function is altered. In such instance, this ability ensures a swift recovery of that function or service provision. Lastly, the ability to adapt is threefold. First of all, it requires an ability to acknowledge or identify changes in one's surrounding. Secondly, it is about adapting to those changes, and, third, learning from that process.

From the definitions and clarifications provided above, one can draw two conclusions. First, it has become clear that the broader documentation on resilience generally adheres to the same understanding of resilience as the strategy on hybrid warfare. The abilities to bounce back and

to adapt, which are academically known as, respectively, engineering and adaptive resilience, generally feed the way the Dutch government understands resilience. Nevertheless, the key word here is “generally”. As the analysis of the government wide resilience documents have shown, there is no coherent definition that all Ministries adhere. Not even the most relevant actors in Dutch security policy have the same definition. The same conclusion was drawn by the report discussed in the previous paragraph, which observed that the political understanding of resilience is divided (ibid). Particularly, this means that different political parties adhere to a different definition. This conclusion suggests that cooperation between different Ministries is not yet at the desired level. Since cooperation forms one of the three pillars of the theoretical framework, and therefore guides the analysis, it will become clear if the policy input is indeed lacking behind on cooperation.

Policy input analysis

The central element of the following analysis will be resilience. As the literature review has shown, resilience is a methodological challenge, meaning that no agreed upon measurement for the strength of resilience exists. Moreover, each context may require different resilience policy. Therefore, to measure societal resilience in the Netherlands would go beyond the scope of this analysis. Instead, in order to avoid that grey area of resilience measurement, this thesis will look at the policy input. It will analyse what elements of resilience building already feature in Dutch policy. Consequently, to link those findings with resilience as a counterstrategy against hybrid threats, they will be juxtaposed to the theoretical framework. More precisely, the analysis will be guided by the elements of social capital, vulnerabilities and cooperation.

Social capital

Social capital will be discussed first. From the theoretical framework, it has become clear that the relevant indicators of that category are: respect for all stakeholders involved, involvement of society, a strong sense of belonging, high levels of participation, the inclusion of societal values in the political debate, transparency and mutual trust. First, the overlap and connection between the different indicators will be discussed, which serves to position them in a logical narrative of social capital. This, in turn, serves to facilitate the actual document analysis. In order to build social capital, it is crucial to involve society more in the decision-making

process of the government. Additionally, society has to be approached with a significant degree of inclusivity. The entire society has to be involved, meaning the inclusion of all different groups and minorities. Doing so would contribute to the indicator of a strong sense of belonging. This indicator also closely links to the role of the political debate. It is important to talk about and respect societal values, which influences the way in which society lives and works together. Once these steps have been taken, the indicator of participation becomes particularly relevant. For the purpose of building resilience, one would not just want to involve society, one wants to use that involvement to make citizens participate. As a government, one should not try to do everything for its citizens, but instead let them take responsibility when possible and together build on a resilient society. Finally, the theoretical framework has also provided some more concrete indicators of societal involvement and participation. First, it is important to respect all stakeholders involved. Society has to be listened to and respected. Part of this respect can be accomplished by high levels of transparency. A transparent government communicates with its people and clarifies why certain decisions were taken. Moreover, it would positively affect mutual trust, which contributes to the power of a government to function properly and to govern.

Involving society & Sence of belonging & respecting and talking about societal values

Within the context of resilience, the Dutch government has attributed significant value to several of the social capital indicators. To improve the coherence of the text and prevent overlap, the indicators of societal involvement and participation have been grouped together with the indicators of societal values in the political debate. It has become clear that the creation of a strong sense of belonging features prominently throughout the resilience strategy. Societal involvement, on the other hand, has been given significantly less attention. Simply put, the analysed documents indicate that policy serves to give the whole society a feeling of belonging to the Netherlands but fails to actually put it into practice and involve society. Regarding the latter, for example, one of the documents proposes to seek a closer connection between citizens and the government, thereby promoting interactivity (Ollongren, 2018b). Moreover, publicity is cited as a key strategy to reduce naivety of society, by which essentially a closer connection between the government and society is implicated (Militaire Inlichtingen- en Veiligheidsdienst, 2019). In contrast, inclusivity and a strong sense of belonging are promoted by several policies. For example, the “Programme Resilient Society” of the Ministry of Social Affairs and Employment (Ministerie van Sociale Zaken &

Werkgelegenheid, 2017) emphasises the significance of high levels of integration and the creation of social cohesion, meaning the feeling of each and every citizen that they are attached to society. Building on this, yet another policy emphasises the need to support vulnerable groups in society (Ministerie van Economische Zaken & Klimaat, 2018b). Finally, while the idea is rather specific, a pluriform media landscape is cited as key element of resilience against disinformation (Ollongren, 2018a). Again, this measure links with creating the importance of inclusivity.

High levels of participation

While involving society is one element of resilience building that serves as an indicator of this analysis, the level of participation also carries significant relevance. The analysis of a wide range of government documents has shown that societal participation prominently features in the efforts of the Dutch government to build resilience. In the context of disinformation campaigns and foreign influencing of elections, the government emphasises the need to promote "active participation" of society and the middle class in particular (ibid; Blok, 2018). The Programme Resilient Society of the Ministry of Social Affairs and Employment, which was introduced in the previous paragraph, considers societal participation as a second step, building on the first step of connecting with society (Ministerie van Sociale Zaken & Werkgelegenheid, 2017). Furthermore, there are several documents that clarify what is meant by societal participation in the eyes of the Dutch government, but are also in line with this indicator. In those documents, the government stresses the importance of improving the autonomy of society. Citizens and companies are encouraged to take more responsibility (Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), 2018a). In fact, in line with that argument, one document mentions the implementation of efforts to improve that autonomy. Particularly, it stresses that the government has to provide a certain degree of protection against, amongst others, foreign influencing (Grapperhaus & Ollongren, 2018). Moreover, it is up to the government to inform the public about measures they can take themselves (Ministerie van Infrastructuur & Milieu, 2018). Finally, a very relevant finding comes from the Agenda Risk- and Crisiscontrol. The Agenda talks about the existence of a "doen-vermogen" in Dutch society, which loosely translates as an ability to act, and how that ability has to be stimulated (Grapperhaus, 2018a).

Respect all stakeholders involved

Regarding the indicator of respect for involved stakeholders, significantly less evidence was found. In fact, two documents were identified containing content on this indicator but those have already been discussed in the previous paragraph under the heading of belonging and involvement. First, the extra support for vulnerable groups in society, which was mentioned in one of the documents, suggests a degree of respect for minorities in The Netherlands. Secondly, the decision to seek publicity more often in an effort to reduce naivety in society, signals a degree of respect and trust on the side of the government with regards to its citizens.

Transparency & trust

In order to build more social capital in a society, which ultimately contributes to higher levels of resilience as well, transparency has been mentioned as an important strategic element. Moreover, high levels of transparency can also be linked with higher levels of mutual trust. As a result, transparency and trust have been combined in this paragraph to analyse the government documents for these indicators of social capital. Both signs of transparency and trust can be identified in the resilience documents. For example, transparency and verifiability of information are emphasised in countering the impact of disinformation campaigns by foreign actors (Ollongren, 2018a). Other documents may not mention the word transparency itself, but stress the relevance of maintaining factual communication (Ministerie van Infrastructuur & Milieu, 2018). Finally, pro-active communication, which can be seen as a sign of transparency, is also mentioned a couple of times. For example, one document on the supervision of telecommunications in The Netherlands mentions that resilience requires a constant effort to mention each and every incident, even minor once, to the right authorities (Agentschap Telecom, 2019). Moreover, organisations are adviced to keep the relevant authorities informed about the measures in place to control and reduce organisational risks (Ministerie van Infrastructuur & Milieu, 2018). To conclude this paragraph, some attention will be given to the indicator of trust as well. Most concretely, one of the analysed documents mentions the importance of maintaining the integrity of local governments (Ollongren, 2018b). As a threat to mutual trust in the Netherlands, a letter to parliament on countering radicalisation cites increased polarisation and societal trust (Koolmees, 2018a). In other words, those developments undermine building trust, which eventually undermines the level of social capital and thus resilience building efforts. Finally, the government emphasises that

trust has taken on new relevance in light of developments in the digital domain and that it is important to uphold high standards of trust there (Ministerie van Economische Zaken, 2017b).

Vulnerabilities

The second category central to this analysis is all about vulnerabilities. In particular, the theoretical framework has shown that vulnerabilities are often exploited and targeted by adversaries using hybrid tactics. Moreover, vulnerabilities could undermine the level of resilience in a state. In other words, if one actively tries to identify vulnerabilities followed by an effort to reduce them, that would contribute significantly to the level of resilience in society. The first indicator is about being self-critical, which will be used to determine if the Netherlands is building resilience by reducing its vulnerabilities. A self-critical government, but the same goes for society and companies as well, will have an effort to actively identify one's vulnerabilities embedded in its policies. The second indicator of this category that was identified in the theoretical framework is about the constant effort required to identify one's vulnerabilities. In order to be truly self-critical, a continuous effort to identify and reduce vulnerabilities is crucial. The final indicator relevant for determining if the Netherlands is taking its vulnerabilities serious is about intelligence. In order to know what one's vulnerabilities are, a government should gather and analyse as much relevant information as possible. Combined, the indicators of being self-critical, providing a continuous effort, and gathering and analysing intelligence, form the analysis of the category of acknowledging and respecting one's vulnerabilities, which is crucial for any resilience building effort.

Being self-critical

The first indicator to be analysed is about being self-critical, which is all about acknowledging existing vulnerabilities and reducing risk to prevent vulnerability in the future. Throughout the Dutch government documents, the latter element of risk is discussed on several occasions. For example, the Ministry of Justice and Security has emphasised that domains with higher levels of risk should be given extra attention (Ministerie van Justitie & Veiligheid, 2017b). While a completely different domain, the Agenda Financial Sector also stresses the need to critically assess existing and new policies and limit the implementation of risky ideas (Ministerie van Financiën, 2018). It cites an improvement of the ability to bounce back as a core reason for the reduction of risk (ibid). Also the first element about

acknowledging vulnerabilities features in several government documents. The Dutch military intelligence service (MIVD) publicly recommends that citizens are more alert about security threats like disinformation campaigns (Militaire Inlichtingen- en Veiligheidsdienst, 2019). Additionally, several documents underscore the importance of mapping vulnerabilities in all domains and at all levels of government (Grapperhaus, 2018c; Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), 2016b). Finally, in order to assess those vulnerabilities, the documents seek to create a better understanding of the threat environment as well (ibid).

Constant effort

That resilience is not a societal characteristic that can be build overnight has become clear by now. Instead, the opposite is true. Building resilience, reducing risks, and identifying vulnerabilities requires a continuous effort of a wide range of actors. Early on in the identification of a new threat, the task of identifying vulnerabilities already starts, but also after a longer period of time, once threats and vulnerabilities have manifested themselves more prominently, it is crucial to assess risks and evaluate efforts to reduce vulnerabilities. This has also been looked for in the wider Dutch resilience policy. Within the context of Dutch counter terrorism strategy, early warning is mentioned as a key element of resilience building efforts (Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), 2016a). On a more generic scale as well, the development of knowledge via the gathering of information is considered as a constant effort (Ministerie van Economische Zaken & Klimaat, 2018b). This seems to be particularly attributed to the digital information domain. The pace in the cyber domain is high, with a constant stream of new information and on a wide range of website and media outlets, which makes keeping up with that pace crucially important (Ministerie van Defensie, 2017). Other documents in which both resilience and the effort of identifying vulnerabilities are linked with the need for constant alertness and vigilance, include: the Factsheet Resilient Vital Infrastructure, Digital Hard- and Software, and the Parliamentary Letter on DDos attacks on Dutch banks (Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), 2016b; Ministerie van Economische Zaken en Klimaat & Ministerie van Justitie en Veiligheid, 2018; Hoekstra, 2018a). Lastly, there are two documents relevant for what seems to be a focus on the institutionalisation of this continuous effort. On the one hand, vulnerable groups in Dutch society are seen as a factor undermining resilience building efforts and in order to strengthen those groups and reduce their

vulnerability, closer attention will be paid to their development via education programmes (Ecorys, 2017). On the other hand, undermining of local government is countered by the development of methods and training schemes which serve to increase the resilience of local government officials and politicians (Grapperhaus, 2018b).

Intelligence

The indicator of intelligence will be the last to analyse and determine the level of resilience in Dutch policy. Identifying and reducing one's vulnerabilities is all about information. about understanding the situation and the threat environment and creating a strong information position from which a coordinated countereffort can be designed. Particularly in the digital domain, information has become a new element of power, which is often exploited by adversaries using hybrid tactics. The importance of all sorts of information, particularly of sensitive data, has also been acknowledged in the Dutch resilience strategy. While the importance of information has been stressed on numerous occasions, the documents hardly go beyond acknowledging the importance of collecting information. The contexts in which the significance of knowledge is emphasised range from counterterrorism and cybersecurity to foreign influencing and vital infrastructure (Netwerk Weerbaar Bestuur, 2018; Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), 2016a; Grapperhaus & Ollongren, 2018; NCTV, 2018a). However, only one document, the yearly report of the MIVD, explicitly mentions the importance of not just gathering information, but also protecting information and preventing it from falling in the hands of adversaries (Militaire Inlichtingen- en Veiligheidsdienst, 2019).

Cooperation

The final category that will discussed to determine the level of resilience in Dutch strategy will be cooperation. From the literature review and theoretical framework, it has become clear that the complexity of both the threat, which is hybrid, and the countermeasure, which is resilience, cannot be dealt with by a single actor. The input from different levels, ranging from local to international, as well as from different domains is necessary to draft coherent policy and strategy. Linked with the previous category of vulnerabilities, the first indicator is all about information. Different from the previous paragraph, however, the first indicator will look at the sharing of information in particular. Within the category of vulnerabilities, the

indicator was about the acknowledgement of information as an important element of resilience strategies, while this indicator particularly serves to identify the process of how that information should be gathered. The second indicator looks more at how the cooperation is understood. Again, the complexity requires cooperation understood in the widest sense possible, which means the crossing of both disciplinary as well as ministerial boundaries. Moreover, the cooperation also requires input from society and companies. Finally, the last indicator is more about the design of strategy, which has to be integral and coherent. While at first sight it might be difficult to see how it is linked with the category of cooperation, the theoretical framework has shown that an integral and coherent strategy has cooperation embedded in its structure. For that reason, it forms the final indicator of this analysis.

Information sharing & interdisciplinary & interagency

Under the category of vulnerabilities, it has become clear that the Dutch government acknowledges the relevance of information and of knowledge. The latter differs from information in that it means that the information is already contextualised. For the collection of the data, as well as its analysis, the Dutch government greatly values the relevance of cooperation. This paragraph will combine the first and second indicator. While it will become clear that information sharing has been mentioned on numerous occasions throughout the Dutch governmental documents, it has often been linked with the actual execution of that intention. In other words, how that information should be shared and with what actors is often mentioned in close relation to the acknowledgement that information should be actively shared. On top of that, this analysis has also looked at cooperation beyond the context of information. All mentioning of cooperation in the Dutch resilience documents has been considered. First, however, the information cooperation will be addressed. “Mutual information-exchange”, “intelligence gathering”, “information sharing”, “provision of information”, and “knowledge development” through public-private cooperation, the Dutch resilience strategy clearly does not shy away from expressing the need to actively and pro-actively share information (Netwerk Weerbaar Bestuur, 2018; Ministerie van Economische Zaken & Klimaat, 2018b; Ollongren, 2017a; Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2017; Conferentie Nederland Digitaal, 2019; Koolmees, 2018a). Additionally, the “Network Resilient Government”, which is a platform for local governments to share their experience with resilience building efforts, mentions that information should also contain advice on possible instruments a government can use to build resilience (Netwerk

Weerbaar Bestuur, 2018). The sheer existence of the "Network Resilient Government" hints at the institutionalisation of cooperation. Throughout the resilience documents, one can identify another example of such institutionalisation: the "Cyber Resilience Centre", which has rather similar tasks as the Network Resilient Government, but, as the name already suggests, focusses on the digital domain instead (Brainport Eindhoven, Rijksoverheid & Provincie Noord-Brabant, 2018).

The analysis has shown that the Dutch government does not just seek to actively share information. Instead, the government wants to take it a step further and change the threat perception of society. In other words, it wants to increase the awareness of several threats the Netherlands faces, as well as the importance of resilience to counter them. While the previous paragraph has looked particularly at the occurrence of several examples of the indicator information sharing, the analysis has found that awareness also features prominent in government documents. Awareness building is mentioned on several occasions throughout the range of documents, all of which in the context of resilience building. One example is the Dutch "Digibeter" strategy, which serves to train and educate society about the opportunities and threats of the digital domain. Cited as one of the core intentions of the strategy is the build awareness about the relevance of digital skills and resilience in the digital domain (Overheidsbrede Beleidsoverleg Digitale Overheid, 2018). Most prominently, however, it features in the context of disinformation campaigns and unwanted foreign interference. Disinformation is widespread in the digital domain and the public has to be educated and made aware of that presence (Grapperhaus & Ollongren, 2018). In particular, the Dutch government focusses on the use of disinformation during politically sensitive times such as elections (Ollongren, 2017b; Ollongren, 2018a).

On top of the cooperation based on information sharing, the government documents also emphasise a general need to cooperate more. This can be divided into three distinct categories: cooperation between different level of government, interdisciplinary cooperation and public-private cooperation. The first one, cooperation at or between different levels of cooperation, has been mentioned on several occasions. Starting at the lowest level, one can identify two cases in which cooperation between local authorities, particularly municipalities, is proposed (NCTV, 2016a; Netwerk Weerbaar Bestuur, 2018). Additionally, those municipalities are advised to cooperate with the regional security authorities in order to consult on security issues and resilience building efforts (Grapperhaus, 2018a). The next level

is the national level. One document mentions that different Ministries and executive agencies should cooperate more with each other (Ministerie van Sociale Zaken & Werkgelegenheid, 2017). Furthermore, the Dutch government mentions the need to seek cooperation with its European allies as well. More precisely, the Parliamentary Letter on unwanted foreign influencing remarks that vulnerabilities have to be assessed at a European level and that the insights from that assessment have to be actively shared using the European platform (Grapperhaus & Ollongren, 2018). Finally, the highest level of cooperation is international. Think, for example, about the role of NATO. While no further specification is provided, the need for cooperation is particularly mentioned in the context of foreign influencing and political undermining (ibid; Ollongren, 2018a).

So far, the previous paragraph has analysed cooperation between different levels of government. This paragraph will look at public-private cooperation in particular. Its relevance has been emphasised by the Dutch government on several occasions. For example, the Dutch Ministry of Defence acknowledges that cooperation always has to be weighed in light of national security classification, but that cooperation will always be sought after when possible (Ministerie van Defensie, 2018a). Moreover, within the context of critical infrastructure, the government acknowledges that a wide range of actors is involved in any effort of making the infrastructure resilient (NCTV, 2016b). More in general, the Dutch Digitisation Strategy and the Cybersecurity Agenda both emphasise the need to engage in public-private partnerships to share knowledge and build resilience (Ministerie van Economische Zaken & Klimaat, 2018b; NCTV, 2018a). In a similar vein, a Parliamentary Letter about DDos attacks on Dutch banks mentions the need to seek cooperation with "knowledge networks" in which several actors work together to share information (Hoekstra, 2018a). Lastly, in one of the documents, cooperation between social media fora and government is put forward as a countermeasure against foreign influencing (Ollongren, 2017a).

Integral and comprehensive

To conclude this first part of the analysis of government wide publications, this paragraph will discuss the final indicator of cooperation, which in turn forms an important element of resilience building. While the use of integral and comprehensive strategies may at first not be perceived as an indicator of cooperation, it is the number of actors needed to design and execute such strategy that links it with cooperation. in particular, because comprehensive

strategies require input from different domains and require different actors, public and private, to execute them. The analysis of the government wide documents on resilience has yielded two documents where integralist and comprehensiveness are explicitly advised. Nevertheless, keep in mind that the IFSS, which has been analysed as a strategic document on hybrid warfare, was also comprehensive. The first strategy that stands out is the National Counterterrorism Strategy. It explains that terrorist threats require a "broad approach" in which different actors from different disciplines work together in a concerted effort (NCTV, 2016a). The second document is a Parliamentary Letter, which also discussed the issue of radicalisation, mentions that radicalisation can best be countered by an "integral approach" (Koolmees, 2018a).

What has to be made resilient?

In order to assess the prominence of resilience as a strategic element throughout Dutch policy, the previous paragraphs have explored the use of indicators of resilience. Those indicators were drawn from the theoretical framework, which identified several elements required for building resilience. Prior to that, the framework identified several areas that have to be made resilient against hybrid threats. Broadly speaking, those areas were placed in two categories: critical infrastructure and continuity of government. Zooming in on those two categories, one can construct a long list of areas that have to be made resilient according to the Dutch government documents on resilience. From that list, both the categories of critical infrastructure and continuity of government can be identified. The following paragraphs set out to describe the extent to which both categories are discussed throughout the Dutch resilience strategy. In doing so, the relevance of Dutch resilience building efforts in light of hybrid threats will be assessed.

The pace at which the digital domain has developed over the last couple of years has significantly impacted risk assessment of critical infrastructure. The growing interconnectedness of different systems is of particular concern. The same observation is reflected in the documents of the Dutch government. As the theoretical framework has shown, energy, food and water supplies, combined with civil communication services, have been identified as areas that require resilience in light of hybrid threats. In general, on can identify several occasions at which critical or vital infrastructure is named as an area requiring enhanced resilience building efforts. Most broadly, the Agenda Risk- and Crisiscontrol

mentions the importance of resilient critical infrastructure in a broad sense of the word (Grapperhaus, 2018a). More specifically, vital interests and critical infrastructure are also mentioned in the context of cybersecurity and economic security (NCTV, 2018a; NCTV, 2018b). The latter particularly mentions the protection of strategic economic information as a core strategy to preserve the continuity of critical infrastructure (NCTV, 2018b). Additionally, while the provided information is rather limited, the NCTV has published a factsheet "resilient vital infrastructure", which indicates its importance in national security strategy (NCTV, 2016b).

On top of the general mentioning of critical infrastructure, other documents also mention more specific domains. For example, the Ministry of Infrastructure and Environment has identified the resilience of vital water infrastructure as a particular area of concern (Ministerie van Infrastructuur & Milieu, 2017). Additionally, resilience is mentioned as a strategy to protect the financial sector. Core financial infrastructure should be made resilience against cyber threats, with a particular focus on defending the ability of money to flow freely (Hoekstra, 2018a). Also the area of civil communication services, which was identified in the theoretical framework, is mentioned in the context of resilience. The Dutch Telecom Agency has labelled the supervision of the resilience of Dutch telecom infrastructure as a priority for the year 2019 (Agentschap Telecom, 2019). Lastly, the Ministry of Defence has identified some critical infrastructure of its own. For example, it has institutionalised the protection of its own systems and network in the "cyber resilience cluster", the "national detection network" and the JIVC (Ministerie van Defensie, 2017). Additionally, on top of the focus on the cyber domain, it is significantly concerned about the actual physical infrastructure like Dutch highways. The resilience of that infrastructure has to be made resilient in order to enhance military mobility, which is of significant strategic importance (Bijleveld-Schouten, 2018).

The second area that was identified as requiring to be made resilient against hybrid threats was the continuity of government. In essence, this area came down to the continued ability of a government to deliver its goods and service and govern its state. In other words, it is about safeguarding and upholding the power to govern. The main observation that can be taken from analysing the government documents relates to the governmental level that is looked at. All documents concerning the continuity of government discuss resilience at the lowest level, the municipal level. As was observed in the Defence documents in the previous paragraph as

well, the effort of making the continuity of government resilient has been institutionalised as well. The most prominent example featuring in the document is the "Network Resilient Government", which aims to provide local governments with the tools and knowledge to respond adequately to situations of disruption (Netwerk Weerbaar Bestuur, 2018). Additionally, there exists an "Intergovernmental Programme", which specifically tries to assist local governments in their efforts to powerfully and effectively address local societal challenges (Ollongren, 2018b). lastly, the Ministry of Justice and Security has a unit "governmental approach" specifically tasked with strengthening the power to govern of local authorities (Ministerie van Justitie & Veiligheid, 2017b).

Weaknesses of deterrence-by-resilience

The paragraphs above have elaborated on the prominence of resilience throughout government-wide documents of the Dutch government. The analysis served to assess the extent to which resilience features as a strategic element in those documents. This, in turn, served to draw conclusions on the ability of Dutch resilience to deter. Furthermore, the latter paragraphs linked the contexts in which resilience has been mentioned with the areas that should be made resilient. Those areas were identified in the theoretical framework. Combined, all elements presented above are positive contributors to the ability of resilience in the Netherlands to deter hybrid threats. Nevertheless, one can also identify some weaknesses that undermine the deterrent capacity of Dutch resilience.

The starting point of this thesis has been to analyse what policies and strategies the Dutch government currently has in place to counter the hybrid threats that the Netherlands is facing. The literature review on this particular topic has shown that some of the core strategic elements that should lie at the foundation of any countermeasure are cooperation and communication. At a national level, hybrid threats require different ministries and government agencies to work together and make the effort to counter hybrid threats a coherent and comprehensive joint effort. While this thesis can only draw on public documents and only analyse the policy input, the three documents on hybrid warfare that have been identified show some weaknesses on the point of comprehensiveness. While the NCTV leaflet is clearly a solid step in the right direction of deterrence, the IFSS and Defence Note are not. The different documents highlight different elements, both in terms of threat analysis as well as countermeasures. Moreover, the IFSS and Defence Note lack a clear definition of hybrid

warfare. The fact that the NCTV document has a clear and workable definition indicates a lack of communication with the ministry of Foreign Affairs and Defence, which were the authors of the IFSS. To a certain degree, that absence of coherence undermines the deterrent capacity of the Dutch effort to counter hybrid threats. That argument can be extended to topic of resilience as well. In the Dutch documents on hybrid warfare, resilience only plays a significant role in the IFSS, while being more marginally mentioned in the Defence Note and the NCTV document. The factor that undermines the dominance of resilience the most is the lack of a definition. Despite the complexity of the term, which has already been established in the conceptual framework, the Dutch government fails to provide clarity. Such clarity is needed to construct effective countermeasures based on resilience. Thus, in turn, the lack of such clarity undermines the deterrent capacity of resilience against hybrid threats.

The absence of clarity and coherence in the documents on hybrid warfare undermines the deterrent capacity of any counterstrategy, including resilience. Similar conclusions can be drawn from the government-wide document on resilience itself. The analysis has shown that the Dutch Ministry of Justice and Security has already made significant progress on the subject of resilience. When purely considering their conceptual understanding of resilience, it is by far the most promising ministry to look at for determining the deterrent capacity. However, resilience is complex and multidimensional, and any strategy based on it should cross the borders of individual ministries. So, while this ministry is well on its way, it is surprising to observe that no other ministry or agency of the Dutch government has provided a definition of resilience. Knowing that a definition exists in one of the Dutch ministries that is conceptually solid, it is astonishing that no other ministries use it. In fact, many even have a different understanding of resilience. This lack of a whole-of-government and coherent understanding of resilience negatively impacts the way adversaries perceive Dutch resilience, thus undermining its deterrent capacity.

Conclusion

Limitations

This thesis set out to study a relatively new concept in the field of security studies: deterrence-by-resilience. In the academic literature, the range of documents that links deterrence and resilience is slightly larger, but the actual term itself has only been used on a few occasions. Writing an article to fit in that niche brings along certain limitations. The link between the two concepts, which themselves individually have been widely studied and theorised, has not been empirically tested, nor has the concept been able to develop into a widely accepted theory. At the same time, however, since the terms individually have a long history of theoretical research, the link is given a certain degree of academic value based exactly on that history. On top of that theoretical limitation, two more practical limitations should be mentioned. This thesis has analysed a wide range of documents from the Dutch government, with a conscious focus on the policy input. The literature review has established that resilience is a methodological challenge, since it is highly context dependent. As a result, only very few studies exist that have attempted to measure the strength of resilience in a state. Because of that, this thesis has looked at the policy input, allowing a comparison to be made between what an effective resilience building effort should look like on the one hand, and what the Dutch government is doing to build resilience on the other. Lastly, this thesis has only been able to analyse public documents. Since certain elements of security policies are often confidential to protect national security, it is likely that also the topic of hybrid warfare has been discussed more extensively behind close door. Since the content of those discussions is confidential, they could not have been part of this analysis.

Conclusions

The central question at the foundation of this thesis set out to analyse a wide range of Dutch policies on resilience to assess the capacity of that resilience to deter the hybrid threats that the Netherlands are facing. In order to frame and guide that analysis, the standing academic literature has first been reviewed. From that review, it has become clear that both deterrence and resilience have been studied as possible counterstrategies against hybrid threats and that their strength as a counterstrategy is perceived as promising. As a result, some scholars have linked both individual strategies, analysing the ability of resilience to serve as a deterrent. Especially the perspective of deterrence-by-denial has proven valuable in that regard, considering that resilience denies potential adversaries gains from their attacks. Building on

that link, the most recent development on the subject of deterrence and resilience has given rise to a new concept of deterrence: deterrence-by-resilience. Since the amount of literature on that concept is rather limited, the review has shown that is rather theoretical. This thesis will take a more practical turn, complementing the existing literature with an analysis of the deterrence capacity of resilience in the Netherlands.

Because of the complexity of both the concept of hybrid warfare and of resilience, the literature review was complemented with a conceptual framework, clarifying both concepts and their use throughout this thesis. For hybrid warfare, the elements of multidimensionality, simultaneous deployment and secrecy have been established as core characteristics that make it so difficult to counter hybrid threats. In particular, however, the framework has shown that the term "warfare" is contested. As a result of that debate, resilience has entered the debate. While the concept may not particularly fit well in the context of warfare and defence, it is particularly relevant for the non-military aspect of hybrid threats. Furthermore, the military perspectives explains the prominence that has been given to deterrence. Regarding the second concept, resilience, three different types have been identified. Since the Dutch government documents all have different definitions or nuances on the term, the differentiation into three distinct terms has allowed more clarity on the contexts in which resilience is being used. As a result, that distinction has not just allowed different understandings to be identified, but also for those identifications to be placed in the right category.

While the conceptual framework served more to clarify and facilitate the document analysis, the theoretical framework has been instrumental in the guiding and structuring of the analysis. First, the NATO framework was introduced which served to establish the areas or systems that have to be made resilient in light of hybrid threats. The two main categories that were identified are critical infrastructure and continuity of government. In the analysis, those categories were used in the third part. There, it became clear that the government-wide documents on resilience explicitly included those categories, which has positively influenced the overall assessment of the deterrent capacity of resilience against hybrid threats. The second part of the theoretical framework then proceeded to describe certain elements that are crucial for any resilience building effort. In other words, the presence of a high number of indicators in the governmental documents would positively influence the achievability of a deterrence-by-resilience strategy in the Netherlands. Consequently, the analysis of the government-wide documents on resilience has shown that the indicators are widely

represented in the analysed documents, which indicates a strong deterrent capacity of resilience. It is that observation, however, that also holds an element undermining the deterrence capacity. Namely, while resilience is widely represented throughout the government-wide documents, those documents do not address the hybrid threats that the Netherlands is facing. The absence of that link, which the section on weaknesses has labelled an absence of coherence, has a negative impact on the deterrence capacity. Moreover, while those hybrid threats have been addressed in the IFSS, the Defence Note and the NCTV leaflet, it has become clear that the IFSS and the NCTV document, which both elaborate on resilience, show no signs of any link or coherence. Lastly, the government-wide documents on resilience have been analysed for their definitions of the term as well, which has revealed that, either, no definition is present, or those documents that do have a workable definition are isolated, meaning that definition is not shared with other ministries. To conclude, one can say that resilience in the Netherlands is well on its way, with many different elements being addressed in policies of many different ministries. Nevertheless, more coherence and cooperation, especially regarding information sharing, is needed to strengthen the ability of resilience to deter. Additionally, a connection should also be made between the documents on resilience and the documents on hybrid warfare, creating a more integral approach to the hybrid threats that the Netherlands is facing and improving the deterrence capacity.

Compounded Bibliography

Agentschap Telecom. (2019, February 4). *Jaarplan Toezicht 2019 Agentschap Telecom*. Retrieved from https://www.rijksoverheid.nl/documenten/jaarplannen/2019/02/04/jaarplan-toezicht-2019-agentschap-telecom

AIVD. (2017, June). *Cybersecuritybeeld Nederland CSBN 2017* (Rep.). Retrieved February 13, 2019, from Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) website: https://www.nctv.nl/binaries/CSBN2017_tcm31-267075.pdf

AIVD. (2018, March). *Jaarverslag AIVD 2017* (Rep.). Retrieved February 13, 2019, from Algemene Inlichtingen- en Veiligheidsdienst website: https://www.aivd.nl/documenten/jaarverslagen/2018/03/06/jaarverslag-aivd-2017

Auditdienst Rijk. (2018, April 16). *Onderzoeksrapport beleidsdoorlichting Artikel 36.2 Nationale veiligheid en terrorismebestrijding.* Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2018/04/16/tk-bijlage-beleidsdoorlichting-nationale-veiligheid-en-terrorismebestrijding

Balzacq, T. (Ed.). (2014). *Contesting Security Strategies and logics*. Routledge. Retrieved November 18, 2018.

Bijleveld-Schouten, A. (2018, March 6). *Beantwoording Kamervragen over de Raad Buitenlandse Zaken met ministers van Defensie* (The Netherlands, Ministry of Defence). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/06/beantwoording-kamervragen-over-de-raad-buitenlandse-zaken-met-ministers-van-defensie

Bilban, C. (2016). *Resilience: Silver Bullet in Challenging Hybrid Warfare?* (pp. 1-13, Working paper No. 210098 SE M4). Austria: National Defence Academy. Retrieved January 9, 2019.

Blok, S. (2018, December 21). *Kamerbrief over hoofdpunten interne notitie 'religie en buitenlands beleid'* (The Netherlands, Ministry of Foreign Affairs). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/12/21/kamerbrief-over-hoofdpunten-interne-notitie-religie-en-buitenlands-beleid

Blok, S., & Bijleveld-Schouten, A. (2018, October 19). *Kamerbrief over de verstoring cyberoperatie en veranderende veiligheidsomgeving* (The Netherlands, Ministry of Defence). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/10/19/kamerbrief-over-de-verstoring-cyberoperatie-en-veranderende-veiligheidsomgeving

Boogers, M., Van Gaalen, J., & Mintzis, K. (2017, December). *Analyse bevindingen Onderzoeksraad voor Veiligheid ten behoeve van het veiligheidsbeleid van het Ministerie van IenM*. BMC Onderzoek. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2018/07/04/analyse-bevindingen-onderzoeksraad-voor-veiligheid-t-b-v-het-veiligheidsbeleid-van-het-ministerie-van-ienm

Bourbeau, P. (2017). Resilience, Security and World Politics. In D. Chandler & J. Coaffee (Eds.), *The Routledge Handbook of International Resilience* (pp. 26-37). New York, NY: Routlegde.

Brainport Eindhoven, Rijksoverheid & Provincie Noord-Brabant (2018, July 1). *Brainport Nationale Actieagenda*. Retrieved from https://www.brainport.nl/uploads/documents/BPE-18015-Brainport-Development-Agenda-Rijk-LR7-spreads.pdf

Brinkel, T. (2017). The Resilient Mind-Set and Deterrence. In P. Ducheine & F. Osinga (Eds.), *Netherlands Annual Review of Military Studies 2017* (pp. 19-38). T.M.C. Asser Press. Retrieved January 9, 2019.

Brinkel, T. (2018). Moraliteit, beleid en weerbaarheid. *Militaire Spectator, 187*(7/8), 373-385. Retrieved November 8, 2018.

Cavelty, M. D., & Prior, T. (2013, October). *Resilience in Security Policy: Present and Future* (Rep. No. 142). Retrieved November 18, 2018, from Center for Security Studies (CSS) website: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analysis-142-EN.pdf

Chivvis, C. S. (2017). *Understanding Russian "Hybrid Warfare" - And What Can Be Done About It* (Publication No. CT-468). Retrieved December 19, 2018, from RAND Corporation website: https://www.rand.org/pubs/testimonies/CT468.html

Conferentie Nederland Digitaal. (2019, March 21). *Opbrengsten Conferentie Nederland Digitaal 2019*. Retrieved from https://www.rijksoverheid.nl/documenten/publicaties/2019/03/21/opbrengsten-conferentie-nederland-digitaal-2019

Connable, B. (2018). Moving to a Practical Deterrence Strategy: How to Make Deterrence Work in 2015 and Beyond (B. Wasser, B. Connable, A. Atler, & J. Sladden, Eds.). In *Comprehensive Deterrence Forum - Proceedings and Commissioned Papers*. Retrieved November 16, 2018, from https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF345/RAND_CF345.pdf

Cordesman, A. H. (2010a, January 21). *Iran's Evolving Threat* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/iran's-evolving-threat

Cordesman, A. H. (2010b, January 25). *How the US Must Expand and Redefine International Cooperation in Fighting Terrorism* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/how-us-must-expand-and-redefine-international-cooperation-fighting-terrorism

Cordesman, A. H. (2010c, November 1). *Iran, Iraq, and the Changing Face of Defense Cooperation in the Gulf* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/iran-iraq-and-changing-face-defense-cooperation-gulf

Cordesman, A. H. (2010d, November 17). *Afghan National Security Forces* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/afghan-national-security-forces

Cordesman, A. H. (2015, September 23). *Russia in Syria: Hybrid Political Warfare* (Commentary). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/russia-syria-hybrid-political-warfare

Cullen, P. J., & Reichborn-Kjennerud, E. (2017). *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare* (pp. 1-32, Rep.). United Kingdom: Ministry of Defence. Retrieved October 20, 2018, from https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare.

Dalton, M., & Shah, H. (2017, September 26). *Framing Next Steps for Security Sector Assistance Reform* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/framing-next-steps-security-sector-assistance-reform

De Graaf, P. (2016). Wat te doen met een olifant in de kamer? *Nationale Veiligheid En Crisisbeheersing, 14*(5/6), 22-23. Retrieved October 20, 2018, from https://www.nctv.nl/binaries/Magazine Nationale Veiligheid en Crisisbeheersing 2016 5_7 interactief_tcm31-234692.pdf

Deterrence [Def. 1993-0029]. (n.d.). In *NATOTerm*. Retrieved November 16, 2018.

Deterrence by Resilience - Are Democracies Proactive Enough in Protecting Western Values? (2018, September 29). Live performance in Riga.

Directie Informatievoorziening en Inkoop (DI&I). (2019, March 13). *Informatieplan J&V 2019*. Retrieved from https://www.rijksoverheid.nl/documenten/publicaties/2016/07/08/de-informatiestrategie-2017-2022-van-het-ministerie-van-veiligheid-en-justitie-informatie-raakt-mensen

Drent, M., & Meijnders, M. (Eds.). (2018). *Horizonscan Nationale Veiligheid 2018* (Rep.). Retrieved February 13, 2019, from Analistennetwerk Nationale Veiligheid website: https://www.nctv.nl/binaries/ANV Horizonscan Nationale Veiligheid 2018 - Def_tcm31-362716.pdf

Drent, M., & Zandee, D. (2016, December 20). HYBRIDE DREIGINGEN EN EU-NAVO SAMENWERKING. *Clingendael*. Retrieved September 30, 2018, from https://www.clingendael.org/nl/publicatie/hybride-dreigingen-en-eu-navo-samenwerking

Ducheine, P. (2016). Nationale veiligheid en hybride dreiging: Twee kanten van dezelfde medaille. *Nationale Veiligheid En Crisisbeheersing*, *14*(5/6), 7-10. Retrieved February 27, 2019.

Dunn-Cavelty, M. (2013). Resilience in Security Policy: Past and Future. *Security Policy, 142*, 1-4. Retrieved October 20, 2018, from http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analysis-142-EN.pdf

Durodié, B. (2004). The Limitations of Risk Management dealing with disasters and building social resilience. *TIDSSKRIFTET POLITIK, 8*(1), 14-21. Retrieved January 12, 2019.

Durodié, B. (2007, November 16). *Cultural influences on resilience and security* (Publication). Retrieved January 12, 2019, from RUSI website: https://rusi.org/publication/cultural-influences-resilience-and-security

Ecorys. (2017, November 6). *Monitor actieprogramma Tel mee met Taal 2016-2018 - Tussenrapportage 2017*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2017/11/06/monitor-actieprogramma-tel-mee-met-taal-2016-2018-tussenrapportage-2017

Filip, L. (2017). NATO RESILIENCE STRATEGY TOWARDS RUSSIAN HYBRID WARFARE. *Journal of Defense Resources Management, 8*(2), 64-71. Retrieved March 11, 2019.

Fjäder, C. (2014). The nation-state, national security and resilience in the age of globalisation. *Resilience, 2*(2), 114-129. Retrieved November 18, 2018.

Freedman, L. (2013). *Strategy: A History*. Oxford: Oxford University press. Retrieved January 24, 2019.

Freedman, L. (2018). The Limits of Deterrence (B. Wasser, B. Connable, A. Atler, & J. Sladden, Eds.). In *Comprehensive Deterrence Forum - Proceedings and Commissioned Papers*. Retrieved November 16, 2018, from https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF345/RAND_CF345.pdf

Giegerich, B. (2016). Hybrid Warfare and the Changing Character of Conflict. *Connections, 15*(2), 65-72. Retrieved November 18, 2018.

Giles, K. (2016). *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power* (pp. 1-71, Publication). Londen, UK: Chatham House. Retrieved September 30, 2018, from https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.

Giles, K., Hanson, P., Nixey, J., Sherr, J., Wood, A., & Kendall, B. (2015, June 5). *The Russian Challenge*. Retrieved September 30, 2018, from https://www.chathamhouse.org/sites/default/files/field/field_document/20150605RussianChallenge.pdf

Glenn, R. W. (2009). THOUGHTS ON "HYBRID" CONFLICT. *Small Wars Journal*. Retrieved November 13, 2018.

Golovchenko, Y., Hartmann, M., & Adler-Nissen, R. (2018). State, media and civil society in the information warfare over Ukraine. *International Affairs, 94*(5), 975-994. Retrieved September 30, 2018, from https://academic.oup.com/ia/article/94/5/975/5092080.

Grapperhaus, F. (2018a, November 12). *Kamerbrief over agenda risico- en crisisbeheersing 2018-2021* (The Netherlands, Ministry of Justice & Security). Retrieved June 4, 2019, from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/11/12/tk-agenda-risico-en-crisisbeheersing-2018-2021.

Grapperhaus, F. (2018b, November 16). *Kamerbrief over versterking aanpak ondermijning: actuele stand van zaken* (The Netherlands, Ministry of Justice & Security). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/11/16/brief-tweede-kamer-versterking-aanpak-ondermijning-actuele-stand-van-zaken

Grapperhaus, F. (2018c, September 7). *Beantwoording Kamervragen over het bericht 'Russische trollen ook actief in Nederland'* (The Netherlands, Ministry of Justice & Security). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/09/07/antwoorden-kamervragen-over-het-bericht-russische-trollen-ook-actief-in-nederland

Grapperhaus, F. (2019, April 18). *Kamerbrief over maatregelen tegen statelijke dreigingen* (The Netherlands, Ministry of Justice & Security). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2019/04/18/tk-tegengaan-statelijke-dreigingen

Grapperhaus, F., Ollongren, K.H. (2018, March 16). *Brief ongewenste buitenlandse inmenging* (The Netherlands, Ministry of Justice & Security). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/16/tk-brief-ongewenste-buitenlandse-inmenging

Hajduk, K. (2017, May 31). *Operational Planning as a State of Mind, Not a Starting Point* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/operational-planning-state-mind-not-starting-point

Hamilton, D. S. (2017). *Going beyond Static Understandings: Resilience Must Be Shared, and It Must Be Projected Forward* (Working paper). Center for Transatlantic Relations. Retrieved February 28, 2019.

Hamre, J. J. (2016, December 15). *What are the main national security challenges facing the Trump administration?* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/what-are-main-national-security-challenges-facing-trump-administration

Hanisch, M. (2016). *What is Resilience? Ambiguities of a Key Term* (Rep. No. 19). Retrieved December 2, 2018, from Federal Academy for Security Policy website: https://www.baks.bund.de/sites/baks010/files/working_paper_2016_19.pdf

Hartmann, U. (2017, September). *The Evolution of the Hybrid Threat, and Resilience as a Countermeasure* (Research Paper 139). Retrieved December 20, 2018, from NATO Defense College website: http://www.ndc.nato.int/news/news.php?icode=1083#

Hersman, R., Hicks, K., King, I., Miller, F., & Vershbow, A. (2017, February 1). Introduction and "Panel 1: Nuclear Deterrence and the NATO Alliance: Risks of Conflict and Prospects for Cooperation". In *The Future of Alliances and Extended Nuclear Deterrence*. Retrieved September 30, 2018, from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170201_Future_Alliance_Extended_Nuclear_Deterrence.pdf?6qgNi5QR_kFL_.6Ee4NEIMMta8TuUWzV

Hoekstra, W.B. (2018a, March 7). *Antwoorden Kamervragen over DDoS-aanvallen op Nederlandse banken* (The Netherlands, Ministry of Finance). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/07/antwoorden-kamervragen-over-ddos-aanvallen-op-nederlandse-banken

Hoekstra, W.B. (2018b, October 8). *Schriftelijk overleg IMF Jaarvergadering* (The Netherlands, Ministry of Finance). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/10/08/schriftelijk-overleg-imf-jaarvergadering

Hoffman, F. G. (2006a). Complex Irregular Warfare. *Foreign Policy Research Institute*. Retrieved October 11, 2018, from https://www.fpri.org/article/2006/01/complex-irregular-warfare/.

Hoffman, F. G. (2006b). Lessons from Lebanon: Hezbollah and Hybrid Wars. *Foreign Policy Research Institute*. Retrieved October 11, 2018, from https://www.fpri.org/article/2006/08/lessons-from-lebanon-hezbollah-and-hybrid-wars/.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Retrieved November 9, 2018.

Hoffman, F. G. (2009a). Hybrid vs. compound war - The Janus choice: Defining today's multifaceted conflict. *Armed Forces Journal*. Retrieved November 13, 2018.

Hoffman, F. G. (2009b). Hybrid Warfare and Challenges. *Joint Force Quarterly,* (52), 34-39. Retrieved November 9, 2018. http://123userdocs.s3.amazonaws.com/d/28/3a/28541563449522436O/af0247b1-0479-4e14-83d8-d08af8049303/HybridWar_21%20cent.pdf

Hybrid threat [Def. 37938]. (n.d.). In *NATOTerm*. Retrieved November 13, 2018.

Inspectie Justitie en Veiligheid. (2017, November 23). *Meerjarenprogramma 2018-2020*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2017/11/23/tk-bijlage-meerjarenprogramma

Jervis, R. (1979). Deterrence Theory Revisited. *World Politics, 31*(2), 289-324. Retrieved November 16, 2018.

Johnson, R. (2018). Hybrid War and Its Countermeasures: A Critique of the Literature. *Small Wars & Insurgencies, 29*(1), 141-163. Retrieved February 28, 2019.

Kasapoglu, C. (2015, November 25). *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control* (Rep. No. Research Paper 121). Retrieved December 21, 2018, from NATO Defense College website: http://www.ndc.nato.int/news/news.php?icode=877

Keijzer, M.C.G. (2018, January 15). *Beantwoording van verzoek tot reactie op de CPB Policy Brief 'Scientia potentia est: de makelaar van alles'* (The Netherlands, Ministry of Economic Affairs & Climate). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/01/16/kamerbrief-over-"platforms-veranderen-de-wereld"

Knopf, J. (2010, February). *Terrorism and the Fourth Wave in Deterrence Research* (Rep.). Retrieved November 16, 2018, from Calhoun: The NPS Institutional Archive website: https://calhoun.nps.edu/bitstream/handle/10945/58519/isa10_proceeding_413360.pdf?sequence=1

Koolmees, W. (2017, December 22). *Beantwoording Kamervragen over reportage 'Meer jonge moslims leven naar strikte islamtische regels. Dreigt segregatie?'* (The Netherlands, Ministry of Social Affairs & Employment). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/22/beantwoording-kamervragen-over-meer-jonge-moslims-leven-naar-strikte-islamtische-regels.-dreigt-segregatie

Koolmees, W. (2018a, April 26). *Kamerbrief Preventie Radicalisering* (The Netherlands, Ministry of Social Affairs & Employment). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/04/26/kamerbrief-preventie-radicalisering

Koolmees, W. (2018b, June 22). *Kamerbrief De Kans om Scheidslijnen te Overbruggen* (The Netherlands, Ministry of Social Affairs & Employment). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/06/22/kamerbrief-de-kans-om-scheidslijnen-te-overbruggen

Koolmees, W. (2019, February 13). *Kamerbrief afbakening verkenning naar informele scholing in Nederland* (The Netherlands, Ministry of Social Affairs & Employment). Rtrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2019/02/13/kamerbrief-afbakening-verkenning-naar-informele-scholing-in-nederland

Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs, 92*(1), 175-195. Retrieved September 30, 2018, from https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_09_Lanoszka.pdf.

Lasconjarias, G. (2017). Deterrence through Resilience: NATO, the Nations and the Challenges of Being Prepared. *NATO Defence College, 7*, 1-8. Retrieved October 20,

2018, from http://www.css.ethz.ch/en/services/digital-library/articles/article.html/ac42738e-f524-462a-bb16-18e5eba459ef/pdf

Major, C., & Mölling, C. (2015, April). *A Hybrid Security Policy for Europe - Resilience, Deterrence, and Defense as Leitmotifs* (Rep. No. 22). Retrieved November 18, 2018, from German Institute for International and Security Affairs website: https://www.swp-berlin.org/fileadmin/contents/products/comments/2015C22_mjr_mlg.pdf

Major, C., & Von Voß, A. (2016, March). *Nordic-Baltic Security, Germany and NATO - The Baltic Sea Region Is a Test Case for European Security* (Publication No. 13). Retrieved December 20, 2018, from Stiftung Wissenschaft und Politik website: https://www.swp-berlin.org/en/publication/nordic-baltic-security-germany-and-nato/

Mattiisen, A. (2016, December 16). *NATO–EU Cooperation in the Context of Hybrid Threats* (Rep.). Retrieved November 13, 2018, from International Centre for Defence and Security website.

McCulloh, T. B. (2012, May 22). *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the "Hybrid Threat" New?* (Rep. No. AY 2012-001). Retrieved November 13, 2018, from School of Advanced Military Studies website.

McInnis, K. (2014, August 29). Four Questions NATO Must Ask. Retrieved September 30, 2018, from https://www.chathamhouse.org/expert/comment/15611

Metrick, A., & Hicks, K. (2018, March). *Contested Seas Maritime Domain Awareness in Northern Europe* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/programs/international-security-program/global-threats-and-regional-stability/contested-seas

Meyer-Minnemann, L. (2017). *Resilience and Alliance Security: The Warsaw Commitment to Enhance Resilience* (Working paper). Retrieved January 9, 2019, from Center for Transatlantic Relations website: http://transatlanticrelations.org/publications/forward-resilience-protecting-society-in-an-interconnected-world/

Michta, A. (2014, November 13). *NATO's Eastern Front* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/nato's-eastern-front

Militaire Inlichtingen- en Veiligheidsdienst. (2019, April 30). VOORUITZIEND https://www.rijksoverheid.nl/documenten/kamerstukken/2018/12/21/kamerbrief-over-hoofdpunten-interne-notitie-religie-en-buitenlands-beleidVERMOGEN VOOR VREDE &VEILIGHEID – MIVD Openbaar Jaarverslag 2018. Retrieved from https://www.rijksoverheid.nl/documenten/jaarverslagen/2019/04/30/openbaar-jaarverslag-militaire-inlichtingen-en-veiligheidsdienst-mivd-over-het-jaar-2018

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2017, October 26). *BZK – Introductiedossier*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2017/10/27/bzk---introductiedossier

Ministerie van Buitenlandse Zaken. (2018, May 14). *Geïntegreerde Buitenland- en Veiligheidsstrategie (GBVS)* (Rep.). Retrieved February 13, 2019, from https://www.rijksoverheid.nl/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs

Ministerie van Defensie. (2017, October 27). *Introductiebundel Defensie*. Retrieved from https://www.rijksoverheid.nl/documenten/publicaties/2017/10/27/introductiebundel-defensie

Ministerie van Defensie. (2018a, November 12). *Defensie Cyber Strategie 2018 - Investeren in digitale slagkracht Nederland*. Retrieved from https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018

Ministerie van Defensie. (2018b, November 15). *Defensie Industrie Strategie*. Retreived from https://www.defensie.nl/downloads/beleidsnota-s/2018/11/15/defensie-industrie-strategie

Ministerie van Economische Zaken. (2017a, October 25). *Overdrachtsdossier ministerie van Economische Zaken*. Retrieved from https://www.rijksoverheid.nl/documenten/richtlijnen/2017/10/25/overdrachtsdossier-van-het-ministerie-van-economische-zaken

Ministerie van Economische Zaken. (2017b, October 9). *Navigeren met wind in de zeilen - Voortgangsrapportage Bedrijvenbeleid 2017*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2017/10/09/rapportage-bedrijvenbeleid-2017-“navigeren-met-wind-in-de-zeilen

Ministerie van Economische Zaken & Klimaat. (2018a, May 31). Strategisch aanvalsplan 2018-2021 The Netherlands: Digital Gateway to Europe. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2018/05/31/strategisch-aanvalsplan-2018-2021-the-netherlands-digital-gateway-to-europe

Ministerie van Economische Zaken & Klimaat. (2018b, June 1). *Nederlandse Digitaliseringsstrategie*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2018/06/01/nederlandse-digitaliseringsstrategie

Ministerie van Economische Zaken en Klimaat & Ministerie van Justitie en Veiligheid. (2018, April 2). *Roadmap Digitaal Veilige Hard- en Software*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software

Ministerie van Financiën. (2018, December 17). *Agenda Financiële Sector*. Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/12/17/kamerbrief-agenda-financiele-sector

Ministerie van Infrastructuur & Milieu. (2017, October 26). *Overdrachtsdossier IenM - Kabinetswisseling 2017*. Retrieved from

https://www.rijksoverheid.nl/documenten/publicaties/2017/10/26/overdrachtsdossier-ienm---kabinetswisseling-2017

Ministerie van Infrastructuur & Milieu. (2018, July 4). *Bewust Omgaan met Veiligheid: Op weg naar een schone, gezonde en veilige leefomgeving – Eindrapportage*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2018/07/04/eindrapport-bewust-omgaan-met-veiligheid-juni-2018

Ministerie van Justitie & Veiligheid. (2017a, December 1). *Samen werken aan Recht en Veiligheid*. Retrieved from https://www.rijksoverheid.nl/documenten/publicaties/2018/02/20/samen-werken-aan-recht-en-veiligheid

Ministerie van Justitie & Veiligheid. (2017b, October 1). Introductiedossier ministerie van Justitie en Veiligheid. Retrieved from https://www.rijksoverheid.nl/documenten/publicaties/2017/11/21/introductiedossier-ministerie-van-justitie-en-veiligheid

Ministerie van Sociale Zaken & Werkgelegenheid. (2017, November 2) *Introductiedossier nieuwe bewindspersonen 2017*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2017/11/01/introductiedossier-ministerie-van-sociale-zaken-en-werkgelegenheid

Ministerie van Volksgezondheid, Welzijn en Sport & Ministerie van Justitie & Veiligheid (2018, April 1). *Actieprogramma Zorg voor de Jeugd*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2018/04/01/actieprogramma-zorg-voor-de-jeugd

Monaghan, A. (2016). The 'War' in Russia's 'Hybrid Warfare'. *Parameters, 45*(4), 65-74. Retrieved December 19, 2018.

Morgan, P. M. (2018). Expanding the Concept of Deterrence (B. Wasser, B. Connable, A. Atler, & J. Sladden, Eds.). In *Comprehensive Deterrence Forum - Proceedings and Commissioned Papers*. Retrieved November 16, 2018, from https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF345/RAND_CF345.pdf

Murdock, C. A. (2010, February 2). *The 2010 Quadrennial Defense Review* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/2010-quadrennial-defense-review-0

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2016a, July 11). *Nationale terrorismestrategie 2016-2020*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2016/07/11/tk-bijlage-nationale-contraterrorismestrategie-2016-2020

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2016b, December). *Factsheet Weerbare Vitale Infrastructuur*. Retrieved from https://www.nctv.nl/binaries/18.%20Factsheet%20Vitale%20Infrastructuur_tcm31-32336.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2018a, April 21). *Nederlandse Cybersecurity Agenda - Nederland digitaal veilig*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2018b, June). *Programma economische veiligheid: de balans vinden tussen nationale veiligheid en een open economie.* Retrieved from https://www.nctv.nl/binaries/WEB_113154_NCTV_Veiligheid_bij_overnames_tcm31-334520.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2019, April). *Χίμαιρα | Een duiding van het fenomeen 'hybride dreiging'*. Retrieved from https://www.nctv.nl/binaries/Duiding%20fenomeen%20Hybride%20Dreiging_tcm31-385687.pdf

Neneth, W. (2015, April 17). *Russia's State-centric Hybrid Warfare* (Rep.). Retrieved October 20, 2018, from International Centre for Defence and Security website: https://icds.ee/russias-state-centric-hybrid-warfare/

Netwerk Weerbaar Bestuur. (2018, April 5). *Intentieverklaring* [PDF file]. Retrieved from https://www.lokale-democratie.nl/netwerkweerbaarbestuur/sites/default/files/files/2018-03-30_Intentieverklaring_Netwerk_Weerbaar_Bestuur_def_%20%281%29.pdf

Niblett, R. (2014, July 18). NATO Must Focus on the 'Hybrid Wars' Being Waged on the West. *Financial Times*. Retrieved September 30, 2018, from https://www.chathamhouse.org/expert/comment/nato-must-focus-hybrid-wars-being-waged-west.

Noordegraaf, M., Schiffelers, M., Geuijen, K., De Morree, P., & Pekelder, J. (2018). *Op weg naar een Weerbare Open Samenleving* (Rep.). Universiteit Utrecht. Retrieved June 7, 2019, from https://www.rijksoverheid.nl/documenten/rapporten/2019/01/09/tk-bijlage-op-weg-naar-een-weerbare-open-samenleving.

Ollongren, K.H. (2017a, December 18). *Kamerbrief over heimelijke beïnvloeding van de publieke opinie door statelijke actoren* (The Netherlands, Ministry of Internal Affairs & Kingdomrelations). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/18/kamerbrief-over-heimelijke-beinvloeding-van-de-publieke-opinie-door-statelijke-actoren

Ollongren, K.H. (2017b, November 13). *Kamerbrief over beïnvloeding van de publieke opinie door statelijke actoren* (The Netherlands, Ministry of Internal Affairs & Kingdomrelations). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2017/11/13/kamerbrief-over-beinvloeding-van-de-publieke-opinie-door-statelijke-actoren

Ollengren, K.H. (2018a, December 13). *Kamerbrief over dreiging desinformatie en beïnvloeding verkiezingen* (The Netherlands, Ministry of Internal Affairs & Kingdomrelations) Retrieved from

https://www.rijksoverheid.nl/documenten/kamerstukken/2018/12/13/kamerbrief-over-dreiging-desinformatie-en-beinvloeding-verkiezingen

Ollengren, K.H. (2018b, July 5). *Kamerbrief plan van aanpak voor versterking lokale democratie en bestuur* (The Netherlands, Ministry of Internal Affairs & Kingdomrelations) Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/07/05/kamerbrief-plan-van-aanpak-voor-versterking-lokale-democratie-en-bestuur

Ollengren, K.H. (2018c, March 6). *Kamerbrief over vrijheid van meningsuiting en journalistiek* (The Netherlands, Ministry of Internal Affairs & Kingdomrelations) Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/06/kamerbrief-over-vrijheid-van-meningsuiting-en-journalistiek

Ollengren, K.H. (2019, January 2014). *Beantwoording Kamervragen over plan van aanpak Versterking lokale democratie en bestuur* (The Netherlands, Ministry of Internal Affairs & Kingdomrelations) Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2019/01/14/beantwoording-kamervragen-over-plan-van-aanpak-versterking-lokale-democratie-en-bestuur

Overheidsbrede Beleidsoverleg Digitale Overheid. (2018, July). *NL DIGIbeter Agenda Digitale Overheid*. Retrieved from https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2018/07/nl-digibeter-agenda-digitale-overheid.pdf

Pernik, P., & Hunter, E. (2015). *The Challenges of Hybrid Warfare* (Publication). Retrieved December 21, 2018, from https://icds.ee/the-challenges-of-hybrid-warfare/

Pernik, P., & Jermalavičius, T. (2016). *Resilience as Part of NATO's Strategy: Deterrence by Denial and Cyber Defense* (pp. 1-9, Working paper). Center for Transatlantic Relations.

Prior, T. (2017). *NATO: Pushing Boundaries for Resilience* (Rep. No. 213). Retrieved November 27, 2018, from ETH Zürich - Center for Security Studies website: http://www.css.ethz.ch/content/specialinterest/gess/cis/center-for-securities-studies/en/publications/css-analyses-in-security-policy/details.html?id=/n/o/2/1/no_213_nato_pushing_boundaries_for_resil

Prior, T. (2018). Resilience: The 'Fifth Wave' in the Evolution of Deterrence (M. Zapfe, Ed.). In O. Thränert (Ed.), *Strategic Trends 2018 - Key Developments in Global Affairs* (pp. 63-80). Zürich, Switzerland: Center for Security Studies, ETH.

Pronk, D. (2018, September 20). *HYBRID CONFLICT AND THE FUTURE EUROPEAN SECURITY ENVIRONMENT* (Rep.). Retrieved September 30, 2018, from Clingendael website: https://www.clingendael.org/publication/hybrid-conflict-and-future-european-security-environment

Pulkkinen, E. (2016). Een nationale allesomvattende veiligheidsaanpak - het Finse perspectief. *Nationale Veiligheid En Crisisbeheersing, 14*(5/6), 4-6. Retrieved October 20, 2018, from https://www.nctv.nl/binaries/Magazine Nationale Veiligheid en Crisisbeheersing 2016 5_7 interactief_tcm31-234692.pdf

Pynnöniemi, K., & Saari, S. (2018). Hybrid influence – lessons from Finland. *NATO Review*.

Radin, A. (2017). *Hybrid Warfare in the Baltics - Threats and Potential Responses* (Rep.). Retrieved November 29, 2018, from RAND Corporation website: https://www.rand.org/pubs/research_reports/RR1577.html

Rathke, J. (2016, July 25). *Rising Ambitions and Growing Resources Mark New German Security Strategy* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/rising-ambitions-and-growing-resources-mark-new-german-security-strategy

Renz, B., & Smith, H. (2016). *Russia and Hybrid warfare - going beyond the label* (pp. 1-62, Working paper No. 1/2016). Kikimora Publications. Retrieved December 19, 2018.

Resilience [Def. 31202]. (n.d.). In *NATOTerm*. Retrieved November 18, 2018.

Responding to Russia: Deterring Russian Cyber and Grey Zone Activities [Interview by J. P. Carlin, R. Ledgett, J. N. Miller, & J. A. Lewis]. (2018, March 19). Retrieved September 30, 2018, from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180316_Responding_Russia_Grey_zone.pdf?C6VA33CdIOqPKkCx7vykJ6NGHlW004ny

Rühle, M. (n.d.). Deterrence: What it can (and cannot) do. *NATO Review*. Retrieved November 19, 2018.

Schaus, J., Matlaga, M., Hicks, K., & Conley, H. (2018, July 16). *What Works: Countering Gray Zone Coercion* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/what-works-countering-gray-zone-coercion

Schwartz, P. N. (2015, September 30). *Syria – A New Russian Asymmetric Challenge* (Rep.). Retrieved September 30, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/syria-–-new-russian-asymmetric-challenge

Shea, J. (2016). *Resilience: A core element of collective defence* (Publication). Retrieved January 13, 2019, from NATO Review website: https://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm

Shekhovtsov, A. (2015, April 24). *The Challenge of Russia's Anti-Western Information Warfare* (Issue brief). Retrieved December 19, 2018, from International Centre for Defence and Security website: https://icds.ee/the-challenge-of-russias-anti-western-information-warfare/

Shevchenko, V. (2014, March 11). "Little green men" or "Russian invaders"? *BBC News*. Retrieved December 13, 2018, from https://www.bbc.com/news/world-europe-26532154

Shirreff, R. (2010, March 23). *Unity of Purpose in Hybrid Conflict: Managing the Civilian/Military Disconnect and 'Operationalizing' The Comprehensive Approach*.

Speech presented in Chatham House, London. Retrieved September 30, 2018, from https://www.chathamhouse.org/sites/default/files/public/Meetings/Meeting Transcripts/230310shirreff.pdf

Snyder, G. H. (1960). Deterrence and Power. *The Journal of Conflict Resolution, 4*(2), 163-178. Retrieved November 19, 2018.

Svitková, K. (2017). RESILIENCE IN THE NATIONAL SECURITY DISCOURSE. *Orbana a Strategie, 2017*(1). Retrieved November 27, 2018, from https://www.obranaastrategie.cz/en/archive/volume-2017/1-2017/articles/resilience-in-the-national-security-discourse.html

Takacs, D. (2017). Ukraine‘s deterrence failure: Lessons for the Baltic States. *Journal on Baltic Security, 3*(1), 1-10. Retrieved November 16, 2018.

The European Centre of Excellence for Countering Hybrid Threats [COUNTERING HYBRID THREATS]. (n.d.).

The National Defense Strategy of the United States of America (Rep.). (2005, March). Retrieved November 9, 2018, from Department of Defense website.

The Netherlands, Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2017). *Cybersecuritybeeld Nederland CSBN 2017*. Retrieved December 13, 2018.

Ullman, H. (2015, March 9). Hybrid War: Old Wine in a New Bottle? *Atlantic Council*. Retrieved December 18, 2018, from https://www.atlanticcouncil.org/publications/articles/hybrid-war-old-wine-in-a-new-bottle

Van Dale. (n.d.). Weerbaar. In *Van Dale*. Retrieved June 7, 2019, from https://www.vandale.nl/gratis-woordenboek/nederlands/betekenis/weerbaar#.XPpQ3i2iE_U

Van der Putten, F., Meijnders, M., Van der Meer, S., & Van der Togt, T. (2018, May 16). *HYBRID CONFLICT: THE ROLES OF RUSSIA, NORTH KOREA AND CHINA* (Rep.). Retrieved September 30, 2018, from Clingendael website: https://www.clingendael.org/publication/hybrid-conflict-roles-russia-north-korea-and-china

Van Engelshoven, I. (2018, July 12). *Verslag OJCS-Raad 22 en 23 mei 2018* (The Netherlands, Ministry of Education, Culture & Science). Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/07/12/aanbiedingsbrief-bij-het-verslag-van-de-onderwijs-jeugd-cultuur-en-sportraad-ojcs-raad-22-en-23-mei-2018

Weitz, R. (2014, November 21). *Countering Russia’s Hybrid Threats* (Issue brief). Retrieved October 6, 2018, from International Centre for Defence and Security website: https://icds.ee/countering-russias-hybrid-threats/

Winter, H., & Woestenburg, N. (2017). *Eindrapportage Criminele beïnvloeding van het lokale openbaar bestuur.* (Rep.). ProFacto. Retrieved June 7, 2019, from https://www.rijksoverheid.nl/documenten/rapporten/2017/10/05/rapport-criminele-beinvloeding-van-het-lokale-openbaar-bestuur.