



Redefining the Battlefields: The Dutch Ministry of Defence's Role in Societal Resilience

A qualitative study on the ministry's potential to contribute to societal resilience-building

R.J.L. (Rob) Baggermans

Radboud University Nijmegen

The Netherlands Ministry of Defence

A thesis submitted for the degree of

Master of Science

19 June 2024

COLOPHON

Radboud University Nijmegen
Nijmegen School of Management
Centre for International Conflict Analysis and Management

Elinor Ostromgebouw
Heyendaalseweg 141
6525 AJ Nijmegen
The Netherlands

Ministry of Defence
Directie Aansturen Operationele Gereedheid (DAOG)
Internship Researcher

Plein-Kalvermarkt Complex
Kalvermarkt 32
2511 CB Den Haag
The Netherlands

Author	R.J.L. (Rob) Baggermans
Student number	1005874
Master's programme	Human Geography
Specialisation	Conflict, Territories and Identities
Thesis supervisor	Dr. W. (Willemijn) Verkoren
Research period	February 2023 – June 2024

Disclaimer

The opinions and conclusions discussed in this study originated from the student of the Radboud University Nijmegen and do not necessarily represent the vision of the Radboud University Nijmegen, the Dutch Ministry of Defence or any other organisation and institution.

ABSTRACT

In the contemporary landscape of hybrid warfare, safeguarding the state, territory and population from multifaceted threats targeting military, economic, political, and social vulnerabilities is imperative. The government has to adapt to set up an appropriate response, which is found in the concept of resilience. This research examines the role of the Dutch Ministry of Defence (MoD) in particular when enhancing societal resilience. Societal resilience-building is approached through the lens of psychological defence within a whole-of-society approach, a Nordic policy response to counter hybrid threats. Initial findings revealed that the primary responsibility for societal resilience in the Netherlands lies with the *Nationaal Coördinator Terrorisme en Veiligheid* (NCTV), with the MoD assuming a facilitating and supporting role. The question arises to what extent the MoD is capable of contributing to societal resilience-building. This study highlights the necessity for the armed forces to collaborate in a whole-of-government approach to address vulnerabilities and bolster situational awareness among government partners. Ultimately, through increased visibility and improved communication, the MoD could contribute to culminating this approach into a whole-of-society approach, fostering a nationwide understanding of hybrid threats to enhance civil awareness and preparedness and strengthen societal resilience.

Key words: societal resilience, hybrid threats, psychological defence, whole-of-society approach.

TABLE OF CONTENT

Preface	V
Abbreviations	VI
Chapter 1 Introduction: The Ministry of Defence in a changing security landscape	1
1.1 Societal relevance	6
1.2 Scientific relevance	9
1.3 Thesis outline	11
Chapter 2 Theoretical and conceptual points of departure	13
2.1 Hybrid threats	13
2.2 Whole-of-society approach	16
2.3 Resilience	18
2.4 Psychological defence	22
Chapter 3 Methodology and data collection	26
3.1 Research strategy	26
3.2 Data collection and analysis	28
3.3 Internal and external validity	29
3.4 Research ethics	30
Chapter 4 Psychological defence in the Nordic context	31
4.1 Civil defence and societal security	31
4.2 The conceptualisation of psychological defence	35
4.3 The operationalisation and implementation of psychological defence	38
4.4 Best practices and challenges	41
Chapter 5 The barriers to enhancing societal resilience	46
5.1 Legal limitations	46
5.2 Societal limitations	51
5.3 Interdepartmental limitations	55
Chapter 6 Societal positioning and the way forward	59
6.1 Interdepartmental	59
6.2 Communicative	62
6.3 Visibility	65
Chapter 7 Conclusion	69
7.1 Discussion	72
Bibliography	73
Appendix	80

PREFACE

Before you lies the study that marks the end of my Master's specialisation Conflicts, Territories and Identities as part of the Human Geography Master. With the conclusion of this work, my seven years of study at the Radboud University Nijmegen have been finalised. This study allowed me to dive deep into the world of hybrid warfare and the nation's battle to come up with an appropriate response. As a topic high on the political agenda, I have shed light on one small piece of the puzzle. Moreover, conducting this research not only generated promising insights into the governance of countering hybrid threats but also gave me personally a better view of the interconnectedness of our government departments, especially in the security domain, as well as the interrelatedness of the various aspects of the state's national security. Similarly to my own experience, I hope this study serves as a wake-up call. The creeping influence of malicious actors, both nationally and internationally, deserves our widespread attention as adversaries aim to undermine the values and the very fundament upon which our democracy is built.

This research was conducted during my time as a research intern at the Dutch Ministry of Defence. The interplay between scientific research and the practical everyday reality of the ministry has proven to be challenging at times but rewarding in the end. Various colleagues within or affiliated with the MoD have helped me to shape my research questions in a way that they were both relevant and feasible. Again, my experience as an intern at the ministry has helped me personally in my quest to shape my future career path by allowing me to explore the intricacies and challenges, as well as the inner workings of the Dutch government. I would like to express my deepest gratitude to the respondents who have dedicated their time, energy and wisdom to help me answer my research questions. Without your support, I could have not succeeded. Furthermore, a word of appreciation goes out to my colleagues, who not only helped me shape my research but also gave me plenty of joy while doing so. The latter is also applicable to my fellow students, who pulled me through the sometimes exhausting periods of hard work and setbacks. Lastly, though, I sincerely want to thank my thesis supervisor, dr. Willemijn Verkoren. Willemijn, your patience and positivity have been indispensable in my journey to complete this study. I truly appreciate the dedication and willingness to help that you have shown over the past months.

Rob Baggermans

Nijmegen, 19 June 2024

ABBREVIATIONS

AIV – *Adviesraad Internationale Vraagstukken*
BZK – Ministry of the Interior and Kingdom Relations
CdS – *Commandant der Strijdkrachten* (Netherlands Chief of Defence)
CHU – Counter Hybrid Unit
CI – Critical Infrastructure
CIMIC – Civil-military cooperation
CSM – Comprehensive Security Model
C&E – Joint Center of Expertise Communication & Engagement
DCo – Directorate of Communications
DGB – Directorate of Policy
EU – European Union
EZK – Ministry of Economic Affairs and Climate Policy
FOI – Swedish Defence Research Agency
HCSS – The Hague Centre for Strategic Studies
InfoOps – Information Operations
I&W – Ministry of Infrastructure and Water Management
OCW – Ministry of Education, Culture and Science
PsyOps – Psychological Operations
Mil PA – Military Public Affairs
MoD – Ministry of Defence
MPF – Psychological Defence Agency
MSB – Civil Contingencies Agency
NATO – North Atlantic Treaty Organization
NCTV – *Nationaal Coördinator Terrorisme en Veiligheid*
RBRK – *Rijksbreed Responskader tegen Statelijke Dreigingen*
StratCom – Strategic Communications
TD – Total Defence

1. INTRODUCTION: THE MINISTRY OF DEFENCE IN A CHANGING SECURITY LANDSCAPE

During the Cold War, NATO members experienced a high level of threat from the communist East. Two major blocs competed over power and dominance, leading to hostility towards one another. It was in 1989, when the Berlin Wall fell, and subsequently in 1991, when the Soviet Union collapsed, that this threat diminished. As a result, Western European states felt safe and NATO's military focus shifted from its first core task (protection of national and allied territory) to its second (maintenance and promotion of international legal order and stability), to be achieved through expeditionary missions in the Balkans or outside the European continent (Bessems, 2021). Simultaneously, NATO members started to neglect their defensive infrastructure and military logistics domestically. By downscaling these capabilities, they diminished the level of deterrence and defence (Scaparrotti & Bell, 2020). However, the 9/11 events, the COVID-19 pandemic, the growing Chinese influence on the world theatre and in the cyber domain, and the Russian invasion of Crimea in 2014 and its violent full-scale attack on Ukraine in 2022 have shown how vulnerable Western European societies are (Wigell et al., 2021; Frizzelle et al., 2022; Antai & Hellberg, 2023). As a consequence, "Europe has woken up from its post-Cold War slumber with NATO returning to its focus on collective defence and deterrence and its ability to strengthen its frontlines at short notice", according to a Clingendael report from July 2019 (Drent e.a., 2019, p. 5).

The above-mentioned vulnerabilities showcase the emergence of new power blocs, with the US and Western allies on one hand and China or Russian adversaries and allies on the other. In this current threat environment, adversaries challenge Western societies through military and non-military measures, both traditional and non-traditional. Besides using hard military power, adversaries make use of clandestine acts, such as intelligence operations, disruptive cyberattacks, economic coercion, disinformation campaigns and influencing political arenas. For example, both China and Russia have been known to engage in extensive espionage, to covertly bribe European politicians, to hack the cyber-infrastructure of a variety of public and private institutions and to spread polarising content and disinformation on social media channels like YouTube, TikTok and X. Additionally, Western states are concerned over the growing foreign investment of Russia and China because of the potential weaponisation of these influences as was the case in Russia's aggressive energy policy towards the West or the Chinese trade war with Western enterprises (Frizzelle et al., 2022). In EU and NATO circles, such non-military acts are called 'hybrid warfare' (Wither, 2020; Elonheimo, 2021). According to Elonheimo (2021), malicious actors such as China and Russia – but in the future potentially others too – use them to "disseminate uncertainty and friction in governments' and citizens' daily lives" (p. 115) and weaken states. In doing so, Elonheimo argues that hybrid threats reveal the vulnerability of open democracies and their security architecture.

The emergence of hybrid warfare has led to a change in the security landscape. Hybrid warfare exposes the grey zone between peacetime and wartime. In this grey zone, there is a war fought out

'below the threshold', referring to the absence of military combat. Belligerents clash in political, diplomatic, economic or social matters, but military confrontation is avoided (Wither, 2020). It generates conflict because it creates tension and competition. Additionally, governments have found it difficult to respond appropriately to these threats due to the uncertainty that these threats bring about as well as the inexperience of government in dealing with them. From the perception of the MoD, it hinders their room of manoeuvre to conduct countermeasures against hybrid threats or, in the worst case, prepare for war. Hybrid warfare is characterising the new state of permanent competition in which the competing geopolitical blocs currently are.

In turn, the changing security landscape requires new thinking in terms of national security and resilience. Just as hybrid threats play out in the social, political, economic or diplomatic realm, so do they alter the targets. Additional to a whole-of-government that entails interdepartmental cooperation involving a broad scale of government actors, the MoD thinks a comprehensive whole-of-society approach mobilising non-state actors as well as the public at large is required to effectively counter hybrid threats (Wither, 2020). As such, preparing for (hybrid) conflict is not just a task for the MoD or the government alone. It requires civilian participation too, because citizens can be targeted as well through covert disinformation campaigns or polarisation. As such, scholars such as Smith (2019) and Wrange (2022) point towards society's responsibility to enhance its awareness and preparedness regarding countering hybrid threats.

In the present era of hybrid war below the threshold, resilience has become NATO's top priority. This is nationally as well as internationally a hot topic among political and military elites, as NATO member states aim to improve their resilience to resist and recover from serious shocks, including conventional armed offensives and/or hybrid attacks, which can deliberately cause or consequently lead to disruption of critical infrastructure (CI) due to their destructive political, economic, and societal damage. CI entails a wide range of infrastructure systems, such as energy and water supply, healthcare, ICT and financial systems, telecommunications, chemical and nuclear industry and transportation networks. A cloak of unpredictability surrounds such threats because they transcend the traditional military realm and instead target a broad scale of the state's vulnerabilities, including but not limited to its citizens, (nuclear) energy industry and ICT. As a base of Western security thinking, resilience as a concept differs from crisis preparedness in that the former stresses the idea of unfamiliarity and unpredictability of crisis events, whereas the latter departs from identifiable hazards. It also differs slightly from 'security' which is about proactive, preventative measures against hazards, resilience goes beyond this by also addressing the reactive capacity of government policy (Fjäder, 2014). Security aims at protecting the state against harm, whereas resilience focuses not only on protection but also on recovery of systems, infrastructures and services. NATO defined resilience as a society's ability to resist and recover from disruptive shocks (NATO, 2022).

Resilience has thus become a key term in Western security doctrines. However, the concept of resilience is not straightforward. It causes confusion among scholars, policymakers and government

officials. Different perceptions and visions make it a complex concept. Understanding resilience is not as easy as it seems, as the concept is broken down into several dimensions, capacities, characteristics, and principles. Among those dimensions are the technical, organisational, economic and societal (Setola et al., 2016; Labaka et al., 2016). For this research, the focus is on societal resilience which is about society's ability to "respond to shocks, absorb them without suffering from severe fractures, and then recover" (Christie & Berzina, 2022, p. 3). Societal resilience can be translated into civil awareness and preparedness. The former stresses awareness among citizens of the threats that hybrid warfare poses and of their own responsibility in the resilience-building of their nation, alongside the defensive capacity of the armed forces. Such awareness could lead citizens to adopt a more critical stance against hybrid influences, for instance in the form of disinformation on social media. Civil preparedness goes one step further, referring to an active civilian role that can mitigate negative consequences and show a willingness to support the armed forces in conflict situations (NATO, 2022).

Zooming in on the concept of societal resilience, a critique that comes to the surface is its supposed conceptual vagueness. Fjäder (2014) argues that the concept of societal resilience requires a certain state of equilibrium that has to be preserved or recovered. Although this is clearly defined for tangible objects, it is much less definable for complex systems like a society. The concept aims at building a resilient society that can resist and recover from disturbances and unexpected events, also known as an all-hazard approach. However, in such an approach, it is unclear how to determine whether and to what extent societal resilience has been established (Fjäder, 2014; Anholt et al., 2021). This vagueness opens the way for a "constant state of exceptionalism and securitisation" in society, while simultaneously serving neoliberal security thinking that places the burden upon the shoulders of the citizens through the culture of civil preparedness (Anholt et al., 2021, p. 553), which will be discussed more in-depth later. Recognising the thin line between stimulating the public and instrumentalising them is important.

Research on societal resilience is valuable because up until now there is little research done on this topic in the Dutch context. "Today's security environment, dominated by hybrid threats, shows that civil and military components need to be better integrated. The changing understanding of security has also changed the role of political power in the military and civilian spheres. Cooperation between the military and civilian sectors is central when it comes to countering hybrid threats" (Smith, 2019, p. 23). As a central actor in the Dutch security domain, the MoD attributes itself to an important role in enhancing said resilience although it is the *Nationaal Coördinator Terrorisme en Veiligheid* (NCTV) that primarily deals with societal resilience. Despite the MoD's limitation in societal resilience-building, it can still contribute to its improvement. An advisory report from the *Adviesraad Internationale Vraagstukken* (AIV) advocated stressing the MoD's role as an interlocutor interacting between the government and societal actors. Improving the connection with society "could be given a more prominent position in the formation of security-conscious Dutch citizens" (2024, p. 45). Thus, a joint comprehensive interdepartmental collaboration translating into a whole-of-government approach,

eventually culminating into a whole-of-society approach is required. In this regard, the Hague Centre for Strategic Studies (HCSS) urges the Dutch government to give clear substance to the MoD's contribution to enhancing societal resilience. According to the authors, the MoD can, as a security actor guarding national safety and security, play an important role as a facilitator in providing a clear structure to society's commitment to resilience, especially in challenging times of hybrid warfare. Similar research was conducted in 2021 in the UK, where the researchers captured it aptly: "Societal resilience is often described as requiring a 'whole-of-society' approach, with Defence [the MoD] providing a supporting role. In this sense, understanding Defence's place in helping a country prepare for and respond to crises is essential" (Caves et al., 2021, p. IV). This role, however, has to be conceptualised and concretely operationalised (Bekkers et al., 2023). Reflection on the MoD's positioning and its role in society taps into discussions on this topic that are vividly taking place within the walls of the ministry and to a lesser extent within the government. Eventually, these discussions should be held within society at large, thus paving the way by conducting research hereupon, according to a defence staff member dealing with national security (personal communications, 7 September 2023).

An essential part of societal resilience is considered to be psychological defence. This policy concept originates from Scandinavian countries, where civil preparedness is consistently higher because countries like Sweden and Finland experience a threat from Russia. Those countries focus on countering psychological warfare, including deception and disinformation campaigns, rumour-mongering and malevolent propaganda. This addresses the cognitive dimension of citizens' minds targeting their awareness and preparedness, thus requiring resilience-building (Houck, 2022). Psychological defence is in line with the notion of societal resilience and serves in this study as a conceptualisation of that type of resilience. In Scandinavian countries, psychological defence doctrines are built up of three components. First, to counter the above-mentioned malicious acts of hybrid warfare. Second, to ensure effective government communication in case of crisis, war or disruption of government services. And thirdly, to strengthen the population's will to defend their homeland (Rossbach, 2017). The idea of the doctrine is to tackle emerging hybrid threats while simultaneously enhancing civil awareness and preparedness. "Psychological defence activities [...] while counteracting operations that occur in peacetime, must be prepared for wartime", according to Rossback (p. 2). In doing so, the concept covers multiple government policies such as those responding to disinformation campaigns and information warfare and those aiming to enhance resilience or public morale by addressing civilian contribution to the state's resilience. In this study, psychological defence is defined as strategies and measures designed to increase the resilience of individuals by stimulating awareness of hybrid threats and stimulating them to contribute to defending the country, despite the government's tendency to place the burden on the individual's shoulders as it aims to include citizens in its security strategy, as argued by Anholt et al. (2021).

Approaching societal resilience through the lens of psychological defence allows for an understanding of how the MoD strategically positions itself in society, thereby enhancing the public's

ability to withstand diverse, hybrid challenges. Additionally, it provides a way to operationalise societal resilience as argued by Bekkers et al. (2023). Because in Scandinavian countries civil preparedness and awareness are much higher, it is valuable to analyse their approach to psychological defence and then – considerate of their national contexts – reflect on the best practices and the associated challenges that can be applied to the Dutch case. It underscores the necessity for strategic reflection and decisive action by the MoD and the broader community to fortify the nation's psychological defence capabilities and resilience. Psychological defence sheds light on psychological warfare, and aims to counter it. However, when mobilising the public to take on their responsibility, there is a delicate line between informing and influencing them psychologically. What justifies the latter and how does it relate to propaganda and framing? Seeing psychological defence in part as a form of strategic communication, what role does the MoD play in this regard and what strategic choices does it face? The underlying debate is heavily polarised, namely “whether it is ever appropriate for military strategic communications to aim to influence a domestic audience” (Fry, 2022, p. 178).

This study hopes to contribute to this debate by providing more clarity on the actual workings of psychological defence, its potential to contribute to societal resilience-building and its consequences for the societal positioning policy of the MoD. Assessing the ministry's societal positioning requires a reflection on its outward communication as that plays a major role in enhancing psychological defence. It requires that the ministry makes strategic policy choices on how or how not to communicate with the general public. However, Fry (2022) points towards the myth that there exists something as value-free information. Behind all military communications hides an attempt to persuade audiences to see the world as the MoD does. The ministry should be cautious in distinguishing stimulation from instrumentalisation. If executed adequately, clear communication will enhance the level of trust that citizens will put in the MoD as a societal partner. Consequentially, it might enable the military apparatus to operate side-by-side with citizens on hybrid issues. To achieve that, however, communication must not occur ad hoc but systemic and strategic (Longstaff & Yang, 2008, p. 3). Therefore, analysing the ministry's outward communication offers a relevant window through which to assess its role in Dutch societal resilience-building strategies.

In this study, the focus will be on the MoD's role in contributing to enhancing these strategies, approached through the lens of psychological defence. If the MoD is to play a role in boosting civil awareness and preparedness, citizens must consider the ministry to be a skilled and trustworthy societal partner. As a result, improving societal resilience requires a careful reflection of the MoD on its positioning in society and the policy that is enacted, as well as the potential pitfalls in enacting such policy. The central research question is thus formulated as follows: *how does the Ministry of Defence position itself as a societal partner in enhancing societal resilience in the current international context of permanent competition and hybrid threats?* Societal resilience will be approached through the lens of psychological defence as the latter provides a useful frame to address and potentially improve the current state of societal resilience, which is extensively conceptualised yet remains vague due to various

interpretations. Departing from the perspective of the MoD, it is useful to assess how the ministry operationalises societal resilience-building strategies, what shortcomings it might face when enhancing said resilience, how these strategies stimulate rather than instrumentalise the public and if psychological defence doctrines offer fertile ground for Dutch security policy.

1.1 Societal relevance

In the current context of permanent competition, hybrid warfare threatens not just the government, but also the well-being of the state and its citizens. Hybrid threats have revealed the vulnerabilities of the present-day security framework, for instance in the cyber domain, where malicious actors can target vulnerable groups without strong supervision (Elonheimo, 2021; personal communications, 3 March 2023). Combined with a whole-of-government approach, military strategists believe a whole-of-society approach must be adopted, to ensure that the state and the citizens' vital interests are protected. This approach aims to foster coordination and collaboration between government departments, civil organisations, the private sector and the population at large through a culture of awareness and preparedness (Gruber, 2017). The goal is to create a comprehensive system of resilience because the state alone is not capable of achieving a proper overarching level of resilience in relation to hybrid threats (Wigell et al., 2021).

The individual citizen plays a pivotal role herein. Sundelius and Eldebald (2023) stress the importance of individual preparedness, because without it is very difficult to achieve a whole-of-society framework. Citizens have grown to become more vulnerable, but not just because of cyberattacks. "In the age of terrorism, global pandemics, rising political tensions between nuclear-armed states, and a deepening climate crisis, [...] preparedness is once again making headway on the political agenda in many countries" (Cronqvist et al., 2021, p. 2). Hybrid warfare has therefore led to the redevelopment of national defence frameworks. This research can contribute to these efforts by shedding light on the specific topic of Dutch societal resilience through psychological defence because as of yet there is little known about such resilience-building strategies within the Netherlands.

During the Cold War, political and military leaders referred to a concept called civil defence, which included civilian preparedness for the possibility of conventional or even nuclear warfare. Citizens were to take on an active role in the national security framework to enhance societal resilience. However, this focus was abandoned after the Cold War. European government shifted their attention to expeditionary missions in peacebuilding, thereby downscaling domestic defence structures. The notion of threats coming from other states became less imminent and, because technological developments paved the way for new threats (e.g. cyber threats), the necessity of an active civilian role in national defence frameworks therefore decreased (Wrangle, 2022). The marginalisation of domestic defence structures was partly shown by the relative decline in defence expenditures – which increased again since 2014 – as well as the abolishment of conscription in 1997 (Schoenmakers, 2022). In an informal conversation with a military strategist, it came to the fore that society seems to have lost its connection

to the military apparatus due to this abolishment (personal communications, 28 August 2023). To close this gap, the MoD believes it should reassess its bond with society at large and reflect on how it positions itself. Taking into account the present geopolitical context, it becomes apparent why a reassessment of the dynamic between the MoD's responsibility and the individual's role is important.

That is because it fits into a broader issue within Dutch society, namely the decreased level of trust and confidence among citizens in their government and political leaders. This decline is partly due to a lack of openness and transparency (Centraal Bureau voor de Statistiek, 2023). In this way, it ties back to the aforementioned statements that the ministry needs to be perceived as a trustworthy societal partner because this issue in Dutch politics affects the MoD as well for being one of the government's branches. What comes to the fore is an interconnectedness between societal trust in politics, the government, and the armed forces. The MoD considers trust as essential for successful cooperation between the military and broader society and requires transparency. Enhancing societal resilience requires a reassessment of the ministry as a reliable partner. Such reassessment is beneficial for the debate because the anchoring of the armed forces within society is under pressure due to the declined confidence. Societal resilience may enhance the relations between the two if carefully carried out. When building resilience, crisis preparedness is not a neutral or isolated activity but is shaped by and influences the larger contexts in which it occurs. In other words, it becomes visible that "planning, executing and experiencing institutionalised forms of emergency preparedness did not historically – nor does it today – take place in isolation from societal, cultural and political agendas", meaning that underlying government agendas might not always become apparent at first but they do exert pressure on policy-making, reflecting the priorities of the government (Cronqvist et al., 2021, p. 3). Those priorities, seemingly well-meant, can be controversially perceived as 'instrumentalising' the public or 'securitising' societal resilience-building.

Securitisation critically refers to the practice of approaching a certain issue as a 'security issue' and characterise such security issues as actual 'threats', thereby elevating it "from the realm of 'normal' politics into the realm of security politics" so that it provides government authorities with space of manoeuvre for extraordinary security measures (Fjäder, 2014, p. 118). These measures may put a strain on civil rights pertaining to for instance the right of free speech or the right to privacy. When governments claim that more and more aspects of daily life are threatened by hybrid warfare (such as the socio-economic or information environment), they redirect such aspects to the security discourse and thereby run the risk of securitising. Due to the emergence of resilience as an object of study, it has been picked up and proposed by governments as a solution against securitisation. The downside of this solution is that the "concomitant commoditization of safety and security 'products' are pursued through the construction of resilience as a 'good' and 'desirable' capacity of the adaptive, resilient subject" (Bergström, 2018, p. 37). Bergström points towards the decentralisation of responsibility, to which he refers as 'responsibilisation': creating "a moral of self-regulating, self-determined and self-sustained subjects that allows governments to step back". It entails the gradual shift in responsibilities from the

government to the individual. In doing so, the government alters the division of responsibilities by gradually pulling away its role in the security domain and placing it on the shoulders of the individual. Bergström describes a downward spiral where citizens and local networks ought to ensure their own security while simultaneously sharing “the cost for the ‘commoditised’ products of societal safety and security” (2018, p. 36). Thus, two interrelated critiques emerge; the risk of securitisation and the process of responsabilisation.

Larsson (2021) also critically refers to this tendency to deliberately place responsibility upon the shoulders of individuals as ‘neoliberal governmentality’. According to him, the government gradually withdraws itself by placing ‘moral’ responsibility framed as civil preparedness in the hands of citizens, who have accepted living in conditions of insecurity. “This type of approach to the spectrum of threats and dangers brings together both security and crisis management such that the wellbeing of states, societies, populations and individuals are increasingly ‘securitized’. [...] A substantial element of security governance now concerns the perceived need for preparedness to face crises that have yet to occur” (Larsson, 2021, p. 307). Within this conceptualisation of neoliberal governmentality hides a notion of resilience, potentially utilised by governments for securitising purposes. When saying crises that have yet to occur, Larsson’s statements can be tied to resilience as resilience departs from the idea that crises are unpredictable and unfamiliar (Fjäder, 2014). The role of citizens in crisis situations is being projected onto an ever-present notion of state security. In other words, citizens have to be prepared at all times.

Although it corresponds with the policy set out by the government insofar as it urges the Dutch population to be alert and prepared, the notion of neoliberal governmentality that Larsson criticized does not seem to match with the line of Dutch policy. The Security Strategy 2023-2029, a comprehensive security approach drawn up by multiple departments under the supervision of the NCTV, states that security is a core task of the government and therefore it is legitimate and right that the people look up to the government for strengthening of national security (NCTV, 2023). The strategy does call on individuals to contribute to a safe and resilient society, but it does not specify how they can be made more alert and prepared, nor does it say anything about who bears responsibility for this preparedness. The Defence White Paper (2022) also does not elaborate on the role and responsibility of citizens, other than stating that the MoD will “seek more connections with society and address new target groups in innovative ways and try to inspire them to contribute to the resilience of the Netherlands” (p. 22). Rather than using a plea for morality and moral responsibility in the resilience discourse, the government takes on the role of ‘supplier/facilitator’ of national security. However, in this reasoning, there is a paradox that Bergström (2018) also recognised. The government enables citizens to take their responsibility and prepare themselves. Rather than citizens supporting the government – the military apparatus in this regard – which is usually referred to as enablement (see Christie & Berzina, 2022), it appears like to opposite is the case here. A sort of reversed enablement, in which it is the government that enables society at large. On the one hand, such efforts could be seen as the empowerment of citizens in

safeguarding their own security and that of their local community. On the other hand, however, this empowerment appears to be an exercise of responsabilisation as it places the responsibility upon the shoulders of the individuals. In the Netherlands, the government stated that safety and security are their responsibility. Yet, without any further course of action, it appears to resort to a certain extent of responsabilisation in Dutch government policy. That, however, points towards the problem at hand: should there be a tendency to include citizens more in a whole-of-society resilience-building effort?

In the 2022 Defence White Paper, the ministry stated that it actively sought to enhance its connection to society and that it wanted to find new ways to address and inspire people to contribute to the (societal) resilience of the Netherlands (Ministry of Defence, 2022b, p. 22). It seemed as if in this specific document the MoD's narrow understanding of resilience only entails reaching out to new, younger employees. The document shows no further operationalisation of the concept of societal resilience, lacks an explanation of what this resilience specifically entails, and does not clearly define the responsibility on the part of the MoD. The document moreover fails to pay attention to the role that citizens themselves have in building societal resilience. "The Dutch society may look at the armed forces as 'the last man standing', but vice versa may that same society be addressed – for instance by the MoD – on its own responsibility" (Bekkers et al., 2023, p. 15).

1.2 Scientific relevance

This study addresses a critical gap in our understanding of how the MoD adapts to counter non-traditional (hybrid) threats and actively engages with and mobilises the civilian population to incorporate them into a comprehensive approach to resilience. This gap is particularly pertinent because the present-day nature of conflicts has changed to war below the threshold. Very little research has been conducted on resilience-building through a civilian-centred approach. Discussions on how the Dutch population should enhance awareness, and prepare for and participate in societal resilience-building efforts are now held primarily within government walls, but will shortly have to be addressed within society. This study seeks to contribute to this debate.

Scholars in the field of security policy often point to a vulnerability that is inherent to modern-day society due to hybrid threats blurring the boundaries between war/peace and crisis/security. As a result, the concept of security is widened to include the current uncertain geopolitical situation coupled with the urgent need to protect ourselves (Larsson, 2021). From a governmental point of view, capable and crisis-aware citizens can ease the pressure on government authorities. The role of these citizens gained prominence due to the crises and external forces that threaten society. Societal resilience-building is often found to be the answer to combat hybrid warfare. Whereas crisis management departs from the idea that crises are identifiable, resilience-building emphasises the unfamiliarity of crisis events. "In this context, resilience has become an essential concept in the field of crisis management and CI protection" (Labaka et al., 2016, p. 22). Because of the interconnectedness and interdependency of present-day

societies and infrastructural networks (e.g. supply chains, energy distribution and digital connectivity), and the uncertainty of hybrid threats, it is nearly impossible to forecast crises and therefore the focus should shift to resilience. This view was reinforced by NATO (2022), who claimed resilience to be an important area for scientific analysis based on assessments of resilience in NATO member states following the changing national security landscape (e.g. the Russian invasion of Ukraine and the Nordstream sabotage).

In scientific literature much has been written about resilience. 'Resilience' is a rather abstract concept which is interpreted in a variety of ways. Resilience-building as a national strategy differs from ordinary defence strategies in that it encompasses a much bigger and broader scale, encouraging a whole-of-society approach. The holistic character of this strategy allows it to involve not just technical but also socio-economic or organisational measures. As such, it stresses the interconnectedness and interdependence of societal and infrastructural systems. Resilience is generally understood as a system's ability to resist and restore from critical disruptions, but due to its diverse theorisation and conceptualisation, its definition can often be interpreted in different ways (Francis & Bekera, 2014; Labaka et al., 2016). Hence the pitfall of resilience as a concept is that a clear understanding is difficult. Existing literature primarily pays attention to defining and conceptualising resilience, rather than providing actual tools for how to operationalise it. A gap between theory and empirical reality is thus created, which makes it difficult to apply measures (Labaka et al., 2016; Mehvar et al., 2021). This is directly linked to the absence of clarity and consensus around resilience and its vague conceptualisation. It can be challenging to overcome this gap as it is hard to identify the most effective resilience-building strategies and evaluate their effectiveness.

Along a similar line, Anholt et al. (2021) point towards the conceptual vagueness of societal resilience and conclude that this might pose a risk for the securitisation of said resilience. However, the authors argue that the flawed definition is not completely unfortunate, because the term's fluidity opens a window of opportunity for scholars to adopt a more multidimensional approach rather than being a closed-off concept. Hybrid threats widen the security domain and the MoD, as a central actor in the security landscape, should redetermine its position. In this positioning, however, the risk of securitisation and violation of democratic values could loom. Simultaneously, the neoliberal spirit allows the government to gradually withdraw itself within the security landscape, prompted by the ideology that the individual citizen is to play a role in countering these new threats. Thus, the question arises how the ministry should contribute to societal resilience-building in a manner safeguarding the democratic values it ought to protect and reinforcing societal trust in the defence apparatus. In this regard, delving into the question of how the MoD positions itself as a societal partner contributing to enhancing societal resilience is multifaceted. In the context of permanent competition where traditional distinctions between the military and civilian realm are increasingly outdated, it is important to shed light on the strategies employed by the MoD to shield the population from hybrid threats. By closely examining the ministry's approaches and positioning, this study seeks to contribute to the academic discourse on

societal resilience, and more specifically, psychological defence in the Dutch context.

This study sheds light on the complexity of societal resilience. It can help to overcome the vagueness of the concept. Generally, that is not a subject that is written about much in the Dutch context. By approaching societal resilience through the lens of psychological defence, this research delves into the relatively underexplored intersection of vaguely conceptualised societal resilience and the poorly operationalised culture of civil awareness and preparedness that is often discussed in the literature. Assessing the concept of psychological defence in the Dutch context allows for a scientific reflection on the security discourse in the Netherlands because it helps elucidate the policy framework of civil participation within the national defence architecture. It does so by analysing the societal positioning of the MoD and examining potential gains and flaws in this framework. Psychological defence provides a way to conceptualise and operationalise societal resilience and allows for a reflection on the Swedish and Finnish security architecture – where this concept is enacted as policy – thereby enriching scientific knowledge on these topics and offering practical leads to implement effective measures. In doing so, it expands the body of work on the gap between theory and practice.

1.3 Thesis outline

The objective of this research is to expand knowledge of the MoD's role vis-à-vis societal resilience-building. As an important actor in the security architecture, the ministry's place within resilience-building strategies to counter hybrid threats will be explored and assessed, based on insights from policy documents and experts in the field, by answering the main research question: *How does the Ministry of Defence position itself as a societal partner in enhancing societal resilience in the current international context of permanent competition and hybrid threats?*

To reach this objective, this research question has been divided into three sub-questions which form the framework for the subsequent chapters. The following chapter entails a theoretical and conceptual framework addressing relevant concepts and insights useful for the purpose and scope of this study. Chapter 3 provides an overview of the methodology and the methods used to conduct this research. Then, chapter 4 addresses the first sub-question: what is understood as psychological defence and to what extent can it be applicable in the Dutch context? It dives into the concept of psychological defence: what does it entail, how is it implemented and what are the best practices? For this, Nordic countries' security policy is subjected to close examination. The fifth chapter sheds light on potential barriers by answering the second sub-question: what are the potential barriers that the Ministry of Defence faces when enhancing psychological defence? Various limitations refrain the ministry from taking on a proactive role one might expect from the armed forces. Following, chapter 6 answers the third sub-question: what are the opinions of stakeholders on the way the Ministry of Defence positions itself within society to execute this role? It discusses how the MoD can overcome the aforementioned barriers to play an effective role that allows the ministry to contribute to societal resilience-building

initiatives. This section is based on in-depth interviews with experts in the field. Lastly, chapter 7 will conclude this study by discussing its relevant insights and providing room for further practical and scientific recommendations.

2. THEORETICAL AND CONCEPTUAL POINTS OF DEPARTURE

“The inclusion of new security threats, however, principally non-military threats, mostly posed by non-state actors, [...] into the national security agendas, presented the state with both new challenges and, arguably, new opportunities. If globalisation has been seen to transform the role of the nation-state, in a similar manner it has been argued as having transformed the concept of national security.”
(Fjäder, 2014, p. 117)

This quote from Fjäder (2014) illustrates nicely how national security agendas have changed and what effects this can have on the existing conceptualisation of ‘national security’. He argues that the globalised world poses new threats to states. These new threats significantly alter security assessments. To sufficiently support assessments, existing conceptualisation also needs to be revised to counter these present-day threats. When the concept of national security changes, so does the proper response to it. This starts with an accurate use of concepts. For this research, besides resilience and societal resilience, key concepts are psychological defence, hybrid threats and the whole-of-society approach. Implementing effective resilience-building strategies starts with fitting conceptualisation. Hence, in this chapter, these concepts will be discussed in-depth.

2.1 Hybrid threats

In past times, traditional warfare consisted of conventional armed attacks. Nowadays, adversaries make use of a wide variety of tactics, both traditional and non-traditional, played out by state and non-state actors in a certain grey area between the normal situation and open conflict; the peace-conflict continuum. In EU and NATO circles, such asymmetric acts are deemed ‘hybrid warfare’ (Elonheimo, 2021), as they include both conventional and unconventional, military and non-military, overt and covert actions. Besides using hard military power, adversaries make use of clandestine acts, such as intelligence operations, disruptive cyberattacks, economic coercion, disinformation campaigns, or influencing political arenas. Examples of hybrid hostile actions in the digital domain include shaping public opinions through blogs, social media, and other channels, denying the service of important websites or defacing them by unauthorised alteration of information. Examples of physically hostile actions are shaping opinions through visual methods (graffiti), using deception through fake calls, or holding (il)legal protests and demonstrations (Bankauskaitė & Šlekys, 2023).

The above-mentioned examples show that in the present-day world, the general public can be on the front line of hybrid warfare, mostly without even being aware of it. Citizens are insufficiently resistant to provocations, as stated by a Strategic Analyst from the Hague Centre Strategic Studies (HCSS) in an informal conversation, adding that critical thinking and awareness are vital components that individuals should have towards their environment, digital as well as analogue (personal communications, 7 September 2023).

The occurrence of threats that we today deem hybrid is not quintessentially a feature of 21st-century warfare. Back in the Cold War, adversaries also deployed a great variety of threats to challenge the opposing bloc. Espionage, military (or even nuclear) threats and propaganda were widespread. However, it is the change in global power structures after the Cold War as well as the rapid development of new technologies and communication platforms that have reshaped present-day warfare, blending conventional with non-conventional, overt with covert tactics, leading to asymmetrical disruptive acts (Berzina, 2020). The strategic deployment of ‘weaponised’ objects – such as information and news provision – to conduct these acts led to a conceptualisation of hybrid threats. Consequentially, this concept is widely utilised in today’s security discourse. Another relevant aspect of the current conceptualisation of hybrid threats is the increased globalisation that has characterised the world in past decades. With information and monetary streams flowing across the globe, hybrid threats encompass funding foreign organisations, organising anti-government protest movements, utilising the cyber realm to commit digital disruptive crimes and using economic leverage (Berzina, 2020).

Similarly to resilience, however, there are problems regarding the conceptualisation. Hybrid threats are perceived differently among stakeholders. Although the concept is an integral part of European security policy, it is presently being used as a catch-all term, complicating the delineation of the responsibilities of several institutions as well as hindering the formulation of clear-cut countermeasures. Looking at NATO for a clear-cut conceptualisation does not help. Terms like ‘hybrid threats’, ‘hybrid influencing’, ‘hybrid warfare’ and ‘hybrid warfare threats’ are used interchangeably and equivalently, without making any distinction (Wigell et al., 2021). Critics argue that the term hybrid warfare is vague, imprecise or even misleading, brings about little that is new, or that when coupling various developments with the military term ‘warfare’, the danger exists of “unnecessarily militarising the language of international politics” (Smith, 2019, p. 15). Caliskan and Liégeois (2021) also believe that the term distracts from a solid and preferred interdepartmental approach they refer to as ‘grand strategy’. Instead, the authors advocate for a “holistic vision of the strategic context [...] through the use of all instruments of grand strategy” (2021, p. 310) and claim that every challenge should predominantly be regarded as a policy issue for statecraft, meaning that a broad set of policy responses in a whole-of-government approach suitable for the situation should be considered, rather than as a security issue – as hybrid warfare supposedly does. In other words, including more and more non-military threats in the security domain poses the risk of securitisation.

Smith (2019), however, points to the value the concept of ‘hybrid threats’ offers for encompassing the complexity of current challenges in the security domain. To help provide conceptual clarity, Smith defines hybrid threats as “coordinated and synchronised action that deliberately targets democratic states’ and institutions’ systemic vulnerabilities, through a wide range of means” (Smith, 2019, p. 17). The wide range of means that she is referring to consists of diverse and multifaceted methods that state and non-state actors can employ to achieve (parts of) their objectives. It suggests that those engaging in hybrid threats use various tools and tactics, including but not limited to disinformation

campaigns, cyberattacks, political disruption or economic coercion. Adversaries often deliberately operate in a way that makes it hard to identify and attribute certain actions directly. Furthermore, she stated that adversaries carefully assess the vulnerabilities and exploit the weaknesses that exist between various authorities and sectors, such as between local and national governments or between the military and the civil realm.

Wigell et al. (2021) distinguish hybrid warfare from hybrid interference and hybrid operations. The three differ in their *means*, *deniability* and *control aim*. Firstly, *means* occupy a pivotal position in hybrid warfare because different means require different tactical responses. The authors distinguish non-military, paramilitary and military means. Economic coercion or disinformation campaigns are exemplary of non-military means. Deployment of armed forces is a military method because it concerns state military force. Paramilitary means imply actions by semi-militarised groups that are not formally linked to the state's military apparatus, such as hacker groups, militias or private military companies. Secondly, the authors make a distinction between plausible *deniability*, implausible deniability, and non-deniability. The latter refers to overt actions, such as in the case of conventional warfare in which there is no question of denying. When adversaries want their actions to stay covert, they seek plausible denial. Some covert actions, however, do not need to stay secret. Actions may cause disruption or give a signal, without forcing the adversary to publicly acknowledge them. In that case, he seeks implausible denial. Finally, the authors defined various strategic *aims*: reflexive, functional and territorial control. Reflexive control aims to provoke a reaction that is favourable to the aggressor because it unconsciously advances the aggressor's agenda. Functional control entails using physical means to target critical infrastructures to disrupt their function. When an aggressor aims to gain a physical presence on the ground, thereby destroying the target's sovereignty, he seeks territorial control (Wigell et al., 2021).

For this study, due to the current security landscape, the emphasis lies on reflexive and functional control. Adversaries' reflexive aim could be undermining the government or its authority by decreasing the level of trust in the government or by consciously polarising groups within society. Functional control is much more tangible, for instance disrupting government services. Because the scope of this research does not extend to the scenario of a conventional attack – i.e. territorial control – this will not be thoroughly discussed. Nevertheless, the culture of civil awareness and preparedness also partly entails the capacity of the general population to adapt to such worst-case scenarios. To utilise a comprehensive and coherent definition of hybrid threats, appropriate in the context of enhancing societal resilience, the following definition will be used: *the combination of conventional and unconventional, military and non-military, overt and covert actions to create ambiguity and confusion on the nature, the origin and the objective of the threat by identifying and exploiting the vulnerabilities of the targets while maintaining the capacity to keep the level of hostility below the 'threshold' of conventional war*, as drawn up by Andersson and Tardy (2015).

It turns out to be difficult to come up with a comprehensive approach to counter hybrid warfare due to the vagueness, uncertainty and sometimes the invisibility of hybrid threats. The problem of

detection and attribution makes it hard for NATO members to respond unambiguously. They struggle with hybrid threats. For example, does cyberwarfare count as an act of violence that allows for an appeal to Article 5? How should stakeholders engage in effective collaboration? To counter hybrid threats, a comprehensive collaboration is a central element in practically all literature on hybrid warfare. This means interdepartmental and cross-cutting cooperation among stakeholders (Smith, 2019). In other words, “since hybrid warfare targets the whole of government and society at large, states require comprehensive means to mitigate threats jointly across authorities, organizations, and citizens” (Elonheimo, 2021, p. 129). Such an approach is most often referred to as a whole-of-society approach and it is considered crucial for effectively countering hybrid threats. The goal is to create a comprehensive system of resilience because the state alone is not capable of achieving a proper level of resilience in the face of hybrid threats (Wigell et al., 2021).

2.2 Whole-of-society approach

Authors on resilience-building strategies and countering hybrid threats, including Gruber (2017), Elonheimo (2021), Wigell et al. (2021) and Bankauskaitė and Šlekys (2023), have stressed the importance of adopting an approach that involves a broad spectrum of actors, ranging from the general public to governmental institutions while also including the private sector.

Hybrid threats can target the general population or public opinion as public support is vital in a democratic state. Without support, the pressure on the government would increase in case of disruption. This diminishes the effectiveness of governmental action. See it as follows: an adversary can target critical infrastructure systems with hacking software to disrupt its functioning. Such an act, however, can be quite overt because actions might be traced to government or government-aligned actors. Aiming for plausible deniability, adversaries can also opt for a more covert approach. Instead of targeting logistical CI, they can aim at the general public through disinformation or inflammatory campaigns to evoke resistance or decrease public support for government actions, for instance, the use of logistical CI for military operations. The individual occupies a central place in enhancing societal resilience because, without individual awareness and preparedness, it is hard to achieve a resilient whole-of-society approach (Sundelius & Eldeblad, 2023, p. 101).

Whatever a resilient whole-of-society approach entails, it is not free of controversies and critiques. Juntunen and Hyvönen (2014) claim that the emergence of resilience has led to a thorough alteration of the security domain in which citizens are seen as mere reactive objects to threats. Due to the unpredictability of the threats, especially hybrid ones targeting citizens themselves, the resilience discourse promotes a self-organising society capable of adapting and bouncing back after disruptions. “Resilience invites us to accept that we are fundamentally vulnerable and that the world is a complex bundle of emergent and overlapping socio-ecological processes to which we can only respond by societal adaptation and assimilation, not through political structures in a traditional manner” (2014, p.

22). What follows is a process of responsabilisation, meant to guarantee the continuation of these socio-ecological processes, but in which the individual is subjected to the “closing down of political spaces, as less and less issues are considered as something to be meaningfully addressed through public policy debate” (Juntunen & Hyvönen, 2014, p. 13). Such securitisation is visible for instance in the growing legal, political and operational constraints on civil society organisations as part of risk management strategies on behalf of governments (HSC & ECNL, 2018).

Setting up a whole-of-society approach is deemed important to create sufficient situational awareness, although the abovementioned critiques should be taken into account in the implementation of such an approach (Labaka et al., 2016). Situational awareness entails having a clear understanding of one’s environment, including factors that impact decision-making and follow-up actions. It involves being aware of relevant information, assessing its implications, and anticipating potential risks. Smith states that this goes beyond knowing your “obvious counterparts”, i.e. your enemies. To optimise situational awareness, one should interact with “actors in the field that are not part of your everyday work but ‘out of area’” (2019, p. 19). It can be enhanced by knowledge-sharing, which Elonheimo (2021) highlights. Through sharing information, people can improve their situational awareness and detect hybrid threats early on. Scholars claim that critical thinking and awareness of the risks are abilities that citizens should possess. Knowledge-sharing is also beneficial on a broader scale, among institutions and organisations. Sharing best practices improves resilience-building, according to Smith (2019). It helps to identify emerging trends, new tactics, and evolving security landscapes, allowing actors to respond timely and take proactive measures.

Knowledge-sharing works best if there is sufficient trust between actors (Elonheimo, 2021). Still, the issue echoes earlier critical notes about whether and to what extent the MoD should be considered one of those actors in societal resilience-building. Important security actors, among which the MoD, deem trust an important element of resilience-building because it eases close and effective collaboration and enlarges the willingness to share information (Finnish Security Committee, 2017; Swedish Civil Contingencies Agency, 2021). Moreover, a sufficient level of trust will reduce the decision-making time necessary as actors are on the same page and rely on shared commitment and responsibility. To build trust, lines of communication have to be short and actors have to communicate openly and transparently. Citizens can be mobilised by avoiding making them feel informed one-sidedly or even instrumentalised, meaning that the government should let the citizens feel heard and their concerns understood. However, it remains unclear how it will guarantee two-sided communication. Furthermore, an important role is attributed to the education of citizens. Well-educated citizens improve the level of situational awareness and public preparedness – both key factors in countering hybrid threats – because they know what to look out for and subsequently how to act (Elonheimo, 2021). For example, when exposed to disinformation, unaware citizens may fall for reflexive control (as defined by Wigell et al.), whereas attentive people may distinguish flows of information more easily.

However, trust and education alone are not sufficient to enhance societal resilience. A high level

of trust can be achieved through transparency. A transparent government is essential when communicating with the general population (Labaka et al., 2016). Informing the public about (military) matters that affect their lives, such as military logistical operations, or broader issues, like hybrid threats, goes much smoother when they are aware and supportive of the cause. Again, maintaining a relationship that appears to be mutually understanding aids in gaining support. However, for the MoD as a central security actor, it can be difficult to find a delicate balance between providing openness and maintaining secrecy. Moreover, the question remains to what extent the ministry should be involved in societal resilience-building and what role it should execute within a broader whole-of-society approach. Maintaining a cooperative form of communication is important because, in case of severe disruption, the already existing lines of communication must serve to instruct the general public about their duties and responsibilities, although these can also be communicated in peacetime. Providing information is vital but overall it seems that trust and support are the two most important features that a culture of public awareness and preparedness must deliver.

In conclusion, situational awareness, education, knowledge-sharing and a sufficient level of trust are important features for a successful whole-of-society approach to strengthen societal resilience against hybrid threats. Although not all features fall under the responsibility of the MoD, some, such as situational awareness and trust, are directly related to the position of the MoD within society. A perceived absent military apparatus will decrease the level of trust amongst citizens in the national defence capacity of their armed forces (Ministry of Defence, 2022a). Nevertheless, an apparatus too present could also put pressure on the bond between society and the armed forces, with the risk of securitisation lurking. The MoD sees it as its responsibility to enhance societal resilience by improving a culture of civil awareness and preparedness. Yet, this commitment should reflect an embedding within a comprehensive whole-of-government approach, respectful of the rule of law and democratic values, to enhance society's resilience – hence the relevance of this research.

2.3 Resilience

Similar to hybrid threats, resilience is a vague concept. The lack of clarity causes confusion, not only among scholars but also between policymakers and government officials lower down the line of command. Different perceptions and visions make it a complex concept. Understanding resilience is not as easy as it seems, as the concept is broken down into several dimensions, capacities, characteristics, and principles. For this study, however, it is essential to elaborate on the complexity of resilience and provide a working definition.

In 2018, Bergström analysed how resilience has become an 'object of knowledge' as "the notion of resilience has come to represent the optimistic belief in, and call for, citizens, households, local communities, cities, and nations to adapt to societal disruptions" (p. 32). He distinguished three conditions that are required to elevate resilience as an object of knowledge, namely scientific

availability, political need and defining events. The first refers to the presence of scientific research, data, and methodologies that are accessible and applicable to understanding resilience. It implies that there must be a sufficient body of knowledge and tools within the scientific community to study resilience effectively. Then, political need pertains to the recognition by political actors, policymakers and decision-makers of the importance of resilience in addressing societal challenges and risks. It suggests that there must be a perceived demand or necessity within the political sphere to prioritise resilience as a policy objective. Lastly, significant occurrences or crises that highlight the importance of resilience are defining events. They prompt action to enhance it, serving as catalysts for elevating resilience as a key concern within society and politics. Therefore, such events can drive policy responses aimed at strengthening resilience capacities. When all conditions are met, resilience can enter the discourse on safety and security, according to Bergström.

Referring to the first condition, an important scientific point of departure is C.S. Holling's first conceptualisation of resilience, drawn up in 1973, which he revised multiple times. Embedded in the ecological school, Holling regarded resilience as a measure, measuring "the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables" (Holling, 1973, p. 14). This definition has often been referred to in resilience literature and contains elements for present-day resilience conceptualisations. In a second definition, Holling later placed more emphasis on the system and its preservation as he redefined resilience as "the ability of a system to maintain its structure and patterns of behaviour in the face of disturbance" (cited in Francis & Bekera, 2014, p. 100). He later added the factor of time in his third definition: "Resilience is the buffer capacity or the ability of a system to absorb perturbations, or the magnitude of disturbance that can be absorbed before a system changes its structure by changing the variables and processes that control behaviour" (cited in Francis & Bekera, 2014, p. 100). In other words, Holling stated that resilience is specifically a measure built prior to potentially disruptive events.

Before the emergence of resilience, the protection of potential targets was improved by adding more and more layers of defence (e.g. physical barriers and surveillance). Nowadays, due to the uncertainty of (hybrid) threats, solely relying on defensive measures is considered insufficient. Therefore, resilience must ensure the ability to "bounce or spring back into shape or position" after a disruption, because unpredictability means that disruptions can never be completely prevented (Egli, 2013, p. 38; Setola et al., 2016). This uncertainty about the next potential disruptive event is what Egli (2013) defines as the idea of inevitability: rather than be surprised we should expect disasters – both natural and human-caused – to happen. The notions of uncertainty and inevitability are often mentioned in the context of crisis and emergency management (Anholt et al., 2021). Uncertainty complicates a thorough threat assessment. As a result, governments and policymakers, strongly encouraged by NATO, lean towards resilience for security policy.

In scientific literature, scholars often break down resilience into several dimensions: technical, organisational, economic, and societal (Setola et al., 2016; Labaka et al., 2016). Firstly, technical

resilience concentrates on the system's ability to perform in case of disruption. For example, software systems should be hacker-proof. Secondly, organisational resilience is the capacity of key stakeholders in CI sectors – both public and private – to decide and act in order to reduce the impact of disruption. It entails, in other words, the network engaged in resilience-building surrounding CIs. Thirdly, the ability to cope with the extra costs that come with a crisis is economic resilience. One could think about financial buffers. Lastly, societal resilience focuses on the societal capacity to reduce the negative consequences of disruption. Labaka et al. (2016) name aiding first responders or knowledge-sharing and securing accurate, objective information channels as examples. Societal resilience is about stimulating the public to participate and take up their responsibility for keeping themselves safe.

The emphasis of this research is on societal resilience, which entails society's ability to “respond to shocks, absorb them without suffering from severe fractures, and then recover”, according to Christie and Berzina (2022, p. 3). The authors incorporate interdependent governance and interconnected networks in resilience-building strategies, emphasising the importance of trust and social bonds in order for the public to contribute to resilience-building. Nonetheless, they warn that the concept has different meanings for different actors. From a national perspective, societal resilience resembles civil awareness and preparedness (Anholt et al., 2021). The population should be capable of mitigating the negative effects of an attack so that it can continue to support military operations. In NATO circles, however, societal resilience has a much more institutionalised character as NATO highlights the need for public-private partnerships and for engaging civil society in resilience-building efforts (Christie & Berzina, 2022).

According to Bergström (2018), besides scientific availability, a political need is required. Societal resilience, encompassing various initiatives such as awareness campaigns and governmental appeals, has significant political implications. What he considers important is the political necessity to frame societal safety and security in the context of active citizenship and local networks; a need that resilience addresses effectively. The new spectrum of threats, threatening vulnerabilities within the state and society shape the need for (societal) resilience. The state cannot cope with hybrid threats alone, thus a solid societal resilience-building strategy is required.

Moreover, societal resilience strategies attribute a different role to citizens. They play a much more active role in resilience-building than in risk and safety management because societal resilience-building initiatives aim to empower actors in society to prepare for and respond to risks instead of solely relying on government authorities, prompted by the realisation that hybrid threats can also target the individual in its private sphere. According to Francis and Bekera, the absorptive (the ability to absorb negative impacts), adaptive (the extent to which a system can adjust), and restorative (the ability to recover) capacities are at the core of what resilience entails. Due to the political need for these capacities, they are common elements of many resilience definitions (Francis & Bekera, 2014; Labaka et al., 2016; Setola et al., 2016; Mehvar et al., 2021) and policy papers. For example, in the Dutch Security Strategy, the NCTV calls upon citizens to be resilient while the government itself adopts a preventative, absorptive

and responsive approach, both nationally and internationally, to overcome current threats (NCTV, 2023).

However, critics point towards the potential downside of the resilience-building discourse. By placing threats beyond the realm of ‘normal’ politics and calling upon citizens and societal partners to contribute to resilience-building efforts, one presents such threats as existential and places them in an extraordinary realm of “panic politics” (Bergström, 2018, p. 35). This is called ‘securitisation’ and was visible in the discourse around COVID-19 and the European migration issue. In the resilience discourse, more and more aspects of daily life are placed within this securitised context due to society’s vulnerability to threats across the hybrid warfare spectrum (Larsson, 2021). How threats are defined can be seen as the outcome of processes of securitisation where the authorities perceive threats and then create a certain idea of what security entails, thus carefully ‘constructing’ threats and initiating policies in response that may infringe on civil rights (Fjäder, 2014). An overemphasis on securitisation may contribute to the militarisation of societal issues, potentially undermining trust and smooth cooperation between the government and society. It can hinder a society-driven development of resilience because it alienates citizens from resilience-building strategies as they feel unheard, their values and rights subordinated to military goals and their contributions overlooked, or – in the worst case – that militarisation evokes feelings of democratic erosion.

Lastly, Bergström (2018) identified disruptive events as an essential requirement for resilience to become an object of knowledge. He points towards both human-caused and natural disasters including but not limited to 9/11, Hurricane Katrina and the 2004 tsunami in Southeast Asia. In recent years, the Russo-Ukrainian war and the dire energy constraints that followed might as well be added to this list. For the Netherlands, these events – alongside 9/11 – have significantly changed the security landscape, which shifted from a threat-based to a risk-based model (De Graaff, 2012). Whereas before the focus was primarily on identifying and mitigating specific threats (e.g. military aggression and organised crime), nowadays the scale and unpredictability of modern threats (e.g. terrorism and cyber attacks) necessitate a risk-based approach. Here, emphasis is placed on assessing and managing the likelihood and potential impact of hybrid threats. Unfortunately, natural disasters in the form of the 2021 floods in the southern part of the country have also put Dutch resilience to the test.

Over the years, it is clear that resilience has become an overarching, interconnected, and widely applied concept. Various conceptualisations in terms of dimensions, capacities, and characteristics prevented a universal understanding of resilience (Francis & Bekera, 2014). This study is centralised around the societal dimensions of resilience, which herein is defined as *the ability of individuals, civil society organizations, private enterprises, and public institutions to resist, recover, learn, and adapt in the face of major shocks including armed attacks, to mitigate harm to the population, and to support the continuity of essential public services including security and national defence*, derived from the conceptualisation by Christie and Berzina (2022, p. 3). The holistic perspective of this definition allows for an approach to what the societal dimension of resilience-building is: a complex and interdependent interaction between the government, individual departments, other key stakeholders and the population

at large. This interaction is firmly embedded in a historical, political and cultural context (such as the perception of threat or the design of the Dutch security architecture) which makes enhancing societal resilience an interconnected endeavour that builds on mutual and equal collaboration between the MoD, other government departments and society at large. To achieve that, the MoD should reassess its societal positioning so that it contributes to mobilising the population to be aware of their role and encourage them to participate in societal resilience-building strategies.

To do justice to the debate on the complexities of enhancing societal resilience as well as to the careful considerations that the MoD should take into account when executing resilience-building strategies means that throughout this study a careful balance will be sought between achieving the aims of the ministry and addressing the concerns and critiques that exist among academia and within society. This means that the issue of securitisation and the grey area between stimulating and instrumentalising the public will be taken into account when analysing MoD policy and engaging in conversations with experts in the field. Eventually, the aim is to elucidate the extent to which security concerns are integrated into societal resilience-building efforts and the implications thereof for public perceptions, trust and collaboration. By providing insights into how security discourses affect government policy, an examination of strategies employed by the MoD can be made to help scholars assess the balance between stimulating and potentially securitising or even instrumentalising the public for the security agenda.

2.4 Psychological defence

In this section, psychological defence will be conceptualised and explained. A more detailed (historical) overview of its emergence into the security framework will be provided in the fourth chapter which dives into the Swedish case and the application of psychological defence in that context whilst exploring commonalities between the context of Sweden and the Netherlands.

As a Nordic policy concept, psychological defence addresses the individual commitment of the civilian population to contribute to the protection and preservation of the country and to counter hybrid threats (Wither, 2020; Antai & Hellberg, 2023; Christie & Berzina, 2022). The concept of psychological defence was first introduced in Sweden as a countermeasure to combat acts of psychological warfare, i.e. acts intended to reduce an opponent's morale committed anywhere in the world against the domestic audience. However, this policy concept soon came to cover various overlapping concepts, for instance, counter-disinformation operations, morale-boosting and resilience-enhancing operations, information warfare, strategic communication or Psychological Operations (PsyOps¹). Originally, psychological defence consisted of three crucial components. Firstly, to counteract everything that hostile

¹ PsyOps are defined by NATO as 'psychological operations are planned activities using methods of communication and other means directed at approved audiences to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives' (2019). In an informal conversation, PsyOps were deemed "modern-day propaganda" (Joint Centre of Expertise Communication & Engagement, personal communications, 20 March 2024).

psychological warfare engages in, such as deception and disinformation. Secondly, to ensure government communication in contexts of crisis or war. Thirdly, to strengthen the general will of the population to defend their homeland (Roszbach, 2017).

Sweden is not the only Nordic country that incorporated elements of psychological defence into its safety and security framework. In Finland, the government regards the psychological aspects of warfare against the background of psychological resilience, which they defined as “the ability of individuals, communities, society and the nation to withstand the pressures arising from crisis situations and to recover from their impacts” (Finnish Security Committee, 2017, p. 22). Like in the Swedish case the Finnish also highlight the population’s will to contribute to their country’s defence. Notably, the Finnish Security Committee call it psychological *resilience*, thereby connecting the psychological aspect to the resilience discourse, whilst in Sweden it is referred to as psychological *defence*.

In this research, the term psychological defence will be utilised rather than psychological resilience, because the latter can also apply to non-military disturbances (e.g. natural disasters) or individual shocking events in the personal sphere and the former is more suitable for addressing the culture of awareness and preparedness and describing the individual’s commitment and engagement with national defence endeavours. That is relevant because the cornerstone of this study is the perspective of the MoD, as the central question is how the MoD positions itself in society to enhance societal resilience. Hence, following this logic, in this study psychological defence is defined as *strategies and measures to increase the resilience of individuals and actors by stimulating awareness and willingness with the aim of contributing to the defence of the country*.

Closely tied to societal resilience and psychological defence are the terms awareness and preparedness, i.e. the culture of civil awareness and preparedness. In establishing this culture, the individual plays a pivotal role, according to the NCTV in the Security Strategy (2023). This starts with individual preparedness because without it, it “is quite difficult to achieve a whole-of-society approach with a strong core of resilience” (Sundelius & Eldeblad, 2023, p. 101). This preparedness is nevertheless difficult to measure objectively. Caves et al. (2021) have identified various elements that enable individual preparedness, including but not limited to the general trust in the government, local community ties, social cohesion and society’s capacity to cope with whatever crisis occurs. Remarkably, both the Finnish and the Swedish governments have stated trust to be of pivotal importance in resilience-building (Finnish Security Committee, 2017; Swedish Civil Contingencies Agency, 2021).

Enhancing psychological defence helps citizens to build societal resilience. The importance of this role is often mentioned, but what this role exactly entails or how citizens should take this up is mostly not discussed. Scholars have therefore called on policymakers to give substance to societal resilience within the national security framework as well as the responsibility that the MoD has therein (Bekkers et al., 2023). As a central security actor, staff members consider the MoD capable of facilitating and providing a clear structure to societal resilience, even in crises, war or hybrid warfare. However, this responsibility has to be conceptualised, concretised and operationalised, because currently, it is

unclear what the specific role of the MoD is in strengthening social resilience. By analysing how the MoD positions itself within society, this research aims to contribute to this role by providing useful insights as to how the ministry can improve this and live up to its societal responsibility when enhancing societal resilience. Some researchers see the role of the ministry as one of coordinating between government departments as well as between government and citizens (Rossbach, 2017).

According to Caves et al. (2021), herein should lie the role of the MoD: to coordinate a societal resilience narrative directed at the population which clearly defines the responsibilities of the government and the citizens. Simultaneously, by demarcating respective responsibilities, a reflection on the MoD's societal positioning is visible as it provides more clarity on where government efforts halt and civil initiatives can fill the void. In doing so, it aims to incentivise the public to contribute to national defence. Some scholars believe the ministry may be well positioned to play a leading role because it is directly linked to ensuring the public will to *defend* (Rossbach, 2017; Caves et al., 2021). Moreover, as Rossbach writes: "If the tasks of psychological defence become the responsibility of many different government agencies, there is a risk that psychological defence will devolve into disparate efforts and become nobody's responsibility" (p. 3). However, that would not rule out that other departments – e.g., the Ministry of Justice and Security (JenV) or the NCTV as an executive agency also play a vital – if not coordinating – role in shaping and facilitating that narrative. Some responsibilities to enhance societal resilience can be assigned by other departments but as resilience is a core aspect of modern defence, it seems that close collaboration with the MoD is required, according to Hans van Leeuwe, Head of the Counter Hybrid Unit (CHU) of the MoD (personal communications, 6 September 2023). Coordinated by the MoD, the government should send a unified and coherent message to the outside world.

Defining the responsibilities of the government vis-à-vis the citizens taps into the critique of responsabilisation and the debate of stimulation versus instrumentalisation of the public. When mobilising citizens, how to ensure two-sided communication rather than one-sided psychological influencing (as the concept perhaps appears to entail), keeping in mind the critique of Fry (2022) that communication inherently and implicitly attempts to persuade the recipient to see the world as the sender does, i.e. persuading citizens to contribute to national defence efforts. Furthermore, when engaging in a dialogue with society, how should the ministry transfer the message without unnecessarily securitising the security discourse? Analysing psychological defence and exploring its potential for the Dutch context allows for a reflection on ethical, legal and social concerns aligned with the deployment of measures to enhance said defence. Moreover, it offers useful insight into the Dutch security domain and permits a comparison with countries that have a policy of psychological defence as an operationalisation of a well-functioning societal resilience strategy within their security landscape.

When adopting a psychological defence strategy, Rossbach refers to this changing landscape: "Psychological defence activities must now deal with both state and non-state actors and, while counteracting operations that occur in peacetime, must be prepared for wartime conditions" (Rossbach,

2017, p. 2). This points towards the peace-conflict continuum: a term used to illustrate the spectrum of societal conditions ranging from peace to conflict. It recognizes that peace and conflict exist on a gradient rather than as complete opposites, with various stages in between. This continuum helps analyse the dynamics of societies in times of peace, crisis and war, acknowledging that factors contributing to peace or conflict can be fluid and interconnected (Wither, 2020). Nevertheless, it also sheds light on the complications that go along with hybrid threats, namely the legal and political difficulties it brings about when moving up on this continuum (Andersson & Tardy, 2015; Wrangle, 2022). Whereas the continuum is fluid, the underlying existing legal and policy frameworks are rigid. There is a clear distinction between peacetime and wartime. The powers and capabilities of the authorities, including the MoD, are significantly limited in peacetime. However, preparing for war – hybrid as well as conventional – costs time and effort and cannot be done on short notice. Bekkers et al. (2023) state that legal and policy frameworks should be revised to fit the current security landscape with war below the threshold and hybrid threats.

Yet, one should understand that peacetime limitations are in place for a reason. Regardless of the fluid peace-conflict continuum – or perhaps because of it – it is important to highlight the critique that actors within the MoD could resort to acts of securitisation in order to democratically bypass the peacetime limitations, as securitising hybrid threats means evoking extraordinary measures to combat these threats. An image might arise of a government overstepping its democratic boundaries, but at the same time securitisation allows the neoliberal government to gradually withdraw and put responsibility in the hands of citizens; the so-called neoliberal governmentality. A policy approach such as psychological defence thus runs the double risk of securitisation and responsabilisation. When analysing the concept it is important to address these concerns as it connects said defence to the larger debate.

In conclusion, psychological defence is closely connected to societal resilience. Set against the bigger framework that is societal resilience, psychological defence emphasises the level of awareness that actors in society should possess to effectively resist or combat hybrid threats. The term offers a lens through which societal resilience can be approached. Enhancing psychological defence requires stimulating a culture of awareness and preparedness. Although these concepts do not bear the same meaning, due to their interconnectedness they are used interchangeably throughout this study.

3. METHODOLOGY AND DATA COLLECTION

3.1 *Research strategy*

Societal resilience is a broad and encompassing concept, consisting of several dimensions, understandings and actors involved, which are all interconnected. As a result, building resilience is a highly interdependent endeavour. Several factors, like the issue around the MoD's societal positioning, complicate the ministry's contribution to societal resilience-building initiatives and thus require a whole-of-government framework, eventually translating into a whole-of-society approach.

This study will hence depart from a holistic philosophy. Holism emphasises the interconnectedness and interdependence of the parts within a system and the need to study the system and the relationships between the system and its environment, contrary to reductionism, which focuses on individual components of the system in isolation. A comprehensive understanding of the complexities surrounding resilience-building within society can be gained by adopting a holistic perspective. In this case, the term system would apply to the MoD, embedded in a wider environment. The meaning of 'environment' is twofold. It refers to the government apparatus as a whole and its various components – such as subsequent ministries – but also to society at large with its variety of actors. Within this environment, the ministry is not solely responsible for building national resilience, but it is regarded as 'first responder' and 'last line of defence' (Ministry of Defence, 2020). As a traditional military organisation, the MoD must cooperate with other government departments to stimulate government-wide initiatives to enhance societal resilience. Since this research was undertaken during an internship at the MoD, the adopted point of view to look at societal resilience-building is that of the ministry. Yet, due to the interconnectedness and interdependence, a holistic approach is favourable to understanding the intricacies and challenges of resilience-building initiatives. A holistic perspective allows for a careful balance between the MoD and other organisations and (societal) actors and the interface between them by considering the wide network of actors in which the MoD is embedded when undertaking (societal) resilience-building strategies. The perspective enables the researcher to assess the ministry's role in these strategies while simultaneously taking into account the bigger picture necessary to accomplish them.

This research is shaped into a theory-development design for multiple reasons. Firstly, due to the gap between theory and empirical reality due to the vague conceptualisation of societal resilience. This vagueness complicates the attribution of responsibilities to various stakeholders. Secondly, although a substantial body of work has been published on the government's role in the grey area, few theories delved into societal resilience-building strategies from a whole-of-society perspective. Lastly, the emergence of psychological defence policy in Nordic countries has not been projected or operationalised within the Dutch context. A theory-development design can lend itself therefore since many developments in the security discourse have emerged in recent years or have shifted due to a changing geopolitical landscape (Verschuren et al., 2010).

The cycle of connecting theoretical findings with newly developed empirical data that

Verschuren et al. (2010) described points towards the grounded theory analysis, which is the core methodology of this research. The cycle is characterised as an “exploratory expedition”, in which the researcher “investigates whether or not the newly found phenomenon has the same characteristics as a similar phenomenon which was previously found” (p. 187). This combination of inductive and deductive strategies that is grounded theory analysis allowed the researcher to continuously compare the theory with the empirical data in an iterative cycle (Bryman, 2016; Flick, 2018). Scientific literature formed the starting point and served as a framework to assess societal resilience-building. Retheorisation was then derived from empirical data, acquired through interviews and/or documents. Data analysis proceeded by coding and categorising identified concepts and connecting them via constant comparison with additional data based on further emerging concepts (Urquhart, 2013).

The grounded theory analysis follows a qualitative research design. For this study, a qualitative approach offered more structure and flexibility to explore the complexity of the topic. This is contrary to quantitative research, which centralises the collection and analysis of numerical data by testing hypotheses that are obtained through structured techniques, such as questionnaires or surveys. A qualitative design can be more exploratory, meaning that it seeks to understand a phenomenon in-depth rather than testing hypotheses or making predictions (Verschuren et al., 2010). This can be particularly valuable when researching the interconnected and often interdependent status of societal resilience-building strategies that are influenced by a wide range of social, cultural, economic and political factors. As a qualitative approach, the grounded theory analysis also allows for the identification of interdependent themes and factors that may not have been previously considered, but which broaden my understanding of the complex and dynamic nature of societal resilience – in this case: psychological defence (Flick, 2018). It collects and analyses non-numerical data, such as policy documents and interviews and challenges to make sense of the data, which can be derived through coding techniques (Urquhart, 2013; Bryman, 2016). To gain a more thorough understanding of the empirical reality, in-depth interviews will provide first-hand perspectives of vital importance when trying to understand all the different dimensions of societal resilience.

The process of grounded theory is iterative, meaning that the cycle of theoretical sampling and collection of data will repeat itself multiple times until a substantive theory can be drawn up. Because of that, there is no linear line of research methods that will be used. This study departs from a theoretical perspective. The substantial scientific literature on hybrid threats, a whole-of-society approach, resilience and psychological defence has been studied, resulting in a literature analysis which subsequently formed a theoretical framework. This framework served as a guideline for the following policy analysis to connect the theory to empirical reality. However, the grounded theory approach allowed for the revision and addition of this framework. Gathered policy documents as well as obtained interviews ought to reflect the empirical reality. As the process was iterative, “data collection and analysis occur in parallel” (Bryman, 2016, p. 576). Coding and categorising helped identify suggestions for new data. Through policy document analysis, the aim was to combine the theoretical ‘what should

be done’ with the practical ‘what is and will be done’ and to transcend the mere descriptive level. The sub-question ‘how should that practically be done’ has been answered through interviews with experts in the field.

3.2 Data collection and analysis

The relevant data consists of scientific literature, policy documents and interviews. The former is used to acquire insights into the status quo of the field of study concerning societal resilience. Most sources have been found through online academic search engines (e.g. JSTOR, Sage Journals, ScienceDirect) when searching for the key concepts explained in the previous chapter. Additionally, sources have been found via the Radboud University library (RUQuest) or upon recommendation. Likewise, policy documents are obtained from government repositories, such as the Senate or the House of Representatives. Relevant documents entailed bills, Memoranda of Understanding, Letters of Intent, Letters of Government, research reports and other government-distributed sources. Sources containing the key concepts or similar relevant concepts were subjected to a close examination of the abstract and findings, after which they were either disregarded or eligible for documentation and further analysis.

Apart from written sources, interviews complement the applied research methods. The interviews lasted approximately one hour. Eight respondents were selected based on their expertise in societal resilience, their involvement with societal resilience-building strategies and their affiliating to either the MoD or a Nordic organisation tasked with enhancing psychological defence, as listed in Table 1. They were informed prior to the interviews. By signing a consent form (see Appendix I), they consented to record and later transcribe the interviews for data collection. Respondents were given the opportunity to participate anonymously; three participated under that condition. Interviews were held in either Dutch or English, with the former being translated into English as close as possible to the original meaning by the author. The set-up was semi-structured, allowing the interviewer to ask questions for a predetermined list of questions (see Appendix II) while simultaneously permitting the interviewee to deviate from the questions as they saw fit and touch upon themes they deemed important for the topic (Longhurst, 2016, p. 143).

Table 1. List of interviews.

	Date	Name	Function	Organisation
1	13 March 2024	Anonymous	Strategic Advisor, Directorate of Communications (DCo)	Ministry of Defence
2	13 March 2024	Anonymous	Senior communication specialist, DCo	Ministry of Defence
3	15 March 2024	Herman Andersson	Research analyst	Swedish Defence Research Agency
4	20 March 2024	Dr. Miriam de Graaff	Head of Joint Center of Expertise Communication and Engagement	Ministry of Defence
5	22 March 2024	Charlotta Collén	Senior Fellow on Transatlantic Defence and Security	Center for European Policy Analysis

6	25 March 2024	Hans van Leeuwe	Head of Counter Hybrid Unit of the Directorate of Policy (DGB)	Ministry of Defence
7	4 April 2024	Anonymous	Policy Advisor, DGB	Ministry of Defence
8	10 April 2024	Lt. Col. Steffie Groothedde	Senior Civil-Military Cooperation Officer	Ministry of Defence

The transcripts were subsequently coded to distinguish interrelated themes. During the coding process, overarching terms and colour schemes aimed to identify categories (see Appendix III). After open coding, these categories were integrated within relevant units, representing various important aspects of societal resilience and strategies to improve it. In doing so, the grounded theory approach attempted to develop new theoretical points of departure “grounded in the data” rather than “derived from existing theoretical formulations” (Willig, 2013, p. 36). This process resulted in a series of themes, including but not limited to psychological defence, (strategic) communication, hybrid threats and legal relations. These categories were then connected to the policy documents to identify a set of boundaries that the MoD faces as well as substantiated views from respondents on how the ministry can overcome them.

3.3 Internal and external validity

In terms of internal validity, there is always a risk attached to grounded theory analysis. The iterative character of this type of analysis and its continuous comparison, and hence the development of new theories, might complicate controllability. As a result, consistency and transparency are of great value. Procedures and techniques should be applied carefully and consistently to allow readers and critics to understand and follow the newly formulated theory and contribute to it themselves (Verschuren et al., 2010). Searching data in the literature and policy documents involves using specific search terms and criteria to identify relevant sources. These terms overlap with the key concepts of this study: (societal) resilience, hybrid threats, psychological defence and the whole-of-society approach. The in-depth interviews will furthermore shed light on the empirical reality. When conducting interviews, the guiding questions will correspond with the derived data that resulted from the literature and policy analysis, ensuring that the questions are clear, unambiguous and to a certain degree standardised.

On the other hand, given its specific focus, the external validity hinges on its potential applicability to other facets of societal resilience. Resilience is currently a hot topic in Western political and military spheres but is still in its infancy. Interconnectedness and interdependence inherent in resilience-building strategies are not exclusive to the Dutch context, nor are they specifically attached to the government. Rather, they resonate across various societal sectors and can be observed in other European nations with similar political and governmental networks. Scholars studying resilience in different contexts of governance may find the insights gleaned from this study thought-provoking and applicable to their research. However, the adopted military perspective on societal resilience-building narrows down the possibility of generating generalisable findings on societal resilience as a whole.

While this study is grounded in a military perspective, it could catalyse broader debate on resilience-building strategies. By exploring this topic through alternative lenses, such as from the private sector or civil society, researchers can uncover parallels and divergences across sectors, furthering our collective understanding of effective resilience strategies beyond the military realm.

The emphasis on the MoD in this research might result in a certain bias, departing from a military and government perspective. That is because the consulted literature and sources are mostly closely connected to or derived from the military, although an effort is made to implement critical voices as well. Nonetheless, such sources further shape this study from a governance perspective. Yet, other perspectives can be recognised to approach this topic as well, such as a community or an economic perspective. This study's chosen perspective, however, is an inevitable consequence of the researcher's positioning in the field, being a graduate researcher at the MoD.

3.4 Research ethics

This perspective furthermore raises some general and context-specific ethical issues. Transparency and clarity are key principles in this regard. When conducting interviews, respondents were informed about the purpose of the research, as well as the procedures and potential risks associated with participation. Consent forms safeguarded correct information and guaranteed the above-mentioned principles. Respondents were notified that they were free to withdraw their participation at any given moment. Upon request, anonymity was provided. The aim was to speak to experts in the field who could shed light on one or multiple components of the research topic. All interviews were recorded to allow for transcripts to be made afterwards. In three cases, transcripts were subjected to a check on sensitive and confidential issues

After completion of the transcripts, the data consisted of recordings as well as transcripts. Both have been treated with the greatest confidentiality and were stored in closed repositories on Radboud University's internal drive, where they were inaccessible to parties other than the researcher and his supervisor. The thesis, with anonymised references to data derived from respondents who participated in anonymity, will also not be made publicly available. After uploading the data, data on devices used to record the interviews will be deleted. In line with the university's ethical codes, this research refrains from inquiry methods likely violating human values and sensibilities as doing so could jeopardise the researcher's reputation and that of Radboud University.

4. PSYCHOLOGICAL DEFENCE IN THE NORDIC CONTEXT

In recent years, the concept of psychological defence has gained increasing prominence in the safety and security architecture, particularly in Nordic countries neighbouring the Russian sphere of influence. As nations grapple with evolving security threats and hybrid warfare, the importance of understanding and effectively countering psychological threats has become apparent in the security discourse (Wrangle, 2022). The reason why is that part of hybrid warfare is cognitive warfare, fought out in the human mind, aiming to change what people think as well as how they think and act (Johns Hopkins University & Imperial College London, 2021). In the cognitive dimension, contrary to the protection of tangible and intangible CIs, human minds cannot be ‘protected’ by security actors like the MoD. That is to say that the ministry is inadequate, nor desired, to intervene in the cognitive sphere and shape one’s worldview. Moreover, the armed forces are prohibited from executing so-called psychological operations (PsyOps) against the domestic audience. However, a role often attributed to the ministry by its staff is raising awareness and enhancing preparedness to combat cognitive warfare. After all, psychological defence is about safeguarding the will to defend through a culture of awareness and preparedness and, as such, a pivotal aspect of improving societal resilience.

This chapter seeks to delve into the operationalisation of psychological defence within the Nordic context, exploring its historical development, conceptualisation and practical implementation as well as its potential implications and challenges for security policy. The question central herein is: what is understood as psychological defence and to what extent can it be applicable in the Dutch context? By evaluating the strategies and best practices of Nordic policy to enhance a culture of awareness and preparedness, the aim is to create an insight into the feasibility of the Nordic psychological defence strategy as a tool to enhance societal resilience in the Dutch security landscape. Although often referring to the Nordic region as a whole, the emphasis will lay on Sweden and Finland because these cases have been subject to closer examination through analysis and interviews due to their progressive and exemplary policy.

4.1 Civil defence and societal security

The emergence of the psychological defence concept is not a standalone development but rather a result of political-military dynamics that have been shaped for decades. These dynamics, influenced by political, geographical and demographical factors, have paved the way for a security landscape in which societal security seems to have a central position in Nordic countries. To understand these dynamics, one must go back to its roots during the Cold War era.

The tensions between the Soviet Union and the United States, and the delicate geographical positioning geographically bordering the former but ideologically leaning towards the latter led to a security strategy among the Nordic countries which entailed a comprehensive and inclusive whole-of-

society approach. The general philosophy among those countries was characterised by preparation for war and invasion, even in peacetime (Larsson and Rhinard, 2020). This preoccupation with war preparedness meant that both Nordic governmental and civil actors – ranging from NGOs and businesses to civil society and the population at large – had to contribute to strengthening national defence (Wither, 2020). Together, these actors gave shape to what was called Total Defence (TD), subdivided into military and civil defence. In Sweden, the Civil Contingencies Agency (MSB) defined TD as the continuous execution of all of society’s activities in wartime. “Total defence includes military activities (military defence) and civilian activities (civil defence). This includes protection of the population, security of supply and psychological defence” (Swedish Civil Contingencies Agency, 2021).

In the Nordic region, a pan-sectoral whole-of-society approach was often seen as a method of establishing TD, which was based “on the idea that national security, and hence wars, no longer operates within a separate environment from all others, but one in which all segments of society are affected by war” (Antai & Hellberg, 2023, p. 3). The military apparatus played a pivotal role in the TD, but it was supported by various civil defence components. The military aspect focused on the use of military strength and capabilities to protect the state. According to Antai and Hellberg, civilian defence had two functions: improve and smoothen operational effectiveness between key actors, such as the private sector and civil society, and anticipate and prepare for (future) hybrid challenges. Within this context of TD, policies for infrastructural development and social services (e.g. housing, healthcare, infrastructure construction) had a ‘war dimension’ and were therefore designed to facilitate both welfare and warfare purposes (Larsson & Rhinard, 2020). Implementing air raid shelters in architectural plans is exemplary in this regard.

Despite implementing the TD concept, its application and association come with certain critiques. TD originated as a response to ‘total war’, in which World War II is a prime example. According to Berzina (2020), both terms are essential counterparts in understanding that war affects the whole of society. Yet, apart from the unpleasant World War II connotation that every aspect of society is confronted with and involved in warfare, it contributes to an unnecessary militarisation of the security discourse (Stoker, 2017). Moreover, it is important to be considerate when using a term like Total Defence because words might shape the reality of the target audience and influence the course of action that is taken (Wrange, 2022). It could lead to a feeling of fear or anxiety among the population. Furthermore, the traditional military threat during World War II is much different from present-day threats, partly due to the development of new technologies but also because of the more unpredictable and asymmetrical nature of hybrid threats. Thus, adaptation of the concept one-on-one must be treated with caution.

After the Cold War, Nordic countries developed a new safety and security perception that took on a considerable holistic attitude, shaped by rapid technological developments, globalisation and privatisation. It led to an expansion of the security notion, including the economic, individual, cyber and societal domains against the background of hybrid threats. Concerning threat perception, the state-

centred point of view was abandoned in favour of a more inclusive understanding, including non-state actors in the perception as well (Wrangé, 2022). The perception moved away from the frame emphasising state survival to a view that incorporated a focus on the well-being of elements *inside* that state: society, rather than the political entity itself (Rhinard, 2020).

Especially among Nordic countries, this perception was shaped through the use of the term ‘societal security’. It built on previous notions of defence because it again highlighted the dual importance of civil and military defence within the security paradigm. The subsequent shift from ‘total’ defence to a similarly encompassing and inclusive – ‘societal’ – approach is therefore not surprising. However, the conceptualisation of this term varied across the Nordic region. In Finland the concept ‘comprehensive security’ is being used, the Danes define ‘security uncertainties’, whereas Sweden and Norway stick with ‘societal security’ (Larsson & Rhinard, 2020). Regardless of the terminology, all strive for an all-hazard whole-of-society approach. However, critics point to the conceptually fluid, open-ended nature of the term. As a result, states like Sweden and Finland seek to enhance societal security and implement similar, but still divergent policies. It comes to encompass a broad spectrum of policies and – similar to total war - this undermines the concept as it “used to mean almost everything, thus it means nothing” (Stoker, 2017). Additionally, the open-ended nature allows politicians, academics, practitioners and even entrepreneurs to utilise the concept as an enabler to pursue or address specific goals – like the securitisation theory argues (Larsson & Rhinard, 2020).

In Sweden, societal security gained prominence after the Cold War ended when influential bureaucrats and politicians sought to reinvigorate Sweden’s TD, particularly its civil defence pillar. They aimed to modernise the traditional ‘war-centric’ thinking to a new set of strategies able to cope with upcoming hybrid threats. Simultaneously, this came along with a shift in operational agencies as new institutions arose that conducted research and focused on crisis management or counterterrorism. This development of societal security did not occur in a vacuum but was a consequence of the conceptual gap of experiencing difficulties in ‘appointing’ new ‘enemies’ in Sweden after the conclusion of the Cold War, when the Russian threat was diminished (Larsson, 2020). Similar to other Western nations, attention shifted to expeditionary missions. In the aftermath of the 9/11 attacks, the fear of terrorists rose to the extent that they became the states’ main security focus.

The concept of societal security is a pillar of the Swedish approach to the protection of the nation. This is an acknowledgement that the challenges of the 21st century are not merely about the integrity of territory but primarily about safeguarding the critical functions of society, protecting people, and upholding fundamental values in the face of many types of threats and risks, including not only terrorist attacks like on 11 September 2001 but also new technological (cyber) threats like hacking and disinformation campaigns. Similar to TD, societal security consists of military defence on one side and civil defence on the other. However, rather than reiterating the more militarised TD interpretation in which civil defence was essentially an extension of the armed forces’ capacities in society, it now embodies many more aspects of societal processes ranging from psychological to economic defence

(Wrangle, 2022). Especially in 2014, when Russia invaded the Crimean peninsula, civil defence has risen in prominence according to a statement made by scholar Herman Andersson of the Swedish Defence Research Agency (FOI) during an interview. According to him: “It was a bit of a new start for the civil defence in general” (interview 3). Since then, the growing urgency to improve defence structures has been accompanied by a changing enemy image and threat perception because Russia became the biggest security threat instead of the post-9/11 fear of terrorists. Andersson suggests that Russian aggression in recent years has stimulated a general sense of awareness among the general population (interview 3). Thus, being a redevelopment of the TD strategy, it is not surprising that societal security shares significant conceptual and practical similarities with the TD idea.

These similarities were obvious when untangling the current security thinking in Sweden. When discussing societal resilience, Andersson continuously referred back to the TD structure. It came to the fore that Sweden has always been very militarised because people have been very well prepared, according to him. Regardless of Sweden's centuries-long neutrality, the Russian threat was always felt. In the Cold War, the Swedish government had worked out a very well-thought-out plan in case war erupted. Every man between the ages of 16 and 70 had an assigned duty, either civil or military defence, for example in the distribution of essential (military) goods, the provision of rescue services or the participation in local defence units. If one's normal occupation was deemed unimportant, he got assigned a new duty (interview 3). This ‘militarisation’ that occurred in Sweden was repeatedly explained by a sort of socio-cultural heritage. It corresponds with earlier statements made by Larsson and Rhinard (2020) about the intertwining of welfare and warfare during the Cold War. However, in recent times militarisation was replaced by the idea that, although the military still plays a pivotal role in protecting the country, the ‘militarised’ notion of civil defence was broadened. As Wrangle (2022) pointed out, it encompasses more types of defence, e.g. economic and psychological. This notion includes issues like preparedness to ensure supply capacity, enhanced awareness about hybrid threats, cyber literacy and election security to safeguard fair and democratic election processes in an era of hybrid warfare.

Whereas the Swedish post-Cold War notion of civil defence is less militarised, in Finland societal security still bears its militarised character. Here, societal security is called ‘comprehensive security’. It was shaped by geopolitical factors such as Finland's proximity and historical ties to Russia, which led to a different interpretation and evolution of the TD (Valtonen & Branders, 2020). The origin of Finnish security thinking lies in the aftermath of Finland's defeat by Russian troops during the Winter War (as part of World War II). This war incentivised Fins to foster a sense of collaborative thinking as well as support within the country. As the Winter War was a total war, the whole nation had to support the armed forces to survive. The established TD created a strong will to defend the country, sparked by the imminent threat from Finland's neighbour (Berzina, 2020). During the Cold War, Finland – although independent from Russia – was forced to follow a neutral course and limit integration with the Western powers, further contributing to country's unique security strategy. After the fall of the Soviet Union, “war was no longer the ‘worst case scenario’ for preparedness planners, since unintentional threats had

joined intentional threats on the perceived threat spectrum” (Valtonen & Branders, 2020, p. 100). The threat perception was widened and TD was replaced with comprehensive security, with a Security Committee taking the lead. This change was supposed to manage hybrid threats better because of a broader approach regarding preparedness planning.

Comprehensive security covers a broad spectrum of security notions, which are all addressed via a model set up by the government: the Comprehensive Security Model (CSM), coordinated by the Security Committee. This committee is, according to Senior Fellow Charlotta Collén from the Center for European Policy Analysis, the primary organ for dealing with any kind of disturbance. The Committee keeps a list of traditional, hybrid and natural threats and consequentially adopts an all-hazard vision incorporating a resilient whole-of-society approach (interview 5; Finnish Security Committee, n.d.). The CSM is built on four pillars: 1) an emphasis on coordination, 2) a phenomenon-led approach that initiates government-wide collaboration based on practical needs rather than administrative decisions, 3) strict adherence to the rule of law, explained by the authors as that responsible government authorities take care of planning and execution, and 4) an emphasis on preparedness (Valtonen & Branders, 2020). The Security Committee is responsible for the first one, coordinating government authorities on a national, regional and local level as well as organisations (e.g. NGOs), civil society and citizens. In the 2017 government resolution ‘Security Strategy for Society’, the role of citizens as noteworthy security actors is highlighted, reflecting “the desire to involve and motivate individuals to ensure their own resilience” (Valtonen & Branders, 2020, p. 95; Finnish Security Committee, 2017). This resilience returns in the last pillar, which argues that thorough preparedness of society as a whole reduces costs and improves security. In doing so, the resolution gives shape to what critics refer to as neoliberal governmentality which in a process of responsabilisation occurs, placing the burden on the individual’s shoulders.

4.2 The conceptualisation of psychological defence

The Cold War-era Total Defence system and the present-day societal security strategy both focus on the well-being of the state respectively its society. Both broad concepts cover various forms of defence, such as economic and cyber vulnerabilities, that can be targeted by hybrid threats. They aim to protect the state’s sovereignty, democratic values and processes, as well as CIs and societal well-being. However, hybrid threats aimed at the cognitive dimensions make the latter vulnerable. To shield societal actors, such as civil society, the private sector and the population at large, from disinformation and prevent external malicious actors from encouraging polarisation, psychological defence is considered to play an important role in building societal resilience in Finland and Sweden.

Psychological defence addresses the dedication of the civilian population to mitigate hybrid threats and protect the country. It thus focuses largely on the cognitive dimension, which distinguishes it from other types of defence that for instance Matthews and Zhang Yan (cited in Wrangle, 2022, p. 580)

describe: military, civilian, social and economic defence. Cognitive warfare, when executed successfully, can influence and shape individual and group beliefs and behaviours to favour an aggressor's tactical or strategic objectives. It has the potential to fracture and fragment an entire society, undermining its collective will to resist an adversary's intentions without resorting to outright force or coercion. Today, cognitive warfare integrates cyber, disinformation and psychological capabilities, leveraging the internet and social media to selectively target influential individuals, specific groups or large amounts of vulnerable citizens. Its tactics include sowing doubt, introducing conflicting narratives, polarising opinion, radicalising groups and motivating disruptive actions (Johns Hopkins University & Imperial College London, 2021).

Andersson tied psychological defence to psychological preparedness, arguing that it entails the willingness to defend as well as resilience against disinformation coming from foreign adversaries. According to him, these two are closely related because disinformation campaigns “make us less willing to fight in a conflict”. Furthermore, it can “separate us as a society” (interview 3). This emphasis on willingness to defend returns in the statements made by the Swedish Defence Research Agency (2021) and the policy of the Swedish MoD (2021).

But how does this willingness translate to the division of responsibilities? In Sweden, the government seems to place the responsibility upon the shoulders of the individuals (Sundelius & Eldebald, 2023). By utilising psychological defence, “we are splitting our effort to defend ourselves” (interview 3). It ties in with the previous notion of societal resilience as a buffer, in which the individual bears the full responsibility for being well-prepared (Larsson, 2021). In 2014, the government clearly stated:

“The balance between public and individual responsibility resides upon the basic view that the individual bears primary responsibility for protecting his or her own life and property. Only when the individual is no longer able to do so can there be a commitment or obligation on the part of the public to intervene.”
(Swedish Government Offices, 2014)

In a scarcely-populated country like Sweden, the government cannot take care of everyone at once in case of large-scale disturbances. According to Andersson: “It’s a little bit that it [society, ed.] needs you, but you also need the society” (interview 3). By his quote, he illustrates that it is important that one can maintain his protection to prevent the government’s resources from falling short, but that for doing so one needs to be able to rely on the local community. Thus, to prevent the burden on the government from overflowing, every Swede must be aware of this division of responsibilities so that he or she knows what to expect, according to Andersson. This should be communicated and legitimised in advance.

This ongoing process of responsabilisation, as described by Bergström (2018) and discussed in the conceptual framework, does not seem to bother the Swedes. The long history of TD has paved the

way for this. The interconnectedness between military and civil defence, underscored by the hybrid warfare targeting non-governmental actors, led Andersson to capture the relationship as “deterrence through the protection of civil defence” (interview 3). According to him, the discussion held within society does not focus on who bears which responsibility or how can the population strengthen the armed forces. Instead, the discourse focuses “on how we [the government, ed.] should protect our citizens, the civil defence, psychological defence and so on. It’s a focus on how we can protect the general public rather than how can we maximise our war effort”. (interview 3). The quote illustrates the perceived necessity to maintain a strong core of civil defence to deter the enemy by promulgating the idea of psychological defence among the Swedes. According to Andersson, the way forward for Sweden appears to be building societal resilience by strengthening the willingness and preparedness to defend, captured in the idea of psychological defence. However, he does not specify how the illustrated discussion in his quote relates to the Swedish Government’s plea for individual responsibility. Therefore, it remains unclear how exactly “deterrence through the protection of civil defence” fits within the Swedish societal security framework.

The Security Committee of Finland has a conceptualisation similar to Sweden. Psychological defence – presented by Helsinki as ‘psychological resilience’ – entails the ability of individuals, communities, society and the nation at large to withstand the negative consequences of disturbances and recover from them. It is explained in terms of the will to defend the country and the commitment to safeguard the livelihood and security of society whenever a disturbance occurs (Finnish Security Committee, 2017). Psychological resilience is embedded within the CSM’s all-hazard approach. According to Valtonen and Branders, this model subordinates all security actors – and the Security Committee regarded citizens as such – to a “competent authority” that has been allocated “central responsibility” (2020, p. 100).

This leaves no doubt that responsabilisation also plays a large role in Finland. However, contrary to Sweden's focus on civil defence, the Finnish national defence ideology focuses more on military defence with a whole-of-society aspect in a supporting role. Mobilising the public to enhance societal and psychological resilience is primarily done by educating them to enable military defence. When asked if this resembles a tendency to ‘instrumentalise’ rather than stimulate the Fins, Charlotta Collén responded: “I do not believe in that at all. I think it is a question of enabling through education” (interview 5). According to her, in the education system Fins are taught to be ‘highly critical’ to help them withstand hybrid threats that target the cognitive dimension of the individual. It appears as if situational awareness and war preparedness run through the Finnish DNA and hence the population has a very clear understanding of the division of responsibilities. The reason for this, according to Collén, is the collective memory of the devastating wars and occupation as well as the threat perception that followed: “We lost the war. [...] Those memories are not going anywhere” (interview 5).

A conceptual prerequisite for a strong core of psychological defence appears to be trust. Besides various scholars (Christie & Berzina, 2022; Caves et al., 2021; Elonheimo, 2021), the Security

Committee make this claim in their Security Strategy for Society. Looking at these necessary conditions to enhance psychological defence, it comes to the fore that factors like overall willingness to defend the country and trust in the government are relatively high in the Nordic region (Larsson & Rhinard, 2020; Kante, 2022), especially among those who have undergone military training (Swedish Defence Research Agency, 2021). The level of trust has historically grown between the government and the population as well as among citizens themselves. In a vast and scarcely populated Sweden, the importance of local trustworthy networks is essential as the government has limited resources to aid everyone all over the country at once. Here, demography combined with geographical factors contributes to this trust, because “you need to have a healthy relationship with everyone” whenever a crisis or war confronts the country, so you can rely on the local networks instead of being utmost dependent on government aid (interview 3). Also in Finland, the political backing of the CSM has remained strong. This points towards the general approval of politicians – and the electorates they represent – for this model, illustrating a sufficient level of trust in government security policy.

4.3 The operationalisation and implementation of psychological defence

Sweden's security landscape is characterised by a multi-layered and decentralised approach to defence and emergency preparedness, with responsibilities distributed across various levels of government and sectors of society. At the national level, the Armed Forces (*Försvarsmakten*) are responsible for military defence, including territorial protection and national security. Additionally, agencies such as the MSB and the Security Service (*Säkerhetspolisen*) play key roles in civil defence, crisis management and counterterrorism efforts. “The central government is small and a lot of things are done within the agencies. [...] The strategies are worked out in general in the agencies” (interview 3). The MSB has published a brochure ‘If Crisis or War Comes’ in 2022 - building upon a long legacy started in 1943 – which aims to enhance the culture of awareness and preparedness and increase the will to defend by giving practical recommendations for how to sustain yourself in case of disturbances (Swedish Civil Contingencies Agency, 2022). Examples are a checklist to safeguard home preparedness, an explanation of how to assess information falsity and information on various types of warning systems and emergency alarms. Larsson argued that these brochures invoke “solidarity and a moral responsibility on the part of individuals to actively contribute” (2021, p. 319), thus fitting neatly into the spirit of neoliberal governmentality that aims to hand over responsibility for ultimate preparedness to the individual.

An important step in Sweden towards strengthening psychological defence was made in the Total Defence Bill (*Totalförsvaret*) 2021-2025. In this bill, the government announced the establishment of a separate agency tasked with developing and coordinating the psychological defence strategy (Swedish Government Offices, 2020). Despite the new agency, the MoD does not elaborate exactly on how it is planning to enhance psychological defence. In 2022 this agency, the Psychological Defence Agency (*Myndigheten för Psykologiskt Försvar*–MPF), was launched. The MPF’s task to develop and

coordinate is a collaborative task together with public authorities (such as the MSB) and other societal stakeholders. “We offer support to government agencies, municipalities, regions, the business sector and organisations as well as contribute to strengthening the resilience of our population” (Psychological Defence Agency, 2022). The agency will perform tasks related to malicious social media campaigns, fund research and help to raise awareness and build public understanding (Sundelius & Eldebald, 2023).

A concrete example of the MPF’s work regards the undermining of trust by malicious campaigns. As a pivotal element in enabling a successful psychological defence strategy, trust is the backbone of the Swedish safety and security strategy. However, Andersson raises the question of whether the traditionally strong bonds of trust within society are “being torn apart when we do not trust each other as we have done historically”. He points towards the rumour that “the government – through social services – is taking children from Muslims and then the children are put in Swedish households in order to make them less Muslim”. Such acts of disinformation aim to encourage polarisation. Thus, the MPF “has been trying to look into [...] who is behind this kind of disinformation campaign. Who is funding it? How is it working? [...] Where are they coming from? Which groups are sending this information and why?” Furthermore, the agency sends out the correct information about how the messages Swedes read were false (interview 3).

Besides being multi-layered, what sets Sweden apart is its strong emphasis on local and regional governance in security matters. Municipalities and county councils are tasked with civil protection and emergency management within their respective jurisdictions. This decentralised approach reflects the state’s commitment to empowering local authorities and fostering community resilience. Local governments are responsible for tasks such as emergency planning and evacuation procedures – all driven by a strong core of psychological defence. The MPF, nonetheless, is responsible for training other agencies on the regional or local level (interview 3). Furthermore, Sweden's societal security extends beyond government agencies by including partnerships with NGOs and private sector entities, such as labour unions and a ‘commerce and business council’ (Swedish Ministry of Defence, 2021). Collaboration between government and civil society organisations is deemed essential for societal resilience-building.

The country’s history of conscription also contributes to its decentralised security posture, as it encourages widespread participation in national defence efforts and fosters a sense of shared responsibility for the country's security. After perceived ‘peaceful’ decades, Sweden reimposed conscripted military service in 2018 to bolster the armed forces’ capacities, having been influenced by geopolitical changes such as the invasion of Crimea (Barndollar, 2024). The conscription is nowadays gender-neutral and selective, meaning that a limited amount of pupils are selected to undergo military training. Indeed, the FOI analysed and concluded that a higher willingness to contribute is shown among those who underwent military training, leading to the conclusion that conscription seemed to strengthen the bond between society and the armed forces, which in turn reinforces psychological defence (Swedish Defence Research Agency, 2021).

In Finland, societal resilience-building is a task dedicated to the Security Committee. That is because psychological resilience is deemed one of society's vital functions, meaning that a threat towards it should be handled immediately (Finnish Security Committee, n.d.). The Committee was established by government decree in 2013. By only defining seven broad 'vital functions', the Committee pushed a whole-of-society (comprehensive security) approach that invites collective thinking of all actors. It furthermore aims to stimulate close collaboration and information-sharing. In doing so, the Committee's execution of the CSM is based on coordination rather than strict command and control (Valtonen & Branders, 2020). The Security Committee consists of "all the highest or second highest-ranking officials – thus not politicians – from every government ministry and department" (interview 5), making it a prime example of a whole-of-government structure.

The way it works is that "the Committee sets the course for safety and security policy [CSM], giving orders to regional authorities or municipalities" (interview 5). The centrally arranged organisation of the CSM apparently does not harm the coordinative foundation of the Committee. Collén explained this as a "network-based way of thinking" based on a "clear division of labour" (interview 5): the government guides society – accepted due to and prompted by historical memory and high levels of mutual trust. Yet, it remains unclear what the exact nature of the interaction between the Security Committee and its partners entails. The Committee organises National Defence Courses, week-long courses designed for people in a 'position of responsibility'. These courses are usually attended by politicians and key leaders, such as CEOs of important enterprises, NGO and media leaders, artists, influencers, university personnel and members of parliament, who are being educated about their role within the defence apparatus (Valtonen & Branders, 2020). For 'ordinary' citizens, counterparts exist that they can attend, which has proven quite popular (interview 5).

Which factors have shaped the evolvement of Finnish and Swedish safety and security policy, including psychological defence? Apart from the demographical and geographical challenges in the Nordic region, political reasons prompted this evolution, like the Nordic countries' ideological path. Larsson and Rhinard argue that the social democratic rooting in Nordic politics has manifested itself in strong public actors in comparison to the private sector. "From the government and parliament via civil and military agencies to regional county boards and local municipalities and companies" (2020, p. 7). It resulted in governments occupying a strong position and enabling them to coordinate a decentralised approach better than their Western European counterparts, who – due to privatisation – have to deal with the private sector more often. Andersson also pointed towards the decentralisation that lies at the core of the Nordic countries' security architecture to explain their approach vis-à-vis Western European countries. "A lot of other countries have this centralised, analysing capacity within the government" but in the Nordic region, governments have transferred large portions of duties and responsibilities to regional and local authorities (interview 3). The governments' strong position allowed them to coordinate this decentralised approach very well.

4.4 Best practices and challenges

At first glance, the societal security models of the Nordic countries are not compatible with the Dutch system. The ever-present threat perception in these countries underlines the importance of strong military and civil defence. Due to demographic and geographical differences, the design of such TD is radically different from the Netherlands, a densely-populated country without an active threat deriving from nearby states. Still, it can be useful to look at the Nordic models because various aspects offer fertile ground for implementation in the Dutch context. Considering the different (historical) development and organisation of Sweden and Finland's security domains, what aspects can be worth analysing within the Dutch context? And what are potential challenges that one has to be aware of when adopting a psychological defence strategy?

The Netherlands does not have an agency dedicated to enhancing psychological defence, like the Swedish MPF. Yet, according to some analysts, it would be beneficial to have a government department dedicated specifically to this task because of the rise of threats targeting the cognitive dimension (Rossback, 2017). Both Collén (interview 5) and Andersson (interview 3) reiterated this with the latter emphasising the importance of “having an organisation that is actually working on it”. Nevertheless, there should be a political consensus on where this agency ought to be accommodated. In Finland, the decision to house the Security Committee within the organisation of the MoD is backed by large political support, because the MoD is capable of coordinating other ministries and governments, according to Collén.

In the Netherlands, the NCTV – part of the Ministry of Justice and Security – plays an important role in the security of society at large, besides the MoD. The latter focuses on hard military defence of domestic or allied territory and supporting civil authorities in case of severe disturbances – if explicitly ordered so by the government (interview 4). The former, on the other hand, takes care of 1) securing the Dutch digital realm, 2) preventing and combating terrorist extremism and 3) enhancing the resilience of “vital sectors, citizens, companies, structures and networks” against threats deriving from state actors (NCTV, n.d.). A part of increasing citizens' resilience can be understood as psychological defence because the NCTV aims to ‘connect, encourage and stimulate’ actors (such as citizens) to take the appropriate measures. At first glance, it appears as if this organ is the primary organ that comes closest to dealing with psychological defence. “The NCTV is responsible for crisis management. There is of course an overlap, because [...] when is something a crisis and when is something conflict or war - it is not always clear how exactly that relationship works” (interview 7). The duties of the NCTV are thus set against the background of crisis management rather than psychological defence. Nonetheless, compared to the MoD, its mandate may seem more in line with combatting hybrid warfare because said warfare plays out below the threshold, i.e. with every means except traditional military combat. The MoD's mandate, on the other hand, prevents the armed forces from deploying clear-cut societal resilience-building strategies, which will be further discussed in the next chapter.

However, assuming that the Dutch MoD would thus have little to do with societal resilience-

building is wrong. An omnipresent culture of civil awareness and preparedness resulting in a high level of psychological defence is favourable for the armed forces. In principle, that does not necessarily translate into the MoD playing a big role in resilience-building initiatives. However, if in the peace-conflict continuum the indicator of (military) conflict rises, it could be that the legal responsibilities and capabilities of the MoD are widened once the legal threshold is war is exceeded. The armed forces then gain more capabilities to deploy military operations domestically. Seen from the ministry's perspective, an alert and prepared society is then the desired point of departure if military conflict erupts. The reason why is explained by Hans van Leeuwe, head of the Counter Hybrid Unit within the Ministry of Defence, as follows:

“There is a turning point. Below the [legal] level [of war, ed.], we are an advisory, requesting and supplying party, whatever can we do to make society run as well as possible. However, above that level, interests also shift. The question then becomes 'What can society do to ensure that the armed forces can run as well as possible?'. [...] If there is a scarcity in war, then priorities must be shifted.”
(interview 6)

Whenever society comes closer to the legal threshold of war, other relationships start to count in which the role of citizens also shifts to an accommodating one. The Finnish civil defence ideology, supportive of military defence, is exemplary in this regard. However, the legal barrier is not there for no reason, namely, to prevent the militarisation of society. Nevertheless, military staff highlight the importance of preparing society for potential war which, according to them, starts in peacetime (interview 4; interview 6; interview 7).

In addition to national defence, deterrence is a principal responsibility of the armed forces (NATO, 2023). In a letter to parliament from then-Minister of Justice and Security Ferd Grapperhaus expressed the expectation that more often his ministry would be calling upon military capacities and resources of the MoD to counter hybrid threats (*Kamerstukken II*, 30821, 2021). Following this logic, the NCTV – embedded in the Ministry of Justice and Security – could thus have to collaborate with the MoD to strengthen the level of deterrence by enhancing psychological defence. Grapperhaus urged the MoD to be prepared for this increased role. Herman Andersson's notion of ‘deterrence through the protection of civil defence’ fits nicely into the Minister's plea, because, according to Andersson, “if you are prepared and if you have the people, the equipment and everything else assigned, you will be able to much easier adapt” (interview 3). Via closer cooperation, military experience in combatting threats can be combined with the NCTV's expertise in hybrid warfare. Deployed effectively, these institutions together could make a significant impact to enhance societal resilience. In subsequent chapters, this will be discussed in depth.

A large part of increasing psychological defence among the public occurs via what Andersson defined as expectation management. Respondents state that people should know what to expect from the government. Christie and Berzina (2022) encourage adopting best practices from the Swedish and

Finnish societal resilience framework. Two of those effective practices are the psychological defence and communication of the government vis-à-vis citizens. Sweden's *If Crisis or War Comes* brochure is exemplary in this regard. Collén seconds it and attributes significant importance to communication. "Resilience thinking must come through examples people understand". In that sense, speaking publicly about scenarios while bringing them down to everyday life is a crucial component of this communication. "It is important to get the buy-in on why these [awareness and preparedness] issues are relevant. And that goes through examples" (interview 5). Another clear example of thorough expectation management is the amount of time citizens ought to sustain themselves in case of war or crisis. This buffer enables responsible authorities to set up a response within a specified time frame. This time frame, however, differs significantly. In Sweden, 'healthy' citizens ought to sustain themselves for at least a week without government support (interview 3; see Swedish Ministry of Defence, 2021) whereas in Finland one has to be able to survive 72 hours (interview 5).

To sum up, because societal or comprehensive security aims to safeguard the vital functions *within* a state, that is where resilience comes to the fore. To protect energy and food supply, financial systems, healthcare provision, IT integrity and social safety and cohesion, all these elements and systems ought to be made resilient to sustain potential disturbances. Societal resilience is an indispensable aspect of a resilient society, especially since hybrid threats can tackle the cognitive dimension of unaware citizens (Houck, 2022). Before the government can enhance the will to defend, it should raise awareness and preparedness. This culture of awareness and preparedness is exactly what adversaries aim to diminish as decreased preparedness undermines the will to defend, and thereby undermines the resilience of society as a whole. Raising awareness is the key to improved cognitive resilience to resist disturbances and psychological defence, as this culture is approached in the Nordic countries, can be the tool to achieve this.

Such a culture is a necessary prerequisite to building societal resilience. The psychological defence doctrine is not one-on-one applicable to the Dutch case, due to geographical, demographical, political and historical differences. However, some elements of the doctrine have proven applicable in the Dutch context. Firstly, to effectively counter hybrid threats in the cognitive dimension, respondents believe the government should prioritise enhancing psychological defence through an increased culture of awareness and preparedness. A new agency akin to the Swedish MPF or the Finnish Security Committee does not necessarily need to be established, but the MoD should reflect on how psychological defence can be improved in a comprehensive and cohesive endeavour. Therefore, secondly, the coordination between the MoD and the NCTV should be strengthened to leverage each other's capacities and expertise for countering hybrid threats. Such collaboration would enable an effective integration of both military (the MoD) and civilian (NCTV) efforts in bolstering the nation's deterrence posture and societal resilience, according to respondents. Lastly, they claim that communication and expectation management are paramount in fostering public awareness and preparedness. By engaging with the public through clear and accessible communication channels and providing practical examples of resilience-

building measures, the government is believed to garner buy-in and support for its security initiatives, empowering individuals and communities to play an active role in enhancing the nation's overall security and resilience. In conclusion, while the Dutch context presents unique challenges and considerations, drawing insights from the Nordic models of psychological defence and societal resilience can inform and enrich the development of tailored strategies to address the Netherlands' security needs in the 21st century.

Nevertheless, there are challenges tied to applying the psychological defence doctrine to the Dutch case. Andersson stated that the existence and danger of hybrid threats is not something on top of mind for most people to think about (interview 3). For the Netherlands, where a solid threat perception is absent, this seems to be particularly the case. The government should inform and mobilise the people, but the question then becomes who should do this? And what is the message the government wants to transfer? What words will be used? In Sweden and Finland, the communication is predominantly one-sided. The government is sending top-down information to civil actors. The only two-sided line of communication is between government departments and high-placed private individuals, as illustrated in the Finnish Security Committee, because they are bound together in a collaborative effort (interview 3). In the Netherlands, the issue seems to be a lack of clear communication between government branches, according to a colleague from the Directorate of Policy (personal communications, 7 September 2023). Furthermore, the challenge remains how two-sided transparent communication with citizens is safeguarded to maintain active engagement in dialogue rather than top-down dissemination of information.

Ultimately, Larsson (2021) underscores the evolving conception of security, which came to encompass a broad spectrum of hybrid threats, and the growing risk of securitising these issues. In the Finnish context, traditional defence communities have sought to maintain control over security discourse, primarily focusing on the state's vital interests. Conversely, in Sweden, a shift towards a social understanding of security has emerged, emphasising society's role in safeguarding security rather than relying solely on military measures (Larsson and Rhinard, 2020). This transition challenges traditional military authorities' control over the security discourse and perhaps necessitates the redistribution of resources across governmental and societal sectors, reflecting a process of responsabilisation. It appears as if the Swedish model is more applicable to the Dutch case because in the Netherlands the societal positioning of the armed forces seems to be more similar to Sweden, with its less militarised notion of societal security, than to the militarised Finnish understanding. Still, the Finnish collaborative endeavour offers useful clues because their CSM strengthens psychological resilience and collective consciousness through the Security Committee as a national dialogue between the MoD, internal security actors and governmental service providers as well as economic, infrastructural and functional heads or representatives to increase feelings of security (AIV, 2024). The Dutchmen should also reflect on the division of responsibilities in the Netherlands and redetermine who ought to coordinate the security domain (should it be up to the MoD to execute this role?) and who bears responsibility for what (where

does citizens' responsibility end and the government's commence?)).

The next chapter will dive into the current division of responsibilities and address the barriers that the MoD might face when taking up a leading role in enhancing societal resilience-building.

5. THE BARRIERS TO ENHANCING SOCIETAL RESILIENCE

“I think that has to do with the task we have as the MoD. It is simply not our duty and so when we start doing things that are not our duty and for which we have no mandate, we are undermining our own democratic state.”

Dr. Miriam de Graaff (interview 4)

This quote by Doctor Miriam de Graaff, Head of the Joint Center of Expertise ‘Communication and Engagement’ (C&E) within the Ministry of Defence, illustrates nicely the dilemma that the ministry faces when discussing the matter of societal resilience-building. The MoD has a clear interest in enhancing societal resilience. Due to well-aware and prepared civil actors, resilience limits the potential disruptive impact of hybrid threats to our society. It contributes to the level of deterrence because it sends out a clear signal to adversaries that an attack may be futile. After all, the population is prepared and able to absorb the negative consequences. However, as the previous chapter already illustrated, societal resilience-building is not a goal that is achievable through military means (interview 7). Or, as De Graaff stated: “It is simply not our duty”. Nonetheless, this does not mean that the MoD cannot play a role in this process. As an important societal partner in the government’s safety and security architecture dealing with (military) threats, the ministry considers itself indispensable when setting up a comprehensive societal resilience-building strategy that enhances psychological defence through a culture of civil awareness and preparedness.

Due to mandate constraints, the armed forces cannot act solely according to their own rationale. Thus, a collaborative approach is required in which the MoD is embedded within a larger whole-of-government perspective. Departing from the idea that the ministry could in some way assist a psychological defence strategy, the central question explored in this chapter pertains to the potential barriers encountered by the MoD in its efforts to contribute to enhancing said defence. By examining these barriers, ranging from organisational limitations to societal perceptions and resource constraints, this chapter seeks to illuminate the interdepartmental landscape within which the MoD operates and the obstacles it must navigate to advance societal resilience initiatives successfully. Understanding these barriers is crucial for devising policy adjustments that can strengthen the MoD's role in a collaborative endeavour enhancing psychological defence capabilities in the face of hybrid threats. Three sets of limitations will be distinguished and discussed: legal, interdepartmental and societal.

5.1 Legal limitations

A core limitation that comes to the fore when assessing the role of the MoD in societal resilience-building is the specific legal framework and the mandate to which the MoD is subordinated. The ministry is first and foremost a military organisation. According to De Graaff, it is tasked with three duties. Firstly,

it must keep the territory of the Kingdom of the Netherlands and its allies safe and secure. Secondly, it must ensure that the rule of law is being followed and respected, not only domestically but also in allied countries. Thirdly, it must assist the civil authorities upon request as well as deliver (humanitarian) aid in case of disasters or crises (interview 4; Ministry of Defence, 2020). The primary responsibility of the MoD herein is described by a Policy Advisor of the Directorate of Policy (DBG) as strengthening the preparedness of the armed forces: “That is our core business, that is what we should safeguard. [...] We do not take the lead in increasing the level of societal resilience, because we cannot do so. It is not our mandate” (interview 7).

The Dutch Constitution defines the armed forces’ three duties, stating “1) the purpose of the defence and 2) protection of the interests of the Kingdom as well as for the purpose of 3) the enforcement and promotion of the international rule-based order” (Article 97, as cited in Ducheine & Bos, 2021). In executing these constitutional duties, the armed forces can fulfil two different roles, according to the *Defensievisie 2035*, a long-term strategic policy framework drawn up by the MoD in 2020, namely that of ‘first responder’ and of ‘last line of defence’ (Ministry of Defence, 2020). The former captures the MoD’s role in absorbing and easing a crisis so that other security and aid organisations can execute their role accordingly. The latter highlights the capacity of the armed forces to assist civil authorities, both in normal and extraordinary situations. Because of the blurring of the three duties in the last decades, it can be reasonably presumed that both roles apply to all the described duties (Ducheine & Bos, 2021). Lieutenant-colonel Steffie Groothedde, a Senior Civil-Military Cooperation Officer, supports this vision, stating that “you [can] no longer speak of three main tasks in a very clear separation. Because the world around us in a hybrid context causes these three main tasks to overlap, you can no longer classify it very straightforwardly” (interview 8).

“Protection of the interests of the Kingdom” is broadly defined. In the National Security Strategy – composed by the NCTV in coordination with other government departments, among which the MoD – these interests of ‘national security’ are conceptualised: territorial security, physical security, economic security, ecological security, social and political stability and a stable international rule-based order² (NCTV, 2023). The armed forces are deployed only if national security is threatened or affected (Ducheine & Bos, 2021). Then, the state can act under its monopoly on the legal use of force. This monopoly is assigned to the National Police and the armed forces, although it is the latter who possesses the most powerful tools of force and is therefore primarily responsible for the protection of the state’s vital interests, according to a Memorandum of Response from the government to the Senate (*Kamerstukken I*, 25367 (R 1593), 1998). The armed forces could also be deployed under the same constitutional duty to assist civil and local authorities, like the National Police (*Kamerstukken II*, 25367 (R 1593), 1997). For example, it occurs in case of (natural) disasters or violent events threatening

² A stable international order can entail many things, in this case including but not limited to: respect for Westphalian norms (sovereignty, peaceful co-existence and dispute settlement), adherence to human rights and a rule-based international financial-economic system (Drent & Meijnders, 2019).

national security, or more specifically, ecological security or social and political stability.

The armed forces are subject to a strict mandate to safeguard the government's monopoly and ensure it is not being abused. The MoD is restricted from acting freely when a mandate is absent to prevent the armed forces from undermining the liberal-democratic values of our society. In a letter of government, Minister of Defence Ollongren emphasised this point by reconfirming that “the armed forces never deploy themselves” (*Kamerstukken II*, 32761/30821, 2023). Without government order or permission, the armed forces cannot operate, according to De Graaff. “We do not have a role unless parliament orders us ‘thou shall protect us now’. If in the Hague nothing is decided, nothing will happen. [Because] that is not allowed. In that sense, the MoD's role is very clear; [...] without a mandate we cannot act” (interview 4). To prevent the erosion of liberal democratic values, this mandate restricts action at the discretion of the military apparatus and instead reinforces government control over the armed forces. Respondents all acknowledge these limitations, yet they all highlight that the MoD should be involved along the sideline of societal resilience-building initiatives due to military expertise and experience in dealing with (military) threats and complex operational situations, as well as because of the ministry's role as last defender. In their eyes, that is because ultimately the consequences of hybrid threats targeting the society's vulnerabilities might affect national security.

Then how does this influence the MoD's role in societal resilience-building? The mandate limits the space of manoeuvre for the ministry to engage in activities aimed at enhancing psychological defence. Psychological defence, or the culture of awareness and preparedness, ultimately plays out in the cognitive dimension. The MoD possesses useful tools to improve awareness in this cognitive defence, namely Strategic Communications (StratCom), defined by NATO (2023) as “the integration of communication capabilities and information staff function with other military activities, in order to understand and shape the information environment, in support of NATO aims and objectives” (p. 2). Groothedde described it as an ensemble for different doctrinal capacities in the information environment (interview 8).

The Joint Center of Expertise C&E distinguishes between Information Operations (InfoOps), Psychological Operations (PsyOps), Civil-military cooperation (CIMIC) and Military Public Affairs (Mil PA). According to C&E's doctrine bulletin, InfoOps and PsyOps aim at “adversaries, potential adversaries and audiences in support of mission objectives” (Ministry of Defence, 2024, p. 35). Both are applicable in the context of a military mission abroad, with InfoOps responsible for information environment assessment and aiming to understand and assess the foreign target audience's perspective. PsyOps, on the other hand, aims to change this perspective by creating an atmosphere of willingness and support by influencing target audience behaviour, attitudes and perceptions vis-à-vis military operations. CIMIC entails communication for understanding and interacting with non-military actors during military operations. Lastly, Mil PA promotes military aims and objectives in an accurate and timely manner to both external and internal (domestic) audiences (Ministry of Defence, 2024). It differs from the first three because it aims to inform and foster trust and understanding transparently rather than

seeking to shape and deceive perspectives, although Fry (2022) stressed that there is no such thing as value-free information. De Graaff seems to agree: “The baseline is that we want to achieve a certain military effect. For that we have various means which all deal with how people behave” (interview 4). Because of their ‘deceptive character’, InfoOps and PsyOps are forbidden against domestic audiences. In the Netherlands, the MoD does not have the mandate to conduct such operations domestically.

Mil PA is legally allowed and that responsibility is assigned to the Directorate of Communications (DCo), which follows the policy guidelines as set out by the DGB. DCo merely follows these guidelines and makes them operational on a communicative level (interview 1; interview 2). It informs the general public about defence-related topics. Groothedde is sceptical about the ‘traditional take on government communication’ that the DCo has (interview 8), focusing on the broadcasting of messages, because of the wrong emphasis placed on nuisance coming from military operations. In conversations with the DCo, the traditional approach has come to the fore when discussing resilience, because resilience is set against the background of military operations rather than against a whole-of-society point of view. Communication with the public mainly serves the purpose of informing them about how military operations might hinder their everyday life, for instance when the armed forces make use of railroads or highways (interview 1). “The MoD is [...] setting up a campaign to raise awareness about increasing numbers of military exercises in the Netherlands as we will cause more nuisance” (interview 6). It appears that, according to respondents, societal resilience thus seems to be measured in relation to the level of nuisance citizens can expect from the armed forces.

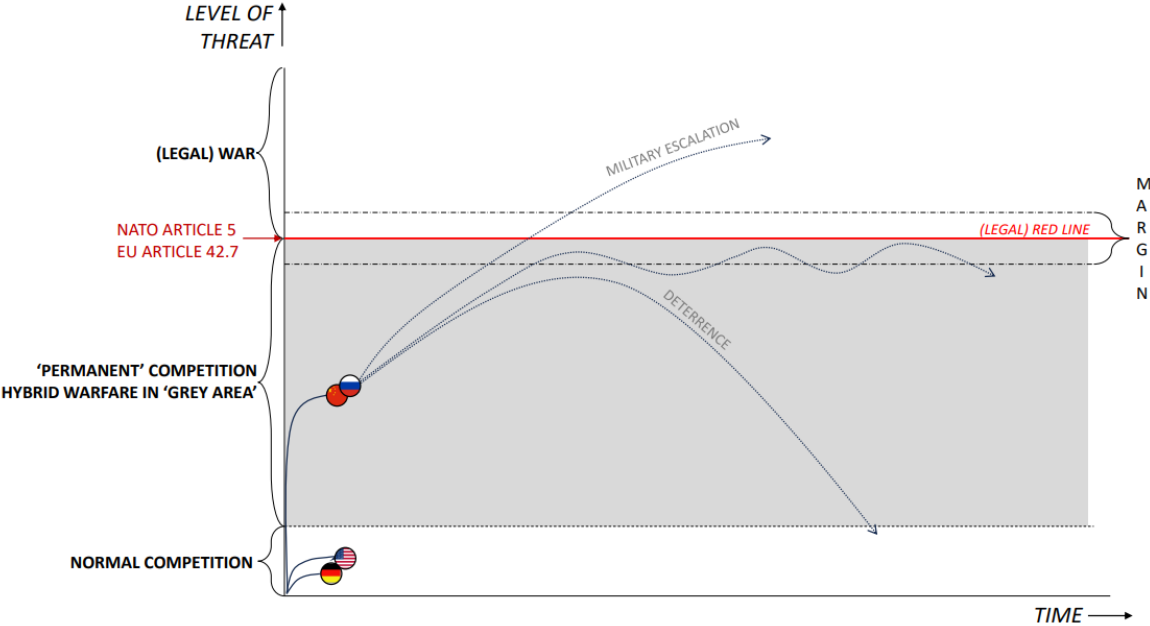
The reason why the ministry is reluctant to undertake more (pro-)active societal resilience-building is its mandate. One clear example in which the armed forces overstepped its mandate occurred in 2020 when it came to the fore that the Royal Army’s Land Information Manoeuvre Centre (LIMC) had unlawfully gathered and analysed personal data to assess the impact of COVID-19 on society. When the news came out, these drawn-up reports caused controversy. The LIMC wanted to practice new warfare tactics in the information environment but lacked a clear mandate to do so (Commissie-Brouwer, 2023). An investigation committee pointed towards the existing legal frameworks and the new threats between which the LIMC was stuck. The committee advised reviewing these existing frameworks to fit the current needs of the armed forces to enable advanced warfare techniques in the information environment. Groothedde stated: “What Brouwer said is that the problem goes beyond the LIMC’s mistake. The entire government should look at the world around us and [assess] how it deals with the hybrid context. Therein you have a different role for the armed forces, so you have to provide the resources to enable the armed forces to prepare differently” (interview 8).

The committee and Groothedde point towards a second barrier that – besides the mandate – limits the ministry: legal boundaries in executive capabilities. Groothedde points to the complexity of attributing a different role to the armed forces in dealing with hybrid threats. According to her, the cognitive dimensions of these threats complicate resilience-building initiatives. She claims that the armed forces *could* play a role in countering those, but that this currently is legally impossible. Within

the government, discussions are ongoing on whether or not to broaden these boundaries and expand military capacities in the information environment (interview 6). Evans (2017) defines important prerequisites for expanding these capacities, namely political consensus and societal support. Parliament decides on the mandate, but to expand the armed forces' capabilities it needs societal support. Moreover, widening the mandate to enable domestic military information operations can be considered problematic from a democratic point of view. The risk of militarisation looms when considering the expansion of the armed forces' legal capabilities. Broadening the legal mandate, particularly in areas related to domestic security or information operations, can lead to increased involvement of military institutions in traditionally civilian spheres (Watkin, 2016). This shift may blur the lines between military and civilian roles, potentially undermining democratic principles and civilian oversight. Furthermore, granting expanded legal powers to the armed forces can heighten societal concerns about the creeping influence of militarism in governance and public affairs (Evans, 2017). Such developments could also impact civil-military relations, altering the balance of power and accountability within a society.

In peacetime, the armed forces play a supportive and facilitating role in society (interview 6; interview 7). Van Leeuwe described it as “an advising, inquiring and supplying party. What can we do to make society run as well as possible?” (interview 6). However, from the perspective of the MoD, it might be desirable to revise current legal frameworks specifically for scenarios when the national security situation deteriorates and the possibility of war emerges. This has everything to do with the peace-conflict continuum (figure 1). It represents a spectrum encompassing various stages ranging from

Figure 1. Peace-conflict continuum illustrated. *Source: Van Leeuwe, personal communications (25 March 2024).*



peace to conflict, with nuanced gradations. At one end of the continuum lies a state of peace characterised by stability, cooperation and absence of violence or hostility. States compete in what is

called normal competition, characterised by peaceful dialogue and negotiations. Relationships with Germany and the US are exemplary in that regard. As one progresses along the continuum, the situation may evolve into heightened tensions, instability or hybrid threats in the ‘grey area’ of permanent competition, marking the transition towards conflict. In this continuum, the nature and increase of threats may eventually culminate in full-scale warfare. The depicted grey area thus represents an increasing threat level, in which the closer one gets towards the red line, the more serious and disturbing the malicious act is, bringing the possibility of war one step closer. States like China and Russia can be found within this grey area. Warfare can be triggered by evoking NATO Article 5 or Article 42.7 of the European Union when one of the members is under attack. According to Van Leeuwe, this is the legal red line after which states find themselves in a state of war (interview 8; Andersson & Tardy, 2015). He advocates for strong deterrence, which is the primary responsibility of the MoD. By deterring potential adversaries and ideally combining this with an attempt to normalise interstate relationships, the possibility of war could decrease. However, to successfully deter, Van Leeuwe argues that it is required to remain ambiguous about where exactly the government’s red line is, illustrated in the figure by depicting a margin around the legal red line (interview 6).

In a state of war, other legal constructs apply, such as state emergency law, which deviates from fundamental rights and temporarily suspends constitutional structures (Ducheine & Bos, 2021). In this situation, the space of manoeuvre for the armed forces is expanded, including in the communication domain and the cognitive dimension. Although this is determined by law, it is not yet practically operationalised, according to the DGB (interview 7). What the armed forces should and could do remains unclear. The claim by Rossbach (2017) that the military should prepare in peacetime for these wartime conditions to effectively counter hybrid threats thus seems futile because these legal wartime conditions and the role of the armed forces therein are far from clear. For instance, state emergency law is being reviewed to assess if it still fits with the present-day security landscape. From the perspective of the MoD, this revision is highly relevant. The ministry urges to make the emergency law more operational, because in an Article 5-scenario “that is not clear at all. At the moment we don’t have a clear vision of what the MoD needs from civil partners, it’s not in writing” (interview 7). Nonetheless, the government should deal carefully with these legal issues to respect the rule of law and ensure enabling the democratic system of checks and balances.

5.2 Societal limitations

A whole-of-society approach with a strong core of civil awareness and preparedness as well as a clear division of responsibilities, similar to a Nordic security model, may help to develop societal resilience-building strategies. However, as discussed in the previous chapter, diverse geographical and demographical differences as well as a disparate threat perception complicate the adaption of such strategies in the Netherlands. In the 1980s and 1990s, the Netherlands witnessed a laissez-faire attitude

towards domestic defence capabilities similar to other Western European states. The government and MoD's focus shifted to expeditionary missions. This set in motion a process of desecuritisation as people felt safe, which impacted the societal understanding of the MoD's responsibility and role in society. With trade, knowledge development and (foreign) investment taking the lead, the focus was on interest rather than on threats.

Closely related to the interest-based mindset that the government adopted is the process of privatisation. By outsourcing government tasks to the private sector, the government had partly outsourced the responsibility for making CI resilient (interview 4), in line with responsabilisation as described by Bergström (2018) and discussed in the second chapter. Van Leeuwe claims "excessive market forces in healthcare, in public transport [and] in the energy sector" to be exemplary of privatisation (interview 6). Privatisation contributed to neoliberal governmentality because the government lost its overview and played a less active role in making critical sectors as well as society as a whole resilient (Larsson, 2021). Resilience-building became subordinated to economic interests which, together with the neoliberal mindset, caused a declined sense of threat perception and urgency.

Around the turn of the century, the 9/11 terrorist attacks fostered renewed securitisation (De Graaf, 2012). The government realised that resilience-building in these sectors is essential because "you work on a chain in which the weakest link determines the strength of the chain", according to Van Leeuwe (interview 6). The dramatic course of events in recent decades, such as the Russo-Ukrainian war and the dependence on Russian gas, has influenced this sense of urgency to such an extent that the government has now realised the need to take back some agency in CI sectors. For instance, Minister Jetten for Climate and Energy addressed in a letter to the House of Representatives the importance of safeguarding public interest by taking back control of the Dutch heat network exploitation (*Kamerstukken II*, 2023, 30196). Similarly in societal resilience-building, the government seems to have understood that despite recent events, citizens – although they develop an increasing fear of threats – do not automatically adopt a culture of awareness or develop a sufficient level of psychological defence. According to De Graaff: "We [the population, ed.] are rather drifted off here in society and think 'we are all safe; nothing will ever happen again'. That is not realistic" (interview 4). Despite the fear, respondents state that society perceives the MoD as a guardian of their security. This societal perception, however, is partially incorrect because hybrid threats can target the individual's cognitive dimension as well. Instead, "the realisation has dawned that [...] the government has a responsibility to stimulate that awareness", in the eyes of the DGB (interview 7). The government has made first steps with the 2019 Security Strategy with a comprehensive plan to enhance resilience, including the improvement of CI protection, strengthening of crisis management and increasing of society's preparedness (NCTV, 2019).

Defence staff are concerned that for many societal actors, security issues – such as the hybrid warfare playing out in the permanent competition – appear to be "something far away" (interview 1). A senior communication specialist within the DCo called it a risk for citizens, stating: "I don't notice [it], so it doesn't exist" (interview 2). However, just like for (military) policymakers and politicians, recent

events have proven to be a catalyst for a changed mindset among societal actors too (Sie Dhian Ho et al., 2022). Almost every respondent stated that events such as the Russo-Ukrainian war in 2022 and the occupation of Crimea in 2014, as well as the downing of flight MH17 in the same year and the COVID-19 pandemic, have triggered a commencing sense of urgency. Yet, how this translated into a responsibility for citizens to improve their awareness and preparedness is unclear. Van Leeuwe explained this in line with the ministry's reasoning, namely due to a lack of situational awareness and situational understanding:

“People often tend to shout things without possessing sufficient situational awareness and understanding. Instead, they immediately go one step further and claim that we [the MoD, ed.] are the only ones capable of handling it, [because] we are good at it [so that] we should do it, without seeing the broader, legal framework and the [im]possibilities and alternatives well enough.”
(interview 6)

In the eyes of defence staff, people seem to look up to the ministry as an authority and they expect a lot from the armed forces. But it is wrong to suppose that the MoD will solve every issue in times of crisis or war. “That is a wrong assumption. It's not *just* the government or *just* the MoD [emphasis added]. [...] But this realisation hasn't kicked in yet” (interview 7).

Respondents believe that an important reason for this is the unclear image of the armed forces. De Graaff attributes this to the “naïve image” that people supposedly have about the armed forces. For the population, it is not always clear “what we actually do, what purpose we serve and what we can do”, although the levels of trust and confidence are relatively high (interview 4; Ministry of Defence, 2022a). Yet, De Graaff claimed the armed forces to be “fairly closed off” as an institution (interview 4). Despite the confidence, defence staff believes that the people's unclear image has an impact, which translates for instance into the number of vacant posts. People are less willing to work for an organisation like the MoD (interview 7). Following this assumption, the unclear image puts a strain on the operational capacities of the armed forces, such as in resilience-building endeavours. The exact number of vacant posts is unclear but respondents have repeatedly addressed the lack of manpower within their departments (interview 4; interview 6; interview 7).

Tackling this issue has multiple benefits for the MoD. The needs of the armed forces and society are considered reciprocal by the DGB (interview 7). By strengthening the bond between society and the armed forces, situational awareness and preparedness could improve. Furthermore, it can solve the shortage of personnel. Hence, the State Secretary of Defence has announced plans to enhance the connection with society – e.g. reaching out to students for a year of voluntary military service – and strengthen the bond of reservists with the MoD (*Kamerstukken II*, 36200 (X), 2023), reiterating earlier plans formulated in the Defence White Paper (2022). From the MoD's perspective, these plans ought to strengthen this bond by fostering an understanding of the challenges and issues the armed forces face. A necessary prerequisite for engagement is a sufficient level of trust. Contrarily to Nordic countries, the

Dutch government struggles with this issue as citizens experience a lack of trust and confidence in their government and political leaders (Centraal Bureau voor de Statistiek, 2023).

This societal barrier undermines societal resilience-building efforts because a trustworthy government that communicates clearly and transparently is a vital component of psychological defence improvement (Elonheimo, 2021). It is too superficial to claim that the government can ‘simply’ enhance said defence by handing out brochures and publishing government-approved updates to mobilise people. Such endeavours are in vain if people do not trust the communicator, meaning that a trustworthy perception is essential for successful cooperation between the military and broader society (Longstaff & Yang, 2008). This perception now is disturbed, in part due to the government’s course of action. The childcare benefits scandal and the issue surrounding natural gas in Groningen are exemplary in this regard. Both heated issues have diminished trust and confidence in the Dutch government. The COVID-19 pandemic has reinforced anti-government sentiments. Hybrid threats can play a role in these developments as (foreign) adversaries can utilise these cases by feeding the sentiments through disinformation campaigns, targeting vulnerable groups or individuals already sceptical towards the state (NCTV et al., 2022).

The issue is thus much broader than just hybrid threats coming from abroad. They manifest themselves domestically as well, playing into the internal dynamics of the relationship between the government and the population. In doing so, such threats reinforce already present societal barriers. To build trust, transparency is thus required. Clear and transparent communication may enhance the level of trust, which in turn would enable the military apparatus to operate side-by-side with citizens in dealing with hybrid threats (Wang & Kapucu, 2008). Lines of communication have to be structural and short and actors have to communicate openly and transparently (Langstaff & Yang, 2008).

The use of StratCom techniques, such as Mil PA seeking to engage with audiences, might offer a fruitful solution, although culturally the connotation of deploying such techniques remains a controversial point. InfoOps and PsyOps deployment remains unlawful, but Mil PA is obedient to the democratic rule of law and is thus useful to transfer a message to specific audiences (interview 8). According to De Graaff, the government and the MoD can be more decisive (interview 4). Although threat perceptions are changing, governments still hesitate to use communicative techniques for societal resilience-building (Fry, 2022). Fry advocates for the disentanglement of propaganda and ‘communications influence operations’, with the former aiming to manipulate and *deceit* with a strategic aim and the latter aiming to “educate, *persuade* and influence” audiences to increase awareness and support (2022, p. 208). She explains propaganda as a ‘reality’, co-produced by both the recipient and the propagandist, based on deception. The difference with communications influence operations is the absence of a co-produced deceptive reality in the latter case, which merely aims to persuade the audience to see the world as the MoD does. Given her assumption that communication is never neutral, she is critical of applying propaganda against domestic audiences, but she does look favourably upon domestic influence operations.

It is favourable for resilience-building against hybrid threats to create a clear distinction between propaganda and communication strategies capable of improving psychological defence. Instead of tackling malicious propaganda with counter-propaganda, a resilience-building approach would call for antipropaganda by “strengthening society’s natural immune system against incendiary rhetoric” through “a more critically reflective, evidence-based attitude towards any claims that are being made” (Oosterveld et al., 2015, p. 24). The authors suggest that a more effective and sustainable way to combat propaganda is not to engage in a tit-for-tat exchange of misinformation, but to empower society to recognise and reject propaganda on its own. By fostering critical thinking and a demand for evidence-based information, society can build a natural resilience to incendiary rhetoric. Respondents point towards the importance of education, dedicating an important role to the Ministry of Education, Culture and Science (OCW) (interview 5; interview 7).

To sum up, societal resilience-building remains a difficult issue. Due to the state removing itself and pushing responsibility upon the shoulders of the private sector and individuals, security thinking has gradually lost its place in the mainstream debate. A series of recent events have caused a re-emergence of (hybrid) threats in the public perception but without any clear division of responsibilities between the state and its citizens. With a state perceived to be absent, conducting societal resilience-building strategies by deploying specific StratCom techniques to educate and ‘persuade’ the population to improve their awareness and preparedness has proven to be a culturally controversial and delicate sensibility within society, with an unclear role dedicated to the MoD. A perceived lack of trust and transparency prevents the government from using the ability to deploy them.

5.3 Interdepartmental limitations

Apart from restrictions caused by the legal foundations of the MoD and the constraints resulting from the ministry’s positioning vis-à-vis society, interdepartmental limitations have a big impact on societal resilience-building efforts. Respondents believe that the complex nature of hybrid threats calls for an integral security approach (interview 1; interview 2; interview 4; interview 6; interview 7; interview 8). The MoD’s limited mandate further requires close collaboration to establish a strong psychological defence. “You are a military organisation so your resources are limited. That does not mean that you cannot do anything, because an option is that you work together with other departments to get this started” (interview 7). Hence, that seems to be why some respondents consistently referred to ‘the government’ rather than ‘the MoD’ or ‘the armed forces’ (interview 7; interview 8). “The first step would be to do so on a whole-of-government level to make sure all departments are involved”, in the eyes of the DBG (interview 7).

In setting up an integral approach to enhance societal resilience, respondents argue that the MoD should collaborate with the NCTV and other security actors (interview 2; interview 6; interview 7). That is because the armed forces are considered indispensable in the security architecture as an organisation

possessing the legal use of force, dealing with and combatting military threats. Hybrid threats can, although not militarily at first glance, harm the preparedness and effectiveness of the armed forces. Think about how a hack of Dutch CI networks can impact both private operators as well as disturb military logistical operations. The NCTV is primarily responsible in the domain of societal resilience. Still, in a whole-of-government approach, the MoD initiates policy initiatives based on the armed forces' knowledge and expertise and creates support among other departments to implement those policies. Subsequently, in an interdepartmental deliberation, these proposals will be discussed and potentially adopted by the NCTV (personal communications, 5 June 2024). Needless to say, the MoD's contribution acts as a stimulator. No respondent argued that the armed forces should take over duties from other departments.

Respondents see the role of the MoD within this interdepartmental cooperation as a facilitating and mobilising one, respecting its mandate-related limitations. In their views, the ministry could assist other departments in preparatory action. Hybrid warfare characteristics reinforce this since military involvement alone in resilience-building initiatives is complicated because of two reasons. Firstly, hybrid threats play out below the (legal) threshold of war, thus democratically limiting the armed forces' options. Secondly, they do not always target a domain for which the MoD is responsible. On the part of the MoD, interdepartmental collaboration requires that the ministry communicate its needs due to its limited capacities. For example, if NATO partners evoke Host Nation Support, the MoD should communicate to other government departments or civil partners what type of assistance it needs, e.g. technical, organisational or capacity-building support. In other words, the ministry is responsible for ensuring that its share is communicated and executed well. The DGB Policy Advisor, however, made clear that this is far from reality. "If war would break out today, we are not ready and we don't have things arranged. [...] "We vaguely have an idea what we need, but nothing is concrete" (interview 7). In the MoD yearly white paper, the intensification of existing cooperation is being investigated, for example in a National Defence Plan and a National Defence Crisis Plan (Ministry of Defence, 2022b). Although, as of now, plans are yet to be determined and operationalised.

Eventually, for the MoD, an interdepartmental approach seems highly favourable because the Dutch governmental resilience thinking appears to be stovepiped. Both Van Leeuwe (interview 6) and Groothedde (interview 8) make this claim. According to them, every department is responsible for building resilience in its own sector. For example, the Ministry of Infrastructure and Water Management (I&W) makes bridges, railways and harbours resilient and OCW safeguards knowledge safety, whereas BZK counters disinformation and the NCTV enhances societal resilience by tackling crisis management. Groothedde attributes this to individual ministerial responsibility and the lack of an integral approach (interview 8). In an advisory report from the Dutch Council of State, the Council confirms this view. Policymakers and officials seem to approach policy issues too narrowly and due to the increasing number of government organs, responsibility is differentiated and a clear division of responsibility gets lost. As a result, the Council urges the government to work together more efficiently (Raad van State,

2020).

The MoD has a key interest in enhancing psychological defence among government partners and society. Yet, in a supportive role, it has proven to be difficult to raise situational awareness and preparedness. Inadequate cooperation between government actors appears to be a cause of this (interview 7). An attempt to tackle this issue was the establishment of the National Security Council (*Nationale Veiligheidsraad*, NVR) in September 2022. The NVR includes the prime minister, the Minister of Defence and the Minister of Foreign Affairs, among other affiliated ministries. This council "provides space for strategic and in-depth multidisciplinary analyses" (*Kamerstukken II*, 36410 (III), 2023). However, the NVR has not appeared particularly effective since its establishment, according to Groothedde: "That should be an organ that approaches security interdepartmentally [...] but that picture emerges insufficiently" (interview 8). The council has been insufficiently operationalised and, as a result, fails to achieve its effect because it is merely a sub-council which does not yet include all other relevant departments. Additionally, it lacks executive instructional powers, according to a report from the AIV (2024).

A more successful tool through which the MoD aimed to improve interdepartmental collaboration is via its contribution to the Security Strategy, in collaboration with the NCTV and the Ministry of the Interior and Kingdom Relations of Netherlands (BZK). In this Strategy, the government set out a three-pillar strategic course: a secured Kingdom in a multipolar world, a resilient democratic and legal order and a resilient and prepared society, subdivided into twelve interrelated points of action (NCTV, 2023). One of those points announced the implementation of a Nationwide Response Framework against Threats from State-Sponsored Actors (*Rijksbreed Responskader tegen Statelijke Dreigingen*, RBRK). The RBRK is a toolkit that aims to address and assess threats interdepartmentally, after which a response deemed fitting will be enacted. It could be military, but might as well be diplomatic, economic or political. This comprehensive approach called for a re-evaluation of the 'threats' under assessment because the scope of targets is widened. Instead of only focusing on potential CI targets, targets like high-valued knowledge and technology are also under review now, according to a 2021 letter to the House of Representatives (*Kamerstukken II*, 30821, 2021). The RBRK thus attempts to design a whole-of-government strategy, bundling multiple departments to set up a comprehensive strategy.

Within the government-wide approach, the MoD plays a pivotal role as a threat assessor. Respondents believe that situational awareness and preparedness among government departments are insufficient, similar to the case for society. In this role, the armed forces further the work with the intelligence services by bringing a military perspective to the response table (e.g. how war would impact civil-military relations and how the armed forces could assist civil authorities). MoD threat assessment, respondents argue, is an important part of national security because the armed forces can – other than intelligence services – undertake action to safeguard national interests. The legal use of force is exemplary herein. Respondents claim that the MoD, as a military organisation principally dealing with

threats, “feels that urgency quicker and earlier than the other departments” (interview 1). The ministry therefore considers itself as having a facilitating role in raising awareness among governmental partners (interview 7). Moreover, due to their experience with crisis management and challenging information environments in complex military operations, the armed forces can assist in improving preparedness. This resonates with their third constitutional duty; assisting civil authorities in case of crises or disasters (Ducheine & Bos, 2021). As ‘last man standing’, they furthermore ought to assist civil authorities in case of disturbances, adding weight to their perspective on (hybrid) threats. This assistance, however, only occurs upon request and after the approval of civil authorities – respectful of the armed forces’ legal boundaries (Bekkers et al., 2023).

To sum up, what ultimately is desired in the eyes of defence staff is an integral security approach with the involvement of governmental and societal actors in a comprehensive endeavour. However, this collaboration does not always play out well due to two reasons. Firstly, the stovepiped architecture of the Dutch government system, combined with the individual ministerial responsibility – meaning that ministers are accountable for (the actions of) their own department – creates a narrow approach to counter hybrid threats and improve psychological defence. Because officials fail to look at other departments, a comprehensive societal resilience-building strategy is deficient. Secondly, other departments may not prioritise situational awareness and understanding, which results in an insufficient threat assessment. The MoD could contribute to this assessment due to its expertise and experience. Thirdly, coordination with other departments is complicated because of unclear communication on behalf of the MoD as to what the ministry requires from its governmental and civil partners. It shows that the connection between these actors appears not to be as efficient as it should be.

In the subsequent chapter, the findings regarding relevant aspects of psychological defence in the Netherlands as well as those concerning the effective barriers that the MoD experiences will result in a closer look into the social positioning of the ministry.

6. SOCIETAL POSITIONING AND THE WAY FORWARD

Previously, in chapter 4 the concept of psychological defence within the Dutch context has been examined, highlighting its significance in enhancing a culture of civil awareness and preparedness for countering hybrid threats. Chapter 5 then explored the barriers and challenges faced by the MoD when contributing to societal resilience-building, including interdepartmental limitations, mandate constraints, and the broader societal context. This chapter will build upon that groundwork by exploring how the MoD navigates these challenges to contribute effectively to societal resilience-building initiatives. In particular, it addresses MoD officials' opinions regarding the ministry's evolving role in safeguarding a whole-of-society solution to counter hybrid threats.

Put bluntly, when approaching societal resilience as a matter of preparing citizens by providing guidance, then the MoD faces certain challenges. The ministry's mandate and capabilities – as a primarily military organisation – are designed to operate within the democratic system. However, these challenges do not exclude the ministry from contributing otherwise, for instance in raising situational awareness and preparedness among other departments and societal partners, so that they can improve their level of resilience or that of the sectors they oversee. In conversations with the DGB, three tracks were distinguished in which the MoD may play an effective role: an interdepartmental track, a communicative track and one focused on enhancing visibility in society (interview 7). These tracks will be analysed to answer the chapter's main question: what are the opinions of respondents on the way the Ministry of Defence positions itself within society to execute this role? Guided by the interviews, this chapter will analyse the respondents' stances vis-à-vis the ministry's role.

6.1 *Interdepartmental*

The effectiveness of the state's counter-hybrid tactics depends partly on the level of interdepartmental collaboration within the government. In that collaboration, “the MoD should know its place”, according to Van Leeuwe (interview 6). He claims the role of the MoD therein is that of a threat assessor, who in collaboration with intelligence services assists other departments with addressing potential vulnerabilities, assessing potential impact of hybrid threats on their sectors as well as creating a durable solution to effectively deal with this. The aim to enhance situational awareness and preparedness among government partners corresponds with the vision of the DGB, because “the MoD occupies a facilitating role to create that awareness” (interview 7).

The process of societal resilience-building occurs in close cooperation between the MoD and the NCTV, with the latter leading the process. An example of raising situational awareness is by engaging in a critical dialogue with other departments about hybrid warfare, discussing the potential impact of a NATO Article 5 scenario on their department and sector: “What impact will that have on my ministry and its mandate? What impact will it have on the sectors involved in my ministry? And what

should we do with that [scenario, ed.]: are we prepared for that – yes or no – and if not, what is required for that?” (interview 7). The platforms on which the MoD can play such a mobilising role are the NVR and the RBRK. Through these platforms, a comprehensive whole-of-government is drawn up. The government has a wide range of what Van Leeuwe refers to as ‘rotary knobs’ that it can turn: “Depending on how the threat develops itself, you can turn those knobs”, which include the possibility to adjust educational programs to raise awareness, limit the activities of foreign news outlets or restrain Dutch enterprises from undertaking business in countries that might cause a threat to our country – as was the case with ASML (interview 6). The government-wide dialogue, such as in the RBRK and the NVR, ensures that the turning of these knobs is well-adjusted.

Normally, the MoD’s role within these platforms is to inform, be informed, and advise (interview 6). Because the ministry is a central security actor, staff believes it can steer the debate to ensure that government interests are balanced and that vulnerabilities are addressed and mitigated. An exemplary case is Chinese foreign direct investment: “Huawei was the most attractive partner when we switched to 5G. From an EZK [Ministry of Economic Affairs and Climate Policy, ed.] perspective this would’ve been the most logical partner, but set against the background of a security issue it was not the best decision because it’s well-known that the state is behind it. If you don’t look at it interdepartmentally, you expose yourself” (interview 8). In this example, collaborating with Huawei could lead to hybrid threats as the Chinese state could then gain access to CI and personal data which undermine societal resilience. In an extreme case, CI’s vulnerability could threaten national security³ yet EZK lacked sufficient situational awareness to assess this threat.

The image might arise that raising awareness opens the door to securitisation measures as the MoD warns other ministries and points out potential vulnerabilities in their departments, processes and sectors. For ministries, these vulnerabilities run the risk of becoming security issues, opening the door for extraordinary measures that expand the reach of security actors which can undermine the democratic system of checks and balances. Surprisingly, respondents responded differently to the risk of securitisation. On the one hand, Groothedde stated that among government partners and in society, the sense of urgency to build (societal) resilience is “felt insufficiently”. Crisis communication seems to have an alarming effect and could therefore contribute to securitisation. Hence, from a StratCom perspective, she claimed that transferring this sense of urgency becomes effective “when crisis mechanisms are used. [...] If one would approach it as a crisis and communicates it as such then one could trigger that sense of urgency more” (interview 8). In an advisory report, she advocates for “an integrated approach in the field of StratCom, specifically focused on security, from the Dutch government” to enhance “stability, well-being and removing the feeling of insecurity” (Groothedde, 2023; interview 8). However, Groothedde referred explicitly to a balanced government-wide

³ In this example, predominantly ‘economic security’ could be threatened, following the NCTV’s conceptualisation of national security (2023). Although not a traditional military threat, because of this exposure, the MoD plays a role in addressing and mitigating the threat.

communication to deploy a crisis communication strategy rather than MoD communication, thereby objecting to the MoD's involvement in acts of securitisation.

On the other hand, the DGB approaches securitisation from an agenda-setting point of view rather than as a communicative strategy. The Policy Advisor within the DGB acknowledged that more and more issues had been deemed security issues, thereby claiming the act of securitisation as 'subjective', meaning that the 'securitiser' yields significant power over which issues are security-related and which are not. This act is influenced by politicians and society which both can determine the political agenda. The respondent claimed that in liberal democracies, the "essence of securitisation" is that a security issue "is put high on the political agenda and receives a lot of attention [...] yet it doesn't mean that we turn to extraordinary measures" (interview 7). The respondent referred to migration as an example: this phenomenon is not necessarily a security issue, but it can derive from security issues. Hence, some concerned citizens frame it as such, leaving space for politicians to subsequently adopt this frame and act accordingly. From this perspective, securitisation is thus merely seen as an act of agenda-setting and its risk is diminished due to the system of checks and balances that are supposed to be in place in a liberal democracy. Still, how this understanding exactly refrains the government from taking extraordinary measures remains unclear.

The advisory and informative role of the MoD was significantly strengthened after the Russian invasion of Ukraine. Respondents claimed that geopolitical alterations changed the (importance of) the MoD's role in societal resilience-building. An example is provided by Van Leeuwe concerning disinformation campaigns coming from Russian state-controlled news outlets in Western European states: "Prior to 2022, we as the MoD have expressed our concerns about this to BZK which is responsible for this. They kept saying: 'No, freedom of expression is important. That is stated in the Constitution. Citizens must be able to listen to them. We trust that our citizens can separate fact from nonsense.' When Ukraine erupted in February 2022, you saw that the EU's first sanctions package included banning such channels to reduce disinformation. That contributes to our [societal] resilience" (interview 6). Hence, security actors' pleas for bans after the changed geopolitical situation had a strong impact on the awareness and preparedness of political and societal actors. The MoD's earlier critiques towards such channels reinforced the MoD's expert role in this interdepartmental cooperation. Due to limitations in its mandate and the following limited decisiveness, the ministry considers its role as stimulating other departments to enhance resilience within their domains. The changing geopolitical situations helped shape this role, as explained by Van Leeuwe's quote (interview 6). This stimulation is regarded as a process of enablement; ensuring that departments (can) take their responsibility.

Another aspect that relates to the interdepartmental track is the discussion around reviewing the existing legal framework concerning the peace-conflict continuum, as discussed in the previous chapter. An important role of the MoD herein is instigating this discussion within government circles – and ultimately within society. In a letter to the House of Representatives, a call is made for reviewing state emergency law to make it fit for the present era of hybrid threats in the grey area of permanent

competition because it is “outdated in many respects, which means that it is necessary to take a closer look at whether the state emergency law is still in line with current and future threats” (*Kamerstukken II*, 29668/26956, 2022). Note that reviewing does not necessarily entail reforming said law. Yet, it is essential to have a clear view of the relations between the armed forces and the civil authorities before and after an Article 5 scenario. Within the MoD, the DGB is currently working on this together with government partners (interview 6). However, this process is far from operationalised and requires significant attention to set this up properly (interview 7). Again, respondents highlight the MoD’s facilitating and instigating role herein.

Ultimately, building societal resilience by enhancing psychological defence requires the ministry to engage in a critical dialogue that reaches beyond a whole-of-government approach and includes society at large. “We are working on it, but we aren’t there yet. Plans are being developed on how to approach that, but those haven’t been worked out yet. These [plans] also largely come down to a bit of communication”, according to the DGB Policy Advisor. Therefore, the subsequent section will dive into the MoD’s communicative role in enhancing societal resilience.

6.2 Communicative

Communication is a crucial component of the MoD’s role. To reduce public complacency, much depends on how the ministry communicates with government partners, civil actors and wider society (Wang & Kapucu, 2008). According to the DCo, the ministry should be “open” and “transparent”, and “in connection to society” (interview 2). These characteristics have been mentioned numerous times by respondents (interview 1; interview 4; interview 6; interview 7; interview 8). Despite the MoD’s mandate-related limitation in societal resilience-building, it can still contribute to enhancing psychological defence. In an advisory report, the AIV urged to ministry to function as a bridge in the formation of security-aware citizens, closing the gap between the government and societal actors and sending a message of assurance to the public. Clear communication plays a pivotal role herein, highlighting the ministry’s role as a stimulator by raising awareness but also entailing the provision of clear expectations of what it requires from society and vice versa, i.e. expectation management. “That is also why the DCo is so important” (interview 7).

For that reason, a closer examination of the DCo is necessary to determine the MoD’s societal positioning. How is the communication strategy designed? What is deemed important? Respondents gave a clear image of the complex challenges that this directorate faces when setting up effective communication campaigns. It bears final responsibility for internal and external communication of the armed forces and their operations. Furthermore, it supports the policy choices that the DGB makes regarding MoD plans and ensures that these are well-communicated and adapted to specific target audiences (interview 1). This requires a deep understanding of the target audiences and the most effective communication methods (Wang & Kapucu, 2008). Monitoring the effectiveness of campaigns

is crucial for measuring success (interview 4). To reach a large and diverse audience, a wide range of communication tools is important, ranging from social media to (local) newspapers, meetings and presence at local or regional events. In addition to informing, the ministry must listen as well. "Communicating starts with listening," according to a senior communication specialist (interview 2). The DCo plays an active role in listening to and engaging with stakeholders, including citizens, interest groups and local governments, to understand how the armed forces are perceived and to identify potential concerns and developments. When the MoD's plans affect specific communities, efforts are made to solicit feedback from those involved (interview 2). This aim for open, timely and two-sided communication, focused on interaction and dialogue, reflects a commitment to effective communication that goes beyond simply broadcasting messages and aims to build sustainable relationships and increase understanding between the armed forces and society. Although in essence this communication entails matters related to MoD-related operations and developments, if well-executed, it could serve as an example to enable MoD communication with governmental and societal partners about the importance of comprehensive societal resilience-building initiatives that highlight the importance of decisive armed forces in a well-prepared society.

Designing a communication strategy is one thing, however, successful execution is another. To ensure that messages are perceived by the audience accordingly, one should reflect critically on the effectiveness of this strategy. According to De Graaff, the applied measurement method fits insufficiently with the intended goal. She distinguished three types: measurement of performance, effectiveness and success – of which the first is given preference within the MoD (interview 4). Measurement of performance merely takes note of the quantity (e.g. "we uploaded so many posts, we put up this amount of posters, there were this many students present in the classroom, our posts had so many likes") rather than the actual effectiveness of the message. With this method of measurement, it remains unclear whether the message resonates with the targeted audience, for instance, critical groups that oppose the government (extremists, conspiracy theorists and anti-government thinkers) or victimised groups who lost their faith in the government (victims of the childcare benefits scandal).

Moreover, limited operational capacities complicate effective communication. The senior communication specialist highlighted the significant successes that consultative groups have in uniting the MoD and critics. An important note is however that these successes are often local and contextual and resolve spatial issues concerning MoD presence in local communities (interview 2). Expanding these practices into psychological defence strategies requires an enlargement of capacities. For example, De Graaff explained that many educational institutions request information sessions on societal resilience, but the capacity to respond to these requests is limited (interview 4). In their strategy, the DCo furthermore frequently stresses the importance of dual communication but the strategy concerning societal resilience still reflects a one-sided stream of communications.

Before the MoD can act as a bridge between the government and society – in line with the AIV's vision – encouraging and mobilising the population to enhance their resilience, it will first have to ensure

that it is perceived as a reliable and credible partner in countering contemporary threats (Hansen et al., 2021). Respondents claim credibility to be an important factor here. They argue that the flawed image of what the armed forces do undermines this credibility. Therefore, according to them, the communicative role of the MoD is partly to shed light on ongoing operations, such as domestic assistance to civil authorities (interview 4; interview 6). For instance, the armed forces provide shelter for conflict-affected refugees on their bases, assist police investigations and dismantle explosives almost weekly. “We are deployed on Dutch territory daily but the ordinary Dutchman doesn’t know this at all. These kinds of things can be visualised much better [...] just purely about what the armed forces do” (interview 4). Thus far, it appears as if communication on the MoD mostly concerns the level of potential nuisance that comes with the armed forces’ operations (interview 2; interview 6).

Instead, to improve the communicative role of the ministry, more attention should be paid to why such operations are crucial, according to multiple respondents (interview 2; interview 6; interview 7). Their perspective emphasises communication concerning the importance of maintaining strong and well-prepared armed forces. Seeing communication as a strategy that contributes to improving psychological defence, Groothedde advocates for the deployment of StratCom techniques because these transmit a message to the Dutch population on the relevance of military endeavours (interview 8). In doing so, this stream of communication could contribute to the MoD’s role in the ‘formation of security-conscious citizens’, as defined by the AIV (2024). Following Fry (2022), however, the ministry should be transparent about the use of StratCom Mil PA techniques for communication as well as how they differ from ‘ordinary’ propaganda.

In the present-day climate of hybrid warfare, disinformation campaigns targeting citizens might aim to weaken the credibility of the armed forces. By spreading fake news, adversaries can undermine the image and capability of the MoD, affecting support for the armed forces. In its communicative role, respondents argue that the MoD must strive for a careful balance when debunking disinformation. In that regard, Van Leeuwe seems to agree with Oosterveld et al. (2015) on refraining from utilising counter-propaganda. According to him, not every kind of fake news or gossip spread about the (operations of) the MoD and the armed forces should be tackled and debunked. “Only exceptionally, if the MoD experiences direct negative consequences to the national security, it should consider debunking. Not just every piece of disinformation” (interview 6). Although seemingly unnuanced in his statement, Van Leeuwe points to a risk of fatigue within society if the MoD constantly makes statements or claims about what they have found to be disinformation. It might lead to citizens turning their back towards the MoD – or the government at large – and feeling disconnected from government initiatives to enhance societal resilience.

To sum up, respondents deem transparent and clear MoD communication essential in uniting government and society and enhancing psychological defence. Deploying communication strategies – including the possibility of using StratCom techniques – could aid the ministry in maintaining a strong connection with society and creating a culture of civil awareness and preparedness. An intention to

maintain a two-sided dialogue with society is present, but in practice, the application is lacking and the operationalisation remains unclear. In the eyes of the defence staff, sufficient knowledge about the armed forces' endeavours contributes to the stimulation of this culture. Hence, transparency about the MoD's contribution to resilience-building initiatives is considered important. Along a similar line, respondents have expressed the desire for the armed forces to be more visible within society (interview 4; interview 6). Enhancing visibility is closely related to the MoD's communicative role, tying the two together. Hence, the subsequent session will discuss this last role.

6.3 Visibility

By enhancing the visibility of the MoD within society, it hopes to transmit a sense of urgency about hybrid threats. To avoid pushing citizens into a certain direction and implicitly advancing an underlying direction and objective, the ministry would do good to carefully transmit this sense through stimulation of a societal debate on how hybrid threats impact society (Fry, 2022). Enhanced visibility would help to initiate this (interview 4; interview 7; interview 8). This debate serves dual audiences: governmental partners in a whole-of-government approach, as assessed in the first section, and society at large, with this section building forward upon the previous section.

The current geopolitical climate impacts the Dutch feeling of security. Citizens tend to fear foreign involvement in Dutch societal sectors and politics, especially since the Russo-Ukrainian war. The possibility of war affecting our country also seems to have influenced people's perception of security (Sie Dhian Ho et al., 2024). As a consequence of this perception of insecurity, respondents deem it important that citizens can turn to capable and trustworthy armed forces that are present and well-prepared, for assurance and guidance. These tasks resonate with the MoD's role as first responder and last line of defence (Ministry of Defence, 2020). By deploying a communication strategy incorporating StratCom Mil PA techniques for informing the public about the armed forces' tasks, duties and achievements, the ministry can go beyond mere broadcasting of messages of nuisance, according to respondents. Instead, as Fry (2022) stated, by exceeding this type of broadcasting, Mil PA allows the MoD to send a message of assurance to the population, adding a cognitive dimension to its messages because people feel protected and reinforced.

Deterrence is deemed one of the government's crucial responsibilities in the peace-conflict continuum (interview 6). Mazarr (2018) distinguishes two types: deterrence by denial and by punishment. The former seeks to deter malicious action by ensuring that it will not have the intended impact. The MoD plays a pivotal role herein by being strong, determined and well-prepared, for instance through the deployment of troops or equipment. "Trained armed forces that are ready for deployment", according to Van Leeuwe (interview 6). However, Mazarr stated that "deterrence by denial should not be equated with military balances alone" (2018, p. 2). Indeed, the ministry shapes said deterrence through the whole-of-society approach as well, by contributing to enhancing societal resilience to ensure

that “hybrid threats don’t affect us because we [society, ed.] are resilient to them” (interview 6). Thus, the MoD’s role in deterrence by denial is dual. Societal resilience-building strategies reinforce this type of deterrence when implemented effectively. Simultaneously, the armed forces’ role contributes to enhancing psychological defence by improving visibility within society.

Deterrence by punishment, on the other hand, urges adversaries to refrain from attacking by threatening with severe penalties (Mazarr, 2018). These penalties could be military but might as well be economic (e.g. embargoes) or political (e.g. sanctions). Generally, this type of deterrence involves governance and thus has less to do with societal resilience than deterrence by denial. Yet, because deterrence by punishment ties in with the whole-of-government approach – like the RBRK – it still offers a way for the MoD to raise awareness and stimulate improving psychological defence. The MoD plays an advisory and supportive role within the RBRK, enabling it to raise issues and discuss vulnerabilities among other departments and incentivise them to build resilience within their underlying sectors (interview 6). In doing so, it has an important role in improving the country’s preparedness which in turn translates into an increased level of deterrence as well as societal resilience.

The two types of deterrence aim to show potent armed forces, both towards adversaries, governmental partners and society at large. According to the DGB Policy Advisor, conducting military exercises alone or in collaboration with NATO allies offers fertile ground for visibility (interview 7). These exercises provide an opportunity for the armed forces to showcase their responsibilities, capabilities and readiness, thereby reinforcing a sense of security among the public. Nonetheless, how these exercises are communicated to the broader society is important. Transparent and informative communication about the purpose and objectives of military exercises helps alleviate concerns and dispel misconceptions. Highlighting its role in maintaining national security can enhance public understanding, garner support and refute the MoD’s ‘closed off’ image, according to De Graaff (interview 4). To safeguard public support, the DCo should ensure that communication surrounding these exercises is content-related – emphasising the urgency – rather than a mere warning for nuisance.

Additionally, other means than deterrence can achieve visibility, especially vis-à-vis the general public which often lacks a clear understanding of threats or how deterrence impacts the threat level (Golby et al., 2013). Respondents suggest starting with an increased presence in the public eye, for instance through uniforms in street view or via media appearances. “Luckily we have some strong personalities who are working on this, such as a couple of retired generals or professors, both military and civilian” (interview 4). De Graaff is referring to former Netherlands Chief of Defence (*Commandant der Strijdkrachten*, CdS) Peter van Uhm and retired Army general Mart de Kruif, who for example launched a podcast in which they discuss geopolitical issues and defence matters for a broad audience.

When improving media visibility, defence staff advocate for a solid MoD narrative. “Every person within an organisation, the things that they say, actions they take [...] will communicate something. The more coherent this process is within an overarching narrative; the more unity of effort is achieved” (Hansen et al., 2021, p. 17). The DGB Policy Advisor reiterated this strongly, stating that

“we should in a unified manner and we should not transmit divergent messages” (interview 7). This applies for all high-ranked military and civilian officials, such as the Minister of Defence, the CdS and the State Secretary of Defence. Currently, those individuals are frequently present on Dutch talk shows like *Buitenhof* or *Nieuwsuur*.

“That kind of appearance is incredibly important to reach a larger audience and help them understand: ‘Okay, this is what is going on, this is what we [the armed forces, ed] need, this is how we get there and this is what we should do’. To transfer that message is super relevant.”
(interview 7)

Various respondents argued similarly (interview 1; interview 2). “I think the awareness grows and that we have capable people to talk about this”, according to De Graaff (interview 4). By appearing in Dutch media, high-ranked officials could catalyse a debate within society about the division of responsibilities, similar to the MoD’s interdepartmental role.

Respondents explain this by referring to the MoD as an expert on military and security issues. Golby et al. (2013) explain this expertise due to the ‘information asymmetries’ between citizens and (military) elites. “The views of senior military officers could be especially influential in shaping opinion because military leaders have distinctive professional expertise”, adding that people with low levels of knowledge rely on expert advice (p. 9). ‘Shaping opinion’ refers to the ability to influence citizens’ perception and understanding of how to tackle hybrid threats. It adds weight to the importance of sufficient visibility of the MoD in public appearances like television broadcasts because visibility provides a platform to address hybrid threats. In doing so, a balanced manner and message of communication is crucial. According to respondents, transparency and a two-sided dialogue about present-day vulnerabilities and the societal division of responsibilities can foster understanding and support for the armed forces rather than risk the critique of potentially militarising the security discourse or society as a whole. However, how this two-sided communication is envisioned remains unclear.

Although the armed forces’ visibility is increasing, utilising this visibility to stimulate a debate on how hybrid warfare impacts society and to highlight the importance of societal resilience occurs insufficiently, according to respondents arguing that the ministry could be more active on this terrain (interview 4; interview 7). Still, in their eyes, neither the ministry nor the government as a whole favours putting responsibility for societal resilience on the individuals’ shoulders. The DGB Policy Advisor rather argued: “The realisation kicked in that this [culture of awareness and preparedness, ed.] doesn’t automatically resonate with the citizens and that the government thus bears a responsibility to stimulate this awareness”, thereby claiming the opposite to be true (interview 7). Respondents believe the aim should be to mobilise government departments and societal actors to prepare for and combat hybrid threats, without losing sight of the MoD’s ultimate responsibility to safeguard national interests and protect its population (interview 4). For instance, through stimulating departments to assess potential vulnerabilities in their sectors or encouraging the population to enhance media literacy to counter

disinformation – i.e. ‘antipropaganda’ as formulated by Oosterveld et al. (2015). Hence, mobilising people to build resilience is a government-wide duty in which the MoD considers itself to play an important role.

The key appears to be the enablement of civil preparedness. Again, it all comes down to psychological defence. Citizens should be aware that they have a part to play and that they should be prepared to do so. However, the government plays a pivotal role in achieving this. According to De Graaff: “People must *want* it, they must be *able* to do it and they must *dare* it [emphasis added]”. In her quote, ‘it’ refers to taking up this role and becoming resilient and well-prepared citizens. In the second and third aspects, the MoD should provide a safe and accessible environment for people to prepare themselves while simultaneously giving clear guidelines on how to prepare (interview 4). Regarding preparation against hybrid threats that target society’s vulnerabilities, the ministry – together with the NCTV – can inform the population about how such threats negatively impact one’s circumstances. For example, a cyber or physical attack on CI can cut people off from the electricity network and the internet. In said scenario, a list of baseline requirements to have in-store could be provided to help people prepare (interview 4). The Swedish pamphlet ‘If Crisis Or War Comes’ is exemplary in this regard (Swedish Civil Contingencies Agency, 2022).

In conclusion, such endeavours aiming to enable societal actors require that the MoD be a visible actor within society. One that is perceived as credible and capable, and that complies with its task to strengthen deterrence vis-à-vis adversaries but conveys a sense of assurance to the domestic audience as well. In addition to deterrence, conducting military exercises and making public appearances also enhances the ministry’s visibility and can garner support – provided that an open and transparent communication strategy adds to a constructive and substantive dialogue about the armed forces’ importance and responsibilities. Altogether, increased visibility could strengthen psychological defence strategies which in turn help to build societal resilience.

7. CONCLUSION

In an era of hybrid warfare, the government must find a solution to protect the state, territory and population from threats targeting a broad spectrum of military, economic, political or social vulnerabilities. The MoD, as an indispensable security actor within the state, is however struggling to position itself to contribute to the protection because hybrid threats also take advantage of the legal system that Western countries implemented to safeguard their democracies. Simultaneously, adversaries not only target the state's CIs but aim for the individual's minds as well, further complicating the state's ability to respond. As a result, states resort to the concept of resilience as an appropriate measure to shield society from malicious hybrid threats.

This study's point of commencement is the MoD's request to research societal resilience-building and the ministry's contribution to it, with the initial assumption that the ministry ought to play an important role. However, soon it appeared that it was the NCTV which is primarily responsible for enhancing societal resilience, with the MoD playing a facilitating and supporting role. The role of the ministry turns out to be limited and should be embedded within an integral whole-of-government approach. The MoD is required to work interdepartmentally to address vulnerabilities and enhance situational awareness and understanding. This approach ideally culminates into a whole-of-society approach that also incorporates society at large by initiating a societal dialogue to make citizens aware of hybrid threats and how these influence them. Increased visibility and two-sided communication contribute to achieving this. However, the MoD's embedding into a comprehensive endeavour hinders dedicating a clear-cut role to the ministry. Additionally, the issues around hybrid warfare are relatively recent, thus complicating a clear government solution. The fact that even within the ministry it is not clear either and therefore opinions are not aligned further complicates this quest.

This study researched the MoD's room to contribute to societal resilience-building by shedding light on the question of how the ministry positions itself within society to enhance said resilience in the current international context of permanent competition and hybrid threats. To find a suitable answer, three sub-questions guided the research, namely 1) what is understood as psychological defence and to what extent can it be applicable in the Dutch context, 2) what are the potential barriers that the Ministry of Defence faces when enhancing said defence and 3) what are the opinions of stakeholders on the way the Ministry of Defence positions itself within society to execute this role?

Firstly, significant attention was paid to the Nordic region where Sweden and Finland formulated psychological defence as a fitting policy response to increase cognitive resilience. Embedded within their societal security doctrine that highlights the dual importance of civil and military defence, these countries stimulated a culture of civil awareness and preparedness within society by building on historical threat perceptions, a high level of trust in the government as well as a strong tradition of engagement between the public and private sector and the population at large. Considering the geographical and demographical differences, the Nordic psychological defence policies are not one-on-

one applicable to the Dutch case. However, some elements of psychological defence could be used to increase Dutch societal resilience. According to respondents it mostly boils down to creating a nationwide dialogue discussing hybrid threats and their impact on societal vulnerabilities. This dialogue should stimulate civil awareness and preparedness to establish a resilient whole-of-society approach, embedded within a strong whole-of-government core. Ultimately, the goal of psychological defence is not to turn citizens into individual policemen safeguarding law and order and monitoring ordinary life. Instead, the doctrine aims to mobilise individuals and empower them with the necessary tools - such as critical literacy and a sufficient level of awareness to be able to prepare for and absorb hybrid threats.

Secondly, when enhancing psychological defence in the Netherlands, the question remains how this should occur and who should be responsible for this. Societal resilience-building should occur in close collaboration with the NCTV, which is primarily responsible. However, the deployment of resilience-building strategies faces certain barriers. Three types of barriers have been distinguished: legal, societal and interdepartmental. The armed forces operate within a legal system that determines their mandate and refrains them from harming democracy through conducting operations domestically, especially in the cognitive dimension. Government control safeguards this, because without permission the armed forces cannot act.

Societal barriers entail the lack of this culture within society. A renewed process of securitisation sparked the realisation that citizens do not automatically enhance their awareness or preparedness and thus that the government should stimulate the development of a sufficient level of psychological defence. Recent events did trigger a sense of urgency within society but respondents argue that an unclear image of the armed forces restrains the MoD from initiating psychological defence. To enhance it, respondents highlight the importance of clear and transparent communication to build trust and reinforce credibility. Some point towards StratCom techniques as useful tools to foster a culture of awareness and preparedness, although this should occur respectful of legal boundaries.

To be able to contribute most effectively to societal resilience-building, respondents dedicate great value to an interdepartmental collaboration within a whole-of-government frame. According to them, the MoD plays a facilitating and mobilising role within this cooperation, respectful of its mandate. However, the absence of an integral strategy and lack of situational awareness and understanding within other government departments, a whole-of-government approach is challenging. The NVR fails to operationalise it, but the RBRK toolkit seems more promising. In those platforms, respondents believe that the MoD should function as a threat assessor, collaborating with the NCTV and intelligence services and amplifying their findings.

Thirdly, the way forward is characterised by respondents by three tracks: interdepartmental, communicative and visibility-enhancing. Interdepartmentally, the MoD should initiate a critical dialogue on how hybrid warfare or a NATO Article 5 scenario impacts other departments and their sectors. Because the ministry is a central actor in the security landscape, it can steer the debate to ensure that government interests are balanced and that vulnerabilities are addressed and mitigated. Moreover,

defence staff believes this dialogue should address reviewing existing legal frameworks in the peace-conflict continuum and assess how mutual dependencies between government departments are influenced by a potential deterioration of the security situation.

Then, via a communicative track, respondents argue the MoD can act as a bridge between the government and wider society in the formation of security-aware citizens among others due to the MoD's reservist base, encouraging and mobilising the population to enhance its resilience. However, communication should exceed broadcasting messages about nuisances related to military operations by emphasising the relevance of these operations. Seeing communication as a strategy contributing to improving psychological defence, they claim that this will garner citizens' support while simultaneously reinforcing the importance of maintaining strong and well-prepared armed forces.

Lastly, MoD staff stress that the communicative track has to be supported by increased visibility within society. This will strengthen the connection between society and the armed forces which aid the MoD to fulfil its connecting role. Via public appearances, a solid narrative can enhance public understanding, garner support and refute the MoD's 'closed off' image. Furthermore, it can constitute a feeling of reassurance and guidance to combat hybrid threats vis-à-vis the population. In doing so, visible armed forces contribute to psychological defence.

Thus, based on insights generated from interviews and policy documents, an image arises of an ambitious MoD that struggles to find appropriate manners to contribute to societal resilience, partly because of insufficient awareness among governmental and societal partners, but also because of the legal limitations preventing the armed forces from contributing in a way that within ministry walls perhaps is desired. The question arises if the MoD is the rightful actor to engage in societal resilience-building initiatives. Surely, as a central security actor, the ministry plays an important role in safeguarding national security. Nevertheless, the legal system in which it is embedded is there to prevent democratic erosion. Throughout some interviews, respondents continuously pointed towards the importance of reviewing the legal boundaries but the logic behind this argument remains flawed. Furthermore, setting up a sustainable whole-of-society approach with a strong whole-of-government core remains challenging when navigating through the peace-conflict continuum and dealing with hybrid threats. Despite that, stimulating a critical and constructive dialogue to achieve this appears to be the way forward for the MoD, as long as it respects its mandate. Recommended is to reassess the ministry's place within the whole-of-department and strengthen partnerships with government and societal partners to set hybrid issues on the agenda without securitising or harming the democratic system the ministry is embedded in. An important prerequisite for improving partnerships is also a reassessment of the MoD's outward communication, which ultimately still remains one-sided, especially regarding hybrid threats. Finding other ways to reach out and engage with citizens could offer potential to enhance psychological defence.

7.1 Discussion

This research is positioned at the intersection of vaguely conceptualised societal resilience and the poorly operationalised culture of civil awareness and preparedness. Similar to the broader debate surrounding resilience, departing from societal resilience remains a plethora of interpretations and understandings. To conceptualise this concept, the choice is made to approach it using the Nordic psychological defence paradigm. It has proven beneficial for two reasons. This paradigm provides a window of opportunity to operationalise and analyse societal resilience and creates a frame through which to approach the MoD's policy in that matter. Simultaneously, it assesses the large potential that this Nordic concept has for Dutch policymaking. The differences inherent to such a comparison urge the researcher to reflect on the architecture of the Dutch security and resilience-building landscape.

This reflection is helpful because of the adopted perspective in this study. Following an MoD-centred perspective, this research contributes to closing the gap between theory and praxis by connecting theoretical implications related to societal resilience-building (such as deterrence, securitisation and responsabilisation) to practical challenges (such as moving up in the grey area, dealing with hybrid threats and countering legal/interdepartmental barriers), derived from experts in the field. Analysing the positioning of the MoD as a societal partner and relating it to a larger societal debate on the tasks, limitations and responsibility of the armed forces in society, this study gathered substantive, practical insights and embedded them within the ongoing scientific debate on operationalising societal resilience building. As a result, this substantiated body of work can contribute to steering the interdepartmental and societal debate.

However, this chosen perspective also puts significant limitations on the results. The results shed light on the governance aspect of societal resilience-building strategies by looking at the space of manoeuvre and positioning of the armed forces. However, because of this aspect, a clear understanding of what role the individual should exactly assume is hard to establish. Moreover, the perspective of how society perceives the enhancement of resilience or psychological defence is left unaddressed. Further research on this more 'social' approach to societal-resilience building could deliver promising results. Furthermore, the hybridity of present-day threats challenges the existing boundaries of MoD effectiveness. The distinction between peacetime and wartime is relatively clear, but the grey area and conflicting jurisdiction within cause confusion and doubt. Close examination of the division of responsibilities within that area could also provide relevant insights.

Although from the perspective of the MoD it might occasionally appear as a challenging feature, the liberal-democratic foundation and the system of checks and balances that lay at the core of our security architecture are the exact delicate vulnerabilities that the government and society should cherish and protect. Democratic elections ought to characterise and preserve these foundations. As of now, it thus will remain a mere prospect of how the new cabinet will approach the above-mentioned issues.

BIBLIOGRAPHY

List of literature

- Andersson, J. J., & Tardy, T. (2015). *Hybrid: What's in a name?* [brief issue 32]. European Union Institute for Security Studies.
- Anholt, R., van Dullemen, C., de Carvalho, J. S., Rijbroek, J., Sieckelinck, S., & Sloodman, M. W. (2021). Understanding Societal Resilience: The Case for Engaged Scholarship. In M. Ungar (Ed.), *Multisystemic Resilience: Adaptation and Transformation in Contexts of Change* (pp. 551-564). Oxford University Press.
- Antai, I., & Hellberg, R. (2023). Identifying total defense logistics concepts: A comparative study of the Swedish pandemic response. *Journal of Humanitarian Logistics and Supply Chain Management*, ahead-of-print (ahead-of-print).
- Bankauskaitė, D., & Šlekys, D. (2023). Lithuania's Total Defense Review. *PRISM*, 10(2), 54–77.
- Bekkers, F., Louw, H. van der, & Heer, B. de. (2023). *De toekomstige Nationale Inzet van de Krijgsmacht*. The Hague Centre for Strategic Studies.
- Bergström, J. (2018). An archaeology of societal resilience. *Safety Science*, 110, 31–38.
- Berzina, I. (2020). From 'Total' to 'Comprehensive' National Defence: The Development of the Concept in Europe. *Journal on Baltic Security*, 6(2), 1–9.
- Bessems, R. (2021). Moving outside the Box: Military Mobility as the Key to Enabling European Security & Defense. *Atlantisch Perspectief*, 45(4), 28–32.
- Bryman, A. (2016). *Social Research Methods* (5th edition). Oxford University Press.
- Caliskan, M., & Liégeois, M. (2021). The concept of 'hybrid warfare' undermines NATO's strategic thinking: Insights from interviews with NATO officials. *Small Wars & Insurgencies*, 32(2), 295-319.
- Caves, B., Lucas, R., Dewaele, L., Muravska, J., Wragg, C., Spence, T. G., Hernandez, Z., Knack, A., & Black, J. (2021). *Enhancing Defence's Contribution to Societal Resilience in the UK: Lessons from International Approaches*. RAND Corporation.
- Christie, E.H., & Berzina, K. (2022). *NATO and Societal Resilience: All Hands on Deck in an Age of War* [policy brief]. GMF – German Marshall Fund of the United States. <https://www.gmfus.org/news/natoand-societal-resilience-all-hands-deck-age-war>.
- Commissie-Brouwer. (2023). *Grondslag gezocht. Onderzoekscommissie Land Information Manoeuvre Centre (LIMC)* [research report].

- Diener, E. & Crandall, R. (1978). *Ethics in Social and Behavioral Research*. University of Chicago Press.
- Drent, M., Kruijver, K., & Zandee, D. (2019). Military Mobility and the EU-NATO Conundrum. In *Clingendael Report*. Clingendael - Netherlands Institute of International Relations.
- Ducheine, P. A. L., & Bos, P. L. J. (2021). *De krijgsmacht: doel, functie, taken en rollen geanalyseerd: Non-Paper tbv De Rollen van Defensie – Onderzoek naar de strategische rollen van Defensie binnen de Nederlandse Veiligheidsarchitectuur*. Amsterdam Law School Research Paper No. 2021-40.
- Egli, D. S. (2013). Beyond the Storms: Strengthening Preparedness, Response, & Resilience in the 21st Century. *Journal of Strategic Security*, 6(2), 32–45.
- Elonheimo, T. (2021). Comprehensive Security Approach in Response to Russian Hybrid Warfare. *Strategic Studies Quarterly*, 15(3), 113–137.
- Evans, K. (2017). War and Peace: Is Militarisation the New Norm?. In Amatrudo, A. (eds) *Social Censure and Critical Criminology* (pp. 275–301). Palgrave Macmillan.
- Fjäder, C. (2014). The nation-state, national security and resilience in the age of globalisation. *Resilience*, 2(2), 114–129.
- Flick, U. (2018). *Doing grounded theory*. SAGE Publications Ltd.
- Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, 121, 90–103.
- Frizzelle, B., Garey, J., & Kulalic, I. (2022). NATO's national resilience mandate: challenges and opportunities. *Defence Studies*, 22(3), 525–532.
- Golby, J., Dropp, K., & Feaver, P. (2013). *Listening to the Generals: How Military Advice Affects Public Support for the Use of Force*. Center for a New American Security.
- Graaf, B. A. de. (2012). Nationale veiligheid in historisch perspectief III. *Magazine Nationale Veiligheid En Crisisbeheersing*, 10(6), 52–55.
- Groothedde, S. (2023). *Strategische communicatie door de Nederlandse overheid (adviesrapport)* [2023.HDV-19].
- Gruber, B. (2017). The Difference Resilience Makes: U.S. National Preparedness - from Civil Defence to Resilience [working paper]. *OIIP working paper*, 93.
- Grzela, J. (2022). Finland's readiness for comprehensive national defence. *Bezpieczeństwo: Teoria I Praktyka*, 3, 211-221.

- Holling, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, 4(1), 1–23.
- Houck, S. (2022, December 27). *Psychological capabilities for resilience*. War on the Rocks. Retrieved November 14, 2023, from <https://warontherocks.com/2022/12/psychological-capabilities-for-resilience/>.
- HSC & ECNL. (2018, March 14). At the Intersection of Security and Regulation. *ICNL*. Retrieved March 13, 2024 from <https://www.icnl.org/post/assessment-and-monitoring/at-the-intersection-of-security-and-regulation>.
- Juntunen, T., & Hyvönen, A.-E. (2014). Resilience, security and the politics of processes. *Resilience*, 2(3), 195–209.
- Labaka, L., Hernantes, J., & Sarriegi, J. M. (2016). A holistic framework for building critical infrastructure resilience. *Technological Forecasting and Social Change*, 103, 21–33.
- Larsson, O. (2021). The connections between crisis and war preparedness in Sweden. *Security Dialogue*, 52(4), 206–324.
- Larsson, S., & Rhinard, M. (Eds.). (2020). *Nordic Societal Security: Convergence and Divergence* (1st edition). Routledge.
- Longhurst, R. (2016). Semi-structured Interviews and Focus Groups. In: N. Clifford, M. Cope, T. Gillespie & S. French (eds). *Key Methods in Geography* (pp. 143-156). Sage Publications Ltd.
- Longstaff, P. H., & Yang, S.-U. (2008). Communication Management and Trust: Their Role in Building Resilience to “Surprises” Such As Natural Disasters, Pandemic Flu, and Terrorism. *Ecology and Society*, 13(1).
- Mazarr, M. J. (2018). *Understanding Deterrence*. RAND Corporation
- Mehvar, S. H., Wijnberg, K. M., Borsje, B. W., Kerle, N., Schraagen, J. M., Kruijf, J. V., Geurs, K. T., Hartmann, A., Hogeboom, R. J., & Hulscher, S. J. (2021). Review article: Towards resilient vital infrastructure systems – challenges, opportunities, and future research agenda. *Natural Hazards and Earth System Sciences*, 21(5), 1383–1407.
- OECD. (2021). *OECD Report on Public Communication: The Global Context and the Way Forward*. OECD Publishing.
- Oosterveld, W. Th., De Spiegeleire, S., de Ridder, M., Sweijts, T., Bekkers, F., Polackova, D., Ward, S., Salah, K. E., Rutten, R., & Olah, N. (2015). The Two Sides of the Security Coin. In *Si Vis Pacem, Para Utique Pacem: Individual Empowrment, Societal Resilience And The Armed Forces* (pp. 19–26). Hague Centre for Strategic Studies.

- Rhinard, M. (2020). Societal security in theory and practice. In S. Larsson & M. Rhinard (Eds.), *Nordic Societal Security: Convergence and Divergence* (pp. 22-42). Routledge.
- Rosbach, N. (2017). Psychological Defence: Vital for Sweden's Defence Capability. *Offprint from Strategic Outlook 7*. Totalförsvarets forskningsinstitut – FOI.
- Salonius-Pasternak, C. (2018). The defence of Finland and Sweden: Continuity and variance in strategy and public opinion. *FIIA Briefing Paper*.
- Scaparrotti, C. M., & Bell, C. B. (2020, April). *Moving Out: A Comprehensive Assessment of European Military Mobility*. Atlantic Council, Scowcroft Center for Strategy and Security.
- Schoenmakers, B. (2022). Maatschappij en krijgsmacht in Nederland. *WO2 Onderzoek uitgelicht 11(3)*.
- Setola, R., Luijff, E., & Theocharidou, M. (2016). Critical Infrastructures, Protection and Resilience. In R. Setola, V. Rosato, E. Kyriakides, & E. Rome (Eds.), *Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach* (pp. 1–18). Springer International Publishing.
- Sie Dhian Ho, M., Elchardus, M., Houtkamp, C., & Van Der Laan, T. (2022). *Tussen hoop en vrees. Bescherming van de gemeenschap en de-globalisering in het jaar van de Ruslandshok*. Clingendael Barometer Alert.
- Sie Dhian Ho, M., Elchardus, M., Houtkamp, C., & Van der Laan, T. (2024). *Tussen hoop en vrees. Van Ruslandshok naar Hamasshok – De verzuchting naar eigentijdse gemeenschapsafbakening*. Clingendael Barometer Alert.
- Smith, H. (2019). Countering hybrid threats. In G. Lindstrom & T. Tardy (Eds.), *NATO and the EU: The essential partners* (pp. 15–24). NATO Defense College.
- Stoker, D. (2016, December 17). *The Myth of Total War*. The Strategy Bridge. Retrieved March 22, 2024, from <https://thestrategybridge.org/the-bridge/2016/12/17/the-myth-of-total-war>.
- Sundelius, B., & Eldeblad, J. (2023). Societal Security and Total Defense: The Swedish Way. *PRISM*, 10(2), 92–111.
- Swedish Defence Research Agency. (2021, December 9). *Vad är försvarsvilja? Och hur viktig är den?* FOI – Totalförsvarets forskningsinstitut. Retrieved March 26, 2024, from <https://www.foi.se/nyheter-och-press/nyheter/2021-12-09-vad-ar-forsvarsvilja-och-hur-viktig-ar-den.html>.
- Urquhart, C. (2013). *Grounded Theory for Qualitative Research: A Practical Guide*. SAGE Publications, Ltd.

- Valtonen, V., & Branders, M. (2020). Tracing the Finnish Comprehensive Security Model. In S. Larsson & M. Rhinard (Eds.). (2020). *Nordic Societal Security: Convergence and Divergence* (pp. 91-108). Routledge.
- Verschuren, P., & Doorewaard, H. (2010). *Designing a Research Project* (2nd ed.). Eleven International Publishing.
- Wang, X., & Kapucu, N. (2008). Public Complacency under Repeated Emergency Threats: Some Empirical Evidence. *Journal of Public Administration Research and Theory: J-PART*, 18(1), 57–78.
- Watkin, K. L. (2016). *Fighting at the legal boundaries: Controlling the Use of Force in Contemporary Conflict*. Oxford University Press.
- Wigell, M., Mikkola, H., & Juntunen, T. (2021). *Best Practices in the whole-of-society approach in countering hybrid threats* [working paper].
- Willig, C. (2013). *Introducing Qualitative Research in Psychology*. Open University Press.
- Wither, J. K. (2020). Back to the future? Nordic total defence concepts. *Defence Studies*, 20(1), 61–81.
- Wrange, J. (2022). Entangled security logics: From the decision-makers' discourses to the decision takers' interpretations of civil defence. *European Security*, 31(4), 576–596.

List of policy documents

- Finnish Security Committee. (2017, November 2). *The Security Strategy for Society* [government resolution]. Retrieved December 7, 2023, from <https://turvallisuuskomitea.fi/en/security-strategy-for-society/>.
- Kamerstukken I* 1997/98, 25367 (R 1593), nr. 226b.
- Kamerstukken II* 1996/97, 25367 (R 1593), nr. 3.
- Kamerstukken II* 2020/21, 30821, nr. 125.
- Kamerstukken II* 2021/22, 30821, nr. 125.
- Kamerstukken II* 2022/23, 29668/26956, nr. 69.
- Kamerstukken II* 2022/23, 30196, nr. 815.
- Kamerstukken II* 2022/23, 32761/30821, nr. 258.
- Kamerstukken II* 2022/23, 36200 (X), nr. 72.
- Kamerstukken II* 2023/24, 36410 (III), nr 2.

- Ministry of Defence. (2020). *Defensievisie 2035. Vechten voor een veilige toekomst* [white paper].
- Ministry of Defence. (2022b, June). *Sterker Nederland, Veiliger Europa. Investeren in een krachtigere NAVO en EU* [white paper].
- Ministry of Defence. (2024). *Doctrine bulletin for Communication & Engagement. Key Doctrine & Operations* (CLAS2024001390, version 1.0).
- NATO. (2019). *Allied Joint Doctrine for the Conduct of Operations* (AJP-3.C.1). NATO Standardization Office.
- NATO. (2023). *Allied Joint Doctrine For Strategic Communications* (AJP-10). NATO Standardization Office.
- NCTV. (2023). *De Veiligheidsstrategie voor het Koninkrijk der Nederlanden* [white paper]. Retrieved November 22, 2023, from <https://www.nctv.nl/documenten/publicaties/2023/04/03/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden>.
- Raad van State. (2021). *Ministeriële verantwoordelijkheid. Een ongevraagd advies van de Afdeling advisering* (W04.20.0135/I).
- Swedish Government Offices. (2014). *Lag om sprängämnesprekursorer och redovisning av krisberedskapens utveckling* [Law on Explosive Precursors and Report on the Development of Crisis Preparedness; government bill 2013/14:144]. Regeringskansliet.
- Swedish Government Offices. (2020, October 25). *Totalförsvaret 2021–2025* [government bill 2020:21:30]. Regeringskansliet.
- Swedish Ministry of Defence. (2021). Main elements of the Government bill *Totalförsvaret 2021-2025*.
- List of other sources**
- AIV. (2024, June 4). *Hybride dreigingen en maatschappelijke weerbaarheid* (AIV-advies 126).
- Barigazzi, J. (2024, March 21). Von der Leyen asks Finland to prepare the EU for war. *Politico*. Retrieved March 27, 2024, from <https://www.politico.eu/article/von-der-leyen-asks-finland-to-prepare-the-eu-for-war/>.
- Barndollar, G. (2024, March 15). Sweden's military conscription system is a model for NATO. *Foreign Policy*. Retrieved May 22, 2024, from <https://foreignpolicy.com/2024/03/15/sweden-nato-military-conscription-model-defense/>.

- Centraal Bureau voor de Statistiek. (2023, May 8). *Minste vertrouwen in Tweede Kamer in 10 jaar tijd*. CBS. Retrieved November 9, 2023, from <https://www.cbs.nl/nl-nl/nieuws/2023/19/minste-vertrouwen-in-tweede-kamer-in-10-jaar-tijd>.
- Drent, M. & Meijnders, M. (2019). *Internationale Rechtsorde als zesde Nationaal Veiligheidsbelang*. Analistennetwerk Nationale Veiligheid (ANV).
- Finnish Security Committee. (n.d.). *Vital functions*. Turvallisuuskomitea. Retrieved March 27, 2024 from <https://turvallisuuskomitea.fi/en/security-strategy-for-society/vital-functions/>.
- Johns Hopkins University & Imperial College London. (2021, May 20). *NATO Review – Countering cognitive warfare: awareness and resilience*. NATO Review. Retrieved March 21, 2024 from <https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html>.
- Kante, L. (2022, November 8). *Bra grund för svenskars försvarsvilja*. Aktuell Säkerhet. Retrieved March 26, 2024, from <https://www.aktuellsakerhet.se/bra-grund-for-svenskars-forsvarsvilja/>.
- Ministry of Defence. (2022a, September 30). *Draagvlakmonitor Defensie*. CHOICE.
- NATO. (2022, September 22). *Resilience, civil preparedness and Article 3*. Retrieved March 4, 2023, from https://www.nato.int/cps/en/natohq/topics_132722.htm.
- NATO. (2023, October 10). *Deterrence and defence*. Retrieved April 1, 2024, from https://www.nato.int/cps/en/natohq/topics_133127.htm.
- NCTV. (n.d.). *Organisatie*. Retrieved March 29, 2024, from <https://www.nctv.nl/organisatie>.
- NCTV, AIVD & MIVD. (2022). *Dreigingsbeeld Statelijke Actoren 2*.
- Swedish Civil Contingencies Agency. (2021). *Strengthening civil preparedness*. National Risk and Capability Assessment 2021 – MSB. Retrieved December 12, 2023, from <https://www.msb.se/siteassets/dokument/publikationer/english-publications/strengthening-civil-preparedness.pdf>.
- Swedish Civil Contingencies Agency. (2022). *If Crisis Or War Comes*.
- Psychological Defence Agency. (2022, February 28). *Mission*. MPF. Retrieved March 27, 2024, from <https://www.mpf.se/en/mission/>.

List of figures and tables

Table 1. List of interviews.

Figure 1. Peace-conflict continuum illustrated. *Source: Van Leeuwe, personal communications.*

APPENDIX



Information about the study on enhancing societal resilience and the role of the Ministry of Defence herein.

Introduction

You have been invited to participate in a scientific research project at Radboud University. Before you decide whether you want to participate in this study, you will receive an explanation of what the study entails. Please read this information carefully.

What is the study about?

This study examines the role of the Dutch Ministry of Defence (MoD) regarding the improvement of societal resilience. This study approaches societal resilience through the lens of ‘psychological defence’, which entails a certain level of civil awareness and preparedness to contribute to societal resilience. By analysing the role that is attributed to the Dutch MoD, I hope to find an answer to the main research question: *How does the Ministry of Defence position itself as a societal partner contributing to enhancing societal resilience in the current context of permanent competition?* By answering this question, I expect to provide meaningful insights into the policy made to improve societal resilience in the Netherlands and I hope to add potentially useful recommendations to the MoD.

What is expected of you?

In this study, you will be interviewed by me, Rob Baggermans. If you consent, an audio recording of this interview will be made to ensure the accuracy of the study. The recording will be used as research data. The interview will take approximately 45 min to one hour. In the interview, I will ask you questions about the various aspects of societal resilience improvement and/or the (communicative) role of the Ministry, as well as your professional involvement herein.

Voluntary participation

You decide whether to participate in this study. Your participation is voluntary and you may decline to answer any given question you wish not to answer. Furthermore, you can stop your participation and withdraw your consent at any time throughout the study, without having to indicate why. You can also have your research data and personal data deleted up to two weeks after participation, by sending an email to rob.baggermans@ru.nl.

What will happen to my data?

Your participation in this study is confidential. Recordings are deleted as soon as the interview report and the transcripts are finished.

The interview notes *can be* anonymised if preferred, meaning that it will be made nearly impossible to trace data back to you. I do this by removing all information leading to you as an individual from the research data, such as your name, contact information, or any other mentioned credentials. If not applicable, your name, organisation, potential rank and a basic description of your function will be used as data for this research. If you wish to exclude any of this information from the research, please indicate so in the box at the end of this form.

The data will not be used for other studies unless you give your explicit consent. The data will be made available for Radboud University for the purpose of archiving and ensuring scientific verifiability. However, this does not need to be made public and can also be anonymised if preferred.



Do you have any questions about the study?

If you would like to know more about the study or processing of the research data please ask me now, or contact me later via email at *rob.baggersmans@ru.nl* or by phone at (+31) 6 20102984.

Consent

If you want to participate in this study, I will ask you to sign the following consent form. Your written consent indicates that you have understood the information and agree to participate in the study.

Informed consent form for the study on enhancing societal resilience and the role of the Ministry of Defence herein.

Statement of consent

I have been informed about the purpose of the study. I was able to ask questions about the study. I am participating in the study voluntarily. I understand that I may withdraw participation and consent at any time during the study if desired. I understand how the data from the study will be kept and what it will be used for. I agree to participate in the study as described in the information document.

In addition, I consent to: *(please check the appropriate box):*

Yes No

- making audio recordings
- use of data about my name
- use of data about my department
- use of data about my rank – if applicable
- use of data about my function
- storage of data to ensure scientific integrity

Name of participant:

Date:

Signature:

Name of researcher: **R.J.L. (Rob) Baggersmans**

Date:

Signature:

Appendix II – List of questions

Topic A: Psychological defence

INLEIDENDE VRAGEN

1. Hoe definieer jij *psychological defence* in de context en het land waarin je werkt?
2. Hoe definieer jij *societal resilience* in de context en het land waarin je werkt?
3. Hoe houdt de organisatie waar je werkt zich bezig met deze concepten?
4. In hoeverre is dit van bovenaf gestuurd?
5. Wat zijn volgens jou de belangrijkste aspecten van *psychological defence*?
6. Hoe zie je de relatie tussen deze vorm van defensie en de weerbaarheid van de samenleving?
7. Welke rol denk je dat zulke defensie speelt in het waarborgen van de weerbartheideiligheid en stabiliteit van een samenleving?
8. Hebben contemporaine conflicten impact op de *psychological defence* en maatschappelijke weerbaarheid? Zo ja, hoe?

DIEPGAANDE VRAGEN

1. Binnen jouw organisatie, hoe wordt *psychological defence* ingebed in bredere veiligheids- en weerbaarheidsstrategieën?
2. Welke uitdagingen ervaart jouw organisatie bij het implementeren van maatregelen voor zulke defensie?
3. Binnen jouw organisatie, hoe wordt maatschappelijke weerbaarheid ingebed in bredere veiligheids- en weerbaarheidsstrategieën?
4. Zie je mogelijkheden voor samenwerking met andere instellingen, bedrijven of academische instellingen om *psychological defence* te versterken?
5. Hoe zou zulke intermaatschappelijke samenwerking eruit kunnen zien op het gebied van *societal resilience*?
6. Hoe communiceert jouw organisatie over *psychological defence* en maatschappelijke weerbaarheid naar andere organisaties, instellingen en organen?
7. Hoe communiceert jouw organisatie over *psychological defence* en maatschappelijke weerbaarheid naar het publiek?
8. Zie je uitdagingen met betrekking tot transparantie en begrip van deze concepten door de samenleving?

9. Hoe betreft jouw organisatie het publiek bij initiatieven ten gunste van het versterken van *psychological defence*?
10. Zie je mogelijkheden om de betrokkenheid van burgers bij maatschappelijke weerbaarheid te vergroten? Zo ja, welke?
11. Hoe wordt vanuit de overheid beleid uitgestippeld om *psychological defence* te verbeteren teneinde maatschappelijke weerbaarheid te versterken?
12. Hoe zie je de toekomstige ontwikkelingen op het gebied van *psychological defence* en maatschappelijke weerbaarheid?
13. Welke stappen zouden genomen moeten worden om deze concepten effectiever te maken?
14. Welke rol heeft het Ministerie van Defensie hierin?
15. Hoe kunnen samenlevingen zich volgens jou in de huidige context van hybride conflicten weerbaar maken?

Topic B: MinDef en maatschappelijke weerbaarheid

INLEIDENDE VRAGEN

1. Wat zijn volgens jou de belangrijkste aspecten van maatschappelijke weerbaarheid?
2. Hoe zou je het definiëren?
3. Welke rol denk je dat maatschappelijke weerbaarheid speelt in het waarborgen van de veiligheid en stabiliteit van een samenleving?
4. Hebben contemporaine conflicten impact op de maatschappelijke weerbaarheid? Zo ja, hoe?
5. Wat is het belang van zulke weerbaarheid, met name in relatie tot het Ministerie van Defensie?
6. Hoe houdt de organisatie waar je werkt zich volgens jou bezig met deze vorm van weerbaarheid?
7. Weet je iets over de manier waarop dit beleid vormgegeven wordt?
8. Wat is volgens jou de rol die communicatie naar buiten toe speelt in het vergroten van maatschappelijke weerbaarheid?

DIEPGAANDE VRAGEN

1. Hoe integreert het Ministerie van Defensie maatregelen voor maatschappelijke weerbaarheid in zijn bredere strategieën?
2. Welke uitdagingen ervaart het ministerie bij het implementeren van dergelijke maatregelen?
3. Hoe werkt het ministerie samen met andere ministeries, departementen en instanties om maatschappelijke weerbaarheid te vergroten?
4. Zie je mogelijkheden voor verdere samenwerking tussen verschillende departementen op dit gebied?
5. Hoe wordt omgegaan met de uitdagingen rondom het communiceren van complexe veiligheidsconcepten naar het brede publiek?
6. Hoe is het communicatieverkeer opgebouwd; eenzijdig of tweezijdig? Hoe wordt dat gefaciliteerd?
7. Welke positie bekleedt Defensie binnen het nationale overheid om de maatschappelijke weerbaarheid te vergroten? Welke verantwoordelijkheden draagt het?
8. Hoe positioneert het ministerie zich binnen de maatschappij om deze weerbaarheid te vergroten?
9. Hoe wordt er over deze positionering nagedacht en naar buiten toe gecommuniceerd?
10. Moet de maatschappelijke positionering van Defensie versterkt worden om maatschappelijke weerbaarheid te versterken? Hoe voorzie je mogelijkheden om dit te doen?

11. Wat voor kansen zie je om de bewustwording en betrokkenheid van burgers en andere belanghebbenden te vergroten?
12. Hoe zou potentieel hierin een rol voor securitisatie kunnen spelen?
13. Waar ligt de lijn tussen burgers informeren, mobiliseren en instrumentaliseren?
14. Wat zegt de verhouding tussen burger en Defensie over de verdeling van verantwoordelijkheden (m.n. *neoliberal governmentality*)?
15. Hoe voorzie je de evolutie van Defensie in het vergroten van de weerbaarheid van de samenleving? Gaat deze voortbouwen of breken met huidig beleid – als er al beleid is?

Topic C: De communicatieve rol van MinDef

INLEIDENDE VRAGEN

1. Wat zijn volgens jou de belangrijkste aspecten van de communicatieve rol die Defensie heeft naar buiten toe? Hoe zou je deze rol definiëren?
2. Welke rol denk je dat maatschappelijke weerbaarheid speelt in het waarborgen van de veiligheid en stabiliteit van een samenleving?
3. Hebben contemporaine conflicten impact op de maatschappelijke weerbaarheid? Zo ja, hoe heeft dat een weerslag op de communicatieve rol van het ministerie?
4. Wat is volgens jou de rol die communicatie naar buiten toe speelt in het vergroten van maatschappelijke weerbaarheid?
5. Waarin ligt de lijn tussen het publiek informeren, mobiliseren en instrumentaliseren?

DIEPGAANDE VRAGEN

1. Welke (communicatieve) strategieën hanteert het ministerie om bewustwording en bereidheid te vergroten? (Hoe) wordt hierin gedifferentieerd?
2. Hoe wordt de effectiviteit van de externe communicatie gemeten?
3. Hoe kan Defensie binding zoeken met de samenleving om dit voor elkaar te krijgen?
4. In hoeverre werkt Defensie samen met andere departementen, ministeries of instellingen om deze communicatieve rol uit te voeren?
5. Wat zegt volgens jou deze communicatieve rol de binding tussen burger en overheid (en over de positionering van Defensie als maatschappelijke partner)?
6. Wat is de verhouding tussen Defensie en burger? En wat zegt dit over de verschillende verantwoordelijkheden (m.n. *neoliberal governmentality*)?
7. Hoe bereidt het ministerie zich voor en reageert het op crisissituaties vanuit een communicatieperspectief (m.n. securitisatie)?
8. Welke rollen spelen vertrouwen en transparantie in (crisis)communicatie en binding?
9. Op welke manier maakt het ministerie gebruik van media en technologie om zijn boodschappen over te brengen? Welke media worden aangewend?
10. Zijn hierin specifieke trends of ontwikkelingen die een belangrijke rol spelen in de communicatieve rol van het ministerie?

Appendix III – Coding scheme

For interviews 1, 2, 4, 6, 7 and 8:

HIGHLIGHTED TEXT	
Green highlighted	Hybrid threats
Light blue highlighted	Whole-of-government approach
Blue highlighted (& white-coloured text)	Tasks for the MoD
Yellow highlighted	Responsibilisation & division of tasks
Grey highlighted	Peace-conflict continuum
Red highlighted	Securitisation & militarisation
Dark green highlighted	Barriers perceived by the MoD
COLOURED TEXT	
Green	Societal resilience
Light blue	Measures taken by government (w-o-g approach)
Red	Communication & perception of MoD
Yellow (& blue highlighted)	Support for MoD
Purple	Legal framework
Orange	(Tasks for the) NCTV
Gold	(Tasks for the) DCo

For interviews 3 and 5, another coding scheme has been applied because of the substance discussed in these interviews. Aspects relevant to the Swedish and Finnish context were discussed, including but not limited to the Total Defence structure, the distinction between civil and military defence, and socio-cultural factors contributing to establishing the Nordic security architecture, as well as measures taken by the respective governments to enhance psychological defence. Hence, the content discussed in these interviews differs significantly from that in the other interviews and as a result a different coding scheme was made, which was applied for interview 3 and 5.

For interviews 3 and 5:

HIGHLIGHTED TEXT	
Yellow highlighted	Defining societal resilience
Purple highlighted	Defining psychological defence
Grey highlighted	Civil defence notion
Green highlighted	The aspect of communication
Light blue highlighted	Socio-cultural heritage
Red highlighted	Government organisation
COLOURED TEXT	
Orange	Civil awareness (in changing geopolitics)
Blue	Mobilisation versus responsabilisation
Red	Legal framework
Green	The aspect of trust
Dark blue	Practical recommendations
Gold	Differences Sweden – Finland