



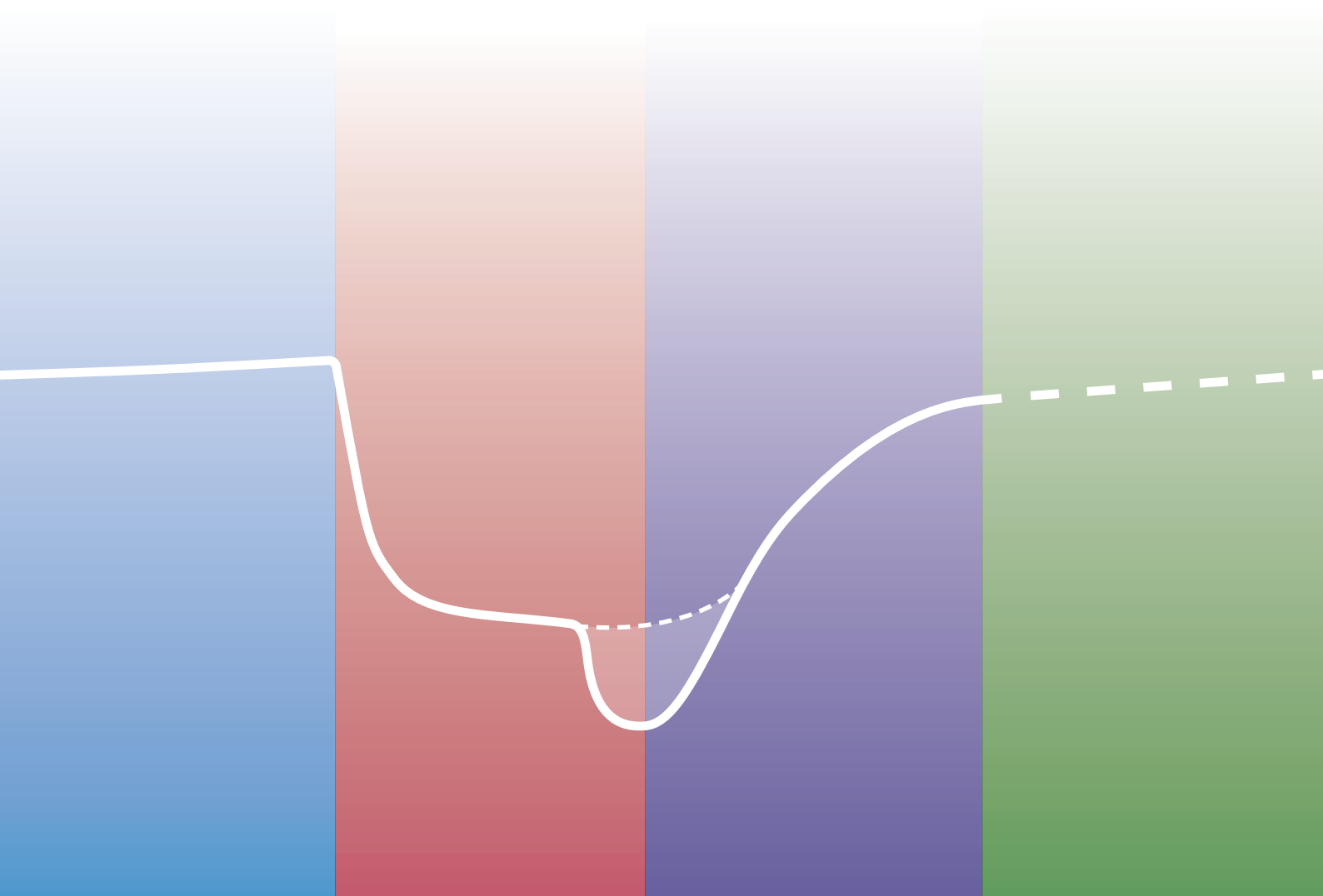
EUROPE

# Resilience quantified

A method for understanding resilience to threats to national security

## Summary

Fook Nederveen, Stijn Hoorens, Erik Frinking and Henri van Soest



For more information on this publication, visit [www.rand.org/t/RRA2357-1](http://www.rand.org/t/RRA2357-1)

#### **About RAND Europe**

RAND Europe is a not-for-profit research organisation that helps improve policy and decision making through research and analysis. To learn more about RAND Europe, visit [www.randeurope.org](http://www.randeurope.org).

#### **Research Integrity**

Our mission to help improve policy and decision making through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behaviour. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit [www.rand.org/about/principles](http://www.rand.org/about/principles).

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

© 2024 RAND Europe. Copyright reserved. No part of this report may be reproduced and/or published by print, photocopy, microfilm, digital processing or otherwise, without the prior written consent of RAND Europe.

RAND® is a registered trademark.

© 2024 RAND Europe. Auteursrechten voorbehouden. Niets uit dit rapport mag worden veeelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm, digitale verwerking of anderszins, zonder voorafgaande schriftelijke toestemming van RAND Europe.

# Summary

---

## Background and objectives

Resilience has become a buzzword in recent years. Especially since the global COVID-19 pandemic, the idea that a resilient society is better able to withstand external threats and recover from them faster or even better has become increasingly popular. The concept of resilience is also a central element in the periodically appearing (national) security strategies of the Netherlands.

The Dutch government is committed to making the country more resilient to a range of threats or risks that potentially endanger national security, from pandemics to catastrophic floods, terrorist attacks or an invasion by a hostile state. These potential threats are identified and mapped out by the National Security Analyst Network (*Analistennetwerk Nationale Veiligheid*) as part of a government-wide risk analysis. Existing risk analyses focus heavily on the potential impact and likelihood of threats occurring, but do not currently include measurements of resilience to these threats. Furthermore, the ambiguity surrounding the concept has resulted in different interpretations of its meaning and its use in different contexts, levels and for different functions.

In the field of national security, resilience has not yet been operationalised in the Dutch policy context. For now, it mainly remains a buzzword. The aim of this research is to change this by developing a method to determine the resilience of Dutch society to the full spectrum of current and future threats and risks in the field of national security. Moreover, this method was to be developed in such a way that it would 1) be flexible and generically deployable to any possible threat (threat-independent), including currently unknown threats; and 2) focus on the resilience of Dutch society as a whole.

## Approach to this research: explore, develop, apply

This research started with an analysis of how the concept of resilience is used and interpreted in policy documentation on the national security of the Netherlands, as well as how the concept is defined and operationalised in Dutch and foreign academic and grey literature. Based on the collected data, we established a working definition of resilience in the context of national security. In addition, we analysed the characteristics, advantages and disadvantages of 15 identified existing approaches to measure resilience on the following criteria:

- **Validity, reliability and robustness:** Does the method or measure provide a reliable and a consistent estimate of resilience to different threats?
- **Replicability:** Is it feasible to run the method periodically and are the results comparable over time?

- **Flexibility and/or generalisability:** Is the method sufficiently future proof to accommodate future developments in threats, interests or capabilities?
- **Cost-effectiveness:** Do the benefits of the method outweigh the required deployment of resources?
- **Information needs:** Is the knowledge available or are the data available to apply the method?
- **Prospects for action:** Does the method provide guidance for taking measures to improve resilience to threats outlined in the Security Strategy for the Kingdom of the Netherlands 2023-2029 (hereinafter 'the Security Strategy')?

We further analysed the methods that met the outlined conditions and scored highest on the criteria we set (validity, reliability and robustness; replicability; flexibility and/or generalisability; cost-effectiveness; information needs; and prospects for action). We then decided to use the resilience matrix as developed by Linkov et al. (2013) and adapt it to better fit the context of Dutch national security. This approach relies on expert judgement. To test its functioning, we applied the method that we developed to three threats scoring high on both likelihood and potential impact in the government-wide risk analysis in 2022. These threats were 1) extreme weather; 2) strategic dependencies; and 3) a disruption in the functioning of the internet. For each threat, we organised a separate virtual testing session with five to seven policy and methodological experts. We then used their feedback to further refine the content and methodology.

## What does resilience mean in the context of national security?

Resilience has only recently gained widespread scholarly attention. Resilience analysis, unlike risk analysis, does not only emphasise the prevention and/or countering of threats, but also the ability of a system to recover from a variety of potential disruptions. Resilience also encompasses a society's ability to absorb, adapt and recover from shocks and disruptions. At the same time, resilience also has a preventive component as it can reduce the impact of threatening actions or act as a deterrent. We define resilience as 'society's ability to be prepared for, resist, absorb and/or achieve a new state of equilibrium after a disruption'. The deployment of policy instruments for national security in the Netherlands is generally divided into different phases that are reflected in this definition: pro-action, prevention, preparation, mitigation (repression) and aftercare. The definition covers the total potential of a country to meet threats and challenges and protect the interests of society. The emphasis lies on Dutch society as a whole rather than individual elements in it, such as citizens or government structures. Another key requirement is a focus on threats that have the potential to disrupt society by harming the six national security interests that the Dutch government distinguishes in its strategies. These security interests are territorial security, physical security, economic security, ecological security, social and political stability and international legal order and stability.

## A method for understanding the resilience of Dutch society against national security threats

### Several ways of measuring resilience already exist

We identified 15 methods of measuring resilience and have classified these into three types: resilience indices (e.g. Resilience Capacity Index by Foster 2012), methods based on *expert judgement* (including the resilience matrix by Linkov et al. 2013) and quantitative approaches (such as the Network Analysis method by Ganin et al. 2016). The assessment of individual methods shows that three methods meet the conditions outlined above. The Resilience Matrix, Network Analysis and a Cost-based approach are all both threat-independent and capable of providing insight into societal resilience.

### Our method is based on the resilience matrix of Linkov et al. (2013)

The resilience matrix of Linkov et al (2013) enables a holistic assessment of a system's resilience at the strategic level by looking at a number of system domains within each phase of the resilience cycle. In the matrix, the phases 'Preparing', 'Absorbing', 'Recovery' and 'Adaptation & Transformation' are presented in the columns, and the domains 'Physical', 'Informational', 'Cognitive' and 'Social' in the rows (see Table S-1). For each cell of the matrix, several capacities were formulated and subsequently scored on a given categorical or ordinal scale through *expert judgement*, for which a group of well-informed experts within the relevant community comes together (virtually). The method does not define specific performance metrics nor specific factors to be maximised. Instead of scoring a set of universally accepted values, the matrix combines key qualitative and quantitative data and insights to arrive at an informed assessment. Additionally, signals about potential vulnerabilities can be picked up along the way. As the matrix is aimed at the strategic level, experts should take (many) different factors into account when determining their scores. The scoring culminates in a populated matrix in which each cell contains an average score which measures the ability of a system to prepare for the manifestation of a threat in that domain, absorb it, recover from it or to adapt and transform the system. Taken together, the completed matrix gives a basic picture of the system's resilience. The scores can be displayed as average values, via colour codes (traffic light), or a combination of the two. An example of the latter variant is shown in the table below.

Table S-1. Example of a completed resilience matrix from Linkov et al. (2013)

		Phases			
		Prepare	Absorb	Recovery	Adaptation & Transformation
Domains	Physical	0.20	0.15	0.25	0.40
	Information	0.32	0.22	0.34	0.12
	Cognitive	0.53	0.05	0.26	0.16
	Social	0.22	0.39	0.20	0.19

Source: Based on Linkov & Trump (2019, 90)

The resilience matrix of Linkov et al. was adapted to the national security context of the Netherlands

We have adapted Linkov et al.'s (2013) matrix to better reflect the specific context of national security in the Netherlands. The domains identified by the authors (physical, information, cognitive and social) in the rows have been replaced by the six national security interests from the Security Strategy. The phases in the columns are unchanged, as they broadly correspond to the phases used in the resilience cycle in Dutch policy documentation. The table below shows what the adapted matrix looks like.

Table S-2. The resilience matrix focused on the national security of the Netherlands

		Stages in the resilience cycle			
		Prepare	Absorb	Recovery	Adaptation & Transformation
National security interests	Territorial security				
	Physical security				
	Economic security				
	Ecological safety				
	Social and political stability				
	International legal order and stability				

Source: Adapted matrix from Linkov et al (2013).

The cells in the matrix are scored by experts

To determine how resilient Dutch society is against a certain threat, the resilience matrix for each phase in the resilience cycle depicts the ability to maintain critical system functions during a crisis. For example, for the 'prepare' phase and the 'territorial security' interest, this means: the ability to prepare for a threat that could disrupt the functioning of the Kingdom of the Netherlands and its EU and NATO allies as independent states in a broad sense, or territorial security in a narrow sense.

Within each phase, we then formulated competences that contribute to maintaining these critical system functions and capabilities that must be preserved during a crisis. For instance, within the 'prepare' phase, we distinguish three competences: understand, prevent and protect (see Table S-3).

**Table S-3. The resilience matrix focused on the national security of the Netherlands**

<b>Prepare</b> Ability to prepare for and prevent disruptions before the threat materialises	<b>Absorb</b> Ability to effectively combat and contain the effects of disruptions	<b>Recovery</b> Ability to restore damage and lost system functions as quickly and efficiently as possible	<b>Adaptation &amp; Transformation</b> Ability to adapt the system and better cope with future threats of a similar nature
<b>Understand</b> Through information gathering and analysis, identify the threat and its possible causes and consequences.	<b>Understand</b> Gathering information to understand the scope of the situation and determine appropriate action.	<b>Reset</b> Restore system functionality by repairing and rebuilding damage, restarting economic activities and disrupted social routines, and supporting the return of the civilian population to a safe location (i.e. return to area of crisis, temporary shelters, hospitals or other infrastructure, as appropriate).	<b>Innovate</b> Generate, analyse and apply lessons identified across stakeholder groups. Incorporate lessons identified in subsequent iterations of the preparedness phase to adapt existing structures, institutions, resources, and so on, and create innovative practices to improve capability to prepare for and respond to future crises.
<b>Prevent</b> Preventing the threat in advance and mitigating the (source of a) potential threat by taking targeted precautions, stimulating awareness of potential risks and threats and forming connections between various stakeholder groups and institutions.	<b>Inform</b> Communicate effectively and efficiently in the event of a crisis to facilitate rapid and appropriate responses from stakeholder groups across society.	<b>Regenerate</b> Return responding personnel and equipment to a response-ready state; including replacing personnel or equipment lost in crisis response and returning society to its pre-crisis state (e.g. basic service delivery, resumption of normal business).	
<b>Protect</b> To best prepare for mitigating the impact of a threat by building, developing and training response capabilities.	<b>Mobilise</b> Ensure that personnel, equipment, capabilities and all necessary resources across society can participate in crisis response as required and with all necessary speed.		

This framework was subsequently used to create a specific set of questions, which experts answered to assess these competences in order to assign a score to each cell in the matrix. The competencies with corresponding question are scored on an ordinal scale from 'Not at all' to 'To a very large extent'. Based on the test results and suggestions from the literature, we recommend using a 6-point scale.

Participants score in several rounds, allowing them to revise their assessments based on each other's knowledge and information

When this method is applied in practice, we suggest that scoring should take place in expert sessions. The government-wide risk analysis (*Rijksbrede Risicoanalyse* - RbRA) underlying the Security Strategy distinguishes between 'threat themes', 'threat categories' and 'scenarios'. Using the resilience matrix, the

degree of resilience can be scored at all levels, but for the sake of feasibility, we suggest doing so at the level of threat categories.

These sessions can be organised around one or more threat categories from the RbRA with experts from all phases of the resilience cycle. Prior to scoring, we recommend sending the experts instructions explaining key concepts and listing the questions. The questions are to be answered in several rounds, with the experts having the opportunity to revise their initial scores based on the discussion of the results. Discussing the group results allows participants to compare them with their own scores. From the resulting explanations and discussions, participants can arrive at new perspectives and insights. As a result, participants make use of each other's knowledge and expertise. If necessary, the final results can be submitted to the participants for their approval.

The resilience matrix can be displayed with average values and/or via colour coding

The steps described above lead to a matrix in which each cell contains a numerical score indicating the capability of a system by competence/phase and national security interest. These numerical scores are calculated as the averages of the individual responses, normalised to a score from 0 to 1. For each cell, the standard deviation is an indicator of the degree of consensus among the participating experts. The completed matrix provides a basic picture of the resilience of the system. This makes it primarily a visual aid. Combined with the minutes of the discussions, the populated matrix can provide points of reference for action and trigger further analysis. This method was applied in three test sessions, each focusing on one threat. The scores from these sessions can be displayed as averages scores, via (traffic light) colour codes, or a combination of the two. The tables below show the first two options for presenting the scores.



Table S-4. Illustration resilience matrix with normalised mean values (dummy scores)

	Prepare			Absorb			Recovery		Adaptation & Transformation
	Understanding (Va)	Occurrence (Vb)	Protect (Vc)	Understanding (Aa)	Inform (Ab)	Mobilise (Ac)	Reset (Ha)	Regeneration (Hb)	Innovate (T)
Territorial security (1)	0.72 (0.22)	0.62 (0.08)	0.48 (0.1)	0.24 (0.14)	0.56 (0.12)	0.4 (0.14)	0.26 (0.2)	0.68 (0.22)	0.52 (0.12)
Physical security (2)	0.46 (0.08)	0.64 (0.16)	0.5 (0.08)	0.42 (0.08)	0.44 (0.2)	0.46 (0.14)	0.3 (0.16)	0.58 (0.24)	0.42 (0.22)
Economic security (3)	0.48 (0.14)	0.44 (0.24)	0.42 (0.18)	0.28 (0.16)	0.52 (0.12)	0.32 (0.24)	0.5 (0.12)	0.64 (0.22)	0.56 (0.28)
Ecological safety (4)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Social and political stability (5)	0.48 (0.1)	0.52 (0.12)	0.44 (0.2)	0.32 (0.18)	0.4 (0.04)	0.36 (0.16)	0.48 (0.1)	0.52 (0.2)	0.42 (0.18)
International legal order and stability (6)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Minutes of discussions at scores:									
1xVa: .....									
2xVa: .....									
Etc.									

Table S-5. Illustration resilience matrix with (traffic light) colour codes

	Prepare	Absorb	Recovery	Adaptation & Transformation
Territorial security	0.6 to 0.8	0.2 to 0.4	0.2 to 0.4	0.6 to 0.8
Physical security	0.6 to 0.8	0.6 to 0.8	0.2 to 0.4	0.6 to 0.8
Economic security	0.6 to 0.8	0.2 to 0.4	0.2 to 0.4	0.6 to 0.8
Ecological safety	-	-	-	-
Social and political stability	0.6 to 0.8	0.2 to 0.4	0.2 to 0.4	0.6 to 0.8
International legal order and stability	-	-	-	-

Minutes of discussions at scores:  
 1xVa: .....  
 2xVa: .....  
 Etc.



## Reflection on the application of the method

The concept of resilience is gaining importance, both in the scientific literature and in domestic and foreign policy arenas around national security. The idea is that increasing societal resilience to threats is as essential as preventing them. The methodology proposed in this report helps to conceptualise and operationalise the concept of resilience. By applying it to different threat categories, it can provide insight into where system functioning may be vulnerable and which competences need to be strengthened to increase resilience as a whole. Using the assessment criteria described above, we reflect on the application of the developed method below.

**Validity, reliability and robustness.** The method is based on a widely accepted theoretical framework for the concept of resilience. In addition, the test sessions provided positive feedback on the operationalisation of the concept of resilience and the thoroughness of the method. Yet, some remarks can be made regarding validity, reliability and robustness. First, the formulation of the specific questions on competences plays an important role. The values in the matrix reflect the interpretation of critical system functions of the analyst(s) involved in applying the method. A second comment relates to the methodological limitations of a method based on expert judgement. The quality of the expert judgements, and thus the validity of the application of the method, depends on the level of knowledge and motivation of the expert panel. The selection and participation of experts is very important. This selection should be representative, ensuring a broad reflection of the policy field. Thirdly, human judgement errors (cognitive biases) play a role in the validity and robustness of the findings, even though we endeavoured to mitigate their impact. Finally, the scale used in the chosen approach affects the validity of the results. We recommend using a 6-point ordinal Likert scale.

**Replicability.** The replicability of the method depends on the continuity of the threat categories in the National Risk Assessment. Both the assessment of impact and likelihood of the different scenarios and the nature of the threats may change in the future. This limits the ability to track developments of resilience in the context of national security over time. There are also drawbacks to using expert judgement to assess the elements in the resilience matrix. Human judgement errors also affect the replicability of the method: repeating the expert session – even with the same experts – may lead to different resilience scores.

**Flexibility and/or generalisability.** The methodology based on the resilience matrix was selected for its flexibility; in principle, it can be applied to all possible threats. In addition, the test sessions showed that the methodology can be easily applied in different situations. Moreover, it is possible to apply the methodology at different strategic or decision-making levels. The method and the different steps remain the same for each different threat. It is possible to use indicators in addition to expert judgement to determine the values in the matrix.

**Cost effectiveness.** The costs and effort for applying the methodology have three main components: preparation materials, selection and invitation of experts, and execution of expert sessions. Especially the selection and recruitment of participants for the expert sessions will require some effort. We recommend making use of existing networks of experts and considering the provision of incentives. We expect the effort required to prepare for the application to be relatively limited. Nevertheless, it is desirable that participants receive clear explanations, instructions and background information prior to the expert sessions.

**Information needs.** The proposed methodology assumes that participating experts bring knowledge and experience about the policy context of the threat category to be assessed. Collectively, participants should have knowledge of key measures and developments of the overall threat domain. In addition, as mentioned above, it is recommended that participants receive background information and instructions in advance.

**Prospects for action.** The values (or traffic light colours) in the resilience matrix that follow from applying the methodology implicitly indicate where the priority should lie for strengthening resilience in the face of the threat in question. Moreover, on top of substantiating their scores, the participating experts already provided their reflection on possible actions and policy instruments during the discussions of the test sessions. These discussions should therefore be documented and reported together with the scores. It is important to note, however, that a low score does not necessarily mean a need for action. It is therefore recommended to give a separate interpretation of the results in the context of the policy instruments available after having applied the method.