



FEBRUARY 2025

NATO and the need to strengthen resilience – the Dutch case

Russia's war against Ukraine has fundamentally changed the security situation in Europe. Western support for Ukraine is framed by Russia as 'we are at war with NATO'. While the tool used by Moscow is to confront the West with a range of hybrid activities of sub-threshold warfare – from suspected sabotage and damaging underwater cables to cyberattacks, disinformation and interference in election campaigns – the Alliance must be prepared for armed conflict with Russia as well. Based on the 'minimum military requirements' Allies are strengthening their contributions to NATO's collective defence. However, in order to operate in a conflict situation, the military will need to be sure of the delivery of fuel, electricity, food and water as well as functioning transport, healthcare and other forms of support.

During the Cold War, NATO labelled this requirement as 'civil preparedness'. Today, the term 'resilience' is used. NATO has a set of 'baseline resilience requirements'. This policy brief analyses NATO's resilience policy, the baseline requirements and what they imply for Allies, with specific attention to the Netherlands.¹ The policy brief ends with specific recommendations for the Dutch perspective and policymaking on resilience in response to the NATO requirements.²

NATO resilience policy and requirements

"We are not at war, but we are certainly not at peace either", said NATO Secretary General Mark Rutte in his first public speech last December.³ The principle of resilience has been a key component of the Alliance since its foundation. It has been enshrined in Article 3 of the founding treaty, which focuses

on NATO's capability to fulfil its core tasks of deterrence and defence, although the term as such was not mentioned in the text.⁴ In the Cold War years NATO used the term 'civil preparedness' or 'civil emergency planning' to underline the need for Allies to ensure that their armed forces in a time of war could continue to operate by receiving all civil support (fuel, medical, transport, etc.) as needed. Following the significantly worsened international security environment over the last decade, the term resilience has gained renewed attention. However, resilience covers a broader range of policies and practices in comparison

1 The scope of this policy brief is limited. The authors do not address the full spectrum of countering hybrid threats, including, for example, responding to disinformation and election interference.

2 The authors would like to thank Bart van der Wal for his support in the research conducted in preparing the policy brief.

3 NATO, "[To Prevent War NATO Must Spend More](#)," Speech by NATO Secretary General Mark Rutte at the Concert Noble, Brussels, 13 December 2024.

4 "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack." See: NATO, "[The North Atlantic Treaty](#)," 4 April 1949.

to 'civil preparedness'. This results from the 'grey zone' conflict – neither peace nor war – that characterises how Russia conducts 'war with NATO': from distorting public opinion through disinformation and interference in election campaigns to suspected sabotage acts, assassination attempts and the damaging or severing of underwater cables in the Baltic Sea. While NATO recognises this broad range of threats, it defines resilience as "the individual and collective capacity to prepare for, resist, respond to and quickly recover from shocks and disruptions, and to ensure the continuity of the Alliance's activities."⁵ This is crucial to withstand major shocks and disruptions including "a natural disaster, failure of critical infrastructure, or a hybrid or armed attack."⁶ Thus, while NATO is using the term resilience, its policy refers to two components: military capacity and civil preparedness.⁷ Throughout the Cold War a great deal of attention was paid to the latter to ensure the continuity of the Alliance's (military) activities, including regular large-scale exercises to practice military mobility.⁸ However, both NATO's organisational capacities in this matter and the attention paid to 'civil emergency planning' on a national level have decreased since then.⁹ Resilience is not solely of importance for preparation in case of an armed attack, but also a crucial component of NATO's credible deterrence.¹⁰ It is described as "the first line of defence" in the NATO 2030 initiative.¹¹ If adversaries are not sufficiently convinced of

NATO's capability to withstand a major shock in the event of a crisis, or even full-scale warfare, they may be willing to test that resilience. To illustrate the enormous relevance of civil preparedness as a crucial component of resilience and an enabler of military capacities: approximately 90% of military transportation utilises civilian assets, and over 70% of satellite communications for military purposes rely on the private sector.¹²

Baseline requirements

Following a renewed focus on defence issues after the Russian annexation of Crimea in 2014, at the Warsaw Summit (2016) Allies agreed on seven baseline requirements to "boost NATO's resilience to the full spectrum of threats".¹³ These baseline requirements are the following:

- 1) an assured continuity of government and critical government services;
- 2) resilient energy supplies;
- 3) the ability to deal effectively with the uncontrolled movement of people;
- 4) resilient food and water resources;
- 5) the ability to deal with mass casualties;
- 6) resilient civil communications systems;
- 7) resilient civil transportation systems.

These seven requirements are a 'translation' of the three core functions of civil preparedness in times of need: continuity of government; essential services for the population; and civil support to the military. Allies "can measure their levels of preparedness" against these seven baseline requirements.¹⁴ The NATO policy underlines that resilience is primarily a national responsibility, but it also states: "To deter, counter or recover from threats or disruptions in the civilian sector, effective action requires clear plans and response measures that are defined ahead of time and exercised regularly."¹⁵ Following the full-scale Russian invasion of Ukraine, a more structured approach to resilience was endorsed by the NATO Summit

5 NATO, "[Resilience, civil preparedness and Article 3](#)", 13 November 2024.

6 Ibid.

7 Euro-Atlantic Resilience Centre, "[NATO's Resilience Concerns](#)", 29 February 2024; NATO, "[Resilience, civil preparedness and Article 3](#)", 13 November 2024.

8 Jonathan Hill, '[NATO – ready for anything?](#)', *NATO Review*, 24 January 2019.

9 Wolf-Diether Roepke & Hasit Thankey, "[Resilience: the first line of defence](#)," *NATO Review*, 27 February 2019.

10 This was declared once again at the 2021 Brussels Summit. See: NATO, "[Strengthened Resilience Commitment](#)", 13 September 2022.

11 The NATO 2030 initiative was launched in 2020 under Secretary General Jens Stoltenberg and outlines various objectives to ensure that the Alliance "remains ready today to face tomorrow's challenges", with a particular focus on cyber space, resilience, and innovation. See: NATO, "[NATO 2030: making a strong Alliance even stronger](#)", no date provided.

12 NATO, "[Resilience, civil preparedness and Article 3](#)", 13 November 2024.

13 Ibid.

14 Ibid.

15 Ibid.

of Madrid in July 2022. It aimed at assessing the national resilience goals and implementation plans of the Allies every four years. The NATO Resilience Committee was established to oversee this process. However, producing these national goals and plans is voluntary.¹⁶ In other words, the resilience assessment is less stringent than the NATO Defence Planning Process (NDPP), by which Allies are held responsible for realising their contribution to the ‘minimum military requirements’.

Impact analysis

The seven baseline criteria form a solid foundation for a NATO-wide strengthening of resilience and, specifically, civil preparedness. The repeated reference to the topic of resilience in recent NATO summits also reflects an increased awareness of the scope of the issue. Nevertheless, scholars point out that the existing seven baseline requirements do not cover all the fields where improvement regarding resilience is necessary. In particular, the vulnerabilities of NATO’s digital infrastructure – the dependence thereon has increased even further since the COVID-19 pandemic – is considered to be a major point of focus for the Alliance, possibly worthy of an individual baseline requirement.¹⁷ Ensuring that in case of an armed conflict payment systems continue to operate should be considered a priority in this regard.¹⁸

Additionally, the degree to which the societies of NATO Allies are psychologically resilient in the case of a major shock, hybrid attacks or armed conflict is debated. This includes the preparedness to fight, and even sustain mass casualties of a similar scale to the ongoing war in Ukraine.¹⁹ Furthermore, the increasing threat

of disinformation – worsened by significant developments in artificial intelligence and a rapidly changing (social) media landscape – will likely continue to affect NATO Allies.²⁰ Similar to the dependence on digital infrastructure and cyber resilience, ensuring that disinformation is dealt with is crucial as it is cross-cutting and vital to the existing baseline requirements.

Ultimately, the challenge of dealing with hybrid threats is continuously evolving, as adversaries will continue to find new ways to test the commitment and resilience of the Allies.²¹ At the Washington Summit in 2024, the need for a “360-degree approach” in national and collective resilience was emphasised.²² In practice, NATO’s role is quickly growing in reaction to the threats posed to underwater cables and other off-shore infrastructure in the Baltic Sea and elsewhere by creating new command elements, by incorporating hybrid threats in exercises and, recently, by sending the Standing NATO Maritime Group 1 to the Baltic Sea. This underlines that the blurred distinction between peace and war is affecting NATO’s approach to resilience. For being prepared for war – and thus to optimise deterrence to prevent armed conflict – improving civil preparedness is a key necessity. Additionally, NATO is already involved in grey-zone conflict which raises the question of potential additional resilience requirements or adapting the existing ones.

Two caveats should be made. First, NATO remains a political-military alliance. NATO’s activities in countering hybrid threats, such as disinformation and election interference, are limited. The same

16 Edward Hunter Christie & Kristine Berzina, [“NATO and Societal Resilience: All Hands on Deck in an Age of War”](#), GMF, 20 July 2022, p. 4.

17 Ibid.; Globsec, [“GLOBSEC’s Public-Private Sector Dialogue #4: Enhancing NATO’s Cyber Resilience”](#), 29 January 2024.

18 Edward Hunter Christie & Kristine Berzina, [“NATO and Societal Resilience: All Hands on Deck in an Age of War”](#), GMF, 20 July 2022, p. 8.

19 Michal Onderco, Wolfgang Wagner & Alexander Sorg, [“Who are willing to fight for their country, and why?”](#), 28 March 2024. Edward Hunter Christie & Kristine

Berzina, [“NATO and Societal Resilience: All Hands on Deck in an Age of War”](#), GMF, 20 July 2022; Dominik Presl, [“Fostering a ‘Will to Fight’ Has to be NATO’s Next Priority”](#), RUSI, 4 April 2024; Ann M. Fitz-Gerald & Halyna Padalko, [“The Need for a Strategic Approach to Disinformation and AI-Driven Threats”](#), RUSI, 25 July 2024; [“NATO, Lawmakers Urge NATO Allies to Reinforce Societal and Democratic Resilience”](#), 16 May 2021.

20 NATO, [“NATO releases revised AI strategy”](#), 10 July 2024; Ann M. Fitz-Gerald & Halyna Padalko, [“The Need for a Strategic Approach to Disinformation and AI-Driven Threats”](#), RUSI, 25 July 2024.

21 Euro-Atlantic Resilience Centre, [“NATO’s Resilience Concerns”](#), 29 February 2024.

22 See: NATO, [“Washington Summit Declaration”](#), 10 July 2024.

applies to cyberattacks on civil infrastructure, to sabotage acts or other ‘hybrid conflict threats’. Secondly, due to its wider set of responsibilities, the European Union also has an important role in strengthening resilience. With its legal and regulatory power, the EU can enhance resilience by lawmaking, for example by building digital resilience and securing supply chains, emphasising the strategic importance of economic stability alongside security goals.²³ Following the ‘Niinistö Report’ the European Council decided in December 2024 “that enhanced and coordinated military and civil preparedness and strategic crisis management are required, in an all-hazards and whole-of-society approach.”²⁴ A Union Preparedness Strategy will be launched for that purpose. The European Council has underscored that “this should be done in synergy with NATO”.²⁵ In this context, the existing EU-NATO Structured Dialogue on Resilience should be further strengthened and both organisations should develop complementary action agendas in order to guide and assist EU member states and NATO Allies in their ‘whole-of-government’ and ‘whole-of-society’ approaches and measures to strengthen their resilience.²⁶

The impact for the Netherlands

In its note to Parliament of December 2024 on resilience the Dutch government states that “a big extra step” is needed to strengthen resilience, also considering the country’s dependency on international cooperation and trade, and its role as a logistical hub for NATO (e.g. the ports of Rotterdam and Vlissingen).²⁷

The whole-of-society approach is underlined, but the note makes clear that setting priorities will be unavoidable considering the magnitude of the task at hand. The first concrete policy options and proposals will be presented by early summer 2025. Implicitly, the Dutch government admits that the country is ill-prepared for countering hybrid threats and strengthening resilience, as the Advisory Council on International Affairs concluded in its report of May 2024: “The Dutch government’s current approach does not adequately match the broad impact of hybrid threats. Despite some good initiatives, such as the Government-wide Response Framework against Hybrid Threats, the government’s response in the face of a threat is often reactive, incident-driven and fragmented.”²⁸

The resilience note to Parliament aims to address this problem and it provides a conceptual breakdown of the ‘resilience task’ into two tracks and six pillars. Track 1 is ‘societal resilience’ with the following pillars: 1. protecting vital and other important processes in society; 2. a ready and resilient society; 3. keeping the Dutch democracy, rule of law and government afloat; 4. a resilient economy. Track 2 is ‘military readiness’ with two pillars: 5. protecting and defending own and allied territory; 6. ensuring civilian support to the armed forces in the performance of their military duties.²⁹ The two main categories – societal resilience and military readiness – provide the impression of adopting the two NATO components of resilience (civil preparedness and military capacity). However, the six pillars do not correspond with NATO’s seven resilience requirements as the Dutch policy is based on the broader approach of resilience, encompassing, for example, the protection of the rule of law and free media, responding to disinformation and acts of sabotage, etc. A closer look at the text of the note to Parliament provides the following result (see chart).

23 As stated in: Mario Draghi, “[The future of European competitiveness](#)”, European Commission, 9 September 2024.

24 European Council, “[European Council meeting \(19 December 2024\) – Conclusions](#)”, para. 17, 19 December 2024.

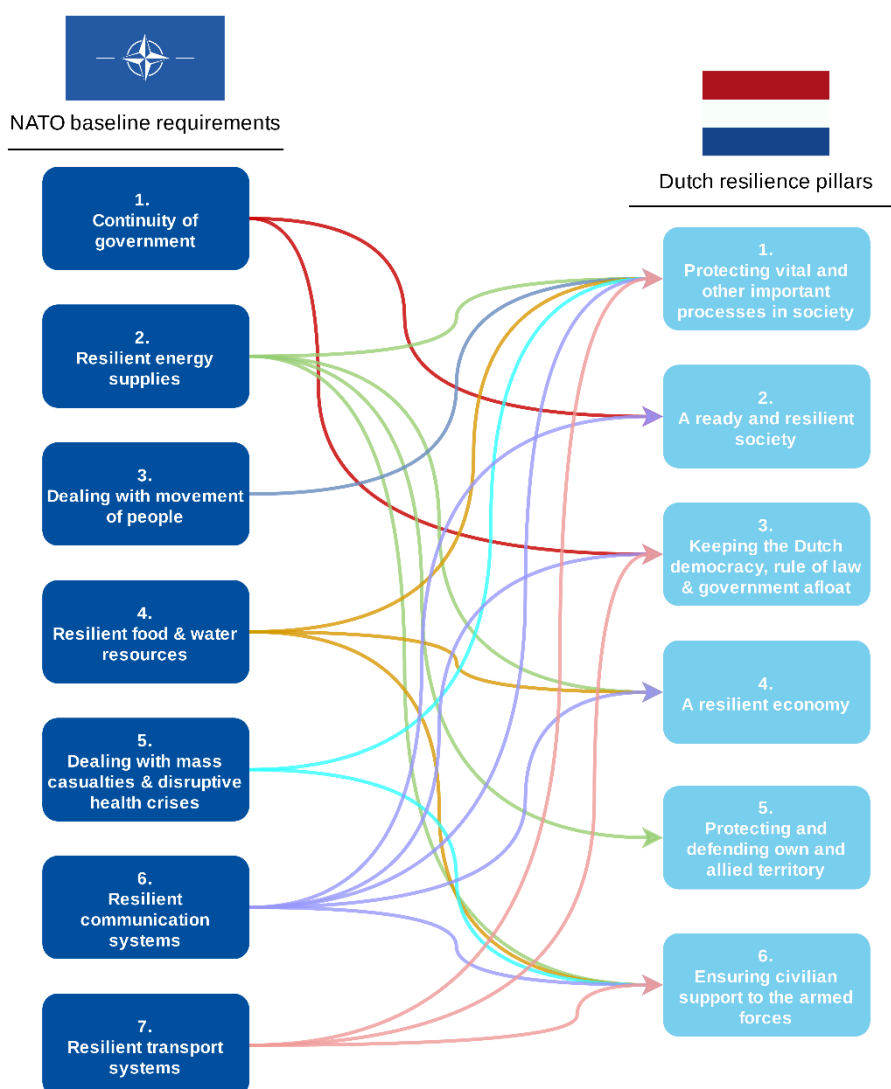
25 Ibid.

26 Mikael Wigell, Harri Mikkola, Tapio Juntunen, “[Best Practices in the whole-of-society approach in countering hybrid threats](#)”, *European Parliament Study - Directorate General for External Policies of the Union*, May 2021.

27 Ministerie van Justitie en Veiligheid, “[Weerbaarheid tegen militaire en hybride dreigingen](#)”, Kamerbrief, 6 December 2024. Translation into English by the authors.

28 Advisory Council on International Affairs, “[Hybrid threats and societal resilience](#)”, Advisory Report 126, 4 June 2024.

29 Ministerie van Justitie en Veiligheid, “[Weerbaarheid tegen militaire en hybride dreigingen](#)”, Kamerbrief, attachment, “[Weerbaarheidsopgave – Versterken van weerbaarheid in het licht van militaire en hybride dreigingen](#)”, 6 December 2024. Translation into English by the authors.



Pillars 1 and 6 dominate in this cross-reference, which comes as no surprise: the NATO resilience objectives are predominantly aimed at ensuring the continuation of the Alliance’s military operations. As the Dutch government has stated that priorities will have to be set, from the NATO perspective the logical priority would be to address the practical implementation of pillars 1 and 6. The strengthening of the resilience of vital infrastructure should be a top priority, as the geographical location of the Netherlands and its importance as a transit country for American reinforcements require both military and civil support. The protection of offshore energy infrastructure (wind farms) and underwater cables in the North Sea also belongs to this priority category. Enhancing cyber security

remains a key element to strengthen the Dutch resilience in a whole-of-society approach. Healthcare is another area of deepening civil-military cooperation to be better prepared for conflict and disaster.

Conclusions and recommendations

NATO’s role, responsibilities and strength – being a political-military organisation with its core task to ensure peace through a credible deterrence and collective defence – complicate the Alliance’s role in enhancing resilience. Nations themselves are primarily responsible for strengthening their resilience, and a large part of their efforts are of a non-military nature, such as safeguarding a functioning government

and the rule of law, countering disinformation and election interference as well as enhancing cyber security, ensuring energy supplies and healthcare. Nevertheless, all these provisions need to be well functioning to support the Allies in delivering their military contributions to NATO uninterrupted and sustained over time.

Article 3 of the NATO Treaty provides the basis for the Alliance's interest in resilience. However, the Alliance's policy with two components (military capacity and civil preparedness), its resilience definition and the seven baseline requirements do not correspond with the wider approach of resilience. Disinformation, election interference and other activities to undermine the cohesion of Western societies are very important challenges of which NATO is aware but not involved in terms of defining baseline requirements. In essence, the way in which NATO has adopted the term resilience is confusing as it deviates from what resilience implies in the true sense.

Nevertheless, the seven baseline requirements are key to optimise the Alliance's deterrence and defence posture. The operations of the NATO forces will depend on civil support. For that purpose, these baseline requirements should be incorporated in national resilience policies, plans and measures. Furthermore, Allies could be held accountable for the implementation of the requirements by NATO, as the current approach of voluntary reporting and reviewing is no longer suitable for the changed security environment. The nature of the threats and the specific contributions of Allies to NATO's deterrence and defence posture should be considered in this process. For example, the Netherlands, with its key role for the reception and transfer of American reinforcements to Europe, should have specific targets concerning civil preparedness to support US forces.

Although more NATO requirements could be considered – such as ensuring stable financial systems – these seem to be more suitable for implementation in the EU context. For that reason, it is essential that the EU-NATO

Structured Dialogue on Resilience and related activities are further strengthened.

The Netherlands recognises the importance of strengthening resilience and implementing NATO's seven baseline requirements. The government has launched a resilience policy with a whole-of-society approach that is wider than the NATO policy and its definition of resilience. The six pillars of national resilience encompass the Alliance's seven baseline requirements, but these pillars contain more elements of resilience measures than those stated in NATO's list. In view of the government's announcement that the first concrete policy steps will be presented by early summer this year, and to provide input to NATO, the following elements could be addressed by the Netherlands:

- **Strengthen the resilience of vital infrastructure**, both physically and digitally. More specifically, public-private arrangements are required to ensure the provision of energy, communication networks, transport (via rail, road, air, sea and waterways), food and water.
- **Intensify civil-military cooperation** for the protection of infrastructure in the Dutch Exclusive Economic Zone (EEZ) of the North Sea. The Dutch Navy plays an important role in protecting offshore infrastructure (wind turbines, cables, etc.), although the use of private actors could be encouraged as this infrastructure is overwhelmingly in private hands.³⁰
- **Enhance cyber security** at all levels of government – national, provincial, local – and of other actors (companies, organisations, universities, etc.) by enhancing public-private cooperation. Furthermore, companies and other actors should be obliged to have a standard clause on cyber security requirements when granted permission by

30 In November 2024 the Dutch Ministry of Defence announced its intention to hire private companies to monitor the Dutch EEZ, at least until the Dutch Navy has more capacity available. See: NOS, "[Defensie wil private bedrijven tijdelijk de Noordzee laten bewaken](#)", 20 November 2024.

public institutions to start or continue their activities.

- **Strengthen the healthcare system** with the aim of increasing the ability to rapidly expand hospitals, and the provision of adequate amounts of medical equipment and medicines. The already existing civil-military cooperation should be expanded. When and where the necessary scope exists, the integration of civil and military hospital branches could be explored.
- **Quickly elaborate the exact needs for civil support to the Dutch Armed Forces**, also for the Host Nation Support which the country must provide as a key transit area for American forces – as announced by the government in the resilience note to Parliament.
- **Exercises should be conducted** as soon as arrangements, government-wide and with private actors, are in place. These exercises should be gradually expanded, involving other actors when new public-private arrangements have been agreed upon. Lessons learned should be used to adapt and improve such arrangements.
- **Rules and regulations slowing down or delaying resilience measures** should be reviewed and amended as required. On the one hand, the Armed Forces and other governmental security actors such as the police could be given more pre-delegated authority to monitor, warn and, if necessary, act to prevent or counter hybrid threats. In this light, adaptation to the current binary legal system which only recognises ‘wartime’ or ‘peacetime’ should be considered. Additionally, private actors could be given a role in supporting counter-hybrid action by assuming an early-warning ‘ears and eyes’ role.

- **Citizen movements within the Netherlands** should be considered in pillar 3, which now seems to be restricted to addressing the issue of refugee flows from abroad. In view of the density of the population (18 million) on Dutch territory, movement control will be of the utmost importance, also in response to natural disasters such as flooding. The planning of reception areas for citizens who must leave their homes is the first step to be taken in this effort.
- In **NATO** the Netherlands could initiate a discussion on the issue of **adapting the NATO resilience definition** to state more explicitly that the seven baseline requirements address the key civil preparedness elements for credible deterrence and collective defence while clarifying that resilience encompasses other key elements that Allies have to address such as countering disinformation.
- In **NATO** the Netherlands could propose to move beyond the current voluntary monitoring and reviewing system of fulfilling the seven baseline requirements by adding resilience to the NATO Defence Planning System (NDPP) or by creating a dedicated NATO Resilience Planning Process (NRPP).
- The Netherlands should promote the strengthening and use of the **EU-NATO Structured Dialogue on Resilience** and propose the elaboration of complementary action agendas.

Together, these recommendations aim at strengthening resilience in the Netherlands in view of the NATO baseline requirements, while at the same time they are meant to contribute to strengthening the Alliance’s credibility and effectiveness as the cornerstone of Europe’s security.

About the Clingendael Institute

Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.

www.clingendael.org
info@clingendael.org
+31 70 324 53 84

 @clingendaelorg
 The Clingendael Institute
 The Clingendael Institute
 clingendael_institute
 Clingendael Institute
 Newsletter

About the authors

Dick Zandee is leading the Security and Defence programme of the Security Unit at the Clingendael Institute. His research focuses on European security and defence issues, EU-NATO, military forces and capability development, defence industry and other security topics.

Karen van Loon is a Research Fellow in the Security and Defence programme within the Security Unit at the Clingendael Institute. Her research encompasses Arctic security as well as European security and defence matters.

Roman de Baedts is a Researcher at the Clingendael Security Unit, working on the Security & Defence programme. His research focuses on security and defence issues, including national and international defence policy, military strategy, and the war in Ukraine.

Disclaimer: The research for and production of this policy brief have been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defense.