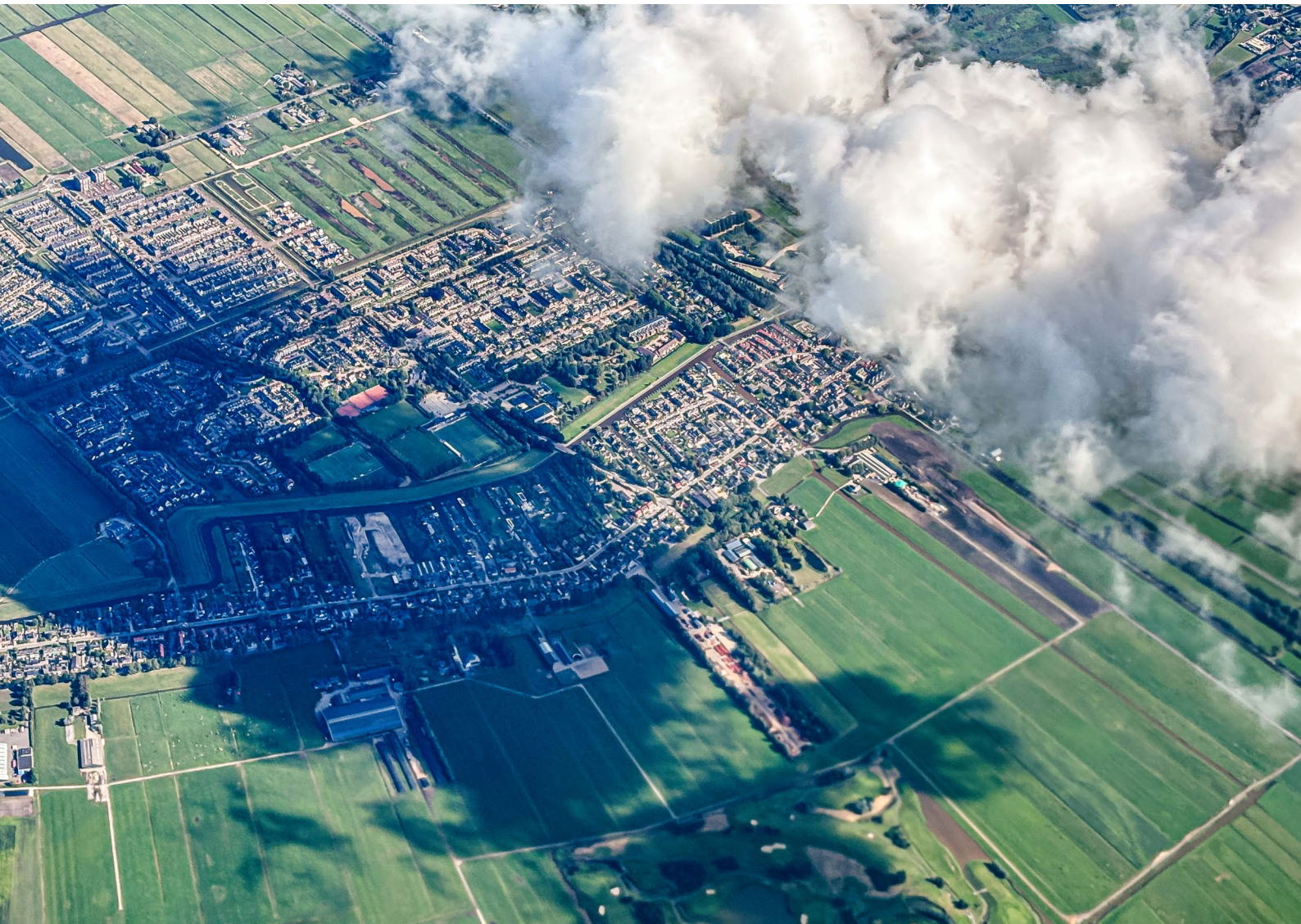
Government of the Netherlands

The resilience task

Boosting resilience in the light of military and hybrid threats



Introduction and context

The international security situation has deteriorated dramatically in recent years, and this is affecting the Netherlands. We are the target of hybrid attacks, such as cyber operations, espionage and sabotage. As a result of Russia's war in Ukraine, for the first time in many years there is a real possibility that the Netherlands could become directly involved in a large-scale armed conflict under the collective defence clause in the NATO Treaty (Article 5).

Although there is already a solid foundation for boosting resilience, it is not enough. In the current climate, amid a worsening security situation, we have no choice but to take further steps. We must, therefore, step up our resilience. With a resilient society, we can protect our security, freedom, prosperity and values. Resilience helps us to prevent conflict and be better prepared if things do go wrong so that we can offer resistance and absorb shocks. Increased resilience also improves our ability to cope with other crises, such as large-scale flooding, a pandemic or the prolonged breakdown of critical processes.

This publication sets out what the government sees as the task of making society resilient in the face of hybrid and military threats. A well prepared society that can absorb shocks and show resilience if the threat becomes a reality. This is not a blueprint, but rather a springboard for a dialogue with society as a whole. Together with members of the public, municipalities, safety regions, civil society organisations, businesses, knowledge institutions and interest groups, we want to explore and develop what we have termed 'the resilience task', and to focus together on what is required and how each of us can help to create a resilient Netherlands.

The resilience task in a nutshell

The resilience task consists of two tracks: societal resilience and military preparedness. Both tracks consist of pillars that are explained in more detail below, namely:

Track 1

Societal resilience

Pillar 1

The protection of critical and other important processes in society

Pillar 2

A prepared and resilient society

Pillar 3

The preservation of our democracy, the rule of law and government

Pillar 4

A resilient economy

Track 2

Military preparedness

Pillar 5

Protecting and defending Dutch territory and that of our allies

Pillar 6

Safeguarding civil support to the armed forces in carrying out their military duties

Track 1 | Pillar 1 | Pillar 2 | Pillar 3 | Pillar 4

Pillar 1 The protection of critical and other important processes in society

The breakdown of important processes can quickly lead to major economic damage or even societal disruption. This is especially true of processes on which many other processes rely, such as the energy supply, mobile communication networks, the internet, positioning, navigation and timing (PNT) by satellite, transport and processes affecting basic human needs, such as emergency care or food and drinking water. We are particularly vulnerable because the armed forces, emergency services and crisis organisations in some cases rely heavily on these vital processes too. In extreme cases, the failure or disruption of such processes may last a long time.

Possible causes could be physical attacks or cyberattacks, or a shortage or the unavailability of certain goods, resources or capacity. As a hub and a gateway to Europe, the Netherlands is a potential target for actors looking to disrupt logistical support to Ukraine or the supply of troops to Eastern Europe, for example.

A conflict also puts pressure on other key processes, e.g. providing shelter to large groups of people or the intake of large numbers of casualties in hospitals. In the meantime, the functioning of the labour market, the independence of the media and the continuation of education must be protected as much as possible. The COVID-19 crisis showed us just how crucial that is.

To protect critical and other important processes in society, we will have to work on:

Boosting the physical and cyber resilience of our critical infrastructure further, specifically in the face of a hybrid threat or military conflict, thus ensuring multiple redundancy. This applies especially to processes on which many other processes depend, such as energy supplies, mobile communication networks, internet, PNT (e.g. GPS and the Galileo navigation system) and transport (via rail, air, road, ports, the North Sea and rivers), and processes affecting basic human needs, such as emergency care, food and drinking water. As also required by NATO, these processes need to be sufficiently robust, redundant and diversified to minimise societal disruption and to support Dutch and allied military operations. Work will also be needed on testing and increasing the recovery capability of critical processes. New solutions to boost resilience should be sought not only nationally, but also in a European and international context, certainly where cross-border markets or production chains are concerned.

Mitigating the risk of dependencies between critical processes and within their supply chains. For instance, the digitalisation of society means that our heavy reliance on energy supplies, PNT and communication networks and the internet could very quickly have extensive disruptive secondary effects. The providers of those critical processes consequently have a task to do in this area. At the same time, users and consumers of these processes have a responsibility to be mindful of potential disruptions or shortages. It is also necessary to reduce the risks created by dependencies in the supply chains of critical providers so as to ensure that they will continue to operate in a threat or conflict scenario in which the regular economy is disrupted.

Track 1

Pillar 1 Pillar 2 Pillar 3 Pillar 4

Committing to boosting the Netherlands' cyber resilience by intensifying public-private cooperation through faster sharing of cyber threats and incidents and joint analysis of the information. Under Programme Cyclotron efforts are being made to establish such a public-private partnership, which includes participation of the intelligence and security services. Furthermore, the Cyber Resilience Network is making a valuable contribution to the effort to boost cyber resilience by intensifying collaboration with public and private partners. As well as accelerating information sharing and joint analysis, the Netherlands needs to be able to mount an active cyber defence. It is vital to enlist joint and public-private efforts to successfully prevent, detect, address and stop attacks on network and information systems in such a scenario. This calls for active cyber protection with the aim of having a better grip on cyber threats.

Providing good access to sufficient, safe and healthy food in all circumstances, including military operations. This is not merely a matter of availability, but also of affordability and in some cases even the allocation and/or distribution of food. Lastly, we should be mindful that the Netherlands is a key transit country for food transport, particularly for the European single market. The Netherlands must be able to continue to play this vital role in the face of a threat or conflict scenario.

Providing effective, versatile and scalable healthcare that is geared to crises or conflicts of any duration, can handle large numbers of casualties and can provide support to Dutch and allied troops. Good, accessible care is a vital foundation of a vibrant and stable society that can continue to function even in the event of a calamity or conflict. Indeed, continuity of care is an important condition for ensuring the continuity of society. The aim is to keep high-quality, public, curative and long-term healthcare in the Netherlands accessible for as many people as possible for as long as possible in times of crisis, disruption and conflict. Not only does regular care need to be maintained; it also needs to be adapted to provide care for migrants and to cope with large numbers of military and civilian casualties. This calls for greater civil-military cooperation in relation to the distribution of patients and the provision of care. This in turn relies on an adequate supply of medicine, the broad deployment of health-care workers and a robust information system. The Dutch Safety Board (OVV) conducted an extensive study of the handling of the COVID-19 crisis, the lessons from which are proving extremely valuable for improving the way in which the government aims to deal with future, long-term crises with national impact. Those lessons will of course be incorporated into the approach.[1]

[1] Parliamentary Paper 25 295 no. 2173, Aanpak Coronacrisis (Approach to the COVID-19 Crisis) – Part 3: January 2020–September 2022, Dutch Safety Board.

Track 1

Pillar 1 | Pillar 2 | Pillar 3 | Pillar 4

Developing the right tools to enable labour market mobilityin the run-up to and during a conflict, also taking account of the current squeeze on the labour market in the technology and IT sectors, for example. In addition, we should explore the possibility of enabling government intervention in the labour market whenever disruption to certain sectors causes job losses or indeed creates a need for more workers. Account should be taken of the implications for labour law and social security, for example with regard to existing labour relations, pay and benefits, and working conditions. Measures taken in this area, for example in the form of government intervention, require close cooperation and agreement with employer and employee representatives as well as with implementing organisations and other authorities. The government is looking at the extent to which measures are necessary and possible in the run-up to and the aftermath of a conflict.

Preparing for the influx and reception of large groups of people as a result of a threat or conflict. Migration flows put pressure on critical infrastructure and services such as healthcare, housing and education. To minimise disruptions to daily life, the influx and reception of large groups of people from EU and NATO countries who are granted temporary protection need to be separated from the regular asylum process. This increases the resilience of the migration system and ensures a more efficient division of responsibilities. A crucial factor for maintaining flexibility is logistical support, such as registration. The Netherlands has previously demonstrated its commitment to accepting refugees, but a prolonged influx of people can adversely affect public support. The government should therefore commit to a robust, flexible migration system, appropriate policies and arrangements regarding influx, return or reception, and free up sufficient financial resources to reduce the burden on services.

Implementing generic measures to improve our ability to cope with a scenario of scarcity, taking into account the need for the continued functioning of society and military operations. Such a scenario could take the shape of a shortage of products (e.g. medicines and water), raw materials, personnel or capacity (e.g. transport capacity or mobile networks). This will require the development of expertise and tools to manage any necessary allocation of scarce resources.

Ensuring the continuity and protection of education and research, the media, cultural institutions and activities and the protection of cultural heritage, so that normal daily life can carry on as far as possible in the event of a threat and in times of conflict.

Track 1 | Pillar 1 | Pillar 2 | Pillar 3 | Pillar 4

Pillar 2 **A prepared and resilient society**

Disruptive hybrid attacks or military conflicts have a huge impact on our daily lives, even if the conflict in question is not taking place in the Netherlands itself. Negative effects could include prolonged power outages, a lack of drinking water or food, or even the destruction of our infrastructure. This will affect our freedom and throw our lives into disarray.

Obviously, a situation like this will cause anxiety and a need for assistance and, in some cases, even lead to social unrest. At the same time, we should be aware that national and local government will not always be able to provide the support and care we would normally expect, certainly in the first few days. Everyone will need to pull together to keep society running, with due consideration for individual ability and societal diversity.

The government needs to have confidence that society will be able to manage without it, temporarily and/or in part. Society must therefore invest more heavily in self-reliance, so that everyone is better prepared for such circumstances because individuals and companies are better able to absorb the first shock or because there are enough networks that can organise mutual support.

If society is to be prepared and adaptable, greater engagement is needed in the necessary preparations for crisis and conflict. This way, we all know what is expected of us in case things should unexpectedly go wrong. It takes all of us together to make a robust Netherlands.

For a prepared and resilient society, we need to work on the following:

Clear and intensified government communication about the threat so that society knows what the preparations are for. This could be theme-based, in the form of, for example, public information about how to recognise disinformation or about possible courses of action to help people cope with such eventualities as prolonged power outages, food and other shortages or damage.[2]

Effective communication and alert systems to warn citizens in the event of danger. For this, the communication and information systems need to be redundant. That is why we are looking at what a hybrid and conflict scenario means in terms of alerting citizens via NL-Alert and whether other options are necessary. To allow for careful decision-making on the future of the Warning and Alert System (WAS), the current method of maintaining the WAS will be temporarily continued for two years from 1 January 2026.

Updating advice on what to do in respect of shelter and evacuation. Here, we consider the current threat context and the specific requirements arising from hybrid threat and conflict scenarios, using as a starting point the 1990 decision to end the government's incentives policy on public shelters.

2 More information can be found in the section 'Communication about the threat and possible courses of action' in the letter to parliament on resilience to military and hybrid threats.

Track 1 | Pillar 1 | Pillar 2 | Pillar 3 | Pillar 4

A national platform or network for public resilience to connect traditional emergency workers, volunteer and other organisations and companies to prepare for major disruptions, system failures, and disaster and crisis scenarios, including a conflict. Here, we will activate society by, for example, linking partners and initiatives, including citizen initiatives, providing access to knowledge and identifying barriers and areas for development. This should be done in conjunction with, for instance, the safety regions, local and regional authorities, implementing organisations, other civil society and crisis partners, businesses and knowledge institutions.

Developing citizen aid further, with due regard for the specific requirements associated with hybrid threat and conflict scenarios. This calls for enhanced cooperation with civil society organisations and alignment with existing initiatives, local and otherwise. These civil society organisations are indispensable in mobilising volunteers and providing emergency aid and are thus vital for our self-reliance. The government can only encourage this and will make every effort to enhance cooperation.

Whole-of-society drills, training and education in relation to a conflict, for instance in the event of prolonged power outages or failures of mobile networks or the internet. This requires the deployment of not only the various layers of both national and international government within existing crisis management structures, but also of the public, companies (critical infrastructure) and civil society organisations. At the request of the House of Representatives, the government will also look into expanding and developing the Leadership in National Security training course.[3]

Increasing youth participation for a resilient society, and learning from existing initiatives and evidence-based youth participation programmes, such as the community service scheme (Maatschappelijke Diensttijd, MDT).

Strengthening the capacity of the mission network to provide consular assistance and support to Dutch nationals in crisis situations abroad, partly through national and international cooperation in crisis management. Central to this is the responsibility of Dutch nationals themselves, and in this context the official travel advisory and the information service (NetherlandsWorldwide) are important communication channels for Dutch nationals about local risks. It should not be assumed that the government will organised a consular evacuation in the event of a serious crisis. Indeed, such a step will only be taken as a last resort in a life-or-death situation if there are no remaining independent or commercial options and if the evacuation is feasible and safe.

3 The undertaking given by the Minister of Justice and Security to explore the expansion of the National Security Course (Leergang Nationale Veiligheid) in the letter to parliament on resilience to military and hybrid threats. Commitment expressed in the National Security, Fire Service and Crisis Management Committee debate on 4 June 2024.

Track 1 | Pillar 1 | Pillar 2 | Pillar 3 | Pillar 4

Pillar 3 The preservation of our democracy, the rule of law and government

Malicious actors have a vested interest in disrupting our democracy, the rule of law and government, thus threatening our democratic legal order. As part of a hybrid conflict, state actors may deploy various tactics, such as sabotage, espionage, disinformation and interference to influence the Dutch population. The Netherlands is already a target of hybrid attacks such as espionage, the hacking of sensitive information or personal data, and cyberattacks designed to take out network and information systems.

It is important, therefore, to recognise the hybrid threat, do our utmost to prevent hybrid warfare, and mount a robust response if an attack does occur. We will move closer to these aims in 2025 with the further development of our approach to state threats. On the one hand, this approach functions as a deterrent, and on the other, it makes clear that subversion of the Netherlands does not pay. International cooperation is vital in this respect.

Attempts to disrupt our democracy, the rule of law and government increase the risk of extremism, radicalisation and polarisation, at the very time when trust in the government is required and the government needs to stand firm. Public administration must continue to function, and fundamental rights must be safeguarded wherever possible.

In the interest of protecting our democracy and the rule of law, work is needed on a proactive approach, which includes the following dimensions:

A strong response capability on the part of the Netherlands to hybrid warfare, including the further development of the government-wide response framework. This instrument enables the government to respond robustly – by various means – to a malicious state actor with the aim of, on the one hand, deterring the actor and causing them to cease their activities and, on the other, mitigating the aggressor's actions or denying them the opportunity to continue them. This involves a wide range of diplomatic and technical measures.

A stronger capacity for geopolitical action by way of international cooperation, both bilateral and in an EU, NATO and UN context. The mission network helps to enhance the quality of our intelligence, both by facilitating the exchange of knowledge and by identifying and interpreting potential threats. In addition, the Netherlands is committed to preventing and managing conflict through diplomatic efforts, including vis-à-vis the aggressor, in order to continue to identify opportunities for bilateral and multilateral cooperation based on shared interests.

Track 1 | Pillar 1 | Pillar 2 | Pillar 3 | Pillar 4

A proactive effort to counter hybrid threats such as sabotage and espionage, including cyber espionage. The same effort must be made in the realm of knowledge security and the cyber domain by improving our comprehensive understanding of the potential or actual hybrid threat, preventing and mitigating vulnerabilities such as potential espionage, sabotage, state interference or influence (covert or otherwise), and increasing the government's ability to 'push back' or 'strike back' in response to hybrid conflict. On the one hand, this approach functions a deterrent and, on the other, it makes clear that subversion of the Netherlands does not pay. This will be put into practice in 2025 with the development of the approach to state threats. We also need to work to strengthen our capacity for geopolitical action by stepping up international cooperation, both bilaterally and within the EU, NATO and the UN.

Reliable intelligence and threat visibility are crucial to enable a proactive effort to counter hybrid threats such as sabotage and cyber and other espionage. This allows the intelligence and security services to identify these types of possibly unprecedented threats to national security and the democratic legal order at an early stage and to prevent or disrupt them as necessary, in anticipation of potential scarcity and crowding-out effects and taking into account the possibility that efforts by the General Intelligence and Security Service (AIVD) or the Netherlands Defence Intelligence and Security Service (MIVD) will need to be rapidly stepped up. Here, firstly, respect for the rule of law in relation to the services' exercise of their powers must remain assured even in exceptional circumstances. Secondly, the services must have the capability to identify threats, unprecedented and otherwise, to national security and the democratic legal order at an early stage and to prevent or disrupt them as necessary.

That means that the AIVD and MIVD, mindful of the legal constraints on their work, must be in a position to step up their efforts in the face of threats to one or more national security interests. This could be necessary even in the run-up to or in the preliminary stages of a conflict. Consideration is being given to how existing legal parameters relating to tasks and powers can be applied to allow these efforts to be intensified responsibly.[4] As well as providing insight into the threat through intelligence investigations, the intelligence and security services also help to boost the resilience of the government, critical sectors, knowledge institutions and parts of the business community. In this vein, efforts are being made to raise awareness of the dangers of espionage, including cyber espionage, sabotage and knowledge theft and to advise on appropriate security measures. For the latter, the AIVD draws up threat assessments and security recommendations.

A proactive response to overt and covert influencing activities. An important part of countering hybrid threats is responding to undesirable – in some cases covert – forms of foreign influencing that undermine democracy and the rule of law. These involve, for example, activities designed to influence public opinion, such as the dissemination of disinformation by state actors[5], as well as overt and covert activities that undermine the integrity of our political and administrative system. We must ensure a government, political system and public debate that are resilient and beyond reproach. Trust in the government requires independent journalistic oversight. In the drive for public resilience, therefore, we acknowledge the importance of the continuity of independent journalism.

4 Undertaking by the Minister of Justice and Security to use the forthcoming letter to parliament – on boosting resilience to military threats – to explore the powers required to make the Netherlands more resilient in a pre-conflict phase. This undertaking was given in the debate of 30 May 2024 about the resilience of Dutch society to subversive activities from abroad..

5 As announced in the progress report on the government-wide strategy for effectively tackling disinformation, the Ministry of the Interior and Kingdom Relations will be conducting a broad exploratory study of vulnerabilities in the open public debate, including the way in which disinformation could influence the Netherlands'' democracy and the rule of law across the board.

Track 1 | Pillar 1 | Pillar 2 | Pillar 3 | Pillar 4

To ensure that the government can function in the run-up to and during a conflict, it is vital that public administration – at both national and local level – can continue to operate and that fundamental rights be safeguarded wherever possible. Work will therefore focus on the following:

Securing and shock-proofing government processes and operational management. To preserve the continuity of government so that democratic control remains possible, public administration can continue and access to an independent judiciary and fundamental rights is optimised, efforts are needed to make government processes and operational management shock-proof. Essential processes and systems, such as general databases, government real estate policy and government communications, both internal and external must therefore be robust, with built-in redundancy.

Preserving democracy, the rule of law and an independent judiciary. Creating a framework together with the judiciary for processing cases in the run-up to and during a potential conflict, as the judiciary may have to make choices and prioritise cases if the need arises.

Continuing our financial benefit and taxation system and the availability of our own financial resources, access to the debt market, protection of government services – such as social security – from digital disruption, and protection of businesses and workers who are unable to do their jobs as usual due to circumstances.

Carrying out a comprehensive review of the necessary redundancy with regard to information and communication systems, including further development of the emergency communication service, so that if all regular communication should unexpectedly fail, the government and other key partners can continue to communicate with each other for the purpose of official crisis decision-making.

Dealing with scarcity: the government must be able to prioritise services and personnel in the event of scarcity or if tasks and powers shift to a subnational level. The government will identify what is required to guarantee a basic operating level for the government and how this can be prioritised. The most essential government processes must continue to function.

A stronger crisis management structure and enhanced decision-making with good links to local, sectoral, national, European, international and military crisis management structures: closer cross-border cooperation, including the possibility of sharing classified and unclassified information, is also needed.[6] Planning and exercises should specifically address conflict. Work is therefore being done to develop various crisis plans.[7] Continuity of crisis coordination and decision-making and the involvement of implementing and civil society organisations should be assured in the event of a conflict. Lessons learned from the Dutch Safety Board's investigation into the handling of the COVID-19 crisis are factored in here.[8]

6 Parliamentary Paper 29 517 no. 251, Ontwikkelingen in het Stelsel van Crisisbeheersing (Developments in the Crisis Management System).
7 Parliamentary Paper 36 410-X no. 45, motion submitted by MPs Sylvio Erkens and Laurens Dassen.
8 Parliamentary Paper 25 295 no. 2173, Aanpak Coronacrisis (Approach to the COVID-19 Crisis) – Part 3: January 2020–September 2022, Dutch Safety Board.

Track 1 | Pillar 1 | Pillar 2 | Pillar 3 | Pillar 4

Exploring the possibilities for structural civil-military crisis coordination, decision-making and leadership: in the event of a military threat, both the Defence organisation and civil society will need to make use of the same limited capabilities, space, products and services. It will also be necessary to harmonise or coordinate certain military operations – such as large-scale troop movements – with civil authorities to allow military operations to proceed smoothly and to mitigate any potential impact on Dutch society. Decisions in the civil domain thus affect actions by the armed forces and, conversely, decisions made in relation to military actions affect the public. This requires deconfliction, prioritisation and intensive cooperation.

An appropriate legal framework, including an assessment framework and public information about it, including in the run-up to a conflict. Consideration is being given to whether there are any gaps that need to be filled in regular and emergency law. Amendments could include possible additional powers or deployment options, in specific threat and conflict scenarios. Further consideration will also be given to whether current emergency law is sufficiently applicable in our digitalised society.

Track 1 | Pillar 1 | Pillar 2 | Pillar 3 | Pillar 4

Pillar 4 A resilient economy

A military conflict or hybrid attack could seriously disrupt the Dutch economy and foreign trade. It is crucial that the economy continue to operate as normally as possible in a situation like this, thus ensuring that we can continue to meet our basic needs, such as food security, energy and healthcare. Moreover, a functioning economy serves to support the deployment of the armed forces. Certain sectors or companies may need to modify their production processes and resources to support strategic goals. For example, companies may be asked to prioritise the production of goods and services that are essential for defence, such as food, medical supplies, means of transport and military equipment.

Survival in an increasingly harsh, turbulent and fragmented world requires costly efforts and tough choices.[9] If the supply of critical products and services cannot be guaranteed, government intervention will be needed in many cases. Any necessary measures must be both effective and proportionate. Early government action is advisable, with minimal market disruption.

The government is therefore working to boost the Dutch economy's resilience to shocks. The business community has a key role to play here, as companies are responsible for setting up their own value chains.

The Netherlands has an open economy in which the distribution of scarcity is largely left to the market. This open, competitive and innovative economy is responsible for our high standard of living and enables public services, such as high-quality education, accessible healthcare and a robust defence organisation. At the same time, this openness means dependence on other countries. That poses a threat if a product, service or technology is crucial for safeguarding public interests and there is a high risk of supply being interrupted. If companies fail to manage these risks properly in their supply chains, the government may decide to intervene. If that is the case, efficiency and proportionality are key.

In the context of building a resilient economy, efforts will focus on the following:

Resilience of government and businesses. The government is committed to closer cooperation with the business community in a united effort to boost economic resilience. In times of scarcity, disruption or damage, it is crucial that our earning capacity be maintained and the continuity of vital economic processes assured. The state financial system must also be sufficiently robust that government revenue and expenditure are not compromised. The role that businesses could play in a military conflict will also be explored, as will the way in which the business community could help to ensure economic continuity in times of crisis. The introduction of the defence and security-related industry resilience bill is a significant step in this process.[10]

9 The Netherlands Scientific Council for Government Policy (WRR) report no. 109, The Netherlands in a Fragmenting World Order, 2024.
10 Parliamentary Paper 31 125, no. 132. This allows the Ministers of Defence and Economic Affairs to direct the strategic stocks and supply chains of a limited number of companies. It will also enable them to direct a limited number of companies in terms of: 1. developing new technology or production methods, 2. engaging specific suppliers, knowledge institutions or other parties, 3. making business resources available, 4. maintaining production methods or facilities, 5. providing services for maintaining and modernising outdated systems and 6. prioritising Ministry of Defence orders. Once it comes into force, the act will provide a legal basis for guaranteeing the supply of defence materiel.

Track 1 | Pillar 1 | Pillar 2 | Pillar 3 | Pillar 4

Boosting production capacity in the Netherlands to guarantee production in a conflict. To guarantee the supply of vital military goods, attention will focus on maintaining stocks of critical raw materials and on increasing strategic production capacity, particularly in sectors of key importance to national security and economic continuity. Companies that fall within the scope of the bill could, in the event of a military threat, be asked to modify their production processes in order to prioritise the production of vital goods and services, such as food, medical devices, means of transport and military equipment.

Continued commitment to our economic security. The government will continue its work to safeguard the Netherlands' economic security by identifying and mitigating risks to national security. This involves issues such as preventing undesirable foreign investment and takeovers of companies that are active in critical sectors or involved with sensitive technologies. Efforts are also being made to stop the loss of sensitive knowledge at both national and EU level. In addition, work is being done to promote the position of strategic sectors and technologies.

Ensuring the robustness of payment and securities systems. To guarantee the continuity of financial services, work is under way to ensure the robustness of payment and securities systems so that funding remains available to both capital markets and the public.

Identifying the risks of strategic dependencies in production chains, and mitigating those risks wherever necessary, for instance by encouraging diversification and circularity, strengthening the Netherlands' industry or examining the possibility of stockpiling. The interministerial Strategic Dependencies Task Force plays a supporting and encouraging role in this respect. Market players themselves bear the main responsibility for mitigating high-risk strategic dependencies, with support from the government. A thorough assessment of the need for and degree of government intervention is always required. If more far-reaching government intervention is deemed necessary, effectiveness and proportionality are key. Early intervention with minimum market disruption is advisable in such cases.

Strengthening small and medium-sized enterprises (SMEs) in critical sectors. In times of crisis, SMEs play a crucial role due to their flexibility and ability to adapt swiftly. They can modify their production processes to support strategic sectors, and help to maintain essential goods and services, such as food, healthcare and transport. At the same time, SMEs are more vulnerable to crises and disruptions, which means that they need to be well prepared. In order to further boost the resilience of SMEs, it is vital to increase their level of risk awareness and to ensure close cooperation between SMEs, larger companies and the government.

Track 2

Pillar 5

Pillar 6

Pillar 5 Protecting and defending Dutch territory and that of our allies

Given the deteriorating security situation, investment in the armed forces remains vital. To be prepared for a conflict, military preparedness needs to be enhanced. This helps in the pursuit of the Defence organisation's three strategic objectives: deterrence of and preparedness for a large-scale conflict, being ready for future warfare and adapting to changing threats, and standing ready to carry out national tasks.[11] In addition, the societal resilience tasks described above are highly significant for the Defence organisation. A lack of societal resilience can put pressure on its capacity, or at worst undermine the work of the military. For example, if citizens are unable to look after themselves for the first 72 hours of an emergency, the Defence organisation may have to provide support, regardless of any military priorities they might have. Various initiatives have already been developed, such as the National Crisis Management Agenda and the National Crisis Management Plan for Military Threats, which contribute to both military preparedness and societal resilience.

After decades of spending cuts, investment in defence has increased sharply in recent years, particularly since Russia's invasion of Ukraine. The present government is raising defence spending to a fixed level of at least 2% of GDP. At the same time, it is clear that 2% will not be sufficient to meet all of NATO's capability requirements, which are necessary to reduce the high risks associated with the implementation of the alliance's new military plans.

While these investments represent a step in the right direction, we still have a long way to go. For the Defence organisation, it is crucial that agreements be reached and preparations made now in order to avoid creating obstacles in an actual conflict.

The government is therefore working towards the following:

Continuation of the growth line, partly by enshrining a structural minimum of 2% of GDP for defence spending in law, in line with the NATO norm. The stipulation of a minimum percentage in legislation gives the Defence organisation the necessary security to make long-term commitments. This contributes directly to a military force capable of operating in current and future security situations. The process of enshrining this in law has now begun.

Legislation that enables the Defence organisation to prepare for a military conflict and which contributes to deterrence. Current legislation is geared towards peacetime, while the Netherlands unfortunately finds itself in a grey zone between peace and war. The Ministry of Defence is working with partners on suitable legislation so that the Defence organisation can perform its tasks effectively and keep the Netherlands safe.

Determining which national tasks the Defence organisation could or should perform in the run-up to and during a conflict and exploring how identified shortcomings can be addressed. Administrative and political agreements should be made for this on the basis of operational capabilities.

11 Parliamentary Paper 36 592 no. 1, Defence White Paper 2024.

Track 2

Pillar 5

Pillar 6

Where necessary, clarifying and expanding political, administrative and operational responsibilities and powers to be applied in a conflict situation. The Ministry of Defence is currently developing a National Crisis Management Plan for Military Threats, which will provide insight into this issue.

Greater engagement of society with the armed forces through the introduction of a service model which enables the Defence organisation to scale up or down according to the threat and the expansion of the pool of reservists and the number of service-year recruits in order to mitigate the substantial personnel shortage.[12] For this purpose, the Defence organisation is working on the development of a voluntary survey of young people in order to increase engagement and intake. Work is also being done to expand the Defensity College programme.

The ability to provide information to the public at all times. The Ministry of Defence must have a robust online platform for informing the public about its activities which also needs to remain operational in crisis situations. The platform (after further updates) will also improve interaction between the Defence organisation and the public.

Assuring the energy security of Ministry of Defence premises and military materiel, whereby the organisation will be better prepared for – and resilient to – disruption caused by, for example, cyberattacks.

Exploring and developing analogue alternatives for the Defence organisation's various systems. Certain forms of training and non-digital resources, such as analogue maps and compasses, will need to become part of the standard package again.

Boosting the armed forces' striking power and the intelligence and security services in the cyber domain, allowing specifically for both the independent and integrated deployment of military cyber capabilities.

Reinforcing the cyber defence of the Defence organisation's networks and infrastructure, in accordance with NATO's Cyber Defence Pledge.

Improving synergy between NATO and the EU with regard to crisis management, resilience issues and an Article 5 situation in order to better align civil and military efforts. This includes seeking synergy between NATO's Resilience Objectives and the EU Disaster Resilience Goals as well as links between the forthcoming EU Preparedness Union Strategy and NATO initiatives.

12 Letter to parliament proposing a model for military service that is consistent with scalable armed forces, BS2024015423, 3 June 2024.

Track 2

Pillar 5

Pillar 6

Pillar 6 Safeguarding civil support to the armed forces in carrying out their military duties

As a country bordering the North Sea and a gateway to Europe's interior, the Netherlands plays an important role in the NATO alliance as a hub and transit country for military materiel and troops, through ports such as Rotterdam and Vlissingen. This is already the case, for example in large-scale NATO exercises, and will be even more so in the run-up to and during a conflict. Our role as a transit country will be tested by movements of military equipment and troops through our ports, airports, roads, railways, rivers and the North Sea. This will have a major impact on regular road, air, water and rail traffic and on the import and export of goods.

A military conflict will also demand an adequate supply of personnel and resources, while the labour market is squeezed, space in the Netherlands is scarce and our resources limited. It is likely that society and the armed forces will have to share the same scarce personnel, resources and capacities in a conflict and that choices will have to be made between their requirements. In the worst case, this could mean that prioritisation will be necessary.[13] For example, space is needed in the Netherlands for housing and emergency accommodation, but the Ministry of Defence also needs space for military exercises, stationing of troops and storage of military equipment. There could also be crowding out in terms of personnel, for example if reservists are called up by the armed forces while they are also essential workers in civil society. During a conflict, the Netherlands will be required to facilitate large-scale reception of and medical care for wounded service personnel and civilians, which will have all sorts of implications for regular care, particularly in terms of continuity, prioritisation and 'crowding out'. Responsive, versatile and scalable care, emergency or otherwise, is needed in such cases, even in the event of what could be a prolonged disruption or conflict.

To support the defence of our country and that of our allies, and to keep society running at the same time, we need to be able to deal with distribution issues, including the associated ethical aspects.

The government is therefore working to:

Identify what the Ministry of Defence needs in terms of civil support in the run-up to and during a conflict and then ensuring that those requirements are met. This relates to different areas, including transport, food, infrastructure, healthcare, energy supplies, the internet and mobile networks. Account must also be taken of ongoing and unfinished processes, such as the NATO Force Model and associated requirements, NATO's new host nation support concept, the National Crisis Management Plan for Military Threats and the National Defence Plan for Critical Infrastructure. As the civil and military requirements are so closely intertwined, the government is also endeavouring to find out what the Ministry of Defence's demands on civil authorities and emergency services such as the police and safety regions (including the fire service) mean for the desired operational capabilities of those organisations.

Achieve a scalable military force that is able to deploy its capabilities (personnel, equipment, infrastructure and expertise) from the Defence organisation as well as from civil society in a short space of time. For this, the armed forces must be able to scale up where necessary and scale down where possible.
A partnership with the civil authorities and emergency services such as the police and safety regions (including the fire service) and various civil parties, including local authorities, businesses and implementing organisations, is crucial in this respect.

13 As set out in NATO's Resilience Objectives.

Track 2 | Pillar 5 | Pillar 6

Explore options regarding prioritisation of military needs over civilian needs. For example, where transport is concerned. If, for instance, a military transit operation requires large quantities of munitions to be transported by rail, prioritisation will be needed to avoid a situation in which the transport comes to an unscheduled and prolonged halt. This could pose a potential risk to public order and security.

Strengthen public-private and civil-military cooperation. Areas concerned include exchange of personnel, logistical support including medical capacity, intensification of collaboration with industry, surveillance and protection, IT infrastructure and digital space. The exchange of classified and unclassified information between military and civil authorities is also crucial.

The EU Civil Protection Mechanism is an important and fully developed instrument for coordinating the European response to disasters and crises and for displaying intra-Union solidarity. Through a more effective and larger-scale response, this addition to national capabilities could take over the armed forces' relief task when necessary.

Strengthen and expand the Defence organisation's knowledge and innovation base, whereby a clear military research and innovation requirement can provide insight into how and where research and innovation can continue, or even be accelerated, in the event of a military conflict or a disruptive hybrid attack.

Test the resilience within NATO and the EU through annual exercises based on different scenarios of increasing threat levels and potential conflict. A good example is NATO's biennial Crisis Management Exercise (CMX), in which NATO's political-military decision-making and crisis-management structures as well as allies' national resilience are tested. The EU's counterpart to CMX, Parallel and Coordinated Exercise (PACE), also involves key EU crisis coordination structures and their interaction with NATO structures. Insights from these exercises serve as guidelines for boosting both national resilience and that of NATO and the EU. The government will work to increase Dutch participation in these events and will look specifically at the internal recommendations and lessons learned that emerge from these exercises, such as the CMX that took place in 2023.

This is a central government publication, drafted under the coordination of the National Coordinator for Counterterrorism and Security (NCTV) and the Ministry of Defence.

government.nl/topics/counterterrorism-and-national-security

December 2024