National Security Strategy

2019

Table of Contents

Summary

National security is a dynamic and multifaceted issue that requires a solid yet flexible approach. This National Security Strategy (NSS) specifies all national security interests that must be protected, as well as how these interests are currently under threat and how we can minimise these risks and threats.

The strategic cycle of the National Security Strategy – which repeats every three years – enables the Netherlands to continually protect itself against the development of threats and risks and intensifies the national security approach in a future-proof manner.

Preventing social disruption and protecting the democratic rule of law

For this purpose, our national security interests are classified into six categories:

1. *territorial security;*
2. *physical security;*
3. *economic security;*
4. *ecological security;*
5. *social and political stability;*
6. *the international rule of law.*

National security is jeopardised when one or more national security interests are threatened to such an extent that this results in or could result in social disruption. With regard to national security, the Netherlands is more dependent than ever on the smooth functioning of the international system of rules, standards and agreements. For this reason, we have added 'the functioning of the international rule of law' to the list of national security interests. This national security interest is not an isolated interest, as it is closely interwoven with the other five national security interests and with other interests and values of Dutch society. As all national security interests can also be threatened via cyberspace, cybersecurity is interwoven into all interests as well. The availability, confidentiality and integrity of essential information services has been added to this NSS as a criterion for territorial security and is therefore covered by the national security process.

Strategic agenda that undergoes periodic assessment

This NSS marks the beginning of a strategic cycle that is periodically repeated to ensure continual assessment of whether the measures to protect national security interests remain sufficiently adequate to tackle all developments, threats and risks that could affect national security. This cycle is repeated every three years, although interim adjustments are made in the event of any new developments, threats or risks concerning national security. In this way, the NSS fulfils the function of a strategic agenda that inventories all of the threats and risks that jeopardise national security and examines the extent to which a comprehensive approach has been established to minimise these threats and increase resilience. As such, the focus of the strategy can change over time and is therefore flexible in nature.

Intensified approach to risks

Current developments concerning threats and risks show that the following security issues require an intensified approach.

- **Threats from state-sponsored actors** will be addressed. This approach consists of generic measures to boost resilience against various types of threats from state-sponsored actors.
- **Polarisation** can undermine our open society. To tackle polarisation, we will implement a broad and overarching approach focusing on the promotion of coexistence. Municipalities, civic organisation and the security chain will make an important contribution to this process.

- Many threats and risks can result in disruption of **critical infrastructure**. To protect against these threats and risks, the government is implementing an intensified approach that will pool knowledge, skills and expertise in order to adequately address national security risks concerning the critical infrastructure.
- The combating of **terrorism and extremism** continues to demand our attention. Reinforcing and intensifying our focus based on actual threat levels whenever and wherever necessary is vital. In addition, efforts will focus on applying the comprehensive approach against all forms of extremism – regardless of their ideological basis – in order to tackle 'new' threats as well.
- The Netherlands can only combat **military threats** by means of effective collaboration and active international policy, e.g. via the EU, NATO, the OSCE and the UN. To maintain our status as a credible ally and partner, we will reinforce and further improve the combat power, sustainability and deployability of our armed forces.
- The approach against **subversive crime** will focus on a broad package of measures as part of a coalition between the government, the business sector and society as a whole. In addition, an ambitious legislative agenda has been established that fully takes into account the practical wishes and preferences of front-line operators as well as constitutional principles. This will substantially boost the approach against subversive crime in collaboration with all of our partners in the field.
- Threats and risks relating to **cybersecurity and cyber threats** will be comprehensively addressed by the government by means of the National Cybersecurity Agenda (NCA), brought into effect in April 2018.[1] This has been formulated in a flexible manner to enable mitigation of the increasing levels of threats.

An intensified focus means the nature of the threat is such that extra and comprehensive attention – in an integrated fashion, albeit within the framework of the existing tasks and responsibilities – is paid to continually minimising all identified threats and risks. The aforementioned intensified focus still requires further specification under the supervision of the line ministries involved.

Continual focus on resilience

The development of the applicable threats and risks means that we must maintain our strong focus on the security issues in the list below. This will roughly involve the following action points:

- The Netherlands will focus on maintaining and **boosting multilateral international systems** via agreements and regulations based on universal values. This focus has been further elaborated in the Integrated International Security Strategy (IISS).[2]
- For the purposes of **combating and preventing natural disasters**, we will concentrate on the issues of climate change, drought, rising sea levels, wildfires, earthquakes, soil subsidence and solar storms. Measures will be taken with regard to carbon reduction, climate-proof groundwater and surface water systems, spatial planning and use of land, among others. The Netherlands will continue its efforts to fulfil the objectives in the Paris Agreement. The water system, which currently focuses primarily on draining away excess water as quickly as possible, must be better equipped to enable retention and infiltration of water. In relation to natural disasters such as forest fires and earthquakes, the usual crisis preparation at the local, regional and national levels is sufficient. Numerous measures will be taken to minimise the risk of earthquakes in relation to gas production in Groningen and the consequences thereof. In the event of an earthquake, a crisis system is already in place.
- Given the potential consequences of a **CBRN** (Chemical, Biological, Radiological and Nuclear) conflict or incident for Dutch national security interests, this threat is given undiminished attention. Another important element in the approach to this issue involves boosting social resilience against any CBRN incidents.
- In the Netherlands, the risk of **infectious diseases** is relatively limited. However, the rise of antibiotic resistance is a cause for concern and a comprehensive and coordinated approach has therefore been formulated for this issue. In recent years, no significant developments that could affect national security concerning infectious animal diseases or zoonotic diseases have been observed.

Development of generic instruments

In addition to the approach to minimise the aforementioned threats and risks, the Netherlands will also focus on increasing the number of generic instruments for the protection of national security – such as the **generic risk and crisis management system** – in order to enable adequate and straightforward measures to be taken against potential and actual incidents and crises. Furthermore, newly developed **knowledge and scientific research into threats and risks** will be integrated and **new technologies and their possible applications** will be monitored for risks to national security. Finally, the **NSS cycle** will be periodically repeated and further developed. The next NSS is scheduled to be published in 2022, although the current NSS will be adjusted in the period leading up to 2022 in the event that threats and risks give cause to do so.

1 Parliamentary Papers 2017/2018, 26643, No. 536.

2 Parliamentary Papers 2017/2018, 33694, No. 12.

Figure 1 **The three pillars of the security approach as defined in the IISS**

Introduction

The Netherlands is constantly changing. Technology is developing at a lightning pace and people, products, organisations and data are becoming increasingly interconnected. As a result, national and international developments are more interwoven than ever before.

Climate change due to global warming is creating new challenges. In addition to opportunities for economic growth and social advancement, these developments also add new dimensions to existing national security issues. Furthermore, new threats (digital or otherwise) can escalate rapidly and significantly affect safety and security within society.

In order to protect national security, the Netherlands must therefore ensure a dynamic approach to security that is flexible enough to respond to new developments, threats and risks[3] and to adjust its levels of resilience. The National Security Strategy (NSS) provides an overview of all threats and risks and specifies their urgency – based on the degree of resilience and their coherence within the national security approach – in order to help protect social continuity and the democratic rule of law.[4]

Closely connected with the IISS, the Policy Document on the Armed Forces and other strategies

The National Security Strategy (**NSS**) connects all local, national and international efforts to protect national security. Where expedient, the NSS refers to underlying substrategies that specify the strategic focus concerning specific threats and risks, such as the Counterterrorism Strategy, the National Cybersecurity Agenda (NCSA), the Delta Programme and the Letter to Parliament on Combating Threats from state-sponsored actors, among others. In close cohesion with the Integrated International Security Strategy (IISS) and the Policy Document on the Armed Forces, the NSS gives a clear picture of all strategic measures at the national level. The NSS also pays specific attention to the overlap between Dutch efforts on the national and international stages; after all, events outside the Netherlands can also substantially affect Dutch national security and the manner in which it is organised. This places greater emphasis on the international nature of national security, as was also mentioned in the report 'Security in an Interconnected World' ('Veiligheid in een wereld van Verbindingen') of the Scientific Council for Government Policy. The increased interconnectivity of internal and external security and the need for a more integrated approach to national security will be implemented in the NSS.

The security approach in the **IISS** is based on three pillars: Prevention, Protection and Intensification. Within these categories, specific objectives have been formulated in order to counter any urgent threats that may develop in the years to come. These measures constitute an anticipatory and preventive approach to security with a long-term perspective. The strategy focuses on preventing danger to the greatest extent possible and protecting the Netherlands against danger whenever necessary based on a modern and effective approach. This also means establishing and maintaining credible deterrence via alliances, as well as paying attention to the root causes of terrorism, irregular migration, poverty and climate change, as specified in the coalition agreement. Finally, reinforcement of the foundations of security – i.e. promotion of the international rule of law and an effective multilateral system – is a vital factor in guaranteeing the security of the Kingdom. The Policy Document on the Armed Forces is based on three core principles:

- **maintaining security** – within both the Kingdom and Europe;
- **establishing security** – both at and beyond Europe's borders;
- **secure connection** – between the Netherlands as a hub country and its supply/distribution channels.

3 In this document, the terms 'threat' and 'risk' are used alongside each other and are considered mutually supplementary. A 'risk' is defined as 'the interplay between the likelihood of an incident occurring and the potential impact of that incident.' The term 'threat' relates to the presence, concreteness and acuteness of danger (sometimes as a blip on the horizon that needs to be identified via an early-warning mechanism). The term 'threat' therefore involves present and demonstrable danger, while the term 'risk' involves potential danger.

4 Including the following definition: the foundation of Dutch society and its constitutional and democratic safeguards.


SAMSUNG
SAMSUNG

The National Security Strategy Cycle

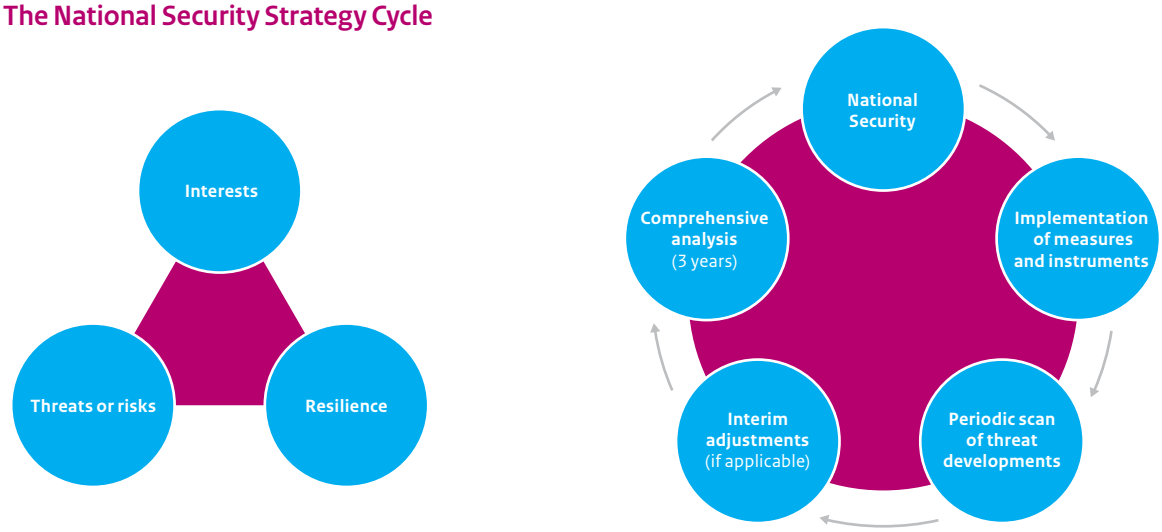
The NSS functions as a strategic agenda, focusing on preventing social disruption and protecting the democratic rule of law. This agenda shows which issues should be focused on in order to protect national security, given the current development of threats and risks. This means the focus of the strategy can change over time and is therefore flexible in nature.

This NSS marks the beginning of a new strategic cycle that is periodically repeated to ensure continual assessment of whether the measures to protect national security interests remain sufficiently adequate to tackle all developments with regard to threats and risks that could affect national security. The NSS specifies all national security interests that must be protected, as well as how these interests are currently under threat and how we can minimise these threats or risks.

Identifying national security interests

The strategic cycle begins by identifying all national security interests that could result in social disruption – damage to the democratic rule of law included – in the event that these interests are seriously compromised. These interests have been methodically crystallised into impact criteria that clearly display the extent to which these interests could be compromised. The interests and the manner in which they are formulated are part of the methodology of the National Security Analysts Network (ANV). The ANV is a multidisciplinary network of knowledge institutes with the objective of boosting the continuity, the safeguarding of knowledge and the multidisciplinary approach concerning analyses of national security.

Figure 2 **The National Security Strategy Cycle**



Identifying developments with regard to threats and risks

Once the national security interests have been defined, an independent analysis is conducted to examine which security developments, threats or risks can affect these interests. This analysis integrates existing analyses and partial analyses such as the Cyber Security Assessment Netherlands, the Terrorist Threat Assessment Netherlands, the strategic monitor, the National Security Profile and reports by the intelligence and security services. In this way, this comprehensive analysis paints a complete picture of all of the main threats and risks to national safety and security and interconnects the internal and external security dimensions. In order to tackle any interim developments in the threat level, mid-term scans are conducted to evaluate whether the NSS needs to be adjusted or supplemented.

Strategic focus on resilience

The NSS focuses on safeguarding the Netherlands' resilience, i.e. its ability to adequately combat threats or risks. This involves all parties who have any degree of responsibility for the processes of prevention, anticipation, preparation, response and aftercare (comprehensiveness). Based on the threat and risk analysis, the NSS provides framework answers to the following questions:

1. *Does the Netherlands have a comprehensive approach to minimise this threat or risk?*
2. *Given the manner in which this threat or risk has developed, does this approach make the Netherlands more resilient?*

Whenever additional attention to a particular threat or risk is required, this will be visibly highlighted in the assessment of this question and included in the NSS. However, if a particular threat or risk does not require any additional attention, this does **not** mean that the threat or risk to national security has reduced. If the current approach is deemed sufficient, then this means that the same level of attention to this threat or risk must be maintained.

The term 'national security'

National security is jeopardised if one or more critical interests of the Dutch state and/or society are threatened to such an extent that this results or could result in social disruption.

The Netherlands uses the above definition of national security. Two essential elements determine the scope of the term:

1. *The Netherlands' critical interests or national security interests must be jeopardised;*
2. *and the threat to these interests must be sufficiently serious that it has resulted or could result in social disruption.*

Six national security interests

Our national security interests are classified into the following categories:

1. Territorial security	The unimpeded functioning of the Netherlands and its EU and NATO allies as independent states in a broad sense, or territorial security in a narrow sense..
2. Physical security	The ability of people to go about their lives in an unimpeded manner within the Netherlands and their own physical environment.
3. Economic security	The unimpeded functioning of the Dutch economy in an effective and efficient manner.
4. Ecological security	The unimpeded continued existence of the natural living environment in and around the Netherlands.
5. Social and political stability	The continued and unimpeded existence of a social climate in which individuals are free to go about their lives and groups are able to coexist within and in accordance with the Netherlands' democratic and lawful state and its shared values.
6. International rule of law	The functioning of the international system of rules, standards and agreements established for the purposes of international peace and security.

As national security can also be affected via cyberspace,[5] cybersecurity has been interwoven into all of the other national security interests. In addition, the integrity of cyberspace has been added as an aspect of territorial security, which includes the availability, confidentiality and integrity of essential information services. If these services are seriously affected or threatened, this could result in social disruption. Examples of such threats include cyberattacks for the purpose of sabotage or spying, as well as outages caused by intentional acts or natural causes.

The ways in which these interests can be compromised have been formulated as impact criteria (see Annex 2). These criteria give an overview of the possible consequences for national security interests based on their severity and likelihood. However, assigning a weighting to each specific element involves more than just simple arithmetic. We have observed that some threats or risks can have a more subversive effect than others. Furthermore, even if some types of threats or risks are not serious on their own, the simultaneous existence of a wide range of these non-urgent threats

5 All ICT resources and services with which all entities could be digitally connected – including permanent, temporary and localised connections – and data that is stored within this domain (e.g. facts and figures, program code, information, etc.), all of which is unconfined by geographical limitations.

and risks could jeopardise the democratic rule of law and therefore potentially result in social disruption. We must also continue to take into account the fact that society is constantly changing, which means resilience levels are also constantly changing. For example, something that is of little concern today could eventually develop into an issue that could cause social unrest. At the same time, the government should exercise restraint identifying social developments as a threat to national security, especially when the developments in question are playing out within an open and democratic society. After all, the nature of national security implies that the gravity of this general interest justifies the government taking action to prevent social disruption if and whenever necessary and using all of the instruments at its disposal. This requires careful decision-making based on transparent criteria that have been embedded into the definition of national security.

The international rule of law, with national security in mind

Traditionally, the Netherlands has always been an extremely international nation with a wide variety of physical and digital hubs, such as the Port of Rotterdam, Amsterdam Airport Schiphol, the access point to the transatlantic telegraph cable and one of the biggest internet exchanges in Europe. As a result of these myriad connections and the potential impact of the development of international threats, the Netherlands is more dependent than ever on the smooth functioning of the international system of regulations, standards and agreements For this reason, we have added 'the functioning of the international rule of law' to the list of national security interests. This national security interest is not a separate interest in itself, as it is closely interwoven with the other five national security interests and with other interests and values within Dutch society.

The international body of rules, standards and agreements is a highly robust entity, so any individual developments that may damage this system will not necessarily be detrimental to national security in the Netherlands. For this reason, national security will only be directly impacted in the event that the functioning of the international rule of law is seriously or extremely seriously compromised (or breaks down entirely), which may result in social disruption. These impact criteria have been formulated by the National Security Analysts Network (ANV) and included in the risk analysis system.

Social disruption

The second dimension of the definition of national security relates to social disruption. This means that any particular development only threatens national security in the event that its severity results in or could result in social disruption and/or actually/potentially jeopardises social continuity. This could be in the form of social or political instability, serious damage to the ecological living environment or loss of fundamental trust in the functioning of society, for example.

Social disruption, therefore, includes a physical aspect that could manifest itself in numbers of victims, destruction or disruption of vital services. In addition, it also involves a sociopsychological aspect, such as disruption of everyday life, lack of clear perspective for action during and after the manifestation of threats or risks and lower expectation patterns in relation to culpability, legitimacy of policy (fairness) and confidence that the authorities can restore the situation.[6] Social disruption can also occur in the event that the continuity or availability of critical processes is affected. These processes constitute the Netherlands' critical infrastructure. The transport and distribution of electricity, access to the internet and provision of drinking water are examples of critical processes. Finally, social disruption can also occur in a more subversive manner, such as criminal subversion or disruption to the democratic rule of law that could result in a loss of faith in institutions.

Different dimensions of national security

In its report entitled 'Security in an Interconnected World') ('*Veiligheid in een wereld van Verbindingen*'), the Scientific Council for Government Policy distinguishes between the dimensions of national security, human security and flow security. Establishing the prism of national security interests as the core aspect of the approach to national security ensures that these dimensions are comprehensively covered by the NSS.

Comparison with international policy

An exploratory investigation into the national security approaches of similar countries[7] demonstrated that many of these governments had identified the same threats and risks that could potentially result in social disruption, with terrorism, cybersecurity and climate change all constituting shared and recurring threats. Other countries have a greater focus on the potential consequences of international issues on national security, such as the impact of failed states, failing governance and instability in and around their sphere of influence. The consequences that international issues like these could have for Dutch national security have been formulated as part of the Integrated International Security Policy.

6 Source: *Maatschappelijke ontwrichting en overstromingen* ('Social Disruption and Flooding') (2014), PBL Netherlands Environmental Assessment Agency.

7 Germany, Sweden, the United Kingdom, the United States, Australia, Canada, France and Belgium.

Core principles: security as a shared responsibility

Within our democratic state, it is vital that people and civic organisations are able to develop and operate within a free and safe environment. Ensuring this free and safe environment is one of the government's core responsibilities, as it is a vital precondition for the protection of the values of our democratic society and our constitutional freedoms. At the same time, this security cannot be guaranteed by the government alone. The business sector, civic organisations and citizens also play a vital role in ensuring local, regional and national security and boosting resilience. The government plays a coordinating role in this process and must act in a distinctive, transparent and by-the-book manner when combating threats or risks, based on the following core principles:

- **The government must protect and promote national security** to ensure that people and civic organisations can optimally develop within a free, safe, democratic and lawful society. Of course, the government will act constitutionally while fulfilling its obligation to protect national security.
- **For this purpose, the Netherlands will operate a cross-societal approach**, within which government bodies, security companies, the business sector and civic organisations collaboratively safeguard national security.[8] All of these parties are involved in the implementation and development of the NSS system. Moreover, efforts will be made to boost awareness and formulate a perspective for action for the predominant risks. Independent and empowered citizens will also play a substantial role. Within this approach, the government represents public interests, encourages all parties to take their individual responsibilities and sets a good example.
- **The Netherlands focuses on early detection and identification of risks and threats** to national security. This means that information exchange among public parties and between public and private parties must be promoted to the greatest extent possible. This knowledge sharing must be done within the applicable legal frameworks and safeguards.
- **There is no such thing as 100% safe.** No matter how substantial or committed the efforts made by all parties may be, it is not always possible to foresee or prevent shocking events. The Netherlands seeks to prevent threats and risks to the greatest extent possible and to respond rapidly and adequately whenever they occur. We also learn from incidents by evaluating them and adjusting policy and planning processes whenever necessary. This ensures continual optimisation of the Dutch security approach.
- **The national security approach is comprehensive and flexible** to ensure it is compatible with developments in the threat, risk and resilience levels.[9] In this regard, it is **inevitable that decisions will have to be made;** if society is unwilling to accept even the slightest risk, then the security measures required will quickly become draconian and prohibitively expensive.
- **National security in the Netherlands does not stop at the borders,** as the influence of international developments on national security is continually increasing. Internal and external security are becoming increasingly interwoven and require greater integration of the national security approach, both in physical space and in cyberspace. For this reason, the Netherlands always seeks collaboration within a European or broader international context when it comes to reinforcing the Netherlands' own national security and protecting the Netherlands' national security interests. This international focus is embedded in the IISS.

8 For example, we emphatically sought collaboration and connection with the business sector for the purposes of the cybersecurity approach, and worked closely with local government bodies and civic organisations when formulating the approach to combat radicalisation.

9 The term 'resilience' also includes developments in threat perception, as described in the Research and Documentation Centre's report entitled 'The road to a resilient open society' (**'Op weg naar een weerbare open samenleving'**), Parliamentary Papers 2018/19, 30821, No. 52.

Trends and developments that influence national security

The Netherlands is an open society in which people can reap the benefits of social and economic developments. Digitalisation, technological development and the Netherlands' international orientation create a wealth of opportunities for citizens and businesses.

However, the openness and international interconnection of the Netherlands also means that internal and external developments can affect our national security. This section describes trends, including megatrends, and developments that can affect the development of new or existing threats or risks to national security and our efforts to protect it.

International developments (political or otherwise)[10]

Multipolar world order: a shift in the international balance of power

There is tension between major global powers, particularly between the USA and the European Union on one side and China and Russia on the other. The increasing assertiveness of China and Russia on the international stage has become particularly conspicuous and, at the same time, it is becoming clear that our transatlantic relationship can no longer be taken entirely for granted.

The shift in the international balance of power to a more multipolar world order means that the power of multilateralism as a means of securing cooperation is waning. This may affect factors such as the financial and economic order and climate agreements. It could also present an obstacle to strategies against cyber threats, hybrid threats and the risk of extremism and terrorism. The world order established after the Second World War, which is based on the democratic rule of law, liberal market economics and the core values of our society (such as human rights, fundamental freedoms and equality), is being increasingly called into question. This multipolar world order is resulting in new types of global friction and polarisation between East and West.

Political instability in the EU

A strong Europe lays vital foundations for our national security and the EU Global Strategy lays the foundations for stability and security policy within the EU. However, the whole 'EU project' is being questioned by a number of parties. The departure of the United Kingdom from the EU is the most extreme example of this, although the popularity of anti-EU parties in most Member States (including France, Hungary, Italy, Austria, the Netherlands, Poland and Sweden) also reflects this development. The diverse range of opinions within the EU on subjects such as migration (Eastern vs Western Europe) and the economy (Northern vs Southern Europe) fuel the forces of populism and create risks for public confidence in the EU and its institutions. Finally, in a number of EU countries, there has been a disturbing erosion of the rule of law.

On the other hand, the Eurobarometer has shown that support for the EU has been increasing in recent years. Brexit is indeed a setback, but the EU has been strongly unified in its response.

10 As also described in the Integrated International Security Strategy.

The EU is also highly capable of identifying and addressing external threats, e.g. those posed by the aforementioned assertive world powers. In other words, there is reason for concern and alertness, but no need to panic.

Political instability in areas surrounding the EU

The continual instability of countries and regions close to the EU's borders also presents possible risks. Some countries provide a sanctuary for criminal, extremist and/or terrorist groups and there is a risk of nearby countries being sucked into a downward spiral of violence and failing governance. Irregular migration pressure in Europe might also increase, which could destabilise European collaboration, solidarity and tolerance, as well as causing polarisation and hostility towards regular migration and the asylum system. In many cases, irregular migration also involves types of cross-border crime, such as human smuggling and human trafficking, the proceeds of which can be used to fund terrorist activities. Finally, it can allow terrorists to 'hitch a ride' with the irregular migrant flow into Europe. It is expected that irregular migration pressure from unstable countries and regions in the vicinity of Europe will remain high in the years to come.

Development of root causes and terrorist threats

Jihadist varieties of political Islam will continue to exist, even after ISIS loses all of its territory in Iraq and Syria. The root causes of the growth of these and other groups have not been removed, and they will always remain potential catalysts of violence, especially in Africa and the Middle East. Although ISIS has been largely defeated and greatly weakened from a territorial perspective, it is highly likely that it will pose different kinds of risk in the years to come. It is becoming increasingly transnational in nature and makes use of modern technology (digital communication, social media, etc.). The loss of ISIS territory means that the problem of returnee combatants is becoming particularly urgent, with specific groups posing a threat due to their combat experience and unabated jihadist ideology.

Other types of terrorism also continue to develop. Right-wing terrorism is on the rise again and there are signs that left-wing extremist groups are becoming more active in the EU in response. This issue is also discussed in the section entitled 'Demographic and social developments'.

Developments in information technology

Cognitive and autonomous information systems

Traditional information systems programmed to conduct specific tasks in accordance with fixed protocols are increasingly making way for self-learning systems that teach themselves new tasks and behaviour with no human intervention and systems that can improvise and independently make decisions based on specific knowledge. The use of such Artificial Intelligence (AI) systems and Machine Learning systems could have consequences for national security.

AI systems are trained using massive volumes of data. When this is done using a biased (ill-considered, incomplete or manipulated) data set, a self-learning system can develop and act in a prejudiced manner, and as time goes by, it becomes impossible to determine the root cause of specific behaviour displayed by the system. If the decisions made by the system affect people or organisations, then the consequences of such behaviour could be extremely serious.

When multiple autonomously operating systems interact, insufficient coordination can result in unexpected disruption of social processes, such as traffic accidents due to a breakdown in communication of autonomously operating traffic systems. The more areas of society into which autonomous systems are integrated and the more dominant they become in specific areas, the greater the risk they present to national security. As they often require interaction – mainly via the Internet – and are unable to operate in isolation, autonomous systems are potentially vulnerable to unwanted infiltration by external actors.

Interconnection of systems and networks

More and more devices – from home, garden and kitchen appliances to bridges and sluice gates – are connected to the Internet nowadays. Hardware and software vulnerabilities enable malicious actors to gain access to the devices themselves, the network to which the devices are connected and the data that the devices collect and process on their users and how they use the device.

The users and providers of these devices often do not pay enough (if any) attention to the potential consequences of such vulnerabilities, as they themselves are not directly affected in the event of a data breach. Digital information systems are a crucial factor in the continuity of businesses and other organisations. If these systems malfunction or are taken down, this can have serious commercial and economic consequences.

Dependence on information technology

Our society has become hugely dependent on information technology. The growing dependence on large foreign tech firms is making the governance of cyberspace increasingly difficult. It is therefore vital to constantly examine how this dependence affects the protection of national interests and how this protection is organised at both the national and international levels.

The EU is striving to achieve strategic autonomy with regard to defence and security. At the moment, information technology in these areas is also heavily dependent on foreign firms, however. For example, the necessary hardware and software is made by non-European companies. The Netherlands and other European countries therefore effectively depend on these market players for vital components of their critical digital infrastructure.

Global financial and economic developments

Restructuring of the global financial and economic order

A shift in the international financial and economic order is currently ongoing and the economic and security-related consequences of this shift have not yet entirely become clear. China's substantial economic vitality is supporting the global economy, which means China holds a substantial interest in the financial and economic status quo. At the same time, China is increasingly questioning the rules on which the liberal market order is based and attempting to mould them in its favour. China is also investing in setting up parallel institutions and new networks that will affect the institutional order. In the long term, the shift in the economic balance of power from the West to China will have political implications that may affect national security.

Technological developments in the financial and economic sectors

Cryptocurrencies – which are independent of any central bank – can be privately issued via new technologies such as blockchain. The main risks stemming from cryptocurrencies is that they are a particularly effective way to launder the proceeds of crime and to fund terrorist activities. For this reason, the EU has decided to extend the scope of the Money Laundering Directive to include cryptocurrencies, and work is being conducted on international anti-money laundering standards for cryptocurrencies. In addition, as of the start of 2020, the Money Laundering and Terrorist Financing (Prevention) Act (Wet ter voorkoming van witwassen en financieren van terrorisme) will oblige cryptoservice providers operating in the Netherlands to apply for a licence. At the end of 2017, at the height of the cryptocurrency bubble, nobody knew what impact cryptocurrencies would have on the stability of the financial system. Since then, national and international studies have been conducted that show that the risks to financial stability are currently limited. However, institutions at both the national and international level will continue to monitor all developments relating to cryptocurrencies and their possible consequences for financial stability.

Economic instability of the EU

The financial crisis (2007-2011) resulted in greater economic instability within the EU, the consequences of which are still tangible and visible today. Eastern and Southern European banks are still struggling with a high volume of problematic loans, which could directly affect the economies of other EU Member States, including the Netherlands, due to negative spillover effects from their banking systems. In addition, the budgets of Greece, Italy and Portugal are still weighed down by high levels of government debt and structural deficits. Increasing Euroscepticism within the EU, combined with the fact that a new credit crisis is not considered impossible, could result in problems for the Eurozone and confidence therein.

Demographic and social developments

Increasing gaps between social groups

Gaps between social groups are increasingly opening up along sociocultural and socioeconomic boundaries, a fact reflected in the clear hardening of the social debate (online and otherwise). The fragmentation or 'parallelisation' of society could be reinforced by the use of social media and the 'media bubble', within which users' opinions are constantly affirmed and they rarely encounter alternative opinions. Feelings of economic subordination or the effects of technological development on employment participation could also result in parallelisation. Fragmentation has always been a factor in Dutch society, although it has intensified in recent years. Certain groups are rejecting fundamental aspects of democratic society and could therefore be or become a threat to the democratic rule of law. In general, society's resilience against such ideologies is still high.

Fluctuating trust in institutions

All of the above developments are concurrent with a decline in trust in politicians and the government. Confidence in authoritative bodies is still high in the Netherlands and is expected to remain so in the future. However, trust in the actions of the people within these institutions is fluctuating, with levels of trust varying greatly between the various subgroups within society. Trust in traditional media, for example, has declined substantially among some groups of young people and they are increasingly seeking their information from alternative sources.

Ecological developments

Climate change

The climate is being affected by ongoing global warming. Extreme weather events could create a risk to national security, particularly events such as extreme hailstorms, excessive rainfall that cannot be sufficiently drained away or the simultaneous occurrence of two extreme weather events. A second development is the rise in invasive species: plants and animals native to more southerly regions are migrating further northwards, which could result in new infectious diseases affecting people, plants and animals.

Reduction of biodiversity and biomass

Biodiversity relates to the variety of life on earth: diversity of genes, species and ecosystems. Further loss of biodiversity and biomass could cause significant damage to the natural environment and agriculture, which could have long-term consequences for ecological security in the Netherlands.

Environmental pressure

The negative effects of human activities on soil, water and air are referred to as environmental pressure. Human activity focusing on the short term, such as groundwater management for the purposes of agriculture, could result in damage to the environment (salinisation) in the long term, causing significant changes to the soil, water and air and reducing their quality.

Predominant national security risks

Trends and developments at the macro level could result in threats and risks to national security. What kinds of threats and risks these are and how they jeopardise national security has been detailed within an integrated risk analysis by the National Security Analysts Network (ANV).

For the sake of readability, the risk categories from the risk analysis have been grouped in accordance with the security issues referred to in this section (see Annex 1 for this classification).

The risk analysis illustrates the following aspects of each specific threat/risk:

- the impact that the threat/risk would have on one or more national security interests;
- the likelihood of the threat/risk actually occurring, as determined by its development in the medium term.

In accordance with these aspects, the eleven predominant national security risks and threats listed below were identified. These constitute threats and risks that seriously or very seriously jeopardise one or more of the six national security interests.

Unwanted interference and influence by state-sponsored actors

Overt and covert interference and influencing activities by foreign governments jeopardise national security. These activities include covert attempts by foreign governments to control their diaspora communities, often using tactics such as intimidation and blackmail. This impacts the national security interest of 'Social and political stability'. This category also includes undesirable influencing activities and disruptive operations with the goal of directly compromising, weakening, undermining and destabilising the Netherlands itself, its democratic rule of law and its open society. This could affect the national security interests 'International rule of law', 'Social and political stability' and, in the event physical violence is used, 'Physical security'. Activities by state-sponsored actors to undermine Dutch society via unwanted influencing activities and disruptive operations are conducted by means of hybrid operations, among other methods. Hybrid attacks are nothing new, although the scale and frequency of these attacks by increasingly assertive states is unprecedented. As part of the constant international competition between various countries, covert hybrid operations to undermine other societies are employed increasingly often. Vulnerabilities in society and the political system are being exploited; given the right circumstances and the right combination of influencing activities, this can have major consequences (e.g. for critical national infrastructure). Furthermore, developments in digital and information technology can facilitate these influencing and undermining activities.

Threats against multilateral institutions and economic resilience

The international order is changing significantly and a diverse range of ever-changing coalitions are operating in a wide range of areas. In combination with polarisation between different population groups, which is putting pressure on our democracies and the consensus regarding international collaboration, this factor creates uncertainty and damages international security levels. Furthermore, the interests of individual countries – and the standards and values on which their society is based – are increasingly being prioritised, which puts pressure on multilateral institutional cooperation. The increasing power and influence of China in Western economies could have major long-term consequences both for the financial and economic systems in the EU and for the operation of multilateral institutions.

As described in the previous chapter, Europe – and hence also the Netherlands – is being confronted by a 'ring' of increasing instability and conflict, which means there is a constant threat of new conflicts breaking out. Within this climate of uncertainty and increasing threats and risks, it is even more important for the Netherlands that the two organisations via which the Netherlands wishes to safeguard its national security interests – the EU and NATO – function smoothly.

However, both the EU and NATO are being threatened by a number of external and internal factors. In the past, cooperation was the key priority and shared interests were the decisive factor in the event of transatlantic tensions, whereas these shared interests are nowadays beginning to be interpreted differently. In some cases, it can be difficult to reach a consensus among EU Member States, which means the EU cannot always put its full weight into the balance of power. This risk could affect the national security interests of 'Territorial security', 'Social and political stability' and 'International rule of law'.

Disruption of critical national infrastructure

The Netherlands' critical national infrastructure comprises all of the processes that are so vital to the smooth functioning of our society that any disruption thereof will have substantial consequences for the Netherlands. As these critical processes are mutually dependent, the failure of just one of them could have a variety of knock-on effects for critical national infrastructure as a whole. In many cases, the dependence between critical processes is not immediately and obviously clear.

Due to the importance of these critical processes for social continuity, any serious disruption thereof could result in national security being jeopardised. The failure of critical processes could particularly impact the national security interests of 'Physical security', 'Social and political stability' and 'Economic security', although it could potentially affect practically all national security interests and all of the underlying impact criteria. As a result, the failure of critical national infrastructure could amplify other predominant risks to national security. The opposite also applies, as practically all of the threats or risks could affect critical national infrastructure.

Recent analyses particularly emphasise cyber threats from state-sponsored actors with the goal of disrupting – or even sabotaging – critical systems. There is a clearly increasing trend in the use of autonomous systems in all kinds of sectors, such as the electricity sector, the financial sector and the industrial sector. These systems often require communication and interaction between various entities (mostly via the Internet) and are unable to work in isolation. As a result, the systems are vulnerable to undesired outside interference.

Terrorism and extremism

Extremism is the active pursuit of drastically disruptive changes to society that could jeopardise the democratic rule of law, possibly using undemocratic methods that could seriously impact the smooth functioning of our democratic legal order. Undemocratic methods such as these can be violent or non-violent, and the most extreme of the violent undemocratic methods is terrorism.

In the Netherlands, it appears that the traditional divide between left-wing and right-wing extremism may become less applicable in the years to come and that new phenomena such as 'identitarian extremism' or 'anti-government extremism' may supersede the classic left-right spectrum. A number of groups are on the rise that ideologically strive to 'keep the white race pure' and oppose 'race mixing' and 'forced transformation' of the population's racial demographic. In addition, increasing numbers of disgruntled citizens and groups are turning against the government for a variety of reasons. Despite the rise of such sentiments, most of which are expressed online, there is uncertainty regarding whether extremists in the Netherlands will become more willing to use violence in the future.

Currently, almost all of the terrorist threats in the Netherlands are related to jihadism, with ISIS supporters continuing to pose a risk. However, the threat posed by Al-Qaeda – and especially its hard core – must not be underestimated either. One potential threat that could arise in the near future is the release from prison of detained jihadists who still maintain their jihadist ideology. In this regard, both attacks by lone actors and large-scale attacks are deemed conceivable or highly conceivable. There are indications that such attacks or other similar types of attack could be carried out and the possibility of other types of politically or ethnically inspired forms of terrorism becoming a threat also cannot be ruled out.

Military threats

The increasing tension between major powers and instability on Europe's outer borders have increased the likelihood of armed conflict. Military developments are also fuelling this risk: in the last year on record (2017), global investment in defence materials was at its highest level since the end of the Cold War. The biggest increases in defence spending were observed in China, Russia and Saudi Arabia, although the combined total spent by the European NATO countries also substantially increased. Other indicators also reflect the increasing military threat level: the increasingly aggressive rhetoric, larger-scale military exercises and multiple violations of territorial waters and airspace all testify to the increasing tension between states. This tension could also create risks for Dutch supply lines, which could potentially impact the financial and economic systems. All forms of military threats constitute a risk to national security.

Given the interconnection between internal and external security, this predominant risk clearly shows that there is a definite link between cyber threats and hybrid conflicts – for example, a military threat that results in a military conflict involving the Netherlands. This could occur as a result of Article 5 of the NATO treaty, in the event that a conflict arises between a NATO Member State and another state. In such cases, other hybrid instruments will also be used alongside military action, including cybertechnology. Scenarios also exist in which Article 5 has not yet been invoked, but where increasing international escalation means it could be likely to happen in the near future. In such situations, it is conceivable that the Netherlands, which could potentially be used as a transit country by other NATO members, could already become an important target for attacks (including cyberattacks). If this kind of predominant risk occurs, then it will impact the national security interests of 'Territorial security' and 'International rule of law'.

Criminal subversion

In a number of cities and municipalities, certain individuals or groups are rejecting, working against, disrupting and/or undermining the authority of local government, such as criminal gangs who hope to establish 'no-go areas'. In the Netherlands, we are not yet observing this to the same degree as in other European countries, although this could nevertheless eventually jeopardise the authority of the government. Criminal influence on public administration, either directly or via interference in the business sector, could result in a lack of trust in the civil servants or other parties involved. The analysis shows that, if this risk becomes reality, then it will particularly impact the national security interest of 'Social and political stability', causing serious damage to the democratic rule of law and substantially impacting society. As criminal subversion is already having a significant impact on a number of cities and municipalities, it has been deemed a predominant risk to national security.

Polarisation and threats to social cohesion

The increasing levels of polarisation are undermining our open society. Polarisation could create a breeding ground for both violent and non-violent extremism and, in the most extreme cases, terrorism. State-sponsored actors could take advantage of this situation via hybrid and other operations. Developments that cause polarisation are an international phenomenon and do not stop at the Dutch borders. This dominant risk impacts the national security interest of 'Social and political stability'.

In addition to spreading undemocratic or anti-democratic messages in order to increase polarisation, extremist groups also try to establish parallel societies (enclaves). For example, they do this by actively rejecting our open society, by obstructing public officials and politicians from performing their duties, by undermining democratic institutions and/or by restricting the basic rights of citizens.

Polarisation can also be intentionally stoked by state-sponsored actors via digital and other methods. As part of the international power struggle, resources are being deployed that undermine the sovereignty and dominance of states, facilitating long-distance activities or hybrid operations designed to intensify polarisation between different population groups.

Cyber threats

The greatest cyber threats to national security – i.e. those with the biggest impact and highest probability – are posed by digital attacks by state-sponsored actors for the purposes of espionage, influence, disruption and sabotage. The activities of cybercriminals could also have a major impact. The likelihood of cyber threats is relatively high.

Technological developments are increasing the levels of dependence, interconnection, complexity and uncontrollability of systems and processes. Furthermore, strategic dependence on foreign suppliers, manufacturers and service providers increases our vulnerability to espionage, disruption and sabotage. The increasing levels of digitalisation mean that the potential damage of digital attacks and the benefits to any malicious actors are also greater. Furthermore, analyses have shown that, due to rapid development and innovation (among other factors), our resilience to cyberattacks is at risk of falling behind. Moreover, cyber threats are not a separate phenomenon and they are often interwoven with other risks. For example, disruption of the electricity supply could result in failure of information systems and vice versa. As a result, it is not always possible to make a clear distinction between cyber threats and other threats affecting cyberspace.

Natural disasters

This predominant risk occurs as a result of the power of nature, usually in the form of a catastrophe caused by natural phenomena. Flooding (from the sea or from a river), wildfires or earthquakes could have severe consequences for society. The same applies to extreme weather, such as heavy storms, blizzards or black ice. Another risk relating to extreme weather is concurrence: the simultaneous occurrence of two separate phenomena, such as peak discharge of the major rivers in combination with a westerly gale. In such cases, water would surge inland from the sea or from Lake IJssel and the rivers would be unable to drain it away into the sea, resulting in a high risk of flooding. Climate change and the accelerated rise in the sea level therefore constitute an important national security development, as climate change is likely to result in more extreme weather events and increase the likelihood of natural disasters in the long term.

Chemical, Biological, Nuclear and Radiological threats

As a result of recent technological developments, there are concerns about the possible use of biological weapons. Furthermore, nuclear arsenals are being modernised and expanded throughout the world and nuclear control treaties are either crumbling (Intermediate-Range Nuclear Forces treaty), expiring (New START) or being ignored (the Non-Proliferation Treaty). In addition, the doctrines for the use of nuclear weapons in a conflict situation are changing. There are also concerns that nuclear and radioactive material could fall into the hands of non-state-sponsored actors, such as groups with violent extremist or terrorist intentions.

The risk of an unstable arms-control regime and potential/actual use of Chemical, Biological, Nuclear or Radiological (CBRN) materials by state-sponsored actors impacts a variety of criteria within the national security interest of 'International rule of law'. The use of weapons of mass destruction (including CBRN weapons) is detrimental to state sovereignty, peaceful coexistence and peaceful settlement of disputes. The national security interest of 'International rule of law' could be jeopardised without this affecting any of the other national security interests in the short term. However, as it tramples all over the fundamental principles of state sovereignty, peaceful coexistence and peaceful settlement of disputes, it would severely weaken the foundations of the international rule of law. This could result in states acting with impunity and set a dangerous precedent, in addition to creating great uncertainty and instability within international relations. Moreover, CBRN proliferation would also constitute damage to multilateral institutions, as the arms-control regime contains a vital system of international treaties and agreements. Finally, the use of nuclear weapons would constitute an extremely serious breach of human rights.

Infectious diseases

This risk relates to acute threats to public health in the event of a crisis caused by a large-scale outbreak of an infectious disease, such as a flu pandemic (although other infectious diseases are possible), a zoonotic disease or an animal disease. If this risk occurs, then it will impact the national security interests of 'Physical security', 'Social and political stability' and 'Economic security'.

Based on the number of flu pandemics in the last 100 years and the frequency at which they occur, it is likely that a flu epidemic will break out in the near future. It is not possible to predict in advance whether it will be a serious or a mild pandemic. The social consequences will be particularly serious if a large percentage of the population falls ill. The outbreak of an animal disease (such as foot-and-mouth disease or African swine fever) remains likely in the Netherlands, despite all of the preventive and preparatory measures taken. Among other factors, this is due to the large number of agricultural animals and pets and the global transport of animals.

We must also remain alert to the issues of vaccination levels in the Netherlands and antimicrobial resistance (AMR). Further decline in vaccination levels could mean a higher risk of outbreaks of infectious diseases in the long term and the Netherlands must continue to protect itself against the increasing threat of AMR from other countries.

Priority assessment of threats and risks: which issues require extra focus?

Security is one of the government's core responsibilities. Whenever any threats or risks present themselves, the government strives to boost the Netherlands' resilience by means of preventive, proactive, preparative and responsive measures, as well as providing any necessary aftercare. We are already making significant progress. Security services, government organisations, businesses and citizens are working together tirelessly to keep the Netherlands safe and to boost resilience.

At the same time, the world around us is continually changing and a solid and flexible strategy to address threats and risks is essential. For the purposes of the NSS 2019 and in accordance with the National Security Strategy Cycle, the development of threats and risks was weighed up against the current strategic efforts made by the government and all of its social partners in order to address these threats and risks. In this context, we provided answers to the following questions in compliance with the core principles:

1. *Does the Netherlands have a comprehensive approach to minimise this threat or risk?*
2. *Given the manner in which this threat or risk has developed, does this approach make the Netherlands more resilient?*

This chapter describes the themes that will result in intensified strategic focus. An intensified focus means the nature of the threat is such that extra and comprehensive attention – in an integrated fashion, albeit within the framework of the existing tasks and responsibilities – is paid to continually minimising all identified threats and risks and boosting resilience. The aforementioned intensified focus still requires further specification under the supervision of the line ministries involved. We need an intensified focus on the approach to state-sponsored threats, reduction of polarisation, protection of critical national infrastructure, counterterrorism, the approach to military threats, the approach to subversion and cybersecurity.

1. Threats from state-sponsored actors will be addressed

An open society and an open economy are the essential foundations on which Dutch society and prosperity are built. Our open society is characterised by freedom, democracy, the rule of law and an international orientation. Our openness allows the Netherlands and its inhabitants to enjoy all of the benefits and opportunities offered by digitalisation and globalisation, among other things.

However, the freedoms that this openness guarantees also create opportunities for malicious state-sponsored actors to conduct activities that undermine national security and thus encroach upon our freedoms. In pursuit of their own interests and their geopolitical objectives, these state-sponsored actors are increasingly deploying a wide range of means that could potentially undermine our democratic state and endanger the stability and openness of Dutch society.

Digital resources are being used by states for the purposes of manipulation (e.g. manipulation of data), sabotage (e.g. by disrupting our critical processes), disinformation (e.g. by distributing false information about elections via social media and other means) and cyberespionage (e.g. seeking to obtain sensitive or confidential information).

Acquisition of and investment in critical national infrastructure or firms that develop high-quality technology could result in an unwanted level of dependence, which could create risks for the democratic rule of law in the Netherlands. The continuity of critical processes could be jeopardised and/or confidential or sensitive information could be leaked. A similar risk could be created via the purchasing of critical services and products. Economic espionage (digital or otherwise) is another significant tool used by a number of states.

Subversion by state-sponsored actors is usually conducted by means of insidious processes that can damage the democratic rule of law and our open society in the long term. Factors that could be compromised include the integrity of political and management decision-making, the independence of the legal system, free and fair elections and fundamental freedoms such as freedom of the press, academic freedom and freedom of speech. Undesirable foreign interference may also spark tension within and between population groups in the Netherlands and isolate them from Dutch society.[11] By means of unwanted interference, state-sponsored actors can also make use of a variety of influencing techniques and manipulate groups such as diaspora communities, students, the media or politicians. Covert funding is sometimes provided for such activities. Another tactic used is the distribution of disinformation.[12]

The strategic approach against threats from state-sponsored actors was submitted to the Dutch Lower House of Parliament on 18 April 2019.[13] This approach consists of generic measures to boost resilience against a variety of threats from state-sponsored actors. In view of the threats posed, the interests at stake and recent case history, the approach will also pay specific attention to the following factors:

1. *unwanted foreign interference focusing on diaspora communities;*
2. *protection of democratic processes and institutions;*
3. *approach to economic security.*

Dutch export control policy also helps to boost resilience against threats from state-sponsored actors by ensuring that exports of strategic 'dual-use' goods, services or technologies do not have unwanted consequences.

2. Combating polarisation via a broad approach based on coexistence

People have concerns about the society they live in and feelings of unease – and even powerlessness – are increasing. There are also concerns about immigration or integration. Others do not feel they are an equal part of Dutch society and feel that they are constantly treated like second-class citizens. This social unease can provide a breeding ground for polarisation and amplification of social divides. Over time, polarisation can weaken social stability in the Netherlands. The survey of citizens' views (COB) conducted by the Netherlands Institute for Social Research (SCP) in the first quarter of 2019 shows that citizens are concerned about increasing differences and polarisation within the community. For this reason, the government will conduct more intensive collaborations to address the issue of polarisation via an overarching strategy to promote coexistence.

As the issue of polarisation is driven by the amplification of differences between social groups, it is vital that the government address all forms of social unease in its policy and communication. Communication will be a vital policy instrument in these efforts. Municipalities and institutions are currently working hard to address polarisation and its effects, and the security chain can also make a significant contribution, e.g. via community police officers who offer a primary point of contact at the neighbourhood level.

3. Intensified approach to protect critical infrastructure

The integrity of critical national infrastructure is an essential factor in the issue of national security. Around 80% of critical processes are run by private parties. Processes are deemed critical based on their expected impact on Dutch national security interests in the event that they are disrupted. The complexity of threats and risks shows that the integrity of information, access to operating and other systems and control over critical national infrastructure or subsections thereof have become important factors in safeguarding national security interests. These factors have come under pressure due to the increasing threat posed by state-sponsored actors and cybercriminals, the increasing online and offline interconnection of systems and organisations and the chain dependences that this creates.

In addition, the issues of which processes and providers (companies, organisations) we need to protect and how we should protect them are constantly subject to change. As a result, we need to adopt a different approach to the system that takes into account how these protective measures are applied not only to the critical providers and processes, but also to chain-dependent factors, businesses,

11 National Security Profile 2016 (National Security Analysts Network, 2016), and Parliamentary Papers 2017/2018, 22233, No. 63.

12 Parliamentary Papers, 2018/2019, 30 821, No. 51.

13 Parliamentary Papers 2018/2019, 30 821, No. 72.

organisations or networks. Responsibility for and knowledge of critical processes is widely distributed across the ministries and the businesses involved and also involves regional and local aspects.

It is very important to the government that consistent and technically up-to-date criteria be used when evaluating national security risks affecting critical national infrastructure, and that clear insight be available into how critical national infrastructure in the Netherlands has been technically and organisationally designed and developed, as this will facilitate timely anticipation of relevant developments. For this reason, the government, in collaboration with all of the parties involved, will develop an intensified strategy for the protection of this critical national infrastructure. A vital part of this intensified strategy is a structure that will pool knowledge, skills and expertise in order to adequately address national security risks relating to critical national infrastructure both now and in the future.

4. Terrorism and extremism: evaluate, intensify and continually develop countermeasures

The battle against terrorism and extremism continues to demand our attention. Malicious actors are still involved in planning attacks in the Netherlands, as was demonstrated by recent events in Utrecht. The threat posed by terrorism and extremism continues to develop.

The recapture of formerly ISIS-occupied territory, the changing strategy of ISIS, the return of travelling combatants into Dutch society, the rise and development of other terrorist groups and possible geopolitical developments (both anticipated and unforeseen) are just some of the myriad factors that complicate this already intensely complex issue. In the near future, the Netherlands will also have to deal with the issue of ex-convicts returning to society after serving their sentence, despite possibly not having renounced their ideology and possibly having made new extremist connections during their detention.

In recent years, work has been conducted to intensify the comprehensive approach in line with the NCTV's National Counterterrorism Strategy 2016-2020. In view of the current threat level, the following aspects of this approach have been reinforced:

- early identification of threats by security services through intensifying investigation into radicalisation and Salafism within the scope of counterterrorism;
- embedding of the strategy against funding of extremism and terrorism;
- boosting digital resilience and strategy against online extremism;
- investment in deradicalisation, rehabilitation and judicial strategy;
- reinforcement of international efforts.

Various types of extremism are on the rise, such as right-wing extremism and identitarian extremism. For this reason, efforts will focus on applying the comprehensive approach against all forms of extremism – regardless of their ideological basis – in order to address 'new' threats as well.

Given the knowledge that the threat is dynamic and uncertain, it remains vital that periodic reflection of the strategy's results be conducted to examine whether the measures are still appropriate to the threat posed at that point in time. In this context, components of the CT strategy 2016-2020 are continually evaluated and the new CT strategy will be formulated based on these findings.

5. Minimise military threats via close collaboration and optimal military effectiveness

The Netherlands' national security is interlinked with world security. In recent years, the primary responsibility of the armed forces – to protect the territory of the Netherlands and its allies – has become increasingly important,[14] although this does not detract from the importance of its other responsibilities. The diversity and complexity of the threats Europe is facing means that the Netherlands and Europe must review their course in order to continually protect our security both now and in the future.

Other countries are substantially boosting their military capacity, as a result of which the military dominance of the Netherlands and its allies is no longer guaranteed. Russia is posing an increasing and comprehensive threat to the interests of the Netherlands, Europe and our other allies. In addition to hybrid, espionage and cyber aspects, this threat also involves a nuclear dimension.[15] Using modern weapons systems, Russia is capable of temporarily or permanently blocking access to disputed areas on land, at sea and in the air or hindering freedom of movement in these areas.

The Netherlands can only combat these threats by means of effective collaboration and active international policy, e.g. via the EU, NATO, the OSCE and the UN. To maintain our status as a credible ally and partner, we will reinforce and further improve the combat power, sustainability and deployability of our armed forces.

In addition to deepening the NATO alliance and European defence cooperation, our armed forces are also equipping themselves for the future in a variety of other ways. Collaboration with civil authorities, the business sector, NGOs, etc. must be facilitated and solidified. We must also anticipate and rapidly respond to new technological developments, acknowledge the increasingly dominant role that information will play in both conflict prevention and warfare and prepare ourselves for conflicts that will simultaneously unfold in a variety of areas of life, including cyberspace.

14 Parliamentary Papers 2018/2019, 34919, No. 1.

15 Draft Public Annual Report (Military Intelligence and Security Service, 2018).

This will require close civil-military collaboration as part of the approach to digital threats and threats from state-sponsored actors.

The objective of the new Policy Document on the Armed Forces, which is scheduled for 2020, is to present a vision and a strategy that defines the role that our armed forces will play in the future given the ever-changing threat level, and what steps must be taken in order to enable it.

6. Highly programmatic approach to combat criminal subversion[16]

Subversive crime includes a wide range of criminal activities conducted with the purpose of undermining society. The terms 'undermine' and 'subvert' predominantly relate to the effects of organised crime: the interweaving of the criminal underworld into legitimate society and its implantation into residential areas and legal sectors. The roots of organised crime are always established in the local community. Perpetrators of organised crime make use of the same legal structures and facilities as regular citizens: transport facilities, financial and legal services, recreational areas, the property market, etc. This interweaving into mainstream society has far-reaching consequences. The combination of substantial criminal assets and access to heavy weapons enables criminal networks to gain influence within social sectors and exercise unwanted social pressure on society. Organised criminals also pose a threat to the integrity of public administration and civil servants, which is detrimental to society's sense of justice, the rule of law and social institutions.[17]

The issue of subversive crime is largely an international problem, although, at the same time, it has strong ties with local communities. In other words, it involves criminal structures that extend around the world, but invest in local roots. As a result, an approach is required that focuses on all levels: local, regional, national and international. The international approach is conducted in collaboration with source countries, transit countries, other EU Member States and neighbouring countries.

Addressing subversive crime is a high priority to the current government and it has therefore adopted a highly programmatic approach to this issue. This approach consists of a wide range of preventive and repressive measures and involves collaboration with a coalition of parties from the government, the business sector and society based on a long-term intensification programme. This approach will be primarily funded by the extra funding specified in the coalition agreement, which will enable the regional parties and national organisations to give a powerful extra boost to the approach. Of the €100 million made available, €85 million will be allocated to regional parties, with the remaining €15 million earmarked to fund national organisations and activities.

The government has elected to develop solid plans 'from the bottom up', involving the parties responsible for executing the strategy in practice: the professionals on the front line who possess the knowledge and expertise about how the strategy can be most effectively intensified.

In addition, an ambitious legislative agenda has been established that fully takes into account the practical needs and wishes of front-line operators as well as constitutional principles. A Strategic Council against Subversive Crime has been appointed to advise the Minister of Justice and Security on how to spend the extra funding and what opportunities to further improve the approach are available. In addition, a task force has been set up that will go out into the field together with front-line professionals and identify concrete opportunities to improve and accelerate the approach. This task force will work closely together with the Regional Information and Expertise Centres and the National Information and Expertise Centre. The establishment of an interim evaluation will boost the learning capacity of the organisations involved and make best practices rapidly available to be shared and – whenever applicable – rolled out at the national level. The lines of accountability to the Lower House of Parliament already run via the Anti-Subversion Programme.

This deployment of the extra resources represents an important step in further improving insight into the problem of subversion, reinforcing the government's executive capacity and boosting government-wide collaboration. These extra resources also enable the approach to be designed in a more thematic manner and encourage innovation of the approach by means of pilots and projects based on the very latest technology.

Subversive and other crime also generates criminal funds. If these criminal gains are not seized, then this will present an incentive for people to commit criminal acts, which in turn will cause significant disruption to our society. It will also erode the sense of justice felt by individual citizens and their confidence that the government is providing effective protection against such crime. The government, together with all partners involved, therefore advocates extra measures and efforts in this regard. In the fight against organised crime and other financially motivated crime, greater focus will be concentrated on exposing criminal cash flows, which will enable more effective interventions to be devised and executed. In addition, we will focus on the four action lines as specified in the Letter to the Lower House of Parliament dated 13 March 2019[18]: prioritising the financial/economic dimension of criminal investigations; continual learning, development and comprehensive connection;

16 The lines of accountability to the Lower House of Parliament already run via the Anti-Subversion Programme.

17 For a more detailed explanation, see: Sluipend gif (Insidious Poison) (Police Academy of the Netherlands, 2018), National Threat Assessment for Organised Crime (Police, 2017) and Ondermijning ondermijnd (Subverting Subversion) (Dutch School for Public Administration, 2016).

18 Parliamentary Papers II, 2018/2019, 29 911 and 31 47 7, No. 221.

internationalisation; and monitoring/adjustment. In the 2018 Budget Memorandum, the previous government made a non-recurrent fund of €30 million available to reinforce the approach for seizing criminal assets.

Based on proposals from ten regional partners and from national partners, a series of concrete reinforcement projects has been devised and initiated. These projects include a focus on boosting comprehensive collaboration and seizure in order to embed the financial and economic perspective into the fight against crime in the Netherlands. In addition, the statutory instrumentation will be optimised. For this purpose, examination will be conducted – based on input from the field and motions passed – of possible areas of improvement in the law to facilitate seizure of criminal assets, particularly within the scope of efforts to combat subversive crime.

Furthermore, it is of vital importance that all legal financial and economic channels used by criminals to launder their money be protected against misuse. The obligations to prevent such misuse have been established in the Money Laundering and Terrorist Financing (Prevention) Act and they are derived from the international standards established by the Financial Action Task Force (FATF) and the European Anti-Money Laundering Directive. This ensures that uniform rules and regulations are complied with when working at the European and international levels. The amendments to the Fourth European Anti-Money Laundering Directive are currently being implemented in the Netherlands. Furthermore, a policy cycle has been established to identify risks of money laundering and to evaluate the approach to money laundering. The reports that have been published on this matter in the recent past have already been submitted to the Lower House of Parliament.[19] The Minister of Finance and the Minister of Justice and Security will submit an action plan for combating money laundering to the Lower House before the summer. Among other issues, this action plan will address the findings of these reports and examine opportunities to facilitate more effective sharing of information between banks.

7. Intensified approach against cyber threats

Our society has become completely dependent on digital devices and cybersecurity has become interwoven into all national security interests. Practically all of our critical processes and services are completely dependent on ICT. As analogue alternatives have almost entirely disappeared and no fallback options are available, our dependence on digitised processes and systems has become so substantial that any damage thereto could result in serious social disruption. Our critical processes are largely dependent on the provision of electricity and data communication services. Any disruption to these services can impact a number of critical processes within as little as a few hours. The range of digital risks to national security are determined by the scale of the cyber threats we face in combination with our current level of resilience.

Risks to digital security have been comprehensively addressed by the Government via the National Cybersecurity Agenda, published in April 2018. This agenda has been formulated in a flexible manner to enable adequate countermeasures to be added against new or intensified threats.

The continual threats, the pressure on resilience levels and our extensive digital dependence demand intensification and acceleration of the strategy against cyber threats. For this reason, extra efforts will be made to boost structural and adaptive risk management within all critical sectors. This will fulfil ambition 7 of the National Cybersecurity Agenda: to boost control of the government-wide approach. In concrete terms, this means that work will be conducted to raise awareness of the risks and the necessary level of digital resilience, to boost and monitor digital resilience, and to increase the government's supervisory capacities in order to ensure all parties involved fulfil their responsibilities and conduct interventions if and when necessary.

Due to the increasing cyber threat level, mutual dependencies and the development of new technologies, it is vital to have a risk-driven strategy concerning exactly what must be protected. Together with the relevant ministries, the national Coordinator for Security and Counterterrorism (NCTV) is going to reassess which interests have the greatest impact on national security and investigate whether critical organisations are sufficiently aware of these vulnerabilities.

Cybersecurity is such a vital issue that support must be provided to all parties involved and monitoring must be conducted to ensure all parties are fulfilling their responsibilities. Together with the ministries and supervisory bodies involved, work is being conducted to reinforce monitoring of digital resilience. For this purpose, basic levels and security objectives are formulated for each sector, enabling the parties involved to fulfil their individual duties of care as derived from the Network and Information Systems Security Act (Wbni). To ensure that the organisations in question fulfil their responsibilities and implement appropriate measures, effective monitoring of digital security is essential.

To make sure that a sufficient level of digital resilience is structurally maintained, collaborative drills and testing are necessary. This government is therefore formulating a broad public-private testing and drill programme. This programme will ensure that the organisations and people involved are capable of responding rapidly and adequately in the event of a crisis.

19 Parliamentary Papers, 2018/2019, 31477, No. 28.

In addition, a certification framework will be established for products, services and processes, derived from the EU Cybersecurity Act.

New technologies such as 5G and AI will result in new and potentially fundamental security issues (both digital and analogue) that will require attention. Within the EU, the Netherlands is becoming increasingly active in the field of cybersecurity via the 'Cyber Diplomacy Toolbox' and the introduction of cyber sanctions, among other methods.

Continual focus on resilience

While some security issues emphatically require extra focus, there are also predominant risks that have already been integrated into the strategy and for which adequate countermeasures are already in place. Given the developments concerning these risks, continual focus is required in order to protect national security. Any reduction of the current approach could result in new risks and threats or cause old ones to rear their head once more.

1. Reinforcement of multilateral institutions

The open society and economy in the Netherlands are facilitated and boosted by the multilateral system of rules and agreements governing trade, security and dispute resolution based on universal values. The IISS shows that the multilateral system as established following the Second World War is coming under increasing pressure. Nation states are now more frequently and explicitly focusing on achieving economic benefits that are relatively national in nature based on a zero-sum attitude to international relations. A similar trend is also apparent on the political and geopolitical stages. This can have consequences for the international rule of law, the fundamental principles of democracy and the universality of human rights, and therefore for the Netherlands' national security interests.

The Netherlands will focus on maintaining and boosting multilateral international systems via agreements and regulations based on universal values. In this regard, the Netherlands will strive – at the EU level – to close the gaps in the World Trade Association's rules to enable a variety of economic systems to operate on a level playing field. For the purposes of combating threats from state-sponsored actors, the Netherlands will strive to boost collaboration within the EU and NATO and will prioritise reinforcement of the multilateral institutions that contribute to national security.

2. Prevention and control of natural disasters

Climate change

Climate change has become an observable fact of life resulting in more frequent bouts of extreme weather, from heavy rain to high temperatures. In summer 2018, the Netherlands experienced 60 hot days in a row and 2 heatwaves. In addition to being extremely hot, it was also extremely sunny and very dry. In total, the Royal Netherlands Meteorological Institute's weather stations measured 2,090 hours of sun, a figure way above the average of 1,639. With an average temperature of 11.3°C, 2018 was the fifth very hot year in a row and, with the exception of 2014, the hottest year since records began. These scenarios are consistent with the upward trend in global temperatures. Among other methods, the Netherlands is striving to achieve climate adaptation and mitigation by implementing measures to reduce carbon emissions and establish climate-proof groundwater and surface water systems, spatial planning and land use (see also the section 'Drought').

Drought

In response to the persistent aridity in 2018, efforts will be made to implement additional structural measures to establish a climate-proof groundwater and surface water system, spatial planning and land use. The water system, which currently focuses primarily on draining away excess water as quickly as possible, must be better equipped to enable retention and infiltration of water. This will enable the groundwater to be temporarily supplemented in the event of excessive rain.

The Ministry of Infrastructure and Water Management is currently working on this project together with all of its water partners, who will be responsible for the following measures:

- The Fresh Water Delta Programme will flesh out plans to boost water availability.
- The Spatial Adaptation Delta Programme will further elaborate the theme of 'drought' for use in stress tests and risk dialogues.
- The Ministry of Agriculture, Nature and Food Quality will take care of the policy objectives relating to the Climate Adaptation for Agriculture and Climate Adaptation for Nature action programmes.
- Municipalities and water boards will conduct stress tests and implement operational measures.

Provincial government bodies will be responsible for the spatial planning of climate-resistant water systems as part of the provincial environment visions and the translation of these visions into policy for municipalities and water boards.

Rising sea level

It is a fact that the sea level will continue to rise throughout this century and beyond. However, how much it will rise and how quickly it will rise is uncertain. Among other factors, this depends on how much greenhouse gas is emitted and how effective international climate policy is. The Netherlands' policy is to achieve the objectives in the Paris Agreement: to limit the increase in the global temperature to 2°C. There is a great deal of uncertainty regarding future emissions and the warming and rise in the sea level that will accompany them. Due to the potentially major implications for the Netherlands, and the Delta Programme in particular, we therefore evaluated the effects of extreme sea level rise that could result from an emission scenario involving a 4°C increase in global temperatures.

The government's objective is to prevent a flood disaster such as the one that occurred in 1953 or river flooding such as in the 1990s. These plans have been formulated as part of the Delta Programme, which has the following objectives:

- to protect the Netherlands from flooding both now and in the future;
- to ensure sufficient supplies of fresh water;
- to ensure climate-proof land use.

The Delta Programme will ensure that the Netherlands is sufficiently capable of withstanding all developments stemming from the effects of climate change and the rising sea level.

Natural disasters, earthquakes, soil subsidence and solar storms

Although these types of natural disaster do occur in the Netherlands and can have a major impact (solar storms can cause disruption and/or damage to communication systems, satellites and the power grid, among other things), they are not considered likely. With the exception of the programmes for earthquakes in connection with gas extraction, no specific national programmes exist for these natural disasters other than the regular crisis preparation measures at the local, regional and national levels.

3. Combating CBRN threats

Proliferation

In the IISS, it is indicated that the proliferation of weapons of mass destruction remains a cause for concern. Some state-sponsored actors and non-state-sponsored actors consider themselves less bound by international agreements, if at all. The risk of accidents, incidents or conflicts involving weapons of mass destruction is increasing. It is therefore vital that insight be gained into the intentions and capacity of state-sponsored actors and non-state-sponsored actors who possess or may possess such weapons and means of delivery. Given the potentially enormous impact that CBRN conflicts[20] or incidents would have on Dutch national security interests, this threat must be given utmost attention.

Within the Netherlands, the intelligence and security services, the police, the Ministry of Justice and Security, the Ministry of Defence, the National Institute for Public Health and the Environment, the Authority for Nuclear Safety and Radiation Protection, social institutions and local government bodies work together tirelessly to ensure timely and adequate identification of CBRN materials (including precursors). However, timely identification within the Dutch borders is only possible if external identification and preventive measures have likewise been effectively organised. For this reason, we collaborate intensively with foreign partners, private institutes and multilateral institutions. A major challenge in this regard is to closely monitor the ability and intent of armed non-state-sponsored actors to use CBRN materials against the Netherlands. So far, these groups only appear to have a limited capacity to convert their technical and logistical capacities into action, but this will remain an area of concern in the near future, so continued investment will be made in detection resources, information exchange and, if necessary, preventive action.

Another important element in the approach to this issue involves boosting social resilience against any CBRN incidents. For this purpose, a variety of organisations and aid agencies have worked together on a multidisciplinary national programme. The Netherlands is a participant in the 2nd EU CBRN Action Plan, the core objectives of which are to prevent attacks, to continually train personnel and to exchange knowledge and expertise between

20 CBRN stands for Chemical, Biological, Radiological and Nuclear.

Member States. This helps to reinforce civil-military collaboration in this area.

Radiation accidents

Radiation incidents relate to any activities (including transport and storage) that involve radioactive materials or devices that can emit ionising radiation. This can range from major incidents or potential incidents at nuclear facilities to minor incidents involving radioactive material at institutions such as hospitals.

The likelihood of a radiation incident at a nuclear facility in the Netherlands is small, as these facilities are extremely safe and comply with strict requirements. Other radiation incidents have a higher likelihood, but a lower impact. The transport of radioactive substances, for example, is subject to extremely strict conditions. In the unlikely event of an incident occurring, emergency plans will come into effect.

4. Combating infectious diseases

In the Netherlands, the risk of infectious diseases is relatively limited, although the risk of an outbreak of an infectious disease, such as a flu pandemic, cannot be ruled out. To ensure the Netherlands is prepared for such an eventuality, central government formulates and executes strategic policy.

The measures for the prevention and control of highly contagious or serious infectious diseases in humans are recorded in the Public Health Act (Wpg). In line with this Act, the Ministry of Health, Welfare and Sport is responsible for the National Immunisation Programme, organised by the National Institute for Public Health and the Environment. As knowledge of vaccinations and infectious diseases is growing, the government is continuously monitoring how the protection provided by the National Immunisation Programme can be maximised. In response to the slight decline in the immunisation level in the Netherlands, the State Secretary for Health, Welfare and Sport has presented a number of improvement measures.[21]

In 2005, the Member States of the WHO (including the Netherlands) made agreements regarding the identification and control of infectious diseases. These agreements are recorded in the International Health Regulations. In the Netherlands, they have been incorporated into the Public Health Act. On the initiative of the Ministry of Health, Welfare and Sport, the Netherlands registered for a Joint External Evaluation (JEE) by the WHO. During the JEE, the preparatory measures that the Netherlands has in place to mitigate public health risks (including infectious diseases) will be evaluated.

Finally, the EU is working together with the Member States to prevent and control infectious diseases and to improve resilience. The European Centre for Disease Control plays a vital role in this regard. The Ministry of Health, Welfare and Sport and the National Institute for Public Health and the Environment closely collaborate with these parties. One concrete example of this European collaboration is the European Commission's Joint Procurement Initiative for pandemic influenza vaccines.[22]

Antibiotic resistance

The rise of antibiotic resistance is a cause for concern that demands a comprehensive and coordinated approach. By means of the antibiotic resistance (ABR) programme, launched in 2015, the government is formulating a comprehensive and strategic approach to the problem. The Lower House of Parliament is regularly kept informed of the progress of this programme. Compared to other countries, the situation in the Netherlands is relatively good. Via international forums, the Netherlands works together with international partners to help improve the situation in other countries. The ABR programme will conclude in 2019. Before the programme ends, the government will examine – in collaboration with parties in the field – whether it should be extended and what adjustments will be required in order to minimise the threat of antibiotic resistance in the future.

Zoonotic diseases

In recent years, no new developments that could affect national security have been observed with regard to zoonotic diseases (diseases that can be transmitted from animals to humans). Measures to prevent, control and combat zoonotic diseases are recorded in the Public Health Act and the Animal Health and Welfare Act (GWWD). The Food and Consumer Product Safety Authority is responsible for monitoring this issue and is authorised to take action. The Centre of Zoonotic Diseases and Environmental Microbiology (part of the National Institute for Public Health and the Environment) coordinates the 'Zoonotic Disease Detection Consultation'. This consultation identifies and evaluates new and existing risks posed by pathogenic microorganisms that could be transmitted to people in the Netherlands from animals, food or the environment. Every year, the National Institute for Public Health and the Environment publishes the State of Zoonotic Diseases report, which contains information and developments concerning zoonotic diseases that are relevant to the Netherlands. The Ministry of Agriculture, Nature and Food Quality and the Ministry of Health, Welfare and Sport possess a shared crisis structure and shared crisis handbooks for zoonotic diseases. These structures are regularly subjected to practical testing.

21 Parliamentary Papers 2018/2019, 32793, No. 338.

22 Parliamentary Papers 2018/2019, 32793, No. 369.

Generic national security instruments

In addition to comprehensive strategies for specific risks and threats, the Netherlands also develops generic instruments for the protection of national security. These include risk and crisis management strategies for all potential or actual incidents, disasters or crises, regardless of their nature or location in the Netherlands,

The expansion of scientific understanding is also a part of this, such as knowledge sharing and the development of new technologies. These instruments contribute to the intensification of the National Security Strategy as a whole. Finally, the periodic review and readjustment of the NSS is also a national security instrument in and of itself.

Development of the generic system of risk and crisis management

In the event of potential or actual incidents, disasters or crises, government bodies work together with private and semi-private partners. Depending on the type of crisis, it must be determined which government policy area is involved, which bodies are designated as competent authorities, which organisations in that policy area participate in a chain and how they relate to each other within that chain. Two types of chain can be established. The general chain deals with general population care (in particular maintaining public order and security) and general disaster response. The partners in this chain include the police, the security regions and the municipalities. The functional chain deals with specific issues, such as power, transport, shipping, food, the environment, etc. Partners in this chain include the Ministry of Defence, the water boards and private sectors and businesses which are of vital importance. Government intervention in the functional chain is generally conducted centrally (by ministers), while intervention in the general chain is conducted at the local level (by mayors). The basic principle of the generic measures is that, to the greatest possible extent, 'new/unknown' crises are addressed within the existing structures. This factor has already been taken into account via the adjustment of the National Crisis Decision-Making Handbook in 2016, which established a more flexible system.

The Risk and Crisis Management Agenda 2018-2021 represents this government's efforts to intensify this system,[23] for example, by ensuring that the function of the Security Regions Act (Wvr) is evaluated in practice. In addition, based partly on the aforementioned developments such as parallelisation of society and increased polarisation (perceived or actual), efforts will also be made to establish future-proof risk and crisis communication to optimise society's capacity to act. Furthermore, civil-military collaboration will be intensified, crisis management in the Caribbean Netherlands will be addressed and cross-regional collaboration as well as collaboration with neighbouring countries will be reinforced.

The results of the comprehensive risk analysis confirm the need to recognise that society and risks to society are continually developing – often slowly, sometimes rapidly. These developments require the Netherlands to continually adapt to and anticipate the ever-changing spectrum of social challenges and the uncertainty that these developments bring. The crisis management system and flexible collaboration within this system must be geared towards this factor.

23 Parliamentary Papers 2018/2019, 30 821, No. 50.

An important point for attention is the observation that the nature and the scale of possible crises are changing. Attacks or digital disruption can occur in a vast range of areas in the Netherlands, causing a variety of chain effects that could have an extremely diverse range of consequences for society. In addition, it could become more difficult to determine the source of possible crises (e.g. in cyberspace) and perpetrators will increasingly be located in other countries. Strategies to combat these types of issues sink or swim based on how effectively the government bodies, public and private security partners (both in the Netherlands and abroad) and citizens are able to cooperate in order to overcome these challenges.

In the light of the aforementioned developments, there is a growing need for a shared strategy and proactive and continual collaboration between the public and private security partners at the national and regional level, as well as within a cross-regional and cross-border context. For this purpose, the provision of essential information concerning the issue of risk management must be improved and an inventory of best practices can be established for collaboration within this new context. Furthermore, the development of new threats and risks will result in adjustments being made to national crisis plans, such as plans in the event of ICT disruptions.

Comprehensive scientific research agenda into the interconnection of internal and external security

The free flow of people, goods, capital and information around the world offers great opportunities for the Netherlands, although it also creates threats. Due to the international nature of these flows, developments in international security are now more directly linked to our own national security. This increasing interconnection between internal and external security demands joint analysis of threats, perspectives for action and the available knowledge, intent, capacity and opportunity to act. One example of more intensive interdepartmental research collaboration is the joint scientific research agenda established by the Ministry of Foreign Affairs, the Ministry of Defence and the Ministry of Justice and Security in 2018. Another example is the attention paid to the theme of security within the mission-oriented top sector policy and innovation policy, coordinated by the Ministry of Economic Affairs and Climate Policy. The objective of the knowledge and innovation agenda is to develop and apply new and innovative solutions to security issues in collaboration with businesses, research institutions and government bodies. The initiatives and the research and other results stemming from this agenda will also be highly relevant to the process of formulating interdepartmental strategy and policy.

Monitoring new technologies and applications and their consequences for national security

Technological developments can have significant implications for national security. New technology and new applications of technology can create both opportunities and threats to national security interests. For this reason, the implications of new developments will be periodically investigated and inventoried. In 2019, on the instructions of the Ministry of Foreign Affairs, the Ministry of Defence and the Ministry of Justice and Security, the National Security Analysts Network and a number of other parties will examine developments in artificial intelligence (AI) and the opportunities and threats for national security that these developments will create.

Periodic updating of the National Security Strategy

The NSS 2019 marks the beginning of a three-year cycle in which developments affecting national security, threats and risks to national security and the degree of resilience to these threats and risks are periodically examined to assess the implications for the strategic agenda, the definition of national security and the approach to national security. To ensure interim developments in the threat level are adequately addressed, a mid-term scan will be conducted during the course of the cycle to examine whether adjustments or supplements to the NSS are necessary. The process of periodically updating the NSS is conducted under the supervision of the Ministry of Justice and Security (via the National Coordinator for Security and Counterterrorism) and as part of a broad collaboration between all of the ministries concerned. In accordance with this cycle, the next NSS is scheduled for 2022, although it will be formulated earlier if the development of threats and risks gives cause to do so.

In conclusion: Development and expansion of the national security approach

National security is a dynamic and multifaceted issue that requires a solid yet flexible approach. The strategic cycle of the National Security Strategy enables the Netherlands to continually protect itself against the development of threats and risks and intensifies the national security approach in a future-proof manner.

The increasing interconnection between risks – as identified by the risk analysis – is a trend that is expected to continue. In our increasingly interconnected world, the safeguarding of national security is becoming increasingly dependent on cooperation and integration. However, this vulnerability also presents a massive opportunity, as the Netherlands is historically renowned for its substantial capacity for cooperation in all areas of life.

Developing the NSS into a comprehensive nation-wide approach

This NSS lays the foundations for a risk management system that will develop into a strategy that spans the entire breadth of Dutch society. National security is an issue that affects everyone, and accordingly, all government bodies, businesses, social organisations, knowledge institutions and citizens must fulfil their own responsibilities in order to realise a secure society.

To achieve this nation-wide approach, a broad collaboration is required in order to implement and develop the NSS, define national security interests, identify threats and risks and organise structural resilience. We will do this via both general and specific measures. In concrete terms, this means we will be engaging partners from different sections of society (via existing networks and other channels) to contribute their knowledge and expertise in order to establish a shared and publicly accessible summary of threats and resilience. This knowledge and expertise will also be used to gauge resilience and intensify the strategic focus on awareness and perspective for action. These efforts are fully in line with our joint responsibility and boost the public and private organisation of national security in order to maximise the effectiveness of the NSS system.

Annex 1

To facilitate effective decision-making concerning the strategic focus on resilience, the risk categories[24] from the National Security Analysts Network's comprehensive risk analysis[25] have been categorised into a number of security issues. These security issues are arranged as follows and a summary of the risks contained in these groups is provided in the section entitled 'Predominant national security risks'.

Threats from state-sponsored actors
- Undesirable foreign interference
- Undesirable foreign influence via hybrid operations
- Threatening of the NL's hub status/supply channels (flow security)

Multilateral institutions and economic resilience
- Pressure on security arrangements
- Disruption of international trade

Critical national infrastructure
- Disruption of critical national infrastructure

Terrorism and extremism
- Terrorism
- Non-violent extremism
- Violent extremism

Military threats
- Military threats
- Hybrid operations via undesirable foreign influence

Undermining of local authorities and criminal subversion
- Subversive crime
- Criminal interference

Polarisation and social cohesion
- Creation of enclaves (non-violent extremism)

Cybersecurity and digital threats
- Digital sabotage
- Impairment of internet services
- Cyberespionage
- Cybercrime

Natural disasters
- Extreme weather
- Wildfires
- Flooding
- Earthquakes

CBRN threats
- CBRN proliferation
- Radiation accidents

Infectious diseases
- Human infectious diseases
- Animal diseases and zoonotic diseases

24 The risk category 'Severe accidents' from the comprehensive risk analysis is not a risk to national security in itself, and was therefore not considered to be part of the efforts to increase resilience.

25 The comprehensive risk analysis by the National Security Analysts Network has been submitted to the Lower House of Parliament.

Annex 2

Table 1

National security interest	Impact criteria
1. Territorial security	1.1 Impairment of the integrity of territory (Dutch or otherwise) 1.2 Impairment of the integrity of the Netherlands' international position 1.3 Impairment of the integrity of cyberspace
2. Physical security	2.1 Deaths 2.2 Serious injuries or chronic illnesses 2.3 Shortages of basic necessities of life
3. Economic security	3.1 Costs 3.2 Impairment of the vitality of the Dutch economy
4. Ecological security	4.1 Long-term damage to the environment and the natural world
5. Social and political stability	5.1 Disruption of everyday life 5.2 Impairment of the democratic rule of law 5.3 Social impact
6. International rule of law	6.1 Impairment of the standards of state sovereignty, peaceful coexistence and peaceful resolution of disputes 6.2 Impairment of the function or legitimacy of or compliance with international treaties and standards relating to human rights 6.3 Impairment of a rule-based international financial or economic system 6.4 Impairment of the effectiveness or legitimacy of multilateral institutions

This is a publication of the NCTV on behalf of the Central Government.

info@nctv.minjenv.nl