# Hybrid threats and societal resilience

Schuwer, H.J.J.; Broeks, J.; Graaf, B. de; Groot, J. de; Haaf, T. ten; Lanschot, N. van; ... ; Jagt, H. van der

Advisory Council
on International Affairs

# Hybrid threats and societal resilience

Advisory Report 126
June 2024

# Advisory Council on International Affairs



**This report was prepared by the**
Peace and Security Committee

**Chair**
Henne Schuwer, LLM

**Vice chair**
Lt Gen (ret.) Jan Broeks

**Members**
Professor Beatrice de Graaf
Jochem de Groot, MA MSc
Maj Gen (ret.) Theo ten Haaf
Nina van Lanschot, MSc
Dr Anna-Alexanda Marhold
Professor Frans Osinga
Dr Gulnaz Sibgatullina
Joris Teer, MSc
Dick Zandee
Anna van Zoest, MPhil

**Former members**
Professor Edwin Bakker
Arend Jan Boekestijn
Lo Casteleijn
Professor Jolle Demmers
Pieter Feith, MA
Lt Gen (ret.) Dirk Starink

**Council advisor**
Dr Hans van der Jagt

**Project staff**
Shila de Vries, MSc
Tessa Postmus, MSc
Quinten Offenberg, BA
Annet Potting

# Table of Contents

# Summary

On 2 July 2022, the Dutch government submitted a request for advice to the Advisory Council on International Affairs (AIV) on the subject of hybrid threats. The request for advice notes that hybrid activities represent a growing threat to national and international security. How can the government – and Dutch society – be better prepared for such threats?

Hybrid conflict is said to exist when certain, often non-military instruments of power are orchestrated and strategically deployed as weapons, without this amounting to armed conflict. Examples of such instruments include political subversion, cyber activities, disinformation, economic destabilisation, corrupt financial practices and actual attacks on critical infrastructure. These are activities which undermine our open society and our democracy under the rule of law, and which take place below the threshold of force, in other words without crossing the legal boundary between war (in the sense of armed conflict) and peace. The threats tend to occur in domains in which the armed forces do not traditionally operate, in the grey zone between war and peace. Hybrid threats, both national and international, are mainly designed to undermine society as a whole, thus putting societal resilience under pressure.

In its advisory report, the AIV discusses the multifaceted phenomenon of hybrid threats from three different perspectives: physical, virtual and cognitive. The physical dimension relates to the world as we experience it through sensory perception. The virtual dimension concerns the processing, protection and dissemination of information. The cognitive dimension is the entirety of perceptions, observations and intentions in society. In addition to the obvious threats in the physical dimension, the AIV focuses in particular on the impact of hybrid activities (or attacks) on the virtual and cognitive dimensions, given that governments find it very difficult to anticipate this type of threat effectively in terms of policy. Physical attacks tend to be more visible and easier to attribute. Furthermore, it is usually clear from the outset who is responsible for physical security and protection; generally speaking, this is also fairly well organised. By contrast, there is much uncertainty about virtual and cognitive attribution and protection.

**Geopolitical urgency**

An open, democratic society is vulnerable. It would clearly take little to disrupt key and vital sectors where 'critical processes' take place, whether in the field of water management, telecommunications, energy, transport, water supply, the production and storage of chemical and nuclear goods, public order, finance or democratic processes. This kind of disruption affects people's socioeconomic security and has wider economic and social repercussions. The primary aim of such attacks, however, is to create psychological effects: fear and uncertainty, diminished confidence in institutions or a general distrust of other people or government authorities.

Hybrid conflict is used to gain a more favourable political and military-strategic position. Rising numbers of both state and non-state actors appear to be using a multitude of hybrid instruments. Russia is often cited as an example in academic literature. Russian military doctrine makes no distinction between conventional and unconventional operations, deliberately focusing on non-military activities such as interference in democratic elections or the funding of anti-democratic proxies.

China equally makes active use of hybrid instruments. Outside its borders, the Chinese state purposefully and actively uses psychological tools and the influencing of public opinion as a means of conflict. The United States also uses hybrid methods and has on several occasions in the past been active at political and diplomatic level in undermining governments, bringing down dictatorships or putting countries under political and economic pressure.

The NATO allies and EU member states are also specifically addressing hybrid threats, both defensively and offensively. The phenomenon of hybrid threats has been incorporated in NATO strategy since 2015, and hostile hybrid activity has been regarded as a justification for the invocation of Article 5 since 2016. In addition, numerous new partnership initiatives and investment programmes have been launched to combat hybrid threats.

The EU takes hybrid threats very seriously. A hybrid threat could trigger Article 42.7 of the Treaty on European Union under which EU member states support each other in the collective defence of the European Union. This applies to both conventional and hybrid attacks.

The EU aims to combat hybrid threats and increase awareness of hybrid threats among member states through numerous initiatives, such as the creation of the EU Hybrid Toolbox, which offers member states a host of instruments to counter hybrid threats. In addition, the specially designed 2020 European Democracy Action Plan and the Defence of Democracy package presented in December 2023 focus on improving the resilience of European democracies, including in respect of external interference. Furthermore, the EU is investing through the European Defence Agency (EDA) in specific hardware and software for new technologies, partly with the aim of countering threats in the virtual and cognitive dimensions.

A key component of today's hybrid threats is made up of increasingly assertive non-state actors. Threats are more and more often the work of terrorist groups or individual civilians, whether or not deployed as proxies by state actors. Furthermore, because many hybrid attacks are carried out using new, often dual-use technologies, large multinational tech companies, global corporations or influential individuals are increasingly involved, wittingly or unwittingly, in modern-day conflicts. On the one hand, they are targets; but on the other hand they are also used as resources.

**The need for further development of international law**

In terms of international law, the phenomenon of hybrid threats is a complex issue. What does the non-intervention principle mean in the context of hybrid threats? Traditional warfare is governed by international humanitarian law and international agreements providing guidelines for the use of force, the treatment of prisoners of war and the protection of civilians. The issue is, however, that hybrid threats occur below the legal threshold of armed conflict. International humanitarian law was not developed with such threats or conflicts in mind. That means that a development of the law is required in respect of hybrid conflict, in which underlying legal principles and human rights apply. Furthermore, how do we prevent the militarisation of civic space in our open democracy? State obligations stemming from human rights are crucial in dealing with hybrid threats and providing protection against them.

Hybrid threats present new challenges in respect of the mandate and statutory framework for the Dutch armed forces too. The armed forces' tasks are laid down in the Constitution, on the basis of which three main tasks were formulated by the Ministry of Defence. Given that hybrid threats – particularly those in the virtual and cognitive dimensions – are not being adequately addressed, the AIV calls on the government to work with legal experts to scrutinise the definition of these main tasks and amend it as necessary, to enable the armed forces to equip themselves and prepare for future threats more effectively.

**Towards greater societal resilience**

Paradoxically, Dutch society and other democracies are under pressure precisely because of their free and open nature. On the one hand, that openness is a great strength and worthy of protection. At the same time, there is an inherent vulnerability. It is vital that the government act proactively whenever Dutch interests are at stake, and that may come at the expense of some of that openness and freedom.

Hybrid threats (or actual attacks) can affect society on many fronts. A whole-of-government approach is therefore required, as is a whole-of-society strategy. All elements of Dutch society should be part of a broader approach to security.

The AIV regards Finland's comprehensive security approach – a society-wide state of preparedness in respect of security issues – as an example of how societal resilience can be strengthened. Although Finland differs from the Netherlands in many respects, there are certainly lessons to be drawn from the Finnish approach. The Finnish government is committed to strengthening civic engagement as well as psychological resilience. Interoperability between national, international and EU counter-measures is being enhanced, as is collaboration between government, including the Ministry of Defence, and national stakeholders. In addition, the protection of critical infrastructure and the vital functional capabilities of society and of services, including emergency services, is addressed specifically, thus helping to boost societal as well as economic resilience.

In the Netherlands too, society as a whole will need to contribute to societal resilience. Article 99a of the Constitution provides for rules to be laid down concerning this joint responsibility. The Dutch government's current approach does not adequately match the broad impact of hybrid threats. Despite some good initiatives, such as the Government-wide Response Framework against Hybrid Threats, the government's response in the face of a threat is often reactive, incident-driven and fragmented. In many cases, this approach leads to the ad hoc creation of crisis teams or a sector-based response. A course of action such as this may well work in the short term, but in order to be well prepared, resilient and quick to respond effectively in the long term, much more is required. There also seems to be a lack of awareness in society as to how significant the impact of potential hybrid attacks or specific threats may be. This awareness needs to be heightened, for example by introducing a national security course based on the Finnish model and expanding the national security course provided by the Netherlands Defence Academy and the National Academy for Crisis Management, which falls under the National Coordinator for Counterterrorism and Security (NCTV), as well as by introducing a form of social conscription, increasing public involvement in political decision-making through citizens' assemblies and expanding the number of reservists.

The Netherlands must therefore show stronger commitment to complying with NATO's seven baseline requirements for national resilience, which focus on the continuity and operation of government services, energy supplies, food and water resources, the ability to deal with large movements of people, the ability to deal with mass casualties, and functioning communications and transportation systems; in other words, the critical processes needed to keep society functioning in times of crisis or war. These requirements should be followed up and aligned with existing EU initiatives designed to counter hybrid threats. The AIV believes, however, that they do not adequately address the threats in the virtual and cognitive dimensions.

The AIV is of the opinion that the Netherlands would benefit from a proactive, anticipatory and comprehensive approach to national security. It notes that the Dutch response to an acute threat is too sector-based and often focused on damage limitation. The AIV further observes that there is a need for anticipation and timely exchange of information to prevent threats and promote policy coherence in order to ensure the necessary consistency across the different sectors. This should be directed by the National Security Council (NVR), established in 2022. The NVR should assess the situation in the Netherlands at least twice a year, concentrating on a vulnerability analysis and a resilience strategy focused specifically on hybrid threats. The NVR should be more effective and operational in nature and should, wherever possible, stand above the ministries, reporting directly to the prime minister. All ministries must be represented in the NVR, as well as financial institutions, security services, businesses and knowledge institutions. A comparison between the threat analysis and the vulnerability analysis should reveal the level of investment required and lead to a plan of action that justifies the investments.

# Recommendations

Hybrid conflict is a many-headed beast. The AIV's advisory report examines many aspects of hybrid attacks, looking in particular at their societal impact in the physical, virtual and cognitive dimensions. Given the great geopolitical urgency and the need to invest in societal resilience, the AIV presents 10 incisive recommendations for the Dutch government.

## ► Society:

1. **Invest in societal resilience and national awareness in respect of hybrid threats.** The issue of hybrid threats affects all of society. It requires a collective change in mentality and a stronger national narrative: Dutch citizens must be aware of threats. In accordance with Article 99a of the Constitution, therefore, the whole of society must collaborate to increase societal resilience: the public, government authorities, private companies, knowledge institutions, civil society – everyone has a key role to play. The AIV also recommends developing a national security course, inspired by the Finnish model, to be offered to Dutch citizens. The national security course provided by the Netherlands Defence Academy and the National Academy for Crisis Management should be developed further and implemented more widely, specifically for those in leadership positions in government, business, civil society organisations such as media and NGOs, and utility companies operating in critical infrastructure; this is to create a shared threat assessment and provide potential courses of action in the context of resilience. It is vital that civic participation be increased in this respect. The AIV is of the opinion that citizens' consultations would be useful in generating support for societal resilience. Through citizens' assemblies, selected by lottery, in which citizens can participate in policy and decision-making processes, society will come to view the issue of security as a collective responsibility. This will also help to boost pluralism as an essential condition for a healthy democracy.

## ► The dimensions:

2. ***Physical:***
   **Protect critical infrastructure, communications and national interests, and address unwanted foreign influence.** An open, democratic society such as the Netherlands is vulnerable. There is an urgent need to step up the protection of critical processes that keep society functioning, and collaboration with businesses, financial institutions and knowledge institutions is essential in this regard. Because a great many public and private actors are involved, these efforts need to be coordinated by the government, taking a whole-of-government and whole-of-society approach. The AIV recommends focusing particular attention on the dissemination of disinformation and the undermining of public order and our democracy under the rule of law. In the case of water management, outdated processes should be modernised and the security of the drinking water supply system should be tightened. Security for the transportation sector and the production of essential goods also needs to be improved. The operational scope for the protection of the financial sector needs to be reinforced in order to enhance financial security, and the security of digital networks, telecommunications and energy supplies should be tightened. Knowledge institutions also need to explicitly take on their share of responsibility for overall security. Collaboration can be sought in an EU context wherever it is deemed likely to bring benefits.

3. ***Virtual:***
**Combat disinformation and regulate social media companies and their platforms.** The influence of tech firms, social media companies and online platforms on the Dutch public is immense. Together with other EU countries, the government should take a critical look at how tech firms and social media companies design their platforms and remind them of their duty of care. With regard to disinformation, the government should develop an education curriculum to promote media literacy and the ability to recognise disinformation. The government should also aim to strengthen a pluralistic media landscape, both online and offline, partly with a view to fortifying democratic processes and institutions.

4. ***Cognitive:***
**Take the Government-wide Response Framework against Hybrid Threats as a guideline, but look more specifically at the virtual and, in particular, the cognitive dimension.** The new Security Strategy for the Kingdom of the Netherlands contains recommendations for a new and strategic security policy, including 12 lines of action, the key elements of which are to work towards a resilient democracy under the rule of law and increased societal resilience, focus on education and protect the Netherlands' critical processes. Threats that may have psychological effects on society need to be investigated further; narratives endorsing the Netherlands' open society, democracy, rule of law and free way of life should be amplified. This should be aligned with the European Democracy Action Plan and the Defence of Democracy package.

### ► Development of the law:

5. **Work towards worldwide regulations under international law regarding attribution and punishment of irregular, unconventional warfare and work on prevention.** A more stringent additional protocol should be developed within the Geneva Conventions, to enable punishment for attacks, particularly in the virtual and cognitive dimensions, that are currently not covered by international humanitarian law, or international law in general. In all cases, existing international and European law provides the guiding principles and also applies to hybrid attacks. The AIV is of the opinion, however, that rules of law should be updated and that further development of the law pertaining to state responsibility and individual liability with regard to hybrid threats is needed. The Netherlands should take a leading role in this matter.

### ► A whole-of-government approach:

6. **Strengthen the National Security Council and ensure good governance.** Prevention of and protection against hybrid attacks requires an integrated approach by national and local government, the private sector and society as a whole. If there is to be collaboration between the different tiers of government, a whole-of-government approach is needed, as is improved interministerial coordination. To this end, the National Security Council (NVR), as the central security authority, requires a more robust mandate. The government should explore the best way to embed the NVR, on the basis that it is a national operations centre with supra-ministerial authority. The government should also investigate how the NVR can be rendered more effective and operational in a practical sense, with the agency positioned above the ministries wherever possible and reporting directly to the prime minister. All ministries would need to be represented in the NVR, as would financial institutions, security services, knowledge institutions and businesses. A comparison between the threat analysis and the vulnerability analysis should reveal the level of investment required and lead to a plan of action that justifies the investments.

7. **Delegate and mandate clearly and combat threats in the virtual and cognitive dimensions, appoint a rapporteur on digital affairs and invest in national training and education with regard to resilience, including cyber resilience.** In terms of the hybrid domain, the Netherlands Defence Intelligence and Security Service (MIVD), the General Intelligence and Security Service (AIVD) and the National Coordinator for Counterterrorism and Security (NCTV) must be given greater powers to identify new types of threat at an early stage, particularly those in the virtual and cognitive dimensions, within the context of the new Intelligence and Security Services Act (WIV), in which supervision is strictly defined. The AIV also deems it necessary to appoint a rapporteur on digital affairs. The right of citizens to be protected also means that citizens must be in a position to protect themselves effectively against digital threats; the government must ensure that this is the case. Digital illiteracy must be actively addressed; the provision of national digital literacy courses could help in this respect. In addition, the Dutch government should further investigate the dangers of the open internet, including the monitoring of subversive networks. At the same time, freedom of expression must be protected at all times. The training of ethical hackers for central government should also be rolled out more quickly; these hackers make the work of cybercriminals more difficult, protect citizens online and help to bolster the cyber resilience of the Netherlands.

## ► Preconditions:

8. **Revise the definition of the main tasks of the Dutch armed forces.** The current definition of the main tasks dates from 2000 and does not adequately cover today's multitude of hybrid threats, particularly those in the virtual or cognitive dimension. As a result, the Dutch armed forces have insufficient operational power to arm themselves effectively against any future attacks. The government must seek definitions that are more in keeping with today's world, taking account of the use of new technologies and threats in all dimensions. The Ministry of Defence should also focus more emphatically on the interaction between government and the public and engage more closely with the whole-of-society approach.

9. **Implement and build on measures and guidelines from the EU Hybrid Toolbox at national level.** Within the EU, the Netherlands should focus on international cooperation to counter hybrid threats. The EU Hybrid Toolbox should be rolled out further and the Netherlands should place greater emphasis on developing tools to counter attacks or threats in the virtual and cognitive dimensions. Alignment should also be sought with the European Democracy Action Plan and the Defence of Democracy package and the measures and guidelines they offer for the Netherlands to develop further and implement at national and subnational level.

10. **Foster interoperability between NATO countries in their approach to hybrid threats.** In respect of cyber resilience in particular, complementary to conventional military deterrence, allies will need to collaborate intensively. There also needs to be greater interoperability between the allies' digital infrastructures, and improved collaboration is needed in the field of intelligence. In addition, NATO must look at whether and, if so, how Article 5 should be invoked in the event of a cyberattack. Article 3 should also be complied with to reinforce collective resilience goals, both military and non-military. The AIV regards the agreed seven baseline requirements and NATO's collective resilience goals as guiding principles for the Netherlands, and the Netherlands should make a concerted effort to pursue these resilience goals in all dimensions of hybrid conflict.

# Introduction

On 2 July 2022, the Dutch government submitted a request for advice to the Advisory Council on International Affairs (AIV) on the subject of hybrid threats.[1] The request notes that hybrid activities pose a growing threat to national and international security. The shifting balance of power, mounting geopolitical rivalry and advances in respect of new technologies are causing huge changes in the international security situation. These developments have implications for the Netherlands' national security in a great many areas.

**Method**

Over the past two years, the AIV conducted an in-depth study of the phenomenon of hybrid threats. The advisory report is based on an extensive literature review and interviews with more than 70 experts, including public administrators and representatives from the private sector, banks, educational institutions, various ministries and the security services. The AIV is extremely grateful to these people for their time and input.

**Structure**

The structure of this advisory report is as follows. The first chapter explains the concept of hybrid threats and provides a definition. The second chapter focuses on national vulnerabilities and the impact of hybrid activities on different sectors of society. The third chapter describes the geopolitical urgency and international developments. The fourth chapter discusses the legal framework. The fifth chapter looks at how societal resilience in the Netherlands can be enhanced. The recommendations for countering hybrid attacks and enhancing societal resilience can be found at the beginning of this advisory report.


KY
95-93
C10
C12

Chapter 1

# Hybrid threats

## 1.1 Non-military threats

A conflict does not have to be fought out by military means to nonetheless be disastrous and have major repercussions. Every day, Dutch society is targeted by attacks on many fronts even though the Netherlands is not at war. To what extent is Dutch society equipped to deal with attacks of this kind? In this report, the AIV examines many threats, such as those posed to our democratic rule of law and to water management.

**Dutch democracy**

Increasing numbers of foreign actors are actively attempting to undermine democratic processes in the Netherlands, such as free and fair elections. One of the main tools used for this purpose is the dissemination of disinformation via social media and networked online groups, whereby misleading information is deliberately propagated with the aim of causing harm to a country. The effect of misleading information is magnified by the use of artificial intelligence (AI), including generative AI, with which alternative 'truths' can be created.

Russia in particular is very active, as illustrated in an analysis by NATO's Committee on Democracy and Security.[2] The state is using disinformation, deepfakes and conspiracy theories to sow division in the European Union.[3] The Czech Republic's Security Information Service (BIS) reported recently that European (including Dutch) politicians had allegedly received money in return for spreading pro-Russian propaganda[4] and that Russia was aiming to roll out an influence operation in Europe in the run-up to the European Parliament elections in June 2024.[5] China is another actor that is becoming increasingly active and is adopting Russian tactics to an ever-greater extent in what has been referred to as the 'Russification' of Chinese influence operations.[6]

These hybrid tactics undermine Dutch democracy under the rule of law. The democratic system benefits from free and fair elections. Every message about a potentially corrupt European or Dutch politician undermines trust in democratic institutions. And that trust is already at a low level. Particularly since the COVID-19 pandemic, the lockdowns and the drastic government actions taken in 2020-2022, there has been profound mistrust among some Dutch citizens towards the government, the media, the judiciary or science. These people find and nurture each other through social media and networked online groups. In a phenomenon analysis in April 2024, the General Intelligence and Security Service (AIVD) warned of the growing group of 'sovereigns', also referred to as 'sovereign citizens' – Dutch citizens who want to reject the authority of the state.[7]

This development shows that hybrid threats, such as the subversion of Dutch democracy, are not necessarily posed exclusively by foreign actors. Domestic actors also engage in such activities or are co-opted and instrumentalised by foreign actors. The cross-border interaction, digital or otherwise, between malicious foreign and domestic actors makes the task of countering hybrid threats highly complex.

**Dutch water**

Dutch water management is also susceptible to hybrid attacks. The Netherlands is renowned all over the world for its water management expertise. Various reclamation projects, such as the Beemster Polder, have even earned a place on UNESCO's World Heritage list.[8] NATO has designated Dutch ports as major European 'landing stages' for military supplies from the United States and the United Kingdom in the event of a continental conflict involving NATO countries.

Precisely because of the Netherlands' unique location, however, water also represents a key vulnerability and a national Achilles heel. Using new technologies, large tracts of the Netherlands could be flooded in a short space of time. Sabotage of dykes, pumping stations and flood defences could cause major disruption. Haarlemmermeer, for instance, a municipality that is home to 160,000 residents and the entire infrastructure of Schiphol airport, including various highways and rail links, could end up under a metre of water very quickly. There are polders where flood waters could rise rapidly to more than two metres in the event of a dyke breach.

The water authorities are targeted by many cyberattacks, some of them minor, every day. In the event of a major hack, sabotage such as this could have direct implications for water management. Digital signals, monitoring, measurements and the operation of bridges, locks and flood defences could all be manipulated as a result. The Netherlands' water supply could also be affected by a cyberattack. The Netherlands Court of Audit raised the alarm about this back in 2019.[9]

## ► 1.2 Hybrid attacks

A hybrid attack can take place without the occurrence of an actual war situation and without crossing the legal boundary between war and peace, in other words below the threshold of force. Such activities also tend to occur in domains in which the armed forces do not traditionally operate, in the grey zone between war and peace. The threats are not necessarily directed at the military, but are intended to undermine society as a whole.

In the case of hybrid conflict, it is not always clear who the perpetrator is or with whom responsibility lies, thus making attribution difficult. A hybrid attack could be carried out either by a state or non-state actor, or by military personnel (combatants) or civilians (non-combatants). The distinction between them is sometimes lost in hybrid attacks, making it difficult for governments to counter them. Furthermore, it is not always immediately clear whether an attack is actually a hybrid attack or, for example, a terrorist attack.

The changing international dynamics and the emergence of new technologies require the state to have instruments at its disposal that enable effective countermeasures against hybrid attacks.

## ► 1.3 DIMEFIL as a framework of instruments for the state

Hybrid conflict has been around for a very long time. For centuries, non-military means have been deployed to gain a particular politico-strategic dominance over a hostile power. Manipulation, psychological warfare, influencing methods and deception are age-old instruments of power.[10] There is therefore a history behind the concept of hybrid conflict.[11] Modern hybrid conflict, however, is of a different nature to earlier variants; today, hybrid instruments are more comprehensive, the players are more numerous and the potential impact of hybrid activities is greater.

The government's request for advice defines hybrid conflict as the integrated use of means covered by the acronym DIMEFIL (see text box).[12]

## DIMEFIL

**Diplomacy.** Hybrid activities in the diplomatic domain could include the suspension of treaties, obstruction of international decision-making and the creation of competing alliances in existing dominated structures.

**Information.** Attempts are made within the information domain to use the dissemination of disinformation to create doubt in the decision-making processes of governments and citizens.

**Military.** Attempts are made within the military domain to use the deployment of conventional military means, military interventions or humanitarian aid demonstratively.

**Economic.** Instruments in the economic and financial domain include the restriction of access to markets, trade routes, raw materials or energy supplies; foreign takeovers or investments; the creation of strategic dependencies through monopolisation or the imposition of economic sanctions or boycotts.

**Financial.** Financial instruments can be used to exert pressure on financial markets in order to reduce government power and undermine political support.

**Intelligence.** Intelligence can be used to develop an alternative political narrative. Influencing (of politicians, media, students, public opinion) and interference (in foreign diaspora communities, for example) can be effected through intelligence services.

**Legal.** Within the legal domain, a hybrid threat campaign could involve raising or lowering legal thresholds or obligations, evasion of liability or the abuse of legal processes to create a new narrative.

This acronym defines hybrid threats on the basis of the principle of state power. That means that the instruments described are exclusively state-based in nature.[13]

This definition places less focus on threats posed by non-state actors, although cyberattacks, disinformation campaigns, the subversion of democratic processes or the cutting of submarine cables could also be carried out by groups or individuals, whether or not they are operating as proxies. Businesses, universities and other knowledge institutions can also be targeted by hacks, commercial espionage and financial blackmail carried out by non-state actors, as shown by the AIVD in a recent publication.[14]

Besides the threat posed by non-state actors, this DIMEFIL definition also pays insufficient attention to the role of new technologies produced for both military and civilian purposes ('dual-use technologies') even though these are in fact increasingly used in hybrid attacks.

## ► 1.4 The dimensions: physical, virtual and cognitive

The broad nature of hybrid attacks, the multitude of potential actors and the possibility of adding conventional military means into the mix make it difficult to give a precise definition of the concept of a hybrid threat. To be able to give specific advice and to delineate the study as clearly as possible in terms of policy, the AIV has looked at three dimensions in which hybrid attacks occur: the physical, virtual and cognitive dimensions.

**Physical**

Military doctrine still regards the physical component as the most important and as playing the guiding role in strategic decision-making.[15] The physical dimension represents the 'real world', which involves physical activities, people, cultures and the interaction between them, as well as the hardware side of information systems and cyber operations.[16] This dimension includes persons (individuals, decision-makers), command-and-control systems, media, and communication technologies such as computers and infrastructure. Military forces are primarily set up to respond to physical threats. Governments use conventional military means to gain a politico-strategic advantage.

**Virtual**

The virtual or information dimension concerns the processing, protection and dissemination of information. Activities in this dimension influence how and where information flows land.[17] The rise of disruptive technologies, such as AI (including generative AI) and quantum technology, will make the virtual world even more closely entwined with the analogue world. The virtual world has become an integral part of life for many; people have become dependent on it. And therefore, at the same time, this dimension represents a huge vulnerability.

The virtual world gives potential aggressors the opportunity to change people's experienced reality. Generative adversarial networks can, for example, enable the creation of lifelike deepfakes – extremely realistic but fake photos and video images of famous and ordinary people and situations.

In a major publication, American think tank RAND draws attention to the burgeoning virtual dimension, warning that virtual activities could cause persistent disruption and manipulation. Particularly with the rise of the Internet of Things and generative AI, as well as algorithmic and big-data-driven decision-making, digitalised societies such as the Netherlands are becoming dependent on networks for information and data collection, sharing, communication, analysis and decision-making.[18]

The front lines of conflicts are increasingly being contested in the covert sphere of intelligence sharing, information dominance, disinformation, data analysis and encryption. Because these threats occur out of sight of the media and society, they often appear invisible. They have a significant impact nonetheless. The AIV explicitly draws attention to the risk of underestimating this dimension.

**Cognitive**

The cognitive dimension could be defined as the entirety of personal perceptions, opinions, observations and intentions (fed by both the physical and virtual dimensions). It involves all aspects of the intellectual, subconscious and emotional functions that determine human decision-making.[19] This dimension covers both individuals and groups and their beliefs, norms, motivations, experiences, emotions and so on.

An attack in the cognitive domain revolves around the creation of a powerful psychological effect, involving deliberate efforts to change world views and perceptions.[20] A vast array of means could be deployed with the aim of transforming the awareness or behaviour patterns of the target.[21]

Psychological warfare, or 'psywar', and the creation of contradictory perceptions have long been used in conflicts, with varying degrees of success. Since time immemorial, physical military means have been deployed in combination with psychological means to ultimately break a nation's mental resilience. Today, these means seem to be applied not only in wartime, but also in times of peace. Researchers expect that there will be an expansion of the role of psywar in peacetime policymaking.[22] And that this battle, fought with virtual instruments, will be played out in the cognitive dimension.

**A war of perceptions**

Physical attacks tend to be more visible and easier to attribute than a virtual or cognitive attack. Furthermore, it is usually clear from the outset who is responsible for physical security and protection; generally speaking, this is also fairly well organised. By contrast, there is much uncertainty about virtual and cognitive protection.

The AIV maintains that hybrid conflict is ultimately designed to influence the cognitive dimension through attacks in the physical dimension (on infrastructure, for example) and by using the virtual dimension.[23] Hybrid threats are increasingly resulting in a battle of perceptions. With the rise of new technologies such as AI, therefore, activities in a networked society such as the Netherlands are proving capable of generating a greater disruptive effect. And that effect is sometimes felt in the physical world too.

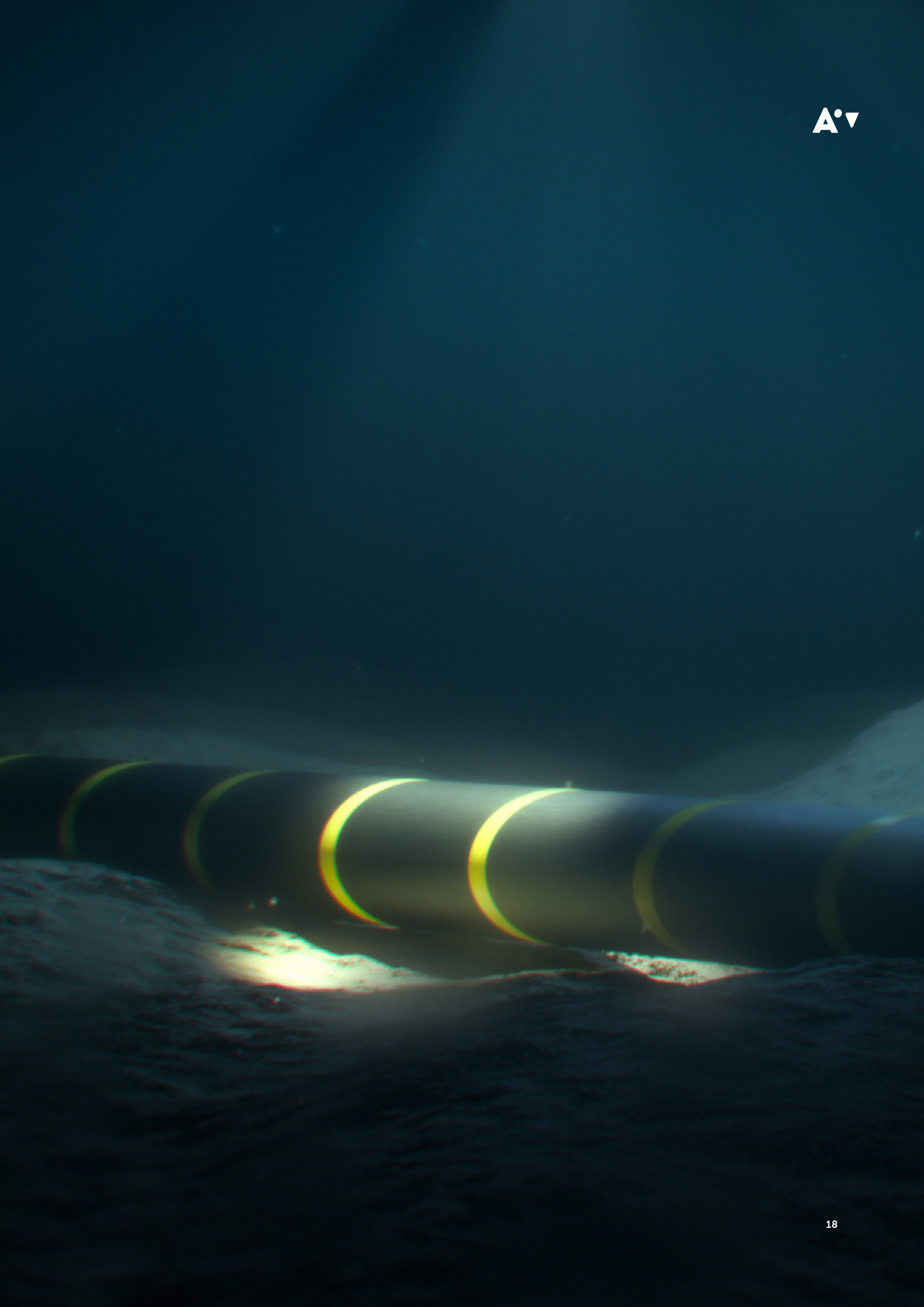
The ultimate aim of a hybrid attack is to change the interpretation of a situation by an individual and in the mass consciousness. The Dutch response in terms of policy should therefore focus more heavily on the virtual and cognitive dimensions. The AIV is of the opinion that national policy frameworks do not take sufficient account of this effect, as a result of which an appropriate response is lacking.

## ► 1.5 Conceptualisation and definition

The Security Strategy for the Kingdom of the Netherlands, published in April 2023, defines hybrid threats as '…threats to national security that manifest themselves largely below the level of open armed conflict. In hybrid conflicts, state and/or non-state actors use multiple means aimed at achieving certain strategic objectives. Such means may include the use of military intimidation, espionage and sabotage, cyberattacks, disinformation campaigns, undesirable foreign interference in diaspora communities, knowledge theft or economic instruments.'[24]

The AIV largely adheres to the core of this definition in the Security Strategy, but also feels at liberty to add elements to it. To provide even-handed advice, the AIV uses a definition which takes account of a certain balance. Too broad a definition would prove unusable for government and parliament, but too narrow a definition would be at the expense of comprehensiveness. This is certainly true where the impact of new technologies or private companies is concerned, although a broader definition would also seem needed given that many hybrid threats do not necessarily arise in the physical world, but increasingly in the virtual and cognitive dimensions. With this in mind, the AIV has adopted the following definition.

> Hybrid conflict is the deliberate infliction of harm in the physical, virtual and cognitive dimensions, using a combination of non-military and military means, such as manipulation, blackmail or sabotage, to achieve certain political or ideological objectives, carried out by both state and non-state actors at the international and national level.



Chapter 2

# National security under pressure

Hybrid activities undermine social cohesion, political stability, economic activity and technological development. In today's globalised and networked world, open democratic societies such as the Netherlands are particularly vulnerable. Interference in democratic processes, commercial espionage, cyberattacks, disruption of critical infrastructure and the abuse of migration flows are just a few examples of the broad range of hybrid instruments that can be used as offensive weapons against open societies. In this chapter, the AIV highlights a number of vulnerable sectors.

## ► 2.1 National vulnerabilities

The National Coordinator for Counterterrorism and Security (NCTV) has designated a number of sectors in which processes take place that are vital for Dutch society to be able to function. These are the energy sector, telecommunications, transport, drinking water supply, water management, production and storage of chemicals and nuclear materials, financial processes, government functions, public order and security, and deployment of the military.[25] The AIV has highlighted a number of sectors for which it will elaborate and examine the actual and potential threats. This does not mean that there are no threats to other (unmentioned) sectors or that such sectors do not involve critical processes.

**Public order, democracy and disinformation**

One disastrous effect of hybrid threats that should not be underestimated is the subversion of democracy and the legal order. This threat predominantly arises in the virtual and cognitive dimensions.

The gap between the government and the public has widened, fuelled by years of widespread government failure in relation to the childcare benefit system affair, the earthquakes caused by natural gas extraction in Groningen and the nitrogen crisis. Disinformation can help to turn criticism of the government into an anti-government mindset. It is partly due to developments such as these – not only in the Netherlands, but also in many other European countries as well as in the US – that the public domain is increasingly becoming a battleground for competing world views, conspiracy theories and alternative truths.

The AIVD, the Netherlands Defence Intelligence and Security Service (MIVD) and the NCTV in their annual 'Threat Assessment State-sponsored Actors' are increasingly reporting deliberate attempts to encourage or exploit certain anti-government sentiments among the public.[26] According to this state threat assessment, the tactics used have included the dissemination of disinformation, media campaigns, hack-and-leak actions, the mobilisation of particular groups and individuals, and financial, facilitative or ideological support for such activities, as well as the covert influencing of individuals, politicians and political decision-making.[27] Fuelled by social media, the line between Dichtung und Wahrheit – as once described by Goethe – would in some cases appear to be wafer-thin.

There is a growing number of people in the Netherlands who are involved in creating a parallel society and another group of people ('sovereign citizens')[28] who want to withdraw from society altogether. The AIV regards these developments as a cause for concern. There is still too little public awareness of this threat and the normalisation of this kind of thinking undermines the rule of law.

The task of countering disinformation is proving to be highly complex. The AIV specifically highlights the risk of targeting proven facts, subjective opinions or other personal opinions that are at odds with a particular view, under the guise of countering disinformation. However, the right to freedom of expression must be protected at all times.

Article 10 of the European Convention on Human Rights (ECHR) and Article 11 of the Charter of Fundamental Rights of the European Union protect the right to freedom of expression and information. In the Netherlands, this right is enshrined in Article 7 of the Constitution. The Dutch government must look closely at how combating disinformation can be reconciled with protecting the constitutional right to freedom of expression.[29]

Businesses and members of the public have a joint responsibility in respect of online activities. On the one hand, citizens are responsible for their own online behaviour and much of the content available online. On the other hand, platforms are responsible for the way in which algorithms are configured and for how they steer internet users' browsing behaviour. Companies must be more diligent in their duty of care in respect of the use of online platforms, as the AIV noted back in 2020 in its advisory report entitled 'Regulating Online Content: Towards a Recalibration of the Netherlands' Internet Policy'.[30] With regard to members of the public, the AIV recommends a substantial boost to the cyber resilience of internet users, hence the urgent need for media literacy and sound digital literacy training.

Democratic processes and public order may also come under pressure because of migration. Migration can be used as a means to put pressure on social cohesion or the rule of law, or to frustrate public processes or create polarisation in society.[31] The fact that migration can be used intentionally as a political weapon to destabilise other societies was illustrated in Belarus in 2021, when President Lukashenko deliberately channelled tens of thousands of migrants, mainly from Iraq, into the EU in a short space of time.[32]

**Water management and drinking water supply**

The Netherlands' current hydraulic engineering works are an international showpiece, but at the same time seriously outdated in some cases. They operate on old computer systems and are connected to digital networks so that they can be operated remotely; the security of these systems leaves much to be desired. Water management – more specifically flood defence and management of water levels – has therefore been designated as a critical process.

The Ministry of Infrastructure and Water Management has indicated that wastewater treatment should also be designated as critical, given that any disruption could have major repercussions, such as disease and pollution. Water authorities, which manage critical infrastructure such as wastewater treatment facilities and dykes, are also represented in the safety regions and work closely with the National Cyber Security Centre (NCSC). Together with Rijkswaterstaat, they are monitored by a specialist computer emergency response team (CERT) that keeps water authorities and Rijkswaterstaat up to speed on cybersecurity developments.[33]

The AIV notes that outdated water management processes need to be modernised as soon as possible. Investment in greater security for operational technology is also necessary for the safe functioning of the systems. In addition, the security of the drinking water supply should be reviewed. The 2021-2026 policy document on drinking water shows the extent to which the water supply could be jeopardised by cybercrime, for example, and the AIV underlines the importance identified in this policy document of a secure and resilient drinking water sector. To achieve this, greater and more efficient collaboration is needed between central government, the provincial authorities, municipalities, water authorities and drinking water supply companies in relation to identifying threats, mitigating risks and addressing vulnerabilities.[34]

### Transport sector

The transport sector is the beating heart of the Dutch economy. The international character of this sector is a great strength, but it is also a vulnerability. Especially now that China is becoming increasingly active in this sector in Europe and in the Netherlands. This was already illustrated in 2019 by the deal between China and Serbia, under which the 'Qilu' train from China's Jinan arrived in Belgrade, the first European railway station on China's New Silk Road – the Belt and Road Initiative (BRI).[35]

Naturally, doing business with China or with Chinese companies does not necessarily constitute a threat. On the contrary, it is extremely important for the Dutch economy and it is part of healthy economic competition and normal trade policy. Caution is advised, however. China's growing assertiveness could eventually lead to over-reliance in the long term, something that has been seen in, for example, the port activities sector. China is more active in water transport than rail transport; for instance in European ports such as Piraeus, Thessaloniki, Genoa, Antwerp, Zeebrugge, Hamburg and Valencia. Even the port of Rotterdam is partly in Chinese hands.

Because of China's position in this respect, there is a genuine risk for Europe – including the Netherlands – that trade flows, vital economic building blocks such as chips and raw materials, and specific products in the transport sector will be used as political levers. In peacetime, this economic rivalry would simply appear to be a trade war, but it becomes an acute issue as soon as armed conflict looms, as in the case of Europe's dependence on Russian gas, which suddenly became a much bigger problem after Russia's invasion of Ukraine.[36]

The risk of sabotage and subversion increases when dependency on rival states such as China is high. As well as being major transport hubs, the Netherlands' busy rail network and heavily used airports are high-risk links. They are essential for the transportation of people, services and goods, which means that sabotage or cyberattacks can have a destructive effect. In 2020, for example, the Court of Audit concluded that Schiphol was highly vulnerable to cyberattacks.[37]

### Essential goods: medicines, chemicals, microchips

There are goods which are essential to keep society functioning and on which citizens rely. The AIV discusses some examples below.

The COVID-19 pandemic showed how important it is to be able to produce certain medical resources independently. The global crisis revealed a major international shortage of specific medicines, which meant that local production was necessary wherever possible in a short space of time. This was not a Dutch problem as such, but applied to virtually every country in Europe. Within the European Commission, therefore, there have since been repeated calls for a new approach to the production of medicines.[38]

In times of crisis, failures in the production and supply of medicines can become a geopolitical lever. The AIV notes that it is high time for the Dutch government to speed up new European and Dutch initiatives to put emergency capacity and production in order.[39] This applies in equal measure to large parts of the chemical industry. The Netherlands is home to major processes in the production of chemical goods, many of them of great international importance, and the security of these processes is vital. Close cooperation with manufacturers and suppliers could guarantee the required security.

The microchip industry (in other words, the semiconductor industry) is also essential for the Dutch economy, but that too is a sector rife with vulnerabilities. There is great interest worldwide in the technology of ASML and NXP. Chips are the lifeblood of a modern and digitalised society; no digital product can function without them. Critical sectors such as the telecommunications, energy, defence and medical sectors all rely heavily on components in which semiconductors are incorporated.

For geopolitical powers, control of the chip industry is important for two reasons: first, the world's most sophisticated chips are used to enhance armed forces' military capabilities and, second, chips are essential building blocks upon which critical sectors in high-tech economies rely heavily.[40]

The lack of clear European industrial and innovation policy, cumbersome procedures in the Netherlands and many other obstacles are weakening the industry. Large-scale subsidies for semiconductors and the powerful industrial policies of the US, Chinese, Taiwanese and Korean governments mean that the Netherlands is in danger of being left behind in the field of semiconductors. This will not only mean the slow demise of an industry that is highly important to the Netherlands, but it will also weaken the resilience of the economy (and thus of society) in the long run.

The AIV considers it important to achieve better harmonisation in the Dutch and European regulations on industrial security issues. European cooperation is necessary, not only between governments themselves, but also between governments and the private sector. It is important as well to speed up the sharing of information for the security of business processes. The AIV is also of the opinion that companies need to put their corporate housekeeping in order with regard to security processes.

**The financial sector**

The financial sector is a real target and banking systems are vulnerable. This vulnerability is exacerbated by the fact that the financial infrastructure in Europe is highly networked and consists of numerous digital connections, electricity supplies and other critical infrastructure. The banking system as a whole, and specifically payment transactions, can only exist under secure, properly functioning connections. If a large-scale attack were to knock out both electricity and digital connections, banks must be able to continue to operate.

A few years ago, the Netherlands Institute for Public Safety (NIPV) looked at the security risks for the financial sector. For instance, the European Central Bank (ECB) monitors the financial solidity of the major banks in the European Union, which must be able to meet their banking obligations at all times.[41] Responsibility for supervising financial institutions, such as banks and pension and investment funds, lies with the Dutch central bank, De Nederlandsche Bank (DNB). The ECB can provide guidance for the DNB with regard to how that supervision is carried out. The Dutch Authority for the Financial Markets (AFM) supervises the conduct of companies.[42] In the Netherlands, if there is an acute risk, for instance of an imminent bank run, the Minister of Finance has the authority to impose a banking moratorium, in consultation with the banks and the security services.

Nevertheless, financial stability and security are more than just a supervisory issue. It is also about how these institutions have organised their security. Banks, pension funds and insurance companies are targeted by cyberattacks on a daily basis. A European security system – the Digital Operational Resilience Act (DORA) – has been developed because of the constant threats; this creates a legal basis for security supervision. The AIV endorses the importance of DORA and argues that financial institutions should take accelerated steps in accordance with the necessary requirements to be 'DORA-proof'.

Closer collaboration between banks and governments is paramount. In the event of a cyber threat, banks are currently required to report serious incidents in their critical processes directly to the NCSC. Depending on the threat or the incident concerned, critical suppliers from the financial sector will take part in the ICT Response Board (IRB), which is facilitated by the NCSC. The IRB is a public-private partnership that convenes whenever an IT crisis, cross-sectoral or otherwise, is imminent.[43]

An important role in security consultations between government authorities and banks is played by the Tripartite Crisis Management Operational Committee (TCO). The purpose of the TCO, which comprises DNB, the AFM and the Ministry of Finance, is to deliver a crisis response to the operational

failure of systems. Other financial institutions are represented as well through advisory groups and the TCO's consultation group.[44] Euronext and Euroclear are also affiliated.

There is now some level of public-private partnership between banks, the police and the security services. The AIV notes that this collaboration is still mainly incident-led. Units dealing with actual security issues are often restricted in terms of what action they can take. Banks seem to be primarily concerned with internal processes and the mitigation of compliance risk rather than focusing on the actual security risks facing Dutch citizens. The AIV argues that, given the fact that banks also have a public duty, this should be better regulated.

The AIV stresses that the financial sector's operational capability should be enhanced for the sake of financial security. The TCO should play a bigger and more coordinating role and should be part of the National Security Council (NVR) (see Chapter 5). The TCO should also be given a mandate to organise crisis management for the financial sector. Improved coordination will contribute to national security, information sharing and cyber resilience.

**Digital connections, telecommunications and energy**

The Netherlands serves as a data hub. Because of the country's favourable location, large data centres are being built and telecommunications are highly sophisticated. The Dutch digital and data infrastructure is extremely complex. Consider, for example, the Amsterdam Internet Exchange (AMS-IX), the internet exchange point through which most of the data from Dutch internet users passes, and in particular also the data between transatlantic partners. Over the past quarter of a century, the AMS-IX has built up a vast and complex network.

At the same time, the huge concentration of dataflows through networks in the Netherlands means that Dutch telecommunications are vulnerable. Every day, telecom and data companies have to deal with cyberattacks, such as distributed denial of service (DDOS) attacks or attacks using ransomware. The telecom sector also faces more traditional threats, such as attacks aiming to shut down power, telephony or electricity at the local level. In a highly globalised and networked world where commerce is largely digital, excessive or unidirectional connectivity also poses a risk. Even though companies such as KPN use the new technology to enhance recognition of unusual data traffic. Supervision in this regard is the responsibility of the Dutch Authority for Digital Infrastructure.

The increasing volume of data traffic has physical consequences: commissioned by Dutch telecom firms and system operators, such as KPN, TenneT, Energienet and other suppliers, more and more cables are being laid on the seabed, intended for, among other things, data traffic and offshore wind energy. In today's geopolitical constellation, submarine cables are globally significant. At the same time, the Netherlands is vulnerable in that area. It is an open secret that many of the submarine cables in the Netherlands come in at IJmuiden and Zandvoort, in the Amsterdam region. As a result of the sharp increase in data traffic and the use of wind energy, the production and laying of submarine cables, by companies including Boskalis, Van Oord, Alcatel Submarine Networks and WIND Subsea Cable Services, has grown astronomically. An initiative was launched recently by 15 national and international telecom companies, together with the municipality of Rotterdam, for the construction of a new submarine cable between the Netherlands and the United Kingdom, known as the 'Erasmus' cable. This cable is designed to strengthen the Netherlands' position as the 'digital gateway to Europe' and to improve services to the Rotterdam region, but also to reduce the vulnerability of and dependency on existing data networks.[45] [46]

This increased cable laying presents some complex security issues. Who, for example, is responsible for protecting the more than a million kilometres of worldwide fibre optic and other types of submarine cables? Generally speaking, it is the companies themselves; they are responsible for physical security. But can they also guarantee the secure passage of data or wind energy along these cables? Will data interception or energy tapping be swiftly dealt with? The recently constructed transatlantic cable link

between the US and Europe, as a result of the surge in online data traffic, shows that such construction not only necessitates ever-closer coordination between multinationals and national governments, but also makes a direct claim on the public space and national security interests.[47]

This applies equally to offshore drilling platforms and wind farms, which are becoming increasingly important for Dutch energy supplies.[48] They are vital for the Netherlands and for the European hinterland to which energy is supplied. Given the number of electricity cables and gas pipelines running through Dutch territorial waters, the kind of sabotage seen recently in the case of the Nord Stream pipelines must be prevented.

The Dutch government is responsible for the public space and the sea up to 12 nautical miles from the coast. Within that area, close cooperation is needed with businesses. In December 2023, the government therefore decided to invest in more robust security for critical infrastructure in the North Sea.[49] There will be increased camera, radar and satellite surveillance for submarine cables (as well as for wind turbines and drilling platforms). Two new ships will also be purchased for the Ministry of Defence for the purpose of intelligence, surveillance and reconnaissance (ISR).

The AIV recognises the importance of these investments, but deems them insufficient for effective surveillance. The government will need to invest substantially in protection of the entire coastline. Customisation will be necessary for specific vital connections. To spread the risk, work will need to be done on the construction of multiple access points where cables reach the coast, a wider spread of cables and a larger number of offshore transformer blocks – the points at which cables from one wind farm converge – as well as a greater quantity of cables.

National initiatives, such as the Dutch Subsea Cable Coalition – a collaborative platform comprising central government, submarine cable companies, telecom companies and investment funds – are considered by the AIV to be extremely relevant and valuable.[50] Collaborative platforms such as this should focus specifically on the protection and security of infrastructure. The AIV urges the government to link the security services and safety regions to initiatives such as these.

**Cyber systems and data**

Cyber threats include unauthorised access to information, espionage, subversion of digital processes by sabotage and the use of ransomware, and violation of digital space, for example through the abuse of global IT supply chains. The recent surge in – and wide availability of – generative AI applications, which are used by both state and non-state actors to execute cyber threats such as phishing and ransomware operations faster, more precisely, more efficiently and with a greater degree of autonomy and complexity, have increased the vulnerability of cyber systems.

The 2022 Netherlands Cyber Security Assessment states that digital security does not need to be explicitly named as a separate national security interest because it acts as a common thread running through the six national security interests listed in the Security Strategy for the Kingdom of the Netherlands: territorial security, physical security, economic security, ecological security, social and political stability and the international rule of law.[51]

The AIV agrees that cybersecurity is a common theme running through the other national security interests. The question is, however, whether this is currently enough to provide sufficient resilience against the wide variety of attacks and to attribute these attacks to the responsible actors. The AIV believes that cybersecurity and cyber resilience affect society as a whole; they should therefore be coordinated at the national level.

Collaboration between the different government organisations as well as between the public and private sectors in respect of cybersecurity is sometimes difficult. In this regard, the AIV endorses the government's commitment to merge the three existing government cybersecurity organisations into

a single national cyber organisation at the end of 2025.[52] Collaboration between the private and public sectors is essential in this area. Joint, large-scale exercises are a good example of such collaboration, as is the cyber reservist training conducted by the Defence Cyber Command (DCC).

Cybersecurity is often still seen by companies as a difficult cost item, one of many others; it is a cost item that many commercial companies, especially small and medium-sized enterprises, do not address specifically because it is too expensive. Costs are estimated to be too high in relation to the perceived risk. In many cases, cyberattacks and data breaches are not even reported by companies, according to findings by the Dutch Data Protection Authority in its recent report on data breaches in 2023.[53] This is despite the fact that millions of people suffer as a result.

Cybersecurity should be the top priority for companies and should be at the forefront of good, sound operational management. This is necessary not only to ensure the security of a business itself, but also to minimise any impact on the rest of the supply chain, as well as on society. The government can impose security requirements on new companies, for example by making an effective cybersecurity plan mandatory on forming a company and registering it with the Chamber of Commerce before a company can start its activities.[54]

The government must also take a good look at its own practices. For instance, how personal records are stored in municipal databases is extremely vulnerable: an attack such as the one in the municipality of Hof van Twente in 2020 could certainly happen in many other municipalities and would have enormous implications for the municipal authorities and residents. But something else that needs to be addressed is the worrying situation that much of the Dutch government's current cybersecurity capacity is in the hands of a British company.[55]

Countering cyber threats requires not only a national but also a joint European approach. A greater focus is needed on societal cyber resilience. The legislative initiatives at the European level, such as the Cyber Resilience Act for cybersecurity in hardware and software products, the NIS2 Directive in respect of companies and organisations in critical infrastructure and DORA for security standards in the financial sector, are important and positive developments in this field.

Brussels should monitor European tech companies and their US and Chinese competitors operating in Europe more. This requires active industrial policy relating to the tech industry. It is precisely by increasing control that European resilience will be strengthened.

According to a recent report by the Clingendael Institute,[56] many European governments – including that of the Netherlands – have entrusted their digital systems to American companies such as Microsoft or Google. Instruments such as Ethics by Design (or Safe by Design), which aim to incorporate ethical and security principles into the design phase of product development, could be useful at national as well as European level.[57]A realistic relationship must also be maintained between the normative guidelines on the one hand and the potential constraints on innovation on the other.[58]

**Knowledge security**

Although knowledge institutions are not officially considered by the NCTV as 'critical', the AIV does regard the knowledge sector as essential for the Netherlands. It is a sector in which influencing and other types of hybrid threat can occur frequently, especially if knowledge security is not safeguarded. Hybrid threats also occur if there is an undesirable transfer of sensitive knowledge and technology, or if knowledge gained in the Netherlands passes directly to hostile powers. In the letter to parliament on knowledge security in December 2022, the Minister of Education, Culture and Science wrote that knowledge and technology were being used by state actors to augment their own military, technological, political and economic power and that they were thus increasingly becoming a strategic instrument of power.[59]

With the increased threats and the growing complexity of technology and knowledge development in general (multidisciplinarity), the importance of knowledge security has increased and the Dutch government has been working in recent years to promote awareness and self-regulation in this area.

To this end, the Ministries of Education, Culture and Science, of Justice and Security and of Economic Affairs and Climate Policy, in collaboration with, among others, the security services and NCTV, have been working closely with universities of applied sciences, research universities, applied research institutions, and so forth. A key consideration here is (and will always be) that the right balance is pursued between security and openness. Knowledge sharing, cooperation and international recruitment are intrinsic and essential components of knowledge development and indispensable in achieving the Netherlands' aim to be a frontrunner in the field of knowledge and innovation.

In the domain of knowledge security and Dutch government policy, existing measures such as export control and sanctions legislation are being brought to the fore and joint efforts are being made to find the right way to embed and implement them within the knowledge institutions. This involves both the consideration of whether particular knowledge can be made public (through publications and/or partnerships), and the possible screening of new employees or students who will be working with certain sensitive technology.

Some of the planned government measures are still being developed. The policy instruments in use, such as the Legal Framework for Knowledge Security Screening, the National Knowledge Security Guidelines and the Contact Point for Knowledge Security, take the problem of knowledge security very seriously. On the international level (within Europe but also more broadly), more work needs to be done on policies to acquire a level playing field. In the meantime, universities are expanding their knowledge security teams and organising internal campaigns to raise awareness of the issue.

There will always be a degree of friction between national security and academic freedom in this domain. Furthermore, not every form of academic affiliation or dependence on foreign technology, knowledge or employees should be seen as a threat. It is important to give knowledge institutions sufficient leeway to determine how to implement the measures, obviously taking security interests into account.

Knowledge security may be at odds with principles such as knowledge sharing and transparency; the very openness that is so vital for knowledge development. Restrictive measures should initially be aimed at PhD researchers and students from Russia, China, North Korea and Iran. Since knowledge institutions themselves are at present responsible for supervision in this area – and they tend to let commercial or private considerations prevail over public interests – it would be advisable for the Dutch government to play a greater role in this supervision.

At the same time, a restriction on knowledge workers or the introduction of overly stringent supervision would run counter to the principle of independent academic research and healthy international competition; the legal scope and applicable international agreements should therefore be carefully considered. It is also necessary to take into account inclusion and diversity and the principle of non-discrimination.[60]

## ► 2.2 Risks throughout the Kingdom: the Caribbean part of the Kingdom

Hybrid threats can occur anywhere in the Kingdom. The government should therefore be mindful of the worrying situation in the Caribbean too, especially the ABC islands (Aruba, Bonaire and Curaçao), where the political and economic instability of neighbouring Venezuela is having a major impact.

The ABC islands are highly dependent on Venezuela in terms of their economy.[61] Venezuelan President Maduro's sudden move to annex two-thirds of neighbouring Guyana means that the situation is worrying for the islands.[62] The Venezuelan president has various means at his disposal to put further pressure on the islands. As a result of the economic and political malaise in Venezuela, large numbers of migrants have increased the pressure on society in Aruba, Curaçao and Bonaire in recent years. In 2019, for instance, between 8,000 and 10,000 refugees, most of them undocumented, were living in Curaçao, among a population of 160,000.[63]

The use of migration as powerpolitical and strategic leverage to put pressure on another country is regarded to be a hybrid threat. Although there are currently no signs that the Venezuelan president is deliberately using migration as a political tool (unlike the president of Belarus), given the major migration crisis in Venezuela in 2018, it cannot be ruled out that this will happen. Both the US Department of Homeland Security and the European Union Agency for Asylum (EUAA) recently repeated their warnings about this eventuality.[64]

As well as potential threats from neighbouring Venezuela, the limited cyber resilience of the Caribbean part of the Kingdom also plays a role. The Netherlands has a responsibility to strengthen this cyber resilience. The situation in the Caribbean part of the Kingdom concerns the Netherlands too. The same applies to the need to counter disinformation and the subversion of democracy. In the relatively small communities on the islands, mainstream society and the criminal underworld are becoming increasingly intertwined, a development that is of great concern to the AIV.[65]

As in the Netherlands, submarine cables also appear to be a growing public issue in the Caribbean part of the Kingdom. This collaboration between government and submarine cable companies raises questions on occasion, as evidenced by the recent request under the Open Government Act regarding authorisations given to Saba Statia Cable System B.V. for the construction, operation and maintenance of a submarine fibre optic cable link in Saba and St Eustatius. The way in which public-private partnerships are managed in the Caribbean part of the Kingdom needs to be addressed.[66]

To better embed the security of the Caribbean part of the Kingdom into a Kingdom-wide strategy, there needs to be closer cooperation with the islands. There also needs to be greater clarity on the relationships between the Ministries of Justice and Security, Defence, and Foreign Affairs concerning the Caribbean. Particularly, on the way their operational capacity is organised during international crises. Furthermore, existing security options in the Charter for the Kingdom of the Netherlands should be investigated, as previously advised by the AIV in 2020 in its report entitled 'Security and the Legal Order in the Caribbean'.[67]

Chapter 3

# Geopolitical urgency

Hybrid instruments are used to gain a more favourable military-strategic position. A variety of resources can be utilised to achieve this.[68] The impact of hybrid instruments is greater than ever before because of globalisation, digitalisation and new technologies. States and non-state actors seem to be opting more deliberately for the hybrid route. The grey zone of hybrid conflict spans a broad spectrum of means, so there is an urgent political and societal need to recognise and make sense of this phenomenon.

## ► 3.1 Russia

When defining hybrid conflict, Russia is often used as a starting point. This is mainly because the deployment of hybrid instruments has been part of Russian military doctrine for more than a hundred years. Russia's military doctrine makes no distinction between conventional and unconventional activities. Deception, political warfare and covert operations are used to acquire as much information as possible about – and weaken – the enemy, using a combination of traditional military operations and non-military means.[69]

Despite the fact that this hybrid strategy has been common for the Kremlin, it was revived in 2013 under the leadership of General Valery Gerasimov, and as such has since been referred to as the Gerasimov doctrine. Consequently, Russia has been able to gain strategic advantages on many fronts, for instance by obstructing election campaigns or by funding extremist and anti-democratic political groups.[70] This was clearly demonstrated at the time of the annexation of Crimea in 2014 and in the eight years that followed, until the actual military invasion of Ukraine in 2022.[71]

Russian military doctrine emphasises the importance of 'maskirovka', i.e. military camouflage, deception and surprise. This is usually integrated into a broader attack, even though there is no war yet, as defined under international law.[72] For example, the Russian military may carry out a cyberattack as part of a larger information war, in which active infiltration of foreign computer systems takes place simultaneously with electronic warfare and psychological operations.[73] In addition, the Russian government uses methods such as deliberately refraining from prosecuting or extraditing ransomware groups in order to cause economic damage (and thus instability) in other countries.[74] Covert funding of specific political parties also falls into the category of hybrid conflict.

The past decade revealed the extent to which the Kremlin was operating within the cognitive domain. The Russian government was openly committed to a powerful national narrative and historical world view: the story of an ancient, powerful Russian empire, a deeply unified Russian culture, a clear and one-dimensional narrative. Like Dmitry Adamsky, we can argue that this narrative reinforces the Russian strategic culture within Russia itself, and at the same time bolsters its 'strategic coercion' towards the outside world.[75] The existence of the battle on the second front – where world views clash – has not yet dawned on the West. Autocratic leaders like Putin try to weaken free democracies, partly by influencing political parties and movements susceptible to the one-dimensional Russian approach. This was also visible in the run-up to the Ukraine war, as the AIV described in the advisory report entitled 'The war in Ukraine: a geopolitical "time shock"'.[76]

## ► 3.2 China

China is an example of a power that uses a multitude of hybrid means without actually going to war in a legal sense. In 2003, it adopted what is known as the 'three-warfares' doctrine, which implies that conflict can be engaged in without the use of force, by using the law, psychological warfare and public opinion.[77] The law is used as a means – legal warfare – to achieve political and economic objectives. The Chinese government uses it, for example, to lay claim to territories.[78]

Chinese psychological warfare aims to disrupt international decision-making, mislead the public and encourage anti-leadership sentiment. Media warfare is also used in this respect. The claim by China's state media that the COVID-19 outbreak in 2019 occurred after the US army deliberately brought the virus to Wuhan was an example of this.[79]

Although the Chinese government seems increasingly focused on co-opting Russia's hybrid strategy, there is a difference, however. The Chinese government sees hybrid conflict as a means of expanding its political and economic influence beyond its borders. Its approach includes the use of economic power, propaganda, cyber espionage and other non-traditional means, but, unlike Russia, emphasises the importance of avoiding military confrontation.[80]

President Xi Jinping sees this deliberate political strategy as a necessity for China: '…we must tighten international production chains' dependence on China, forming powerful countermeasures and deterrent capabilities based on artificially cutting off supply to foreigners.'[81] The media, universities, NGOs and businesses are also being used to achieve this political goal.[82]

## ► 3.3 United States

Despite the fact that the government's request for advice focuses particularly on hybrid threats from Russia and China – and these countries do indeed put great pressure on Dutch (and EU) security – it is worth remembering that Western countries are not averse to using hybrid means either.

The US has in the past been actively involved at political and diplomatic level in operations to undermine or overthrow governments, or to put countries under political and economic pressure. Americans often refer to this as counterinsurgency.[83] The US approach focuses on the use of non-military means to secure political goals. The US government uses modern technology to achieve military-strategic objectives. This technology is used for various means, such as political influence and economic destabilisation.

The US Department of Defense is undertaking more and more activities in the grey zone 'to reinforce deterrence and frustrate adversaries', especially in the cyber domain.[84] The lack of national borders makes it difficult for states to operate in cyberspace, so the US is committed to establishing a global network of allies and partners to protect the cyber domain while enabling states to take timely action against threats in this domain.[85]

## ► 3.4 NATO

NATO is also active in the hybrid domain, both defensively and offensively. A growing number of NATO countries are recognising the need to address hybrid threats, which is why NATO itself is committed to counter-hybrid measures. The battle against hybrid activities is playing an increasingly important role within NATO[86] and there has been a NATO strategy to counter hybrid threats since 2015. NATO's Joint Intelligence and Security Division investigates and analyses threats which affect member countries or which could potentially pose a risk. In addition, NATO invests in civil and military instruments to make member countries more resilient to hybrid threats. Since 2016, the Alliance has regarded hybrid threats against member countries as a threat that could trigger Article 5 (see Chapter 4).[87]

NATO has also established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) for the investigation and analysis of cyber threats, and the Defence Innovation Accelerator for the North Atlantic (DIANA) programme specifically for the further development of emerging disruptive technologies, such as AI and quantum technology, in partnership with businesses and the research community.[88]

Since April 2022, NATO has been stepping up the political dialogue with four Asia-Pacific partner countries in order to intensify cooperation in the field of cyberspace, new technologies and countering disinformation. Individual Partnership Cooperation Programmes have been developed to counter the aforementioned threats and to foster collaboration on climate change and maritime security.[89]

NATO cooperates with the EU on countering cyberattacks. A NATO-Ukraine Platform on Countering Hybrid Warfare has also been established and the Alliance is working with several expertise hubs in Finland, Latvia, Estonia and Lithuania. In terms of NATO-EU cooperation, there is still much to be gained in terms of information exchange and shared communications.[90]

NATO emphasises, as set out in its 2022 Strategic Concept, that it will invest in the fight against hybrid threats. This shows that NATO is taking the use of hybrid tactics very seriously. NATO has made a firm commitment to invest in active strategic communication (StratCom), for which it has established a specific knowledge centre, the NATO Strategic Communications Centre of Excellence.[91] The AIV wonders where the line is drawn between strategic communication and outright influencing or propaganda. It is precisely amid the rising tide of disinformation that this becomes an important issue for the NATO allies.

## ► 3.5 European Union

The EU is also becoming increasingly active in the hybrid domain. Russian disinformation campaigns, as part of broader-based Russian hybrid conflict activities, are seen as a major threat to the EU.[92] The annexation of Crimea in 2014 and subsequent violations of international treaties have put Russia's disinformation campaigns in Europe into the spotlight.[93] In 2016 and 2017, the focus on hybrid threats in the context of the Russia-Ukraine conflict increased with the establishment of the Hybrid Fusion Cell, created within the European External Action Service (EEAS).

In 2016, the European Commission published a Joint Framework on countering hybrid threats, the aim of which was to counter and raise awareness of hybrid threats and to strive for effective communication and cooperation to deal with those threats.[94] The EU has stipulated that hybrid threats could trigger Article 42.7 of the Treaty on European Union (TEU), under which EU member states assist each other in the collective defence of the European Union.[95] This assistance clause has only ever been invoked by France, following the terrorist attacks in Paris in 2015. Nonetheless, the EU has determined that this article can also be invoked in the event of a cyberattack, or another

type of hybrid attack. Although experts consider it unlikely for the article to be invoked in such circumstances, it is certainly not beyond the realms of possibility.[96]

In 2017, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) was founded by its first nine participating states, along with the EU and NATO. This organisation is based in Helsinki and helps to strengthen the resilience of participating states through research, training and expertise in the field of countering hybrid threats.[97] The Hybrid CoE is not officially an EU or NATO organisation and is open to all EU member states and European NATO member states.

The EU is currently developing a European version of a response framework for hybrid threats, the EU Hybrid Toolbox, as decided on by the Council of the European Union in June 2022.[98] This toolbox provides EU member states with various practical instruments with which to counter hybrid threats. There is also the Foreign Information Manipulation and Interference Toolbox (FIMI Toolbox), which provides a structured method of tackling disinformation. Hybrid threats, however, involve far more than just disinformation, as pointed out by the Council of the European Union.[99] Unlike the versatile EU Hybrid Toolbox, the FIMI Toolbox is more limited in scope, as it is mainly used to counter disinformation and is only used against hybrid threats in the broader sense if no other EU instruments are available.

In addition, the specially designed European Democracy Action Plan from 2020 and the Defence of Democracy package presented in December 2023 focus on making European democracies more resilient, including to external influence. Furthermore, the EU is investing through the European Defence Agency (EDA) in specific hardware and software for new technologies, partly to counter threats in the virtual and cognitive dimensions.

There are currently several far-reaching European initiatives regarding hybrid threats, such as the EU Cybersecurity Strategy and the European Energy Security Strategy.[100] In the 2022 Strategic Compass, the EU indicated its intention to invest in cyber defence policy and cyber diplomacy and to develop instruments with which to counter foreign interference and manipulation.[101]

In order to strengthen societal and economic resilience in Europe and simultaneously limit the growing dependence on China, the European Commission presented the Global Gateway investment project in 2021. Through this project, the EU aims to make investments in infrastructure projects and economic partnerships outside Europe, rising to €300 billion in 2027. This project – intended as development cooperation, but certainly not without European industrial interests – officially breaks with the long-established tradition under which the West, and particularly Europe, did not wish to participate in industrial politics. The EU also sees it as a way to increase European strategic autonomy and geopolitical relevance.[102]

## ► 3.6. France and Germany as examples

A major, insightful RAND study examined how many countries had organised their deterrence and resilience around operations in the grey zone of hybrid conflict.[103] Examples of EU member states relevant to the Netherlands are France and Germany.

France is frequently targeted by cyber and information operations by the Russian government. These activities peaked during the 2017 elections, when Emmanuel Macron was the target of a disinformation campaign and a cyberattack. The disinformation campaign consisted of alleged revelations about his sexual orientation and secret offshore bank accounts. These allegations came from groups linked to the Russian government.[104]

Germany too is regularly hit by cyberattacks.[105] In 2015, government websites were attacked by the CyberBerkut hacker group when the then prime minister of Ukraine, Arseniy Yatsenyuk, visited Berlin for a meeting with Angela Merkel. The German intelligence service discovered that 16GB of data had been stolen from the computers of 14 members of parliament by the Fancy Bear group as well. The same group was later found to have carried out cyberattacks on some 200 journalists.[106]

In November 2016, a German telecom company suffered a cyberattack. Moreover, German politicians and political parties are often the victims of hostile cyber activities as well. The German armed forces are also targeted by cyberattacks, espionage and disinformation. At the beginning of 2024, Russia published the confidential conversations of German air force officers who were preparing a briefing for the German defence minister. The conversations had been conducted via the online meeting platform Cisco Webex.[107]

## ► 3.7 Terrorist groups

Hybrid threats are being posed with increasing frequency by terrorist groups, using any means at their disposal to disrupt society. Because of the use of different means of attack against states, this is often referred to as irregular or asymmetric conflict.[108] Due to a complex mix of military, non-military and technological means as well as the often unclear identity of actors (subgroups of combatants), the distinction between combatants and non-combatants from an international law perspective is sometimes very difficult to make. This distinction is obviously vital for the proper application of international law.

A common modus operandi is apparent in how Islamic State conducts its bloody terrorist conflict, and how many African terrorist groups do. Local groups use dual-use technology to produce their own new types of weapons.[109] These groups operate ruthlessly; they murder and decapitate people, rape women and sow widespread fear – the effect of an attack in the cognitive dimension. Through social media, they usually manage to present their perception of the struggle against the West quite successfully. The frequent use of hybrid means makes it difficult for states to distinguish clearly between combatants and non-combatants.

## ► 3.8 Multinationals and tech companies

Multinationals, tech companies and their directors also play a major role when it comes to hybrid threats. The infrastructure needed to conduct operations is largely in private hands. As a result, the influence of private parties – tech companies such as Microsoft, Google and SpaceX – in the geopolitical force field is on the rise.

The AIV expects that the increased geopolitical role of some multinationals, as well as the dual-use application of certain new technologies, will lead to an increase in the number of hybrid threats. A situation is looming in which powerful individuals, companies and states will enter the international political arena, playing by different rules than states.[110]

The AIV therefore urges the Dutch government to accelerate the regulation of – and increase the supervision of – large tech companies. At the same time, it is these very companies that the government needs in its efforts to strengthen societal resistance, so collaboration is most certainly needed between the private sector, the government and the public.

## Big Tech and the Digital Services Act

In today's world, in which information is crucial, the dominant role of tech companies in the digital infrastructure carries many vulnerabilities. Apple, Google and Telegram, for example, have succumbed to pressure from the Kremlin to stop offering opposition leader Alexei Navalny's Smart Voting app to users. The platforms had refused when initially requested by the Russian authorities, but after hefty fines and threats to prosecute local staff, a letter was published stating that the app may contain 'illegal information' and would therefore no longer be available in the app stores. Instagram was accused of shadow banning in connection with the war between Hamas and Israel, thus providing one-sided information to users.

Besides playing a crucial role in information and digital infrastructure, tech companies have a great deal of market power. The five largest tech companies, the 'Big Five' – Amazon, Meta, Google, Apple and Microsoft – have a combined market value of more than €6 trillion. With this kind of market power, the gatekeepers of our information supply can exert considerable influence on the public debate. An additional problem for the EU is that many companies are US-owned or dependent on Chinese technology.

In 2022, the EU adopted the Digital Services Act, which places legal responsibility on tech companies regarding disinformation, fake news, propaganda, manipulation and criminal activities. The law thus restricts a revenue model from algorithms based on illegal or dangerous content. Legally enforceable measures have proven to be an important tool, provided they are implemented in an EU context. Despite strong lobbying to water down the law, the tech giants, with the exception of companies such as X, seem to be complying largely with the new regulations because of the high economic stakes of the European market.

Sources (all in Dutch):
1. 'Apple, Google en Telegram zwichten onder druk van het Kremlin', Raam op Rusland.
2. 'Instagram beticht van censureren pro-Palestijnse posts, "moeilijk hard te maken"', nos.nl.
3. 'De macht van bedrijven als Google en Apple is gigantisch. Zo trekken Europa en de VS de teugels aan', De Correspondent.
4. 'Negen vragen (en antwoorden) over de Digital Services', Zembla, BNNVARA.

Chapter 4

# A legal conundrum

Hybrid threats do not involve armed conflict in the traditional sense. This raises a number of legal questions. The rules for a 'traditional' armed conflict are laid down in the law of war, under which states and non-state actors are bound by provisions to protect individuals when military force is being used and to make armed combat as humane as possible. There are peacetime rules, too. But when hybrid threats arise in the virtual or cognitive dimension, for example, there are significant legal challenges.[111] What are the main legal and ethical concerns when considering hybrid activities?

## ► 4.1 The legal framework

Hybrid threats arise in the grey zone between war and peace. Given that hybrid threats can take so many different forms, however, decisions need to be made on a case-by-case basis with regard to how the law applies and what the consequences will be.

Both international and national law can be applied to hybrid threats. There may also be interaction between different areas of law. In the case of an armed attack, international humanitarian law (IHL) will apply at the level of international law; this also applies to attacks on infrastructure, water or energy, or other civilian targets. In the event of damage to vital goods outside an armed conflict, it has to be determined what legislation applies; that could be national criminal law as well as human rights legislation. Measures under national law, including criminal law, could thus also be taken against attacks not covered by IHL. This can, of course, only be done with due regard for international laws relating to the jurisdiction.

Hybrid threats do not fall under the IHL definition of an armed attack. This is not as simple as it seems. An important feature of hybrid conflict is that it encompasses activities that are not necessarily covered by the law of war, which addresses the use of force in both symmetric and asymmetric warfare. Traditional warfare is governed by laws of war that provide guidelines for the use of force, the treatment of prisoners of war and the protection of civilians. There are, however, technological advancements in the field of robotics, AI and the use of big data, particularly in the private sector, for which there is as yet no legislation or consensus with regard to the security aspects.

In the event of a specific hybrid threat and in terms of how international law might apply to it, three crucial questions therefore need to be answered: (1) Has there been a violation of the prohibition of the use of force? (2) Which area of law applies to a specific hybrid threat and what are the legal implications? (3) Can the hybrid threat be attributed to a state in connection with state responsibility and what are the implications if not? These questions are explained in brief below.

**Prohibition of the use of force**

Under Article 2(4) of the UN Charter, states must refrain from using force against another state. Whether or not a hybrid attack should be regarded as the use of force depends on the effects of the action in question. For example, a cyber operation will fall under the prohibition of the use of force if the effects are similar to those of a conventional combat action.[112]

If a hybrid attack indeed entails a violation of the prohibition of the use of force, the state that is the victim (injured party) of that armed attack has the right of self-defence under Article 51 of the UN Charter, provided the conditions in this article are met (immediate notification to the UN Security Council, proportionality and necessity).

Even if the hybrid activity does not violate the prohibition of the use of force, it could still contravene the non-intervention principle. In its judgment in the Nicaragua case, the International Court of Justice (ICJ) held that states were not permitted to use methods of coercion to interfere in the affairs of another state.[113]

**Which area of law applies to a specific hybrid threat?**

At the level of international law, a distinction is made between hybrid activities in peacetime and those in times of war. But what does that mean in situations where the line between war and peace is blurred? In the event of an armed attack, IHL applies, but hybrid threats could comprise activities that are not covered by this legislation.[114]

**Applicability of human rights**

The relationship between IHL and international human rights is the subject of robust debate. In times of war, IHL allows a combatant to kill another combatant. This is, however, at odds with the right to life guaranteed under international human rights law. Initially, the consensus was that international human rights would only be applicable in peacetime situations and not in times of war.[115] This also applies in the case of skirmishes that are not sufficiently intense to qualify as 'armed conflict'.

Today, however, it is generally accepted that both IHL and international human rights legislation can apply in times of war: in some situations only IHL is applicable, in others only international human rights, and in some cases both areas of law apply simultaneously.[116]

In the 2018 report entitled 'Legal challenges related to hybrid war and human rights obligations' in respect of hybrid threats and war (the terms 'hybrid threat' and 'hybrid war' are both used in the report), the Council of Europe stated explicitly that human rights must be respected at all times.[117]

**Hybrid activities in peacetime**

Because hybrid threats occur outside the context of war, the question is which international rules apply. As regards the use of force, including its use outside a combat situation – for example in the context of law enforcement by the police, when maintaining public order or in the event of a drone attack outside the context of armed conflict – this will almost always be at odds with the human rights regime.[118] Under this regime, the use of lethal force may be used only in narrowly defined situations and is subject to rigorous restrictions.

**Hybrid threats outside IHL**

Hybrid activities may also fall outside the scope of use of force and/or of direct violations of human rights. Consider, for example, economic coercion, which does not fall into either of these two categories, but may still constitute a violation of EU law (the Anti-Coercion Instrument) or international law (the laws of the World Trade Organization).[119] Another example would be the principle that states must ensure that activities in their territory do not cause serious damage to the environment of another state, in other words the 'prevention of transboundary harm arising from hazardous activities'.[120]

In all cases, existing international and European law is decisive, and also applicable to hybrid threats. Nevertheless, the AIV believes that further development of the law is needed and that the rules of law in this area need to be updated. The Netherlands could join forces with other countries in this matter and play a leading role.

**Responsibility**

Responsibility under international law can be significant in relation to hybrid attacks if those attacks can be attributed to a state. The rules concerning state responsibility are laid down in the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), which were produced by the UN's International Law Commission and which largely reflect customary international law.[121] States can thus be held responsible for internationally wrongful acts, such as the destruction of infrastructure. What is essential here is that it concerns a violation of an international obligation (as stipulated in a treaty or customary law) that a state has, and that the violation can be attributed to that state. This applies to all international obligations by which states are bound, whether it concerns a violation of the prohibition of the use of force, IHL or any other obligation under international law.

The challenge in the case of hybrid attacks, however, is that it is often difficult to determine the entity responsible, which is essential in the context of attribution. This is particularly true when it comes to something intangible, such as the subversion of democracy and the rule of law. It can also be the case that a non-state actor, such as a terrorist group, an individual or a proxy, is found responsible for the attack or threat. In that case, attribution through the application of ARSIWA becomes more difficult, because the rules only apply to state actors. Attribution to a state of actions carried out by non-state actors is not impossible, but the threshold for doing so is high. If a non-state actor is found to be responsible for the damaging effects of a hybrid attack in another state, redress will need to be sought through national legislation.

If a hybrid threat results in a breach of an international obligation that is indeed attributable to a state, this may, under certain conditions, mean that the injured state has the right to take countermeasures (Article 22 of ARSIWA). In the context of a cyberattack, for example, the EU Cyber Diplomacy Toolbox is relevant.[122]

Nevertheless, in the absence of state responsibility, there may be individual responsibility. Because of the complexity involved in applying this effectively, the AIV believes that further development of the law and an update are needed here as well. Here too, the Netherlands could take a leading role.

## ► 4.2 NATO Article 5 and TEU Article 42.7

NATO states that a cyberattack could constitute grounds for a NATO ally to invoke Article 5, although there are no specifications regarding the damage suffered. However, this ambiguity is used strategically as a deterrent so that the limits are not deliberately tested.

There was recently a written exchange of views between the Permanent Committee on Foreign Affairs of the Dutch House of Representatives and the Minister of Foreign Affairs regarding the International Cyber Strategy. In that exchange, the minister stated that the repercussions of a series of significant cyber operations could potentially be classed collectively as an armed attack if those repercussions are similar to the repercussions of an attack with conventional weapons.[123]

Considerations can also be found in NATO communiqués suggesting that a hybrid attack could trigger action under Article 5. Account should of course be taken of the fact that actions under Article 5 are extremely rare, partly because NATO decisions are taken by consensus.[124] The invocation of Article 42.7 of the Treaty on European Union (TEU) on collective defence is another option for EU member states that would allow joint action to be taken against hybrid threats, although this too is unlikely to happen in practice.

## ► 4.3 Lawfare: the law as a hybrid tool

A hybrid attack does not necessarily have to involve a formal declaration of war; parties using hybrid means are indeed unlikely to declare war. The grey zone, not covered by IHL, is in some cases even deliberately exploited as a hybrid means. This is known as lawfare, and it is used both by parties that feel bound by IHL and parties who, by contrast, usually operate outside those lines.

Lawfare is used to deliberately circumvent existing legislation. The grey zone allows freedom of action and gives parties the option of deniability, which often results in non-attribution. It is thus difficult for the opponent to react and as a result, an armed response can generally be avoided.[125]

The use of lawfare is not restricted to parties operating under the IHL threshold. For some legal experts, it is often a clear violation of international law, even though states are not condemned for using it.[126]

## ► 4.4 The constitutional mandate of the Dutch armed forces

Anything can in effect be used as a weapon in hybrid activities; Mark Galeotti calls this the 'weaponisation of everything'.[127] Besides the legal repercussions as set out above, this also has implications for the way in which the Netherlands itself legislates the use of military means.

The tasks of the armed forces are officially set out in Articles 97, 98, 99, 99a and 100 of the Constitution, with Article 97 in particular providing guidance in respect of the armed forces' tasks. That article states: 'There shall be armed forces for the defence and protection of the interests of the Kingdom, and in order to maintain and promote the international legal order.' Paragraph 2 of the same article goes on to state: 'The Government shall have supreme authority over the armed forces.'[128]

On this basis, the Ministry of Defence formulated three main tasks in the 2000 Defence White Paper. These tasks are still regarded as guiding principles within the armed forces and are defined as follows. The Netherlands has armed forces (1) to protect national and allied territory, including the Caribbean parts of the Kingdom; (2) to maintain and promote the international legal order and stability, and (3) to support civil authorities in law enforcement, disaster relief and humanitarian aid, both nationally and internationally.[129]

These three main tasks are based on the relevant articles of the Constitution and on international treaties; they are not incorporated as such in the Constitution, nor are they defined by law.[130] They are the product of a policy choice on the basis of which the military still leans heavily today, almost a quarter of a century later. The armed forces' mission statement, according to the academic commentary, also applies to deployment in the digital domain (recognised since 2012 as the fifth domain of military action alongside land, air, sea and space).[131]

The military is often seen as the 'last man standing', not only in war, but also in societal crises. In the case of threats in the virtual or cognitive dimension, however, it is not clear what this actually means or whether the military is even in a position to act as society's last hope. Indeed, the proliferation of new types of threat makes it difficult for the military to manoeuvre, especially when these threats arise outside the context of war. How should the armed forces respond to future threats that might not be covered by the existing constitutional mandate or by the three formally defined main tasks?

This issue was previously addressed by the Brouwer commission of inquiry (2022), which investigated the actions of the Royal Netherlands Army's Land Information Manoeuvre Centre (LIMC), a unit which processed data of individuals in the Netherlands in 2020 without any legal basis for doing so. The commission's findings were as follows:

> 'The armed forces are caught between existing frameworks and new threats; current developments require adjustments to the existing frameworks. Emerging threats posed by hybrid conflict go to the very heart of the armed forces' main tasks and require the adaptation of existing legal and policy-based frameworks.'[132]

Looking specifically at the Dutch armed forces, the AIV drew the government's attention to the shift that is currently taking place with regard to their main tasks, in its advisory letter 'Choices for the armed forces' (March 2022).[133] At the time, the AIV argued that in the context of international conflict, and partly because of the 'hybridisation' and increased technologisation of conflict, there is an increasing overlap between military and civil threats. The AIV noted at the time that these threats directly affected the resilience of Dutch society as a whole. Against this background, combined with the rapidly changing, multidisciplinary approach to conflict, the AIV was of the opinion that the three main tasks of the Defence organisation did not provide sufficient scope for effective deployment of the armed forces against all aspects of hybrid threats in all dimensions.

When the twice-yearly report on the readiness of the Dutch armed forces was presented to the House of Representatives in September 2021, the Minister of Defence acknowledged that the Dutch military was insufficiently prepared for future threats or for new types of threat: 'The Dutch armed forces exist for the purpose of national security and also operate in international crisis and conflict situations and in the event of disasters. To this end, the armed forces have three main tasks. At this point in time, the Defence organisation is not sufficiently equipped to protect the Kingdom against future – and some current – threats.' The minister made these comments six months before the Russian invasion of Ukraine led to heightened international tensions and brutally shattered the peace on the European continent.[134]

Looking at the present day, the AIV cannot help but note that, despite the many additional billions currently being invested in defence, there has been no great improvement in the situation. And this is related not only to the investment, but also to the tasks.

The current definition of the armed forces' main tasks takes insufficient account of the broad scope of hybrid means of attack in all dimensions. Given that hybrid threats in the current geopolitical landscape, particularly those in the virtual and cognitive dimensions, cannot be effectively addressed and countered by the armed forces, the Netherlands is at risk.

The AIV therefore calls on the government to collaborate with legal experts in reviewing the definition of the main tasks, which are not expressly incorporated in the Constitution but were conceived by the Ministry of Defence itself and recorded in an explanatory memorandum, and have them amended and updated where possible. Precisely because the military revolves heavily around the three main tasks, it would be advisable to refocus the armed forces' remit on threats in all three dimensions.[135] Such a change would be possible, given that neither the tasks established by the Ministry of Defence nor the explanatory memorandum are laid down as such in law. Although it would not change the official or legal basis of the armed forces, it will allow the implementation of tasks to be arranged differently.

It would also be appropriate here to include Article 3 of the North Atlantic Treaty in the considerations, which states that NATO allies 'separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.'[136] Again, it is not sufficiently clear how the Netherlands (and NATO allies) have catered for this responsibility against the background of the most recent types of hybrid threat.

## ► 4.5 A constitutional duty for society

In the Constitution, most of the Netherlands' defence tasks are assigned to the armed forces. The armed forces can act on behalf of the government at the high end of the spectrum of force and therefore serve as the state's 'instrument of force'. However, because attacks and threats do not occur exclusively in the military domain, the armed forces must work more closely with all of society. Dutch citizens themselves can contribute to collective defence and societal resilience.

The issue of defence does not just concern the military or the police. It concerns society as a whole; the public also have a role to play. This has already been the focus of attention from the legislature in the past. In 1997, a proposal was made via an explanatory memorandum accompanying a proposed amendment to Article 97 of the Constitution to update the definition of the armed forces' tasks. The memorandum said the following with regard to the role of society in the nation's defence:

> 'While the existing constitutional provisions do not preclude the imposition of civil defence obligations, they do falsely create the impression that modern warfare is purely about military defence. By mentioning civil defence in so many words, this false impression is dispelled. Furthermore, the proposed provision ensures that if civil defence obligations are imposed on civilians, this can only be done through the intervention of the legislature.'[137]

Partly for this reason, the constitutional amendment of 2000 included an additional article for the purpose of civil defence, in addition to the 'defence articles' for the armed forces. In naming the tasks for the armed forces, as laid down in Articles 97, 98, 99 and 100 of the Constitution, the legislature at the time added Article 99a. This article reads:

> 'Duties may be assigned for the purpose of civil defence in accordance with rules laid down by Act of Parliament.'

The legislature thus made it clear that the defence of the Netherlands was not exclusively a task for the armed forces, but for society as a whole. The academic commentary to this article includes the following:

> 'The legislature may impose obligations on people in connection with civil defence. This refers to non-military measures to protect the population and their property in the event of a natural disaster, act of war or other emergency. This may entail, for example, the deployment of doctors and nursing staff to locations where they are urgently needed, the deployment of civilians to keep road and water routes open or the repair and safeguarding of drinking water and energy supplies'.[138]

This constitutional article, which is now almost 25 years old, remains as important as ever. The AIV notes that the Dutch government could invoke Article 99a of the Constitution more emphatically than it does now, thereby making a clear call for the establishment of civil defence or public resilience. The AIV is aware that the article focuses mainly on 'duties' that can be imposed on society, and that there would probably be little appetite for this in the current social climate. The AIV is of the opinion, therefore, that it might be more palatable to consider a milder approach to motivate and stimulate the public. The government should explore the possibilities for shaping societal resilience with a greater involvement of the public than is currently the case.

The AIV notes that this resilience must apply to all three dimensions, that is the physical, virtual and cognitive dimensions. And that will be no easy task, as increasing societal resilience in relation to an economic attack, corrupt financial practices or an attack on critical infrastructure is probably easier to imagine than it would be in relation to an attack in the virtual or cognitive dimension.

The way in which society should be prepared and brought into action in respect of hybrid threats in all three dimensions will be discussed in the following chapter.

Chapter 5

# Building resilience

Security concerns us all and it is not free. Not all Dutch people seem to be aware of this.[139] Nevertheless, security is a vital element of the national and public consciousness. The AIV believes that the people of the Netherlands should be involved and mobilised to a greater extent in organising national security and societal resilience, in accordance with Article 99a of the Constitution. There should be close collaboration between government and the public and between the public and the armed forces.

## ► 5.1 The Netherlands' three-track approach

It is not only the armed forces that are tasked with making the Netherlands more resilient; national defence is a task for society as a whole. An open society and open economy, including the knowledge economy, are inherent in a democratic country governed by the rule of law such as the Netherlands. Dutch public interests benefit from trade, transparency and global networks. If it is in precisely those areas that threats to the quality of life arise, a security framework needs to be developed.

For the past five years or so, hybrid threats have been the focus of attention in the context of societal resilience, as evidenced by, for example, the 'Defence Vision 2035', 'Threat Assessment State-sponsored Actors' and 'A stronger approach to threats from other countries'.[140] In 2022 the 'National Risk Assessment of the Kingdom of the Netherlands' was published (compilers include the AIVD, the Netherlands Organisation for Applied Scientific Research (TNO), the MIVD and the National Institute for Public Health and the Environment (RIVM)). It aimed to identify current threats in order to make government authorities, the public and businesses resilient against hybrid and other threats.[141]

The Netherlands needs to arm itself against potential hybrid attacks, which is why the government is proposing to take proactive measures whenever Dutch public interests are compromised. The government has said that the Netherlands intends to work towards building knowledge, promoting and protecting economic security, preventing undesirable knowledge and technology transfer, countering undesirable foreign interference and protecting democratic processes and institutions.

Foreign interference is a major problem, including in the Netherlands. Recent reports from the Czech intelligence service revealed how Russia had given cash incentives to a network of European politicians and policymakers to boost the pro-Russian narrative.[142] Prime Minister Mark Rutte branded these developments as a 'threat to our democracy, to our free elections, to our freedom of expression, to everything'.[143]

The government has drafted guidelines to counter foreign interference, proposing three tracks to be pursued.[144] These are the *diplomatic track:* entering into dialogue with states that engage in undesirable interference and consistently holding them accountable, and taking diplomatic steps against the states concerned where necessary; the *resilience track:* raising awareness and increasing the resilience of vulnerable groups that could be susceptible to undesirable foreign interference; and the *administrative/criminal-law track:* coordinated action and disruption in the event of current or imminent incidents, using a combination of administrative and criminal law measures.[145]

## ► 5.2 Towards a government-wide response

The NCTV coordinates the 'Government-wide response framework for hybrid threats' and the underlying assessment framework. These are administrative and policy-based instruments used by the government to tackle hybrid threats. Broadly speaking, this involves sharing information, identifying response options, assessing international support for a joint response, coordinating a counteraction, analysing its impact and accurately identifying legal options as well as seeking a mandate. The response framework makes it possible to deploy a coordinated government-wide response against a specific state actor known to be behind a malicious action. The NCTV is currently working on a broader resilience concept in relation to hybrid threats.[146]

Hybrid threats are also an intelligence issue. Indeed, intelligence and security services tackle hostile influence and covert activities in the grey zone between war and peace on a daily basis. Within the parameters of the new Intelligence and Security Services Act (WIV), the MIVD and AIVD are trying to find ways to pre-emptively counter hybrid attacks. This is no easy task, however, because those legal frameworks do not always adequately provide for situations involving new types of attack in the virtual and cognitive dimensions, enabled by the latest technological capabilities.

Alongside institutional actors, the public can also be mobilised against hybrid threats. The AIV maintains that a precondition for this is that societal resilience in the Netherlands be increased and collective awareness of security issues heightened. There is no start or end point in the grey zone between war and peace, so permanent awareness and constant preparedness of society as a whole are essential. If the Netherlands wants to increase societal resilience and heighten collective security awareness, cooperation with the private sector and knowledge institutions is vital. To this end, the AIV is looking not only at the government-wide response framework but also at the model that is being used successfully in Finland.

## ► 5.3 Is the Finnish model right for the Netherlands?

Following the annexation of Crimea and the heightened Russian threat, Finland changed its national security strategy around 2017. It moved away from the 'total defence concept' in favour of the comprehensive security approach, in pursuit of national and societal resilience with a greater impact on Finnish society in terms of intensity than had previously been the norm. The comprehensive security concept is a kind of collaborative model designed to strengthen societal and national resilience, bringing together vital parts of society and stakeholders. All civil society organisations and citizens have a role to play.

Finland's security strategy concerns the protection of vital public interests, which is achieved jointly by authorities, businesses, NGOs and citizens. Responsibilities and tasks are defined by law. The supervisory body is the Finnish Security Committee. This committee sets the agenda, gives advice and provides an annual security report to the prime minister and the government. The annual report includes both public and private perspectives; it contains a report on the annual state of security in Finland and is considered to be of the utmost strategic importance. The committee also issues publications on the national security strategy and national cybersecurity.

Government and society meet in the Finnish Security Committee, which includes representatives from ministries, the security services, the armed forces, CEOs of critical businesses, universities, infrastructure, the financial sector and a number of NGOs. The committee is chaired by the Minister of Defence.

In addition to the Security Committee, there is a national fund – raised through taxes – which is used to increase and maintain resilience. The fund, which amounts to billions of euros, is managed by the National Emergency Supply Agency (NESA).[147] NESA is affiliated to the Security Committee; it is an institution that provides the country with stockpile management in the event of a crisis, either due to hybrid threats or in times of conventional war. Partly for this reason, Finnish companies are required to put some of their production capacity at the service of the state. Almost 1,000 companies from different sectors are involved.

NESA is an organisation dedicated to national preparedness. It manages a state fund for strategic vital expenditure, critical materials, products, fuel, and so on. It is also responsible for compensating businesses that incur costs for the purpose of boosting resilience and replenishing essential supplies. NESA also gathers information relating to potential threats. Banks and businesses are involved too. NESA can operate fairly independently, but ministerial responsibility for NESA rests with the Minister of Economic Affairs.

This Finnish prevention method also has a clear cognitive effect. In reality, the comprehensive security model is mainly about reinforcing psychological resilience and national collective awareness. Through enhanced interaction between international and EU activities, defence, the national security system, the economy, infrastructure, functional capabilities of society and service provision, a sense of collective security can be increased. This is only possible if citizens themselves actively contribute. In Finland, some 50,000 shelters have been built to accommodate nearly 5 million citizens. These are maintained collectively. There is also an efficient public alarm system. In addition, most Finns have shelters and enough provisions in their homes to survive the first 72 hours of a crisis.

Besides the Security Committee and NESA, Finland also has a National Defence Course as a third major instrument to promote societal resilience. This course, which is certified and highly regarded, is funded from the Ministry of Defence's budget. It is a 3½ to 4-week course in which civilian trainees are divided into different cohorts and groups. These groups meet once every so often for course sessions, thus creating networked groups of citizens trained in societal resilience. The Chief of Defence invites people to attend this course, taking account of the different backgrounds and sectors these individuals represent.

## ► 5.4 Greater societal engagement

The threat level in Finland is of course different to that in the Netherlands. Nevertheless, the AIV is of the opinion that the Finnish approach provides sufficient starting points and interesting angles that are relevant to Dutch security policy. The AIV considers it to be of national importance that Dutch citizens be asked to make an active contribution to the reinforcement of societal resilience. It should be relatively straightforward to reorganise security networks in the Netherlands. The task of mobilising society to improve security requires a collaborative effort.

To protect the Netherlands' open society, public order and the democratic legal system, the whole of society needs to be involved in thinking about security policy. This starts with raising security awareness among the public, government authorities, businesses and other private actors and providing them with the tools they need to build resilience.

The Netherlands Defence Academy (NLDA) recently joined forces with the NCTV to launch the National Security Course, the aim of which is to increase knowledge about the Defence organisation and security issues and to promote a shared network of people who could, or already do, play a role in terms of national security. Course participants come from the government, knowledge institutions and the private sector. The AIV regards such initiatives as confirmation of the assumption that this is the right time to work on broad-based societal resilience. The AIV would encourage a further roll-out

and institutionalisation of this curriculum into a fully-fledged, society-wide course, with a focus on hybrid threats and foreign influence and interference. The course should be developed further and implemented more widely, specifically for those in leadership positions in government, business, civil society organisations such as media and NGOs, and utility companies operating in critical infrastructure; this is to create a shared threat assessment and provide potential courses of action in the context of resilience.

The Ministry of Defence will have to focus more explicitly on the interaction between government and the public. Efforts to expand the reservist pool, the further roll-out of a social conscription system and the recently launched Defence Service Year (an opportunity for young people to gain experience of working in the military) could feature more prominently in promoting security awareness among Dutch citizens.

To strengthen societal resilience, civic engagement and civic participation will also need to be increased. The AIV sees great potential in the use of citizens' assemblies, which have already been established in various countries.[148] In a citizens' assembly, a group of citizens are asked to draw up recommendations for their respective municipality, province or country.[149] A citizens' assembly consists of a group of around 100 to 250 people – selected by lottery and ideally reflects society – in which participants conduct extensive dialogue with each other and possibly with politicians or policymakers and have freedom of access to information.[150] A number of Dutch cities and provinces are currently experimenting with citizens' assemblies, usually on societal issues such as municipal waste, fireworks and climate policy, and there is now a National Citizens' Assemblies Network.[151] Initial results have been positive.[152] Other countries have already been using citizens' assemblies such as this for some time now.

It is partly through citizens' assemblies that pluralism, an essential condition for a healthy democracy, can be strengthened. This is also why the Council of Europe recently set up a European citizens' assembly, in which a group of Europeans deliberate on the future and strengthening of democratic resilience in Ukraine.[153]

Societal resilience also includes protection against cyberattacks. As the AIV set out in Chapter 2, it is precisely in the sphere of digital connections that the Netherlands is vulnerable. Members of the public need to be equipped to protect themselves properly against cyberattacks. Citizens themselves have a responsibility here – how do they arrange their cybersecurity at home? – but so too does the government. The provision of digital literacy courses and improvements in digitalisation could help, as could the further expansion of school subjects to promote media literacy and the ability to recognise disinformation. Government supervision of digital developments also needs to be intensified. The AIV is pleased to note that both the Senate and the House of Representatives have now set up a permanent committee on Digital Affairs. The AIV believes the appointment of a rapporteur on digital affairs to be the next necessary step.

## ► 5.5 A European whole-of-government approach

The European Strategic Compass provides for the development of the Hybrid Toolbox. The Netherlands was one of the initiators of this feature. The toolbox encourages EU member states to improve interoperability in their fight against hybrid attacks and the actual implementation of counter-hybrid instruments. The EU Council Conclusions of 21 June 2022 regarding a framework for a coordinated EU response to hybrid campaigns represented the first step in the implementation and further development of this toolbox.[154]

The AIV endorses the importance of intensive EU coordination on hybrid threats.[155] The toolbox is important, but does not yet address actual operationalisation or crisis management in the event of serious disruption. In addition to the EU, the Netherlands itself should also take a critical look at its own supervision and apply itself to the further development or implementation in the Netherlands of measures and guidelines arising from the Hybrid Toolbox, the Democracy Action Plan and the Defence of Democracy package.

## 5.6 The Netherlands and NATO's baseline requirements for national resilience

The Dutch government is lagging far behind the Nordic countries in terms of the whole-of-government and whole-of-society approach. The Netherlands' current approach does not match the broad scope of threats or attacks. The government's actions are often incident-driven, fragmented and reactive. Nevertheless, the AIV believes that both approaches are necessary to deal effectively with the broad range of hybrid threats. It is with good reason that experts have been known to describe a hybrid attack as a 'holistic attack', precisely because of its broad impact.[156] If the Netherlands is to arm itself against this, broad-based national coordination is required.

The Dutch approach tends to result in an ad hoc creation of crisis teams or a sector-based response. In the healthcare sector, for example, there was no flexible layer to allow upscaling in a crisis, as became clear during the COVID-19 pandemic. Furthermore, in terms of security, the designated safety regions currently function reasonably well, but the focus is exclusively sector- and region-based. As a result, there is insufficient oversight of the international nature of hybrid threats.

The Dutch approach is therefore inconsistent with Article 3 of the North Atlantic Treaty, according to which NATO member states should, separately and jointly, in common with other states, ensure that their own resilience and defence are in order. Besides the urgent need for allies to spend a minimum of 2% of GDP on defence, their societies must also be prepared for non-military attacks.

Since the 2016 NATO summit in Warsaw, where hybrid threats were discussed specifically, the seven baseline requirements for national resilience have been established. These baseline requirements focus on the continuous functioning of public services, energy supplies, food and water supplies, the ability to deal with large movements of groups of people, the ability to deal with mass casualties and the guaranteed functioning of communication and transportation systems. In other words, the critical processes needed to sustain society, not in the least in times of crisis or war.

The seven baseline requirements make it possible to harmonise the resilience of the different states, which is important in terms of interoperability. Hybrid threats do not stop at national borders. At the NATO summit in Madrid in 2022, therefore, the old Civil Emergency Planning Committee (CEPC) was revitalised and renamed the NATO Resilience Committee, which is the advisory body for allies' resilience and civil preparedness. Important guidelines have been drawn up to which countries have committed and under which countries must ensure that their resilience is in order.

> 'Each NATO member country needs to be resilient against military and non-military threats and challenges to the Alliance's security, such as natural disasters, disruption of critical infrastructure, or hybrid or armed attacks. Resilience is both a national responsibility and a collective commitment rooted in Article 3 of the North Atlantic Treaty.'[157]

At the NATO summit in Vilnius in July 2023, the NATO allies decided to translate the requirements into definitive resilience objectives. The Netherlands started national implementation of these objectives, coordinated by the NCTV, in autumn 2023.

The AIV considers the NATO requirements to be highly important, and essential for establishing societal resilience. When defining national resilience objectives, it is vital that societal stakeholders such as businesses, financial institutions and knowledge institutions be involved as well as partner states.

The AIV notes, however, that NATO's proposed resilience objectives centre mainly on physical civil resilience goals. Less emphasis is given to threats arising in the virtual and cognitive dimensions. Consequently, the NCTV will need to concentrate its efforts on integrating this type of threat into security analyses. In addition, the Netherlands will need to call for a greater focus within NATO on threats in the virtual and cognitive dimensions.

## ► 5.7 The National Security Council, a vulnerability assessment and the resilience strategy

The starting point for NATO's collective resilience is a national vulnerability assessment. Every year, countries identify their vulnerabilities on the basis of the seven baseline requirements and draw up a specific plan of action to address those vulnerabilities.

This assessment considers not only the continued functioning of society at national level but also how that society can continue to support the deployment of national armed forces as well as the deployment of NATO as a whole. An example for the Netherlands in this respect is its role in host nation support. The Netherlands is a transit country for troops moving from countries such as the US, Canada and the UK and as such plays an important role with its infrastructure in the support and sustainment of the deployment of NATO troops.

This requires a proactive, anticipatory and comprehensive whole-of-government approach from the Netherlands. In troop movement exercises, the Netherlands has now been designated as a transit and host nation. That means that when large-scale military movements occur, the Netherlands plays a major role with its railways, port facilities, logistic processes and air bases, which are all directed by the Royal Netherlands Army's Territorial Operations Centre (TOC). This NATO task is, however, still too heavily directed by the Ministry of Defence, together with other civil stakeholders. The same applies to the EU's Permanent Structured Cooperation (PESCO) project, in which the Netherlands plays an important coordinating logistic role as well. Exercises such as this could be more firmly embedded in the Dutch national consciousness; citizens could make a more active contribution in this respect.

The AIV believes that the National Security Council (NVR), which was established in 2022, should be the designated umbrella organisation in this respect. The NVR should review the security situation in the Netherlands at least twice a year. On the first occasion, it would do so on the basis of a threat assessment by the MIVD, AIVD and NCTV, in which the government focuses on identifying the threats posed by potential adversaries and actors and the response to them. On the second occasion, the NVR should look at Dutch government and society and at critical processes: how vulnerable is society? What can the government do to mitigate that vulnerability pre-emptively? And what can society itself do to help?

Specific sectors of society could take the lead in producing these vulnerability assessments; they are after all best placed to know where the potential threats lie within a sector. As preparation for the discussion in the National Security Council, the different sectoral contributions should be merged into a single overarching vulnerability assessment, aligned and analysed for cross-sectoral impact in order to prevent fragmentation.

Besides a vulnerability assessment, the NVR will also need to produce a 'resilience strategy', focusing specifically on hybrid threats. Based on the vulnerabilities of the critical processes, a clear political choice will also have to be made about what interests need to be defended and for what purpose certain policy choices are made. The strategy should not be produced in isolation and should not be fragmented. The NVR will need to operate across sectors.

## ► 5.8 Institutional reinforcement of the NVR

The AIV maintains that the NVR should be organised differently. At the moment, the Council still 'only' functions as a cabinet subcommittee, which by no means includes all ministries or stakeholders. Neither does the current body have any formal executive powers to issue instructions. Its current set-up suggests too narrow a view of national security. Given that hybrid conflict affects so many sectors, a much broader approach is needed in the NVR. An attack could after all occur in a much wider area than just the 'traditional' security domains.[158]

The AIV is of the opinion that the NVR will therefore have to be strengthened. Horizontal and vertical integration will have to be guaranteed and ideally, the council would be positioned above the ministries wherever possible, reporting directly to the prime minister. All ministries should be represented in the NVR, as should the security services, businesses and knowledge institutions. The financial sector should also be represented, for example through the incorporation of the TCO in the NVR (see Chapter 2). The AIV believes there should be a more explicit focus on threats in the virtual and cognitive dimensions.

To more centrally embed, direct and align the above vulnerability assessments and resilience strategies, a consultative body or executive committee at senior civil service level is required for the National Security Council. This consultative body or executive committee should be supported by its own secretariat.

## ► 5.9 A different institutional form

Besides an altered and broader configuration for the NVR, a different type of body could also be considered. Given that hybrid threats actually affect all ministries and that resilience is a society-wide issue, the AIV believes it would be advisable to establish an overarching governance structure.

HCSS recently published a comprehensive study on how the Dutch government could structure an effective response to hybrid threats. The report talks about a 'proactive counter-hybrid response', whereby the Dutch government would not merely react in the event of an attack, but would actually anticipate hostilities.[159] The government should also seek measures that strengthen its own resilience while at the same time weakening the capabilities of an adversary, provided, as HCSS points out, that this is both desirable and permissible as well as compatible with the legal frameworks to which the Netherlands adheres as a liberal democracy.

This counter-hybrid campaign would effectively link together strategic, tactical and operational actors. For this to happen, it is essential that government authorities, businesses and knowledge institutions, as well as the armed forces and society in general, are more aligned with each other. Like HCSS, the AIV believes that with this aim in mind, the Dutch government should create institutional or legal frameworks to streamline cross-domain cooperation. An integrated counter hybrid campaign also requires political support.

This counter-hybrid approach requires a resilient society. And this resilience needs to resonate in the governance structure. Resilience issues must, therefore, be clearly designated and mandated. The United Kingdom has a minister of state for communities and resilience, in the Department for Levelling Up, Housing and Communities. This minister deals intensively with a wide range of societal resilience matters, such as the coastguard, waterways, crisis management in emergency situations, financial crises, port facilities, support for local authorities, businesses and so on. It might also be possible for the Netherlands to appoint a minister or state secretary for societal resilience, to address the broad societal impact of hybrid threats and increase society's resilience.

# Endnotes

1 'Request for advice on hybrid threats', the Minister of Defence and the Minister of Foreign Affairs, 12 July 2022.

2 Rodrigue Demeuse and Joëlle Garriaud-Maylam (2023), 'The Russian War on Truth. Defending allied and partner democracies against the Kremlin's disinformation campaigns', General Report, 8 October 2023.

3 'Undermining Ukraine. How Russia widened its global information war in 2023', Atlantic Council, Research report, 29 February 2024.

4 'Tsjechische geheime dienst: "Rusland betaalde cash aan bevriende Nederlandse en Europese politici"', *Algemeen Dagblad*, 28 March 2024.

5 Minister of the Interior and Kingdom Relations. 'Reactie op verzoek van het lid Wilders over het bericht dat volgens de Tsjechische geheime dienst Rusland cash betaalde aan Nederlandse en Europese politici', 1 April 2024.

6 Paul Charon and Jean-Baptiste Jeangène Vilmer (2021), 'Chinese Influence operations. A Machiavellian Moment', IRSEM.

7 'Met de rug naar de samenleving. Een analyse van de soevereinenbeweging in Nederland', AIVD report, 9 April 2024. Soevereinenbeweging ondermijnt democratische rechtsorde | Nieuwsbericht | AIVD.

8 Unesco | Beemster Polder.

9 Cybersecurity vitale waterwerken niet waterdicht | News item | Court of Audit.

10 Rob de Wijk, Frank Bekkers and Tim Sweijs, 'Hybride dreigingen en hybride oorlog: consequenties voor de Koninklijke Landmacht',HCSS Security report, 15 October 2020.

11 Reference can be made in this respect to the theory of unrestricted warfare of the Chinese military theorists Qiao Liang and Wang Xiangsui or Thomas Huber's compound warfare. See Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing 1999); Thomas M. Huber (ed.); *Compound Warfare. That Fatal Knot* (Pacific University Press, Forest Grove, Or. 2004). Hoffman, 2007, p. 8.
The actual founder of the modern Western interpretation of the concept of hybrid warfare was Frank G. Hoffman. Around 2007 he applied the concept to the asymmetrical conflicts between the state of Israel and non-state actors (proxy militias) such as Hezbollah and Hamas.

12 'Request for advice on hybrid threats', the Minister of Defence and the Minister of Foreign Affairs, 12 July 2022.

13 David Kimsey, Jin Woo Kim, John McCoy et al., 'Utilization of the DIMEFIL Framework in a Case Study Analysis of Security Cooperation Success', *Small Wars Journal*, 8 November 2020.

14 'Hybrid and cyber-threats by foreign actors', European Commission, Competence Centre on Foresight, 21 December 2021;
Cf. M. Normark (2019), 'How states use non-state actors: a modus operandi for covert state subversion and malign networks, Hybrid CoE'.
AIVD, 2021 annual report.
Cf. 'China vormt grootste bedreiging voor kennisveiligheid, zegt de AIVD', 17 April 2023. China vormt grootste dreiging voor kennisveiligheid, zegt de AIVD - ScienceGuide

15 Martin Crilly and Alan Mears, 'Multi Dimensional and Domain Operations (MDDO)', Wavell Room, 26 January 2022. https://wavellroom.com/2022/01/26/mddo/

16 Zsolt Haig and Veronika Hajdu (2017). 'New Ways in the Cognitive Dimension of Information Operations', *Land Forces Academy Review*, 22(2).

17 Petra Vejvodová (2019), 'Information and Psychological Operations as a Challenge to Security and Defence', *Czech Military Review*, no. 3, 83-96. DOI: 10.3849/2336-2995.

18 RAND (2019), 'The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment', Research report.

19 'Cognitive Warfare: Strengthening and Defending the Mind', NATO's Strategic Warfare Development Command, 5 April 2023.

[20] Georgii Pocheptsov (2018), 'Cognitive Attacks in Russian Hybrid Warfare', *Information & Security*. An International Journal, vol. 41, pp. 37-43.

[21] Yuriy Danyk, Chad M. Briggs, 'Modern Cognitive Operations and Hybrid Warfare', *Journal of Strategic Security*, Vol. 16, No. 1 (2023) 35-50. Cf. 'The Emerging Risk', RAND.

[22] Pocheptsov, 'Cognitive Attacks'.

[23] Sandor Fabian. (2019). 'The Russian hybrid warfare strategy – neither Russian nor strategy', *Defense & Security Analysis*, Vol 35, No 3 (tandfonline.com); Cf. Frank G. Hoffman (2007), 'Conflict in the 21st century: the rise of hybrid wars', Potomac Institute for Policy Studies. Arlington, Virginia.

[24] NCTV (2023). 'Security Strategy for the Kingdom of the Netherlands'. For European definitions and approaches, see also: Dick Zandee, Sico van der Meer, Adája Stoetman (2021). 'Countering hybrid threats. Steps for improving EU-NATO cooperation', Clingendael Report.

[25] Overview of critical processes, drawn up by the NCTV: https://english.nctv.nl/topics/critical-infrastructure-protection.

[26] AIVD, MIVD, NCTV, 'Threat Assessment State-sponsored Actors 2', November 2022; NCTV, Rijksbrede Risicoanalyse Nationale Veiligheid.

[27] AIVD, MIVD, NCTV (2021). 'Threat Assessment State-sponsored Actors'.

[28] Soevereinenbeweging ondermijnt democratische rechtsorde | Nieuwsbericht | AIVD.

[29] The Scientific Council for Government Policy is currently working on an advisory report that will extensively discuss the functioning of democracy and the use of media. See: https://english.wrr.nl/topics/media-and-democracy.

[30] 'Regulating Online Content: Towards a Recalibration of the Netherlands' Internet Policy', AIV advisory report no. 113, 24 June 2020.

[31] Monica den Boer and Mark Helgers (2022), 'Schermutselingen aan de Europese buitengrens. Tijd voor een integrale strategie', *Militaire Spectator*, vol. 191, no. 7/8, 410-421.

[32] 'Migrants say Belarusians Took them to E.U. Border and Supplied Wire Cutters', *The New York Times*, 13 November 2021. Cf.: Desperate Iraqis the latest pawn in Belarus standoff with EU | CBC News; Baghdad to Lithuania: how Belarus opened new migration route to EU – LRT Investigation – LRT.

[33] Alexander Leeuw (2021), 'Dagelijks duizend cyberaanvallen bij een waterschap', *Binnenlands Bestuur*, 6 September.

[34] Beleidsnota Drinkwater 2021-2026. 'Samen werken aan een toekomstbestendige drinkwatervoorziening', Ministry of Infrastructure and Water Management, p. 11. Cf. https://www.trouw.nl/binnenland/hoe-kwetsbaar-is-onze-drinkwatervoorziening~bf1b14ee/.

[35] First Chinese freight train arrives in Serbia - Xinhua | English.news.cn (xinhuanet.com).

[36] Joris Teer and Mattia Bertolini, 'Reaching Breaking Point: The Semiconductor and Critical Raw Material Ecosystem at a Time of Great Power Rivalry', HCSS, October 2022.

[37] 'Rekenkamer: veel mis met digitale beveiliging van Schiphol' (nos.nl).

[38] Advocated by European Commission Vice-President Margaritis Schinas and Commissioner Health and Food Safety Stella Kyriakides: Europa heeft een nieuwe aanpak op het gebied van geneesmiddelen nodig. - Europese Commissie

[39] The AIV is therefore concerned by the fact that major pharmaceutical company InnoGenerics – responsible for patent-free medicines – went bankrupt in 2022 while it is not immediately clear how the Netherlands can build up emergency stockpiles of medicines.

[40] Chris Miller, (2024), 'Taiwan's security came into question just when they became an irreplaceable supplier of chips', Atlantic Commission, 18 January. Cf. Joris Teer, Mattia Bertolini, and Benedetta Girardi (2023), 'Great power competition and social stability in the Netherlands: The risks of Russian gas, Chinese raw materials and Taiwanese chips to vital sectors', Research report, The Hague Centre for Strategic Studies (HCSS), March. https://hcss.nl/news/great-power-competition-and-social-stability-in-the-netherlands/.

[41] 'Bestuurlijke netwerkkaarten crisisbeheersing', Netwerkkaart 27: Financieel verkeer. Netherlands Institute for Public Safety, February 2021.

42 Ibid.

43 Ibid.

44 'Begroting Monetaire Zaken 2023', De Nederlandsche Bank; Cf. 'Bestuurlijke netwerkkaarten crisisbeheersing', Netwerkkaart 27: Financieel verkeer. Netherlands Institute for Public Safety, February 2021.

45 'Grote interesse bij bedrijven voor ontwikkeling van een nieuwe onderzeese datakabel die Londen en Rotterdam verbindt',Dutch Data Center Association, 14 September 2023 (dutchdatacenters.nl).

46 Cf. 'Een onderzeese datakabel tussen Londen en Rotterdam voor een betrouwbaarder internet', Innovation Origins, 16 September 2023.

47 'Undersea 'hybrid warfare' threatens security of 1bn, Nato commander warns', *The Guardian*, 16 April 2024.

48 Frank Bekkers and Esther Chavannes (2019), 'Geopolitiek en maritieme veiligheid. De visie van HCSS op de toekomstige inrichting van de Koninklijke Marine', *Marineblad*, December.

49 https://www.rijksoverheid.nl/actueel/nieuws/2023/12/19/defensie-koopt-middelen-en-materieel-om-noordzee-te-beschermen.

50 For the Dutch Subsea Cable Coalition, see: https://ecp.nl/project/zeekabel-coalitie/.

51 AIVD, 2022 Cyber Security Assessment Netherlands, 4 July 2022.

52 The National Cyber Security Centre (NCSC) of the Ministry of Justice and Security is being merged with the Computer Security Incident Response Team for digital services (CSIRT-DSP) and the Digital Trust Centre (DTC) of the Ministry of Economic Affairs and Climate Policy.

53 'Rapportage datalekken 2023', Dutch Data Protection Authority, 10 April 2024.

54 The AIV believes that businesses that specifically serve a national interest in this respect must receive recognition for this. The granting of OKTT status (which allows an organisation to receive timely government information on incidents and threats so that they can inform other organisations or the public accordingly) by the Minister of Justice and Security to the CISO Circle of Trust Foundation (CCoT) is a positive development in this regard. See (in Dutch): Stichting NL CISO Circle of Trust verkrijgt OKTT-status | Nieuwsbericht | Nationaal Cyber Security Centrum (ncsc.nl). This was apparent during the banking crisis in 2008, and more recently in 2022, when Credit Suisse bank lost billions of euros in a very short time due to media reports about corrupt financial practices, speculation and mismanagement. In the end, the bank could be saved; however, there was substantial panic in the Europe's financial sector, including in the Netherlands

55 NCC Group (previously Fox-IT).

56 Alexandre Gomes and Maaike Okano-Heijmans (2024), 'Too late to act? Europe's quest for cloud sovereignty', Clingendael Report, March.

57 Cf. 'Autonomous weapons. The importance of regulation and investment', AIV advisory report no. 119, CAVV advisory report no. 38, 3 December 2021. See also the interview with Professor Bart Schermer, 12 May 2021: https://ddma.nl/kennisbank/ bart-schermer-consideratie-met-een-ethische-werkwijze-hoef-je-niet-bij-elke-nieuwe-wet-je-businessmodel-aan-te-passen/.

58 Bart Schermer (2022) 'De gespannen relatie tussen privacy en cybercrime', Inaugural address delivered at Leiden University, 7 November 2022.

59 Letter to the House of Representatives on progress made in the approach to knowledge security in higher education and academia (in Dutch), 23 December 2022.

60 This applies in particular to organisations such as the Education Executive Agency (DUO) and their attitude to students with a migration background. Cf. Kabinet maakt excuses voor indirecte discriminatie bij controles op de uitwonendenbeurs | Nieuwsbericht | Rijksoverheid.nl (in Dutch). See also (in Dutch): https://www.nrc.nl/nieuws/2024/03/01/rapport-indirecte-discriminatie-bij-controles-op-fraude-met-uitwonendenbeurs-a4191795.

61 'Curaçao ligt aan de ketting van een land in crisis', *NRC*, 13 January 2018.

62 'Guyana warns Venezuela's Maduro he risks becoming pariah ahead of talks', *The Guardian*, 14 December 2023.

[63] When it comes to the ABC islands, relations between the Netherlands and Venezuela have been tense for more than a century. In the 1902-1908 period, the two countries even came to the brink of war.

[64] 'Venezuela – Country Focus', European Union Agency for Asylum Country Focus report, November 2023; Rafael Romo, 'Maduro's immigration card could influence America's election, not just Venezuela's'. CNN, 7 February 2024.

[65] Cf. 'Security and the legal order in the Caribbean: Steps necessary to future-proof the Kingdom of the Netherlands', AIV advisory report no. 116, 10 September 2020.

[66] https://www.rijksoverheid.nl/documenten/woo-besluiten/2023/05/26/besluit-op-woo-verzoek-over-machtigingen-onderzeekabel-saba-en-sint-eustatius.

[67] Cf. 'Security and the legal order in the Caribbean', p. 9.

[68] Rob de Wijk, Frank Bekkers and Tim Sweijs, 'Hybride dreigingen en hybride oorlog: consequenties voor de Koninklijke Landmacht', HCSS Security report, 15 October 2020.

[69] Brin Najžer, The Hybrid Age. *International Security in the Era of Hybrid Warfare* (Bloomsbury Publishing Plc, London, New York, Dublin, 2020).

[70] David Ignatius, 'Is Russia trying to sway the U.S. election?', Belfer Center for Science and International Affairs, 31 July 2016; Christian Kaunert, 'EU Eastern Partnership, Hybrid Warfare and Russia's Invasion of Ukraine', 11 August 2022.

[71] 'The War in Ukraine: a Geopolitical "Time Shock"', AIV advisory letter, 18 October 2022. Cf. Frans Osinga, 'Putin's War, A European Tragedy: Why Russia's War Failed and What It Means for NATO' (2024), in: Maarten Rothman, Lonneke Peperkamp and Sebastiaan Rietjens (ed.), *Reflections on the Russia-Ukraine War*. Leiden University Press, pp. 123-146.

[72] Michael Connell and Sarah Vogler, 'Russia's Approach to Cyber Warfare', CNA research paper, March 2017.

[73] S.C. Morrell and M.E. Kosal, 'Military Deception and Strategic Culture: The Soviet Union and Russian Federation', *Journal of Information Warfare*, Vol. 20, No. 3 (summer 2021), pp. 127-145; Michael Kofman, 'Russian Hybrid Warfare and the other Dark Arts', War on the Rocks, 11 March 2016.

[74] Russia is active in both the physical dimension and the virtual and cognitive dimensions. Various groups that are active in the cyber domain are tolerated – such as criminal organisations that make their money by means of ransomware attacks on non-Russian businesses and government authorities – or are even actively deployed by the Russian government. This is apparent from, for instance, an analysis of various cyber sabotage groups affiliated with the Russian military intelligence service GRU, such as the cyber group Sandworm. Sandworm has been linked to 'Unit 74455', the GRU's Main Centre for Special Technologies. This unit was established to undermine the Ukrainian armed forces and society by means of cyber operations. Its three main tasks are cyber espionage, active cyberattacks and online psychological influence, which are also used to support conventional warfare operations. An extensive analysis of the unit by Mandiant, a leading international firm in cybersecurity and cyber intelligence and part of Google, describes how over the years this unit's cyber operations have also been conducted outside Ukraine, with major consequences for free societies, NGOs, journalists, civil society, knowledge institutions and businesses. Multilateral organisations such as OPCW have also been targeted. For this reason, Google has designated this group as an 'Advanced Persistent Threat' (APT44).
See also the condemnation by the EU member states of Russian cyber activities conducted by APT28, i.e. Fancy Bear: 'Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation', 3 May 2024.
See: Gabby Roncone, Dan Black, John Wolfram et al., 'APT44: Unearthing Sandworm', Mandiant-Google report, 2024.
Cf. 'Google's Mandiant elevates Russian threat group Sandworm to APT44', Cybernews.

[75] Cf. Dmitry Adamsky (2023), *The Russian Way of Deterrence. Strategic Culture, Coercion, and War*. Stanford University Press.

[76] AIV advisory letter 'The War in Ukraine: a Geopolitical "Time Shock"'.

77 Michael Raska, 'China and the "Three Warfares"', *The Diplomat*, 18 December 2015.

78 The most pertinent example is the claim that Taiwan is part of China, which would legitimise annexation. See Dean Cheng (2012), 'Winning Without Fighting: Chinese Legal Warfare', The Heritage Foundation.

79 'China Spins Tale That the U.S. Army Started the Coronavirus Epidemic', *The New York Times*, 13 March 2020.

80 Andrew Scobell, 'The Chinese Way of War', in John Andreas Olsen and Martin van Creveld (eds), *The Evolution of Operational Art: From Napoleon to the Present* (Oxford, 2010; online edn, Oxford Academic, 1 January 2011).

81 Xi Jinping (2020) 'Major Issues Concerning China's Strategies for Mid-to-Long-Term Economic and Social Development', CSIS Interpret: China, 31 October. Cf. Timothy R. Heath, Derek Grossman, Asha Clark (2021), 'China's Quest for Global Primacy. An Analysis of Chinese International and Defense Strategies to Outcompete the United States', RAND Research report.

82 J. Aukia (2021). 'China as a hybrid influencer: Non-state actors as state proxies', Hybrid CoE Research Report No. 1.

83 J. Willard, 'The US and Hybrid Challenges: Past, Present and Future', in: M. Weissmann, N. Nilsson and B. Palmertz (eds.), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (Bloomsbury Collections 2022) pp. 157-172; I. Käihkö, 'The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession', *The US Army War College Quarterly: Parameters*, 51(3), 2021, pp. 115-127.

84 https://smallwarsjournal.com/jrnl/art/counter-hybrid-warfare-winning-gray-zone.

85 US Department of Defense, Fact Sheet: 2023 DoD Cyber Strategy.

86 In 2015, NATO Secretary-General Jens Stoltenberg put into words the multifaceted meaning of hybrid threats for NATO: 'Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them'. Keynote speech by NATO Secretary-General Jens Stoltenberg at the opening of the NATO Transformation Seminar, 25 March 2015.

87 NATO - Topic: Countering hybrid threats.

88 Through a large grant programme, the DIANA programme invests in support and development of new technology. There is a particular focus on bringing together scientists, engineers, industry and end-users (government). For more on NATO's DIANA programme, see https://www.diana.nato.int/about-diana.html.

89 NATO - Topic: Relations with partners in the Indo-Pacific region

90 Dick Zandee, Sico van der Meer and Adája Stoetman (2021), 'Countering hybrid threats: steps for improving EU-NATO cooperation', Clingendael report.

91 For the NATO Strategic Communications Centre of Excellence, see: StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia (stratcomcoe.org).

92 action_plan_against_disinformation.pdf (europa.eu).

93 Non-intervention provisions in the United Nations Charter; Helsinki Final Act of 1975; 1990 Paris Charter; 1997 Treaty of Friendship, Cooperation and Partnership between Ukraine and the Russian Federation; 1994 Budapest Memorandum on Security Assurances. Cf. The Crimean Factor: How the European Union Reacted to Russia's Annexation of Crimea | Warsaw Institute.

94 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

95 For an explanation of Article 42(7) of the Treaty on European Union on collective defence, see https://eur-lex.europa.eu/EN/legal-content/glossary/collective-defence.html. Cf. Report of the parliamentary committee debate on the 2022 Defence White Paper: A stronger Netherlands, a safer Europe (in Dutch).

96 P.A.L. Ducheine and B.M.J. Pijpers, 'Cyberoperaties en de EU', *Militaire Spectator*, 1 August 2022.

97 What is Hybrid CoE? - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats.

98 For the EU Hybrid Toolbox see: https://www.consilium.europa.eu/en/press/press-

releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/. Cf. Kenneth Lasoen (2022), 'Realising the EU Hybrid Toolbox: opportunities and pitfalls', Clingendael Policy Brief, December.

99 Cf. https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/.

100 CCDCOE

101 According to the Strategic Compass of the European Union, hybrid activities are used to exploit an opponent's weaknesses and make them work to one's own advantage. This is done by deploying using various instruments in a coordinated manner, without ever crossing the threshold of formal warfare. Cf. Factsheet 'Countering Hybrid Threats', Strategic Compass of the European Union, March 2022.

102 Jakob Albers, 'Is Europa's antwoord op China's Nieuwe Zijderoute meer dan een druppel in de oceaan?', *MO Magazine*, 17 March 2023.

103 Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk and Marta Kepe (2019), 'Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War', RAND Corporation.

104 Morris et al., p. 45.

105 Morris et al., pp. 53-57.

106 https://www.zeit.de/gesellschaft/zeitgeschehen/2017-12/fancy-bear-russland-hacking-ap-us-geheimdienst.

107 https://duitslandinstituut.nl/artikel/58396/rusland-heeft-top-duitse-luchtmacht-afgeluisterd.

108 Rob de Wijk, Frank Bekkers and Tim Sweijs, 'Hybride dreigingen en hybride oorlog: consequenties voor de Koninklijke Landmacht', HCSS Security report, 15 October 2020.

109 Cf. Richtsje Kurpershoek, Alejandra Muñoz Valdez and Wim Zwijnenburg (2021), 'Remote Horizons. Expanding use and proliferation of military drones in Africa', PAX for Peace research report.

110 'Elon Musk bezoekt met premier Netanyahu verwoeste kibboets', NOS, 27 November 2023. https://nos.nl/video/2499464-elon-musk-bezoekt-met-premier-netanyahu-verwoeste-kibboets.

111 Alvaro Pastor (2024), 'Cognitive warfare', HAL open science.

112 A. Nollkaemper, *Kern van het internationaal publiekrecht*, 9th edn, Boom Juridische Uitgevers, The Hague, 2022, p. 343, note 4. In this context, see also M.N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd edn, (Cambridge University Press 2017), which focuses on how jus ad bellum and jus in bello (IHR) apply to cyber operations.

113 Nollkaemper, p. 242 and ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, ICJ Reports 1986, para. 205.

114 Cf. AIV/CAVV advisory report 'Autonomous weapons. The importance of regulation and investment', pp. 32-33. See also: Berenice Boutin, 'Legal Questions Related to the Use of Autonomous Weapon Systems', Paper prepared for the AIV/CAVV Combined Advisory Committee on updating the Advisory Report Autonomous Weapons (CAAW). Asser Institute, June 2021. For a further legal elaboration, see also: Linell A. Letendre, 'Lethal Autonomous Weapon Systems: Translating Geek Speak for Lawyers', International Law Studies, vol. 96 (2020), pp. 278-282.

115 R. Heinsch, 'International Humanitarian Law', in: C. Rose et al (eds), *An Introduction to Public International Law* (Cambridge University Press, (2022) p. 234.

116 Ibid.

117 Cf. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en.

118 J. Brown (2018), 'An Alternative War: The Development, Impact, and Legality of Hybrid Warfare Conducted by the Nation State', *Journal of Global Faultlines*, Vol. 5, No. 1-2 (October-December), pp. 58-82.

119 https://data.consilium.europa.eu/doc/document/PE-34-2023-REV-1/en/pdf and www.wto.org.

120 Nollkaemper, p. 408 and ICJ, Legality of the Use by a State of Nuclear Weapons in Armed Conflict, Advisory Opinion, ICJ Reports 1996, para 29.

121 Cf. AIV/CAVV advisory report 'Autonomous weapons. The importance of regulation and

investment'.

122 The EU Cyber Diplomacy Toolbox (cyber-diplomacy-toolbox.com).

123 Report of written consultations on the International Cyber Strategy, House of Representatives (2023).

124 CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence. Cyberattacks and Article 5 – a note on a blurry but consistent position of NATO.

125 J. Brown (2018). 'An alternative war: The development, impact, and legality of hybrid warfare conducted by the nation state', *Journal of Global Faultlines*.

126 Ibid.

127 Mark Galeotti, (2022), *The Weaponization of Everything. A Field Guide to the New Way of War*. Yale University Press. New Haven.

128 For an explanation of Article 97, on the armed forces, of the Constitution, see denederlandsegrondwet.nl.
K.T. Meijer, 'Artikel 97 Grondwet. Wetenschappelijk commentaar', written on the basis of the commentary on Article 97 by J. van Schooten-van der Meer in: A.K. Koekkoek (red.), *De Grondwet. Een systematisch en artikelsgewijs commentaar*, Deventer: W.E.J. Tjeenk Willink, 3rd edn (2000).
See: Nederlandsche Rechtsstaat. Over grondwet en rechtsstaat

129 Ibid.

130 Ibid. For the 2000 Defence White Paper, see: Parliamentary Papers, House of Representatives 1999/2000, 26 900, no. 12, p. 41. Letter from the Minister of Defence to the President to the House of Representatives of 21 September 2021, Parliamentary Paper 34 919, no. 82.

131 Ibid.

132 Inquiry report 'Grondslag gezocht', Brouwer Committee, 1 December 2022. Cf. 'De internetninja's van de krijgsmacht lopen stuk op een privacymuur', NRC, 25 January 2023.

133 AIV advisory letter, 'Choices for the armed forces', March 2022.

134 Letter from the Minister of Defence to the President of the House of Representatives of 21 September 2021, Parliamentary Paper 34 919, no. 82.

135 Cf. Explanatory memorandum. Statement that there are grounds for considering a proposal to amend provisions of the Constitution concerning defence, 2 June 1997. Parliamentary Paper 25 367, no. 3.

136 Article 3 of the North Atlantic Treaty: NATO - Official text: The North Atlantic Treaty, 04-Apr.-1949.

137 Cf. Explanatory memorandum. Statement that there are grounds for considering a proposal to amend provisions of the Constitution concerning defence, 2 June 1997. Parliamentary Paper 25 367, no. 3.

138 'Artikel 99a- Grondwet. Wetenschappelijk commentaar', by J.M. van Schooten, Gert-Jan Leenknegt and Maurice Adams. In: *Nederlandsche Rechtsstaat. Over grondwet en rechtsstaat*: https://www.nederlandrechtsstaat.nl/grondwet/inleiding-hoofdstuk-5-wetgeving-en-bestuur/artikel-99a-civiele-verdediging/.

139 This emerged from Clingendael's annual Foreign Affairs Barometer, a survey conducted among the Dutch population: https://www.clingendael.org/research-program/foreign-affairs-barometer.

140 Defence Vision 2035: https://english.defensie.nl/downloads/publications/2020/10/15/defence-vision-2035.

141 National Network of Safety and Security Analysts, National Risk Assessment of the Kingdom of the Netherlands 2022.

142 David Crossland and Bruno Waterfield, 'Exposed: hard-right European politicians "on Putin's payroll"', *The Times*, 28 March 2024. Cf. 'Poland investigating Russian espionage, security agency says', Reuters, 28 March 2024. See also: David Bremmer, 'Tsjechische geheime dienst: Rusland betaalde cash aan bevriende Nederlandse en Europese politici', *Het Parool*, 28 March 2024.

143 'Poland investigating Russian espionage, security agency says', Reuters, 28 March 2024.
'Kamer wil snel debat over Russisch geld naar Nederlandse politici', *Trouw*, 28 March 2024.

144 Letter to the House of Representatives on the approach to state threats and presentation of the

'Threat Assessment State-sponsored Actors 2'.

145 Ibid.

146 'Letter to the House of Representatives on state threats', 28 November 2022.

147 The National Emergency Supply Agency - Huoltovarmuuskeskus.

148 Cf. Eva Rovers (2022), 'Komen politici er niet uit? In deze landen vragen ze het aan burgers' *De Correspondent*.

149 AIVD, MIVD, NCTV, 'Threat Assessment State-sponsored Actors 2', November 2022.

150 Tim Wagemakers (2024), 'Amsterdam wil afvalprobleem aanpakken met een burgerberaad: hoe zinvol is dat?, *Het Parool*, 4 March.

151 For the National Citizens' Assemblies Network, see: https://burgerberaad.nu. Cf. https://www.binnenlandsbestuur.nl/bestuur-en-organisatie/burgerforum-moet-goed-zijn-ingebed-samenleving-en-politiek.

152 'Burgerberaden: "Áls het lukt, dan heb je ook wat"', *VNG Magazine*, No. 2, 2 February 2024.

153 In 2024, the Council of Europe set up a citizens' assembly for the project 'Strengthening democratic resilience through civic participation during the war and in the post-war context in Ukraine'. See also: The Council of Europe project on civic participation announces the selection of coordinators for Citizens' Assemblies in Ukraine.

154 Cf. Kenneth Lasoen (2022), 'Realising the EU Hybrid Toolbox: opportunities and pitfalls', Clingendael Policy Brief, December.

155 See also the model drawn up by Hybrid CoE in Helsinki: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf. Cf. 'Fortifying Defence. Strengthening Critical Energy Infrastructure against Hybrid Threats', European Defence Agency research report, 26 May 2023.

156 Mark Galeotti, 'Why is Russia jamming plane signals across Europe?', *The Spectator*, 22 April 2024.

157 Statement by NATO's Resilience Committee, 7 October 2022: NATO - Topic: Resilience Committee.

158 Jos Heijmans, 'Eindelijk hebben ook wij een nationale veiligheidsraad', *RTL Nieuws*, 5 November 2022.

159 Gerben Bakker and Tim Sweijs (2024), 'Campagnes tegen hybride dreigingen: een handleiding', The Hague Centre for Strategic Studies research report.

Annex I

# List of persons consulted

- **Martijn Adelaar**
  Deputy Head of Mission, Dutch embassy in Finland
- **Aleksi Aho**
  Analyst, European Centre of Excellence for Countering Hybrid Threats, Helsinki, Finland
- **Stefania Benaglia**
  Head of the Foreign Policy Unit, Centre for European Policy Studies, Brussels
- **Govert-Jan Bijl de Vroe**
  Ambassador, Dutch embassy in Finland
- **Sylvia Bijl**
  Director of Budget Affairs, Principal Directorate of Finance and Control, Ministry of Defence
- **Lieutenant General Elanor Boekholt-O'Sullivan**
  Deputy Director-General of Policy, Ministry of Defence
- **Brigadier General Professor Han Bouwmeester**
  Professor of Operational-Military Studies at the Faculty of Military Sciences (FMW) of the Netherlands Defence Academy (NLDA), Breda
- **Martin van Buuren**
  Acting deputy ambassador to Estonia
- **Özlem Canel**
  Dutch ambassador to Estonia
- **Allard Castelein**
  Former Chief Executive Officer of the Port of Rotterdam
- **Vladimir Cibic**
  Chief Security Officer, KPN
- **Tanja Cuppen**
  Chief Risk Officer, ABN AMRO
- **Dr Ingrid d'Hooghe**
  Senior Research Fellow at the Clingendael China Centre, Clingendael Institute
- **Koen Davidse**
  Director-General of Policy, Ministry of Defence
- **Guido Dierick**
  Former Chief Executive Officer, NXP
- **Leen van Duijn**
  Former Vice-President of Security Services, KLM
- **Liselot Egmond**
  Defence counsellor, Permanent Representation of the Kingdom of the Netherlands to NATO
- **General Onno Eichelsheim**
  Chief of Defence, Ministry of Defence
- **Marc Gazenbeek**
  Deputy Secretary-General, Ministry of Defence
- **Nienke Griffioen**
  Director of Banking Supervision, De Nederlandsche Bank
- **Mariliis Gross**
  Deputy Director, National Security and Defence Coordination Office, Estonia
- **Hannust Dea**
  Policy adviser, Estonian embassy in the Netherlands
- **Hanna Haruaki**
  Policy adviser, National Defence Unit, Ministry of Defence, Finland
- **Colonel Leen van Hijum**

Policy adviser, Military Strategic Element, Netherlands Defence Staff, Ministry of Defence

- **Lieutenant General Dick van Ingen**
  Military Representative to NATO and the EU Military Committee
- **Natalie Jaarsma**
  Ambassador-at-Large for Security Policy and Cyber, Ministry of Foreign Affairs
- **Andres Kangur**
  Policy adviser, Prime Minister's Office, Finland
- **Janne Känkänen**
  Director, National Emergency Supply Agency (NESA), Finland
- **Kirsi Karlamaa**
  Director-General of the Transport and Communications Agency Traficom, Finland
- **Vesa Kekäle**
  Senior adviser, Unit for Russia, Ministry for Foreign Affairs, Finland
- **Käsper Kivisoo**
  Strategic adviser, Prime Minister's Office, Estonia
- **Professor Geert-Jan Knoops**
  Professor by special appointment in the politics of international law at the University of Amsterdam and lead counsel at the International Criminal Court in The Hague
- **Carry Knoops-Hamburger**
  Director, Knoops Advocaten, and legal assistant at the International Criminal Court in The Hague
- **Major Pherdi de Koning**
  Staff adviser, Ministry of Defence
- **Geert Kuiper**
  Director of Strategy and Knowledge, Directorate-General of Policy, Ministry of Defence
- **Eero Kytömäki**
  National Security Adviser, Ministry of the Interior, Finland
- **Roger van Laak**
  Dutch ambassador in the EU Political and Security Committee
- **Karel Lannoo**
  CEO, Centre for European Policy Studies – CEPS, Brussels
- **Carolin Laubre**
  Adviser on International Cooperation, Ministry of Defence, Estonia
- **Hans van Leeuwe**
  Head of the Counter Hybrid Unit, Ministry of Defence
- **Professor Lokke Moerel**
  Professor of global ICT law at Tilburg University and member of the Dutch Cyber Security Council
- **Erwin Medendorp**
  Integral Safety Manager, University of Twente
- **Colonel Vahur Murulaid**
  Defence Attaché, Embassy of Estonia
- **Dr Mart Normaa**
  Director, Cooperative Cyber Defence Centre of Excellence – CCDCOE NATO
- **Marje Pihlak**
  Deputy Head of Mission/Counsellor, Embassy of Estonia, The Hague
- **Thijs van der Plas**
  Permanent Representative to NATO
- **Rear Admiral Peter Reesink**
  Director of the Netherlands Defence Intelligence and Security Service (MIVD), former Director of Operations of the Netherlands Defence Staff
- **Aernout Reijmer**
  Chief Information and Security Officer, ASML
- **Dr Sebastian Reyn**
  Deputy Director, MIVD
- **Kusti Salm**

Permanent Secretary, Ministry of Defence, Estonia

- **Fanny Sauvignon**
  Researcher, Centre for European Policy Studies – CEPS, Brussel
- **Captain (N, ret.) Jukka Savolainen**
  COI Director, Hybrid CoE, Finland
- **Professor Bart Schermer**
  Professor of Law and Digital Technology (specialising in Privacy and Cybercrime), Leiden University, Member of the AIV Human Rights Committee
- **Pieter-Henk Schroor**
  Head of Resources and Armaments, Counsellor at the Permanent Representation of the Kingdom of the Netherlands to NATO
- **Maarten Schurink**
  Secretary-General, Ministry of Defence
- **Joost Smits**
  Head of Financial Stability, Ministry of Finance
- **Hester Somsen**
  Deputy National Coordinator for Counterterrorism and Security and Director for Cybersecurity and State Threats
- **Kalev Stoicescu**
  Research Fellow, International Centre for Defence and Security
- **Professor Carel Stolker**
  Chair of the Stolker Committee and Former Rector Magnificus & Chairman of the Executive Board/Professor emeritus Private Law, Leiden University
- **Liisa Talonpoika**
  Ambassador, Hybrid Affairs, Ministry for Foreign Affairs, Finland
- **Professor Teija Tiilikainen**
  Director of the European Centre of Excellence for Countering Hybrid Threats, Helsinki, Finland
- **Petri Toivonen**
  Secretary-General for the Comprehensive Security Committee, Finland
- **Rear Admiral (ret.) Maarten Tossings**
  Member of the Executive Board and Chief Operating Officer, TNO
- **Taavi Turu**
  Senior Policy Officer, Dutch embassy in Estonia
- **Madis Vaikmaa**
  Policy Adviser on Strategic Communication, Prime Minister's Office, Estonia
- **Lieutenant Colonel Ben Valk**
  Researcher, Cooperative Cyber Defence Centre of Excellence – CCDCOE NATO
- **Justus Veldhuizen**
  Permanent Representation of the Kingdom of the Netherlands to the EU
- **Jeroen van der Vlugt**
  Chief Information Officer, Ministry of Defence
- **Hans de Vries**
  Director of the National Cyber Security Centre
- **Bartjan Wegter**
  EU counterterrorism coordinator; Minister Plenipotentiary at the Permanent Representation of the Kingdom of the Netherlands to NATO
- **Dr Peter Weijland**
  Programme Director of Knowledge Security, Leiden University
- **Dimitri van Zantvliet**
  Cybersecurity Director, Dutch Railways (NS)
- **Patricia Zorko**
  Deputy Director-General, Rijkswaterstaat
- **Beate Zwijnenberg**
  Chief Information Security Officer, ING

# List of abbreviations

| | |
|---|---|
| **AFM** | Dutch Authority for the Financial Markets |
| **AI** | Artificial intelligence |
| **AIV** | Advisory Council on International Affairs |
| **AIVD** | General Intelligence and Security Service |
| **AMS-IX** | Amsterdam Internet Exchange |
| **ARSIWA** | Articles on the Responsibility of States for Internationally Wrongful Acts |
| **CCDCOE** | Cooperative Cyber Defence Centre of Excellence |
| **CEPC** | Civil Emergency Planning Committee |
| **CERT** | Computer Emergency Response Team |
| **DDOS** | Distributed Denial of Service |
| **DIANA** | Defence Innovation Accelerator for the North Atlantic |
| **DIMEFIL** | Framework of state instruments against hybrid threats |
| **DNB** | De Nederlandsche Bank |
| **DORA** | Digital Operational Resilience Act |
| **ECB** | European Central Bank |
| **EEAS** | European External Action Service |
| **EU** | European Union |
| **FIMI** | Foreign Information Manipulation or Interference |
| **HCSS** | The Hague Centre for Strategic Studies |
| **HYBRID COE** | European Centre of Excellence for Countering Hybrid Threats |
| **ICJ** | International Court of Justice |
| **ICT** | Information and communication technology |
| **IHL** | International humanitarian law |
| **IRB** | ICT Response Board |
| **ISR** | Intelligence, surveillance and reconnaissance |
| **LIMC** | Land Information Manoeuvre Centre |
| **MIVD** | Netherlands Defence Intelligence and Security Service |
| **NATO** | North Atlantic Treaty Organization |
| **NCSC** | National Cyber Security Centre |
| **NCTV** | National Coordinator for Counterterrorism and Security |
| **NESA** | National Emergency Supply Agency |
| **NGO** | Non-governmental organisation |
| **NIPV** | Netherlands Institute for Public Safety |
| **NVR** | National Security Council |
| **RIVM** | National Institute for Public Health and the Environment |
| **TCO** | Tripartite Crisis Management Operational Committee |
| **TEU** | Treaty on European Union |
| **UNESCO** | United Nations Educational, Scientific and Cultural Organization |
| **UN** | United Nations |

Advisory Council on International Affairs

PO Box 20061
2500 EB The Hague
The Netherlands
W: www.advisorycouncilinternationalaffairs.nl
E: aiv@minbuza.nl