Advisory Council
on International Affairs

Hybrid threats and societal resilience (summary)

Summary of Advisory Report 126
June 2024

Advisory council on international affairs

Chair
Prof. A.G. (Bert) Koenders

Members
Lt Gen (ret.) Jan Broeks
Dr Dorette Corbey
Tanya van Gool
Professor Janne Nijman
Bram van Ojik, MA
Professor Paul Scheffer
Henne Schuwer, LLM
Professor Annelies Zoomers

Executive secretary
Professor Dirk Jan Koch

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

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 countermeasures 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.

Advisory Council on International Affairs

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