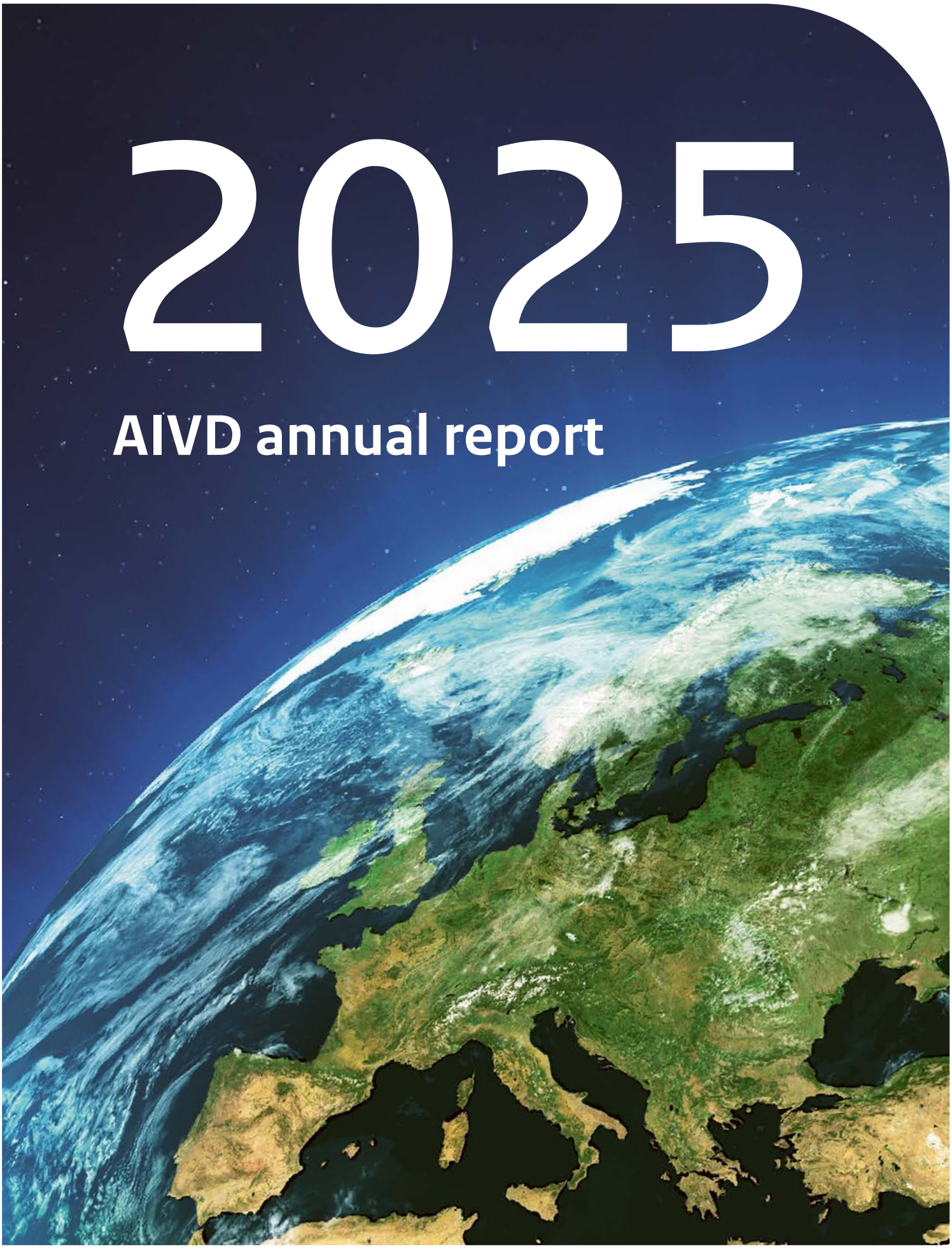
General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

2025

AIVD annual report



Contents

Foreword

How do you act sensibly in a world full of conflict and conflicting interests, in particular when you did not seek out these conflicts yourself? It is a question which the Netherlands is currently confronted with.

It is also a question which the AIVD is constantly considering. After all, it is our responsibility to protect the national security of the Netherlands. This requires effective action, regardless of what the domestic or international threats are. In a certain sense, this annual report can be read as an answer to how we took on this challenge in 2025.

The AIVD always starts by investigating the facts, even when others try to hide these. We assess these facts independently and apolitically, in all their nuance and regardless of if these facts are comfortable to face – and often they are not.

For example, it is an uncomfortable fact that in 2025 Russia's regime took an even more aggressive attitude towards European countries. In its words: the regime paints our freedoms as perverse and threatening, and attempts to undermine the unity in and amongst European countries. And in its actions: Russian hackers carried out cyberattacks on e.g. the Dutch police and the Signal and WhatsApp accounts of Dutch dignitaries and military personnel.

It is also an uncomfortable fact that China – a country we welcome as a trade partner with open arms – has for years been secretly and illegally trying to obtain the knowledge of our companies and knowledge institutions, and that the threat of this has become more widespread and serious in 2025. This threatens our autonomy and the innovation and earning capacity of the companies of which the Netherlands is so proud.

Such activities are not isolated incidents. They are part of the broader objective of various countries to gain more power in the world (China, and to a lesser extent Russia) or in the region (e.g. Iran and North Korea) and reshape the world order into their own autocratic ideology.

This dynamic further intensified in the first months of 2026. With its overwhelming military actions in Venezuela and Iran, the United States has made it clear that it will interfere if it believes other countries pose a threat to the United States' position or pose a danger to US vital interests.

Simone Smit
Director General General
Intelligence and Security Service

The long-term consequences of this, also for the national security of the Netherlands, are as yet unclear. But more clearly than in years prior we see an unstable and unpredictable world order, after decades in which stability and predictability formed the foundations for growth and peace.

This annual report describes what our investigations reveal about activities by other countries against Dutch security interests, and what we uncovered and stopped on the basis of these investigations. This is also the case for threats with connections to actors abroad and in the Netherlands. For example, we gained more insight into how other countries sometimes use criminal networks in the Netherlands.

This also applies to extremist and terrorist threats.

We believe that we again managed to prevent jihadist violence. The AIVD issued at least eleven official reports on this, on the basis of which the police could carry out arrests. A point of concern is that six of the arrested individuals were under the age of 24, which highlights the further increase in pro-ISIS sentiments amongst young people in the Netherlands.

The arrests show another important trait of the AIVD's actions: we aim to better enable our partners to do their work for the security of the Netherlands. The AIVD therefore closely cooperates with its partners in the security chain: the MIVD and the NCTV, the police, and the Public Prosecution Service in particular. And we are increasingly cooperating with the commercial sector and other parts of the public administration. We further improved and expanded these relationships in 2025.

Internationally too we have further joined forces, because it is evident that in the current world order, we stand stronger together. We have intensified our cooperation with European partner services to such an extent that it would not be an exaggeration to talk about a turning point. A notable example is that in 2025 the AIVD more than doubled its intelligence contributions to the Single Intelligence Analysis Capacity of the European Union.

Foreign services like cooperating with the AIVD because we have something to offer. Without patting ourselves on the back too much, we are good at what we do. Our tasks require this from us. This touches upon another trait of the AIVD: we stay true to ourselves. We improve our strengths (including in the field of technology, in which we want to be innovators), safeguard our independence, and know what we have to protect. We are the intelligence and security service of a free and resilient democracy. And that is precisely why our people give their very best.

In this way – based off facts, joining forces with those who share our interests or values and can increase our security, and serving society – the AIVD spent 2025 working in the interest of the national security. This is work to be proud of.

1. The world in which the AIVD operates

On 24 and 25 June 2025 the NATO Summit took place in The Hague. The Summit was extra loaded due to the many conflicts in the world. Through security screenings and cyberinvestigations the AIVD contributed to the security of this event. In the intelligence community too, international cooperation became ever more important in 2025. Photo: ANP

1.1

Achieve effects through intelligence: prevent and eliminate threats

The AIVD safeguards the national security of the Netherlands. Since our establishment shortly after the Second World War we have protected the Netherlands against national and international threats. We protect the democratic legal order: the social order based on law and democracy. The democratic legal order has a big impact on our quality of life and coexistence.

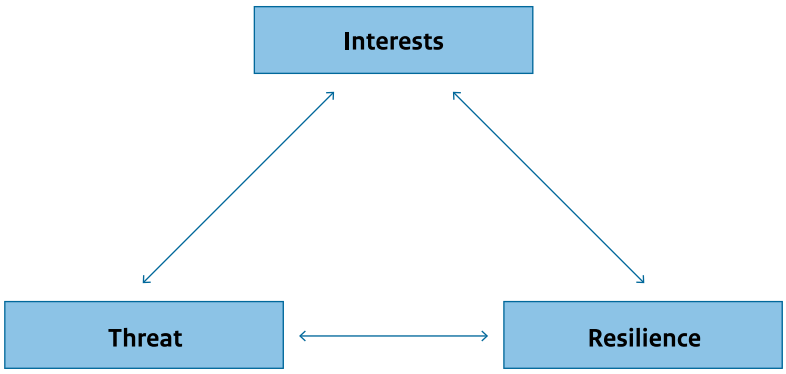
A multitude of threats

In 2025 there were many threats against the Dutch national security and democratic legal order. The jihadist movement posed a continued terrorist threat. Anti-institutional extremists sent threats to individuals such as journalists and lawyers. The right-wing extremist ideology forms a breeding ground for violence. There are connections between state actors and criminal networks. Through espionage other countries try to covertly obtain information on and exert influence in the Netherlands. This year the threat posed by countries with an offensive cyberprogramme has turned out to be even bigger than previously estimated. Russia is preparing for a lengthy confrontation with the West. The threat from China is becoming more widespread and serious. The developments in Venezuela are cause for concern in and about the Caribbean part of the Kingdom of the Netherlands. Instability in the Middle East puts pressure on Dutch security interests. Countries such as Iran, Russia, and North Korea are attempting to obtain knowledge and resources in the West for the (further) development and production of their weapons of mass destruction. This multitude of threats is discussed in more detail in this annual report.

Interests and resilience

Each threat should be seen in relation to two other aspects: the 'interests to be protected'[1] and the resilience of the Netherlands against these threats. When there is a high level of resilience, a threat has less impact on the interests. The reverse is also true. Discord within society makes the Netherlands more vulnerable to state-sponsored interference and extremist movements that try to capitalise on this. This lowers society's resilience.

[1] The six national security interests are territorial, physical, economic, and ecological security, social and political stability, and international legal order and stability. Organisations also have their own interests to protect.



Geopolitical shifts can cause changes to every part of this threat triangle. The ever-advancing technologisation of the world and also climate change can for example in the long term have an influence on this.

Countries and topics of investigation

The countries and topics the AIVD and MIVD investigate are recorded in the so-called Integrated Order Intelligence and Security (*Geïntegreerde Aanwijzing Inlichtingen en Veiligheid*, or GA I&V). The GA I&V is determined by the Ministers of the Interior and Kingdom Relations, Defence, and General Affairs, in consultation with the Ministers of Justice & Security and Foreign Affairs. Additionally, the Intelligence and Security Services Act (*Wet op de inlichtingen- en veiligheidsdiensten*, Wiv 2017) provides room to investigate threats against the national security that are not mentioned in the GA I&V. The current GA I&V is in effect until the end of 2026. The contents of the GA I&V are classified. However, the AIVD's investigation priorities are public and detailed in a letter containing the annual plan, which is published in December.

Legal framework

For the protection of the democratic legal order it is of vital importance that the AIVD and MIVD themselves also operate within a legal framework: a framework which protects democracy and allows citizens to trust that the services carry out their tasks with fundamental safeguards, such as independent oversight.

The six legal duties of the AIVD which have been recorded in the Wiv 2017 are:

- Investigate organisations and persons that pose a threat (A task);
- Carry out security screenings (B task);
- Promote security measures (C task);
- Gather intelligence about foreign countries (D task);
- Draw up threat and risk analyses (E Task);
- Check certain persons and organisations in the AIVD's systems (F Task)

The legal framework should enable the service to properly continue carrying out these various tasks – also with all technological and geopolitical developments which are happening in quick succession and which have a big impact on the threats the AIVD attempts to prevent and eliminate. This is why the legislation pertaining to the service is in need of change. The Wiv is currently being reviewed.

> **For more information, go to: aivd.nl/ambtsbericht**

Achieve effects through intelligence

Through high-quality and unique intelligence the AIVD provides its national partners, such as the ministries and the Public Prosecution Service, with insight into all kinds of threats and increases their ability to act. For example, the Public Prosecution Service can take action on the basis of so-called official reports that are issued by the AIVD. In 2025 the AIVD issued 93 official reports to partners at a local and national level. That is 20 more than in 2024.

In 2025 the AIVD also published a large number of security advisories, in part due to the NATO Summit in The Hague. Prior to the Summit, the AIVD together with the National Cyber Security Centre (*Nationaal Cyber Security Centrum*, NCSC) issued ten cybersecurity advisories about tactics, techniques, and procedures which are often used by state(-sponsored) actors. The purpose of cybersecurity advisories is to offer the recipients of the information, such as the organisers of the summit, concrete perspective for action for taking security measures. In this way, the AIVD contributes to the resilience against state(-sponsored) actors.

A different type of product the AIVD issues for protection and security is the threat product. In 2025 the AIVD published more threat products than in 2024. This increase is partially the result of an increased demand by the National Coordinator for Counterterrorism and Security (*Nationaal Coördinator Terrorismebestrijding en Veiligheid*, NCTV) and the Public Prosecution Service, and new issues which arose in 2025. Investments were made in additional capacity for this field. On the basis of these threat products the NCTV, the Public Prosecution Service, and local administrations can adjust or implement security measures. They do this for representatives of the democratic legal order, such as politicians, journalists, or scientists.

Now that Europe is increasingly taking responsibility for its own security, European cooperation is more important than ever, also to the services. That is why in 2025 the AIVD more than doubled the number of intelligence contributions to the Single Intelligence Analysis Capacity of the European Union (SIAC). These contributions strengthen the intelligence position of the European Commission, the European External Action Service, and the Council of the European Union.

In addition to increasing the perspective for action of our partners, the AIVD itself is also an acting service. On the basis of intelligence and by actively taking action, the service attempts to prevent state-sponsored actors, organisations, or persons from threatening our (inter)national security interests, undermining the democratic state under rule of law, or attacking institutions. In cooperation with national and international partners the AIVD can choose to actively disrupt someone's actions if it sees that these pose a threat to the (inter)national security.

The service shares its intelligence with others. The AIVD does this in order to inform the government, companies, and citizens of threats and in this way increase resilience. For example in 2025 together with the MIVD and German intelligence service Bundesnachrichtendienst (BND), the AIVD published information on the intensification of Russia's use of chemical weapons in Ukraine. The service also provides information to society through thematic analyses, brochures, and (cyber)security advisories..

> **For more information, go to: aivd.nl/beveiligingsadviezen**

Cooperation is crucial

Within each area of investigation, cooperation is a crucial factor for preventing and eliminating threats, provide and keep insight into the interests to be protected, and increase the resilience of the Netherlands and its partners. The AIVD is active in many national and international cooperation frameworks and frequently has a leading role. The AIVD does this as a combined service: the AIVD has both an intelligence and security task, and is also a SIGINT service. This is a unique combination in the world and is of great additional value in international cooperation. We join forces with the MIVD in order to combine our strengths. We also cooperate intensively with many other partners including companies and knowledge institutions. Our cooperation with private parties can be strengthened only if the legal framework for the service allows for this.

1.2

Development: technology as a crown jewel, weapon, and shield

Technological developments have a big impact on the current changing world order and contribute to shaping this. These developments also influence the intelligence and security domain. This section will look into this further on the basis of the aspects interests, threat, and resilience.

Interests: technology as the crown jewel

In the Netherlands companies, knowledge institutions, and the government hold knowledge and technology that cannot be found anywhere else in the world at such a high level. It is this unique knowledge and these high-tech products in which state(-sponsored) actors are interested.

State(-sponsored) actors overtly and covertly attempt to obtain this knowledge and technology, for example through cooperation, investments, and company takeovers. The more this unique knowledge is protected by the Netherlands and EU against legal (but undesirable) acquisition, the more they attempt to use covert ways instead: state actors develop concrete intelligence activities in order to obtain this knowledge and technology. Together with the MIVD and national and international partners, the AIVD contributes to the resilience against this undesirable knowledge and technology transfer.

Threat: technology as a weapon

State(-sponsored) actors use technology as a weapon. In this way they can carry out cyberattacks from anywhere in the world. Using generative AI it becomes possible to automate more and more of these attacks with limited technological knowledge, and as such carry out attacks more quickly and at a larger scale.

Technology can also be a geopolitical instrument of power: countries can restrict access to technologies and exert pressure in this way. Because of this it is of strategic importance for every country to independently (continue to) have access to technology or critical points of control in the entire production (chain) for this technology.

Technological developments do not just play a role in cyberthreats; technology is relevant to all kinds of threats that are described in this annual report. Technology makes carrying out attacks easier and threats more complex.

For smaller countries such as the Netherlands it is essential to identify strategic dependencies and handle these with care. And above all: it is essential to (continue to) cooperate with other countries and forge effective partnerships with the private sector.

Identify the interests that are to be protected
In order to prevent undesirable knowledge and technology transfer it is becoming increasingly important to designate the interests that are to be protected. Which knowledge, technological development and/or intellectual property must be kept within our own control at all costs? What are the 'crown jewels' and in which way could undesirable access to these interests undermine our (ambition to obtain a) leading position?

In 2025 the AIVD and MIVD again disrupted a number of undesirable attempts at obtaining knowledge or technology. Moreover intelligence investigation into undesirable acquisition of advanced Dutch technologies yielded various insights, including about covert investments, circumvention of export restrictions, and acquisition of company secrets through (cyber espionage.

Resilience: technology as a shield

The multitude of complex and interconnected threats require resilience from all of society. Part of the general resilience of a society is its digital resilience. Smart application of technology can help with this. The aforementioned generative AI can automate an increasingly large part of the defence against cyberthreats.

Technological innovation is essential to the AIVD in order to be able to continue carrying out its legal duties now and in the future. That is why the service has made it a goal to be an early adopter of relevant technologies. Developments are made within the organisation to make this possible. For this too strengthening national and international cooperation with companies, knowledge institutions, and other parts of the government are a priority. A Chief Science & Technology Office (CSTO) has been established to provide direction to this. The AIVD and MIVD furthermore are investing in a joint digital infrastructure.

1.3

International cooperation: more important than ever

International developments have an increasing impact on the Dutch national security. International cooperation is crucial in order to effectively protect the national security interests,. The AIVD has a large international network of partner services with which it cooperates. By cooperating the AIVD can make use of the knowledge and expertise of these services and additionally also share its own knowledge and expertise. In every form of cooperation the main goal is to anticipate, eliminate and/or prevent threats, and increase the resilience of the Netherlands and its partner countries.

The AIVD strives to be an active, trustworthy, and efficient partner. The service also tries to make the impact of our intelligence as big as possible through so-called intelligence diplomacy and strengthening the relations with certain countries, or through contributing to sanctions enforcement. In 2025 the AIVD strengthened its intelligence cooperation with the European Union and NATO. This for the promotion of geopolitical decision-making and to support Dutch foreign and security policy.

Trust and due care

Trust is essential in the cooperation between intelligence and security services. Due care is also of great importance in determining the nature and intensity of each cooperation. This is why the AIVD assesses its partner services on a number of criteria: democratic embedment, respect for human rights, professionalism and trustworthiness, legal powers and technical capabilities, and level of data protection. This assessment is a legal obligation and is done in collaboration with the MIVD. These assessment memorandums are amended when the AIVD and MIVD see a reason for this.

AIVD enters into strategic partnerships with services where cooperation is of great importance and where the AIVD considers the result of the cooperation to be very valuable. This requires constant investment into the relationship with these services. During all cooperations the AIVD is mindful of the quid pro quo balance. At the same time, the AIVD ensures that it can always cooperate with any partner service and within the provided legal framework should the situation require this.

In addition to bilateral cooperation with other services, the AIVD also cooperates with partners at a multilateral level. Multilateral cooperation takes place at e.g. an EU level.

To illustrate: EU cooperation

Because of intelligence, policymakers are better-informed when drafting policy. This is also true at an EU level – including for the Common Foreign and Security Policy and the Common Security and Defence Policy of the EU. These two policy frameworks in part have the purpose of improving the international security. In order for the EU to make well-substantiated choices, member states also share intelligence in an EU context.

INTCEN and SIAC: intelligence with global impact

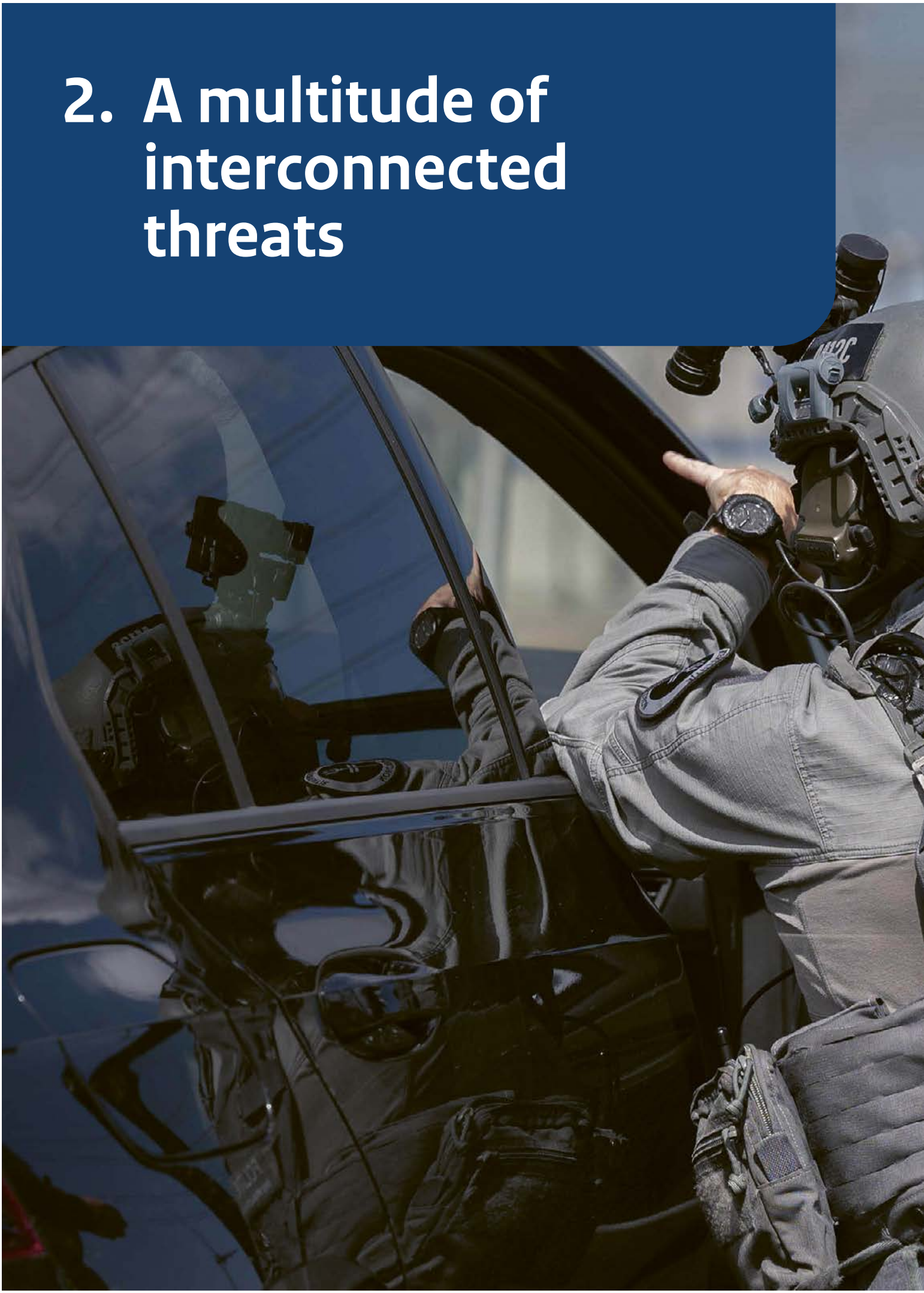
The AIVD places great value on INTCEN, the Intelligence and Situation Centre, and the European Union's overarching cooperation SIAC, the Single Intelligence Analysis Capacity, for sharing intelligence in an EU context. SIAC is the exclusive portal for sharing strategic intelligence with European institutions: it makes intelligence products for EU policymakers on the basis of voluntary intelligence contributions by EU member states. SIAC and INTCEN do not independently gather intelligence. This is because protecting the national security is exclusively a task reserved for the EU member states.

The AIVD contributes to the strengthening of SIAC. In 2025 the AIVD more than doubled the number of intelligence contributions made to SIAC with regard to 2024. These contributions strengthen the intelligence position of the European Commission, the European External Action Service, and the Council of the European Union. In a number of cases these contributions resulted in concrete EU measures, including sanctions.

Strengthening the liaison network

The AIVD has a number of liaison officers across the world. Their most important task is to further the cooperation with partner services and multilateral organisations. They additionally provide Dutch embassies with advice on security issues. In 2025 the AIVD further expanded this foreign presence.

2. A multitude of interconnected threats



An employee of the Special Interventions Service. Over the past year official reports issued by the AIVD enabled the police to carry out several arrests. It is highly likely that this helped remove violent threats. The AIVD issued official reports on matters such as jihadist, anti-institutional, and right-wing extremist threats. Photo: ANP

2.1 Extremism

The AIVD investigates persons and organisations which, either because of the objectives they pursue or through their activities, give cause for suspicion that they pose a threat to the continued existence of the democratic legal order, or to the (physical) security or to

other vital interests of the state. Because of the nature of their objectives and activities, some of these movements are labelled as extremist by the AIVD. The AIVD defines extremism as: a willingness based on ideological motives to carry out non-violent and/or violent activities which undermine the democratic legal order.

The democratic legal order can be undermined in both violent and non-violent ways. Examples of non-violent ways are systematically inciting hatred, intentionally spreading disinformation, demonisation, and intimidation. Violent ways include for example assault, arson, or other more serious forms of violence. An extreme form of extremism is terrorism: to (threaten to) commit violence for ideological reasons against human lives or to cause significant disruptive damage to society with the goal of striking terror into (part of) the population, achieving societal change, and/or influencing political decision-making.

In 2025 the AIVD's investigations focused on both types of threats, particularly within Islamist extremism, anti-institutional extremism, left-wing extremism, and right-wing extremism. The following sections deal with these topics.

> **For more information, go to: aivd.nl/extremisme**

- **The most significant terrorist threat still stems from jihadism.**
- **Through its propaganda ISIS attempts to inspire its supporters to carry out attacks, or arrange attacks itself in spite of the global pressure on the organisation.**
- **The jihadist movement in the Netherlands mainly consists of ISIS supporters.**
- **Notable in 2025 is the further increase in young supporters (under 24 years) and the number of persons on whom the AIVD issued official reports.**

2.1.1 Islamist extremism

In 2025 too the most significant terrorist threat still stems from jihadism. In December 2025 this could be seen in the large attack at Bondi Beach in Sydney, Australia, targeting Jewish participants in a Hanukkah celebration.

Jihadism

The jihadist-terrorist threat to the Netherlands stems almost solely from ISIS. This threat is partially posed by (aspiring) attackers who are linked to and directed by ISIS. Another part of the threat stems from ISIS supporters who are inspired to plot attacks without any contact with ISIS or who in some cases are directed by ISIS members through online contact.

Directed threat ISIS

Over the past years the increasing threat posed by ISIS has led to increased offensive activities countering ISIS. For example, local authorities, together with international partners, carried out interventions in e.g. Pakistan and Syria. There was also a military offensive against ISIS in Puntland, Somalia. This decreased ISIS' capacity, but ISIS is resilient and very adaptable. When the pressure on ISIS eases, the threat of attacks directed by them will increase again relatively quickly.

Additionally the AIVD remains alert of the threat posed by networks and persons in Europe that are affiliated with ISIS. The past years several members of these networks developed plans for an attack. On 21 July 2025 a Tajik ISKP member who lives in the Netherlands was sentenced to five and a half years in prison for membership and financing of ISIS.

In the summer of 2024 several persons were arrested in Belgium, Germany, and Austria for possible attack plans. The majority of these persons have since been released or deported to their country of origin. Because of the arrests, deportations, and pressure on ISIS from outside of Europe, the terrorist threat posed by these networks at this moment has decreased. In time these networks may become active again if ISIS is capable of increasing its capacity and developing plans in order to direct attacks in Europe.

Additionally (former) ISIS members from Syria are sporadically turning up in the Netherlands and other European countries. Together with national and international partners the AIVD focuses on identifying and disrupting these individuals and networks. On 26 May 2025 two Syrian men suspected of participation in ISIS in Syria were arrested following the issuance of an official report by the AIVD.

ISIS supporters in the Netherlands

Although the global pressure on ISIS increased in 2025, this has not translated into a decrease in the threat posed by supporters in the Netherlands or of the appeal or accessibility of ISIS online. In 2025 the AIVD issued official reports on nineteen individuals in relation to jihadism. For eleven of them the AIVD had indications that a threat of violence was imminent. The police arrested them following these official reports. Six of the arrested individuals were younger than 24 at that time.

The increase in the number of young people (under 24 years) supporting ISIS who are under investigation by the AIVD has further increased. Young persons now form a third of the jihadists under investigation. On social media platforms the jihadist ideology is broadly available and easily accessible. This is partially due to the activities of young jihadists who post, moderate and/or further spread online jihadist content at a large scale. These platforms are additionally the most significant meeting point for young jihadists. It is an easy way for them to meet like-minded individuals. In many cases these contacts remain at a surface level and do not develop into more serious contacts or physical networks.

Occasionally the AIVD sees that young jihadists manage to transition their online contacts into (also having) offline contacts. This is true for the eight persons the police arrested in April 2025. Although in general it is unclear to what extent young jihadists are willing to act on their concerning statements, the AIVD deems a threat of violence possible from a number of persons within this network. This is why the AIVD issued the official reports, which contributed to these arrests. Their online radicalisation fits within the picture the AIVD highlighted in the publication A web of hate (April 2025).

The AIVD does not just counter the threat of attacks. The AIVD attempts to curb the growth of the jihadist movement by disrupting online network formation and the spread of the ideology. In seven cases the official reports of the AIVD were (partially) aimed at limiting the inflammatory and radicalising effects of such online activities. The AIVD furthermore works to prevent the travel of jihadists from the Netherlands to join ISIS abroad. In four cases in which official reports were issued in 2025 there were signs of possible travel plans. Although the travel plans are only sporadically more concrete and ISIS is difficult to reach in many places in the world, their supporters seemingly remain interested in travelling to join them. The same is true for individuals in other European countries.

Hamas

The AIVD investigates the possible threat the terrorist organisation Hamas poses against the Dutch national security. The AIVD identified two methods of operation by Hamas in Europe, ranging from activist action to possible preparations for terrorist actions. First, for years there has been an active ‘political’ network in Europe which gathers financial support for Hamas and dedicates itself to activism, lobbying, and other influencing activities in Europe. In the Netherlands there are a dozen active individuals who can be linked to this European network.

This Hamas network in the Netherlands has been active for years with propaganda, lobbying, and fundraising for Hamas (in Gaza). In comparison to 2024 the AIVD has gained more clarity on the involvement of the Hamas network in the Netherlands in pro-Palestine and anti-Israel protests.

The AIVD has found that this network is involved with broader organisations which organise demonstrations on behalf of a larger part of the Palestinian community. In 2025 these demonstrations did not lead to violent incidents. The AIVD does observe that these demonstrations can lead to discord in society.

The second method came to light through a number of arrests in Europe: persons who could be linked to Hamas were involved in hiding and moving firearms and ammunitions on the directions of Hamas members in Lebanon. It appears as though Hamas was working on building up the capacity to commit violence in Europe. As yet it is not clear with which goal this capacity was being developed and directed. Some of the individuals arrested were not only suspected of Hamas membership, but also of preparing attacks on Jewish and/or Israeli targets. The criminal investigations are still ongoing.

> **For more information, go to: aivd.nl/terrorisme**

2.1.2 Anti-institutional extremism

> **In 2024 and 2025 official reports issued by the AIVD led to the arrest of two large groups of anti-institutional extremists willing to use violence and the find of firearms, large amounts of ammunition, and other potential means of attack such as heavy fireworks, igniters, and castor beans. With this, the violent threat posed by these two groups has been removed.**

> **Anti-institutional extremism can lead to terrorism.**

Firearms, a large amount of ammunition, and castor beans (the main ingredient for the toxin ricin): these are all items the police found during the arrest of eight persons in the context of an investigation into anti-institutional extremism in June 2025. They were arrested following official reports from the AIVD. Some individuals in this group are suspected of terrorism-related offences.

In 2024 another group of ten persons had already been arrested on suspicion of terrorism. In November 2025 the court ruled that the group was not a terrorist organisation, but a criminal organisation which was inciting a terrorist offence. By arguing for local militias and citizen's arrests, they could have moved others to actually arming themselves and using physical violence. Some members of the group were also sentenced for illegal possession of weapons. The Public Prosecution Service filed an appeal against part of this judgement, because it did not agree with the court's judgement that three of the suspects did not form a criminal or terrorist organisation.

In 2025 the AIVD issued official reports on 14 persons in relation to anti-institutional extremism. For 13 persons this was in relation to anti-institutional terrorism.

Anti-institutional extremists believe that there is an evil elite who want to oppress, enslave, or kill the people. The Covid pandemic and the measures taken during that period continue to be important topics within this movement. As in 2024, in 2025 migration was an important topic. By allowing or stimulating mass migration, the elite would be able to further oppress the population. This broad evil elite narrative resonates within all strata of society. There is a very small percentage of supporters who pose a violent threat. They target persons that supposedly represent this elite.

With some regularity e.g. members of government, bailiffs, journalists, judges, and local administrators receive threats from those with anti-institutional extremist beliefs. This has caused some to indicate they want to step down from their position.

Manifestations of violence

The two court cases above show that this new form of extremism can also take violent forms. Several European security services have concluded the same thing in relation to similar groups in their own countries. However, it concerns a very small minority of anti-institutional extremists.

Anti-institutional terrorism is a different type of threat than for example jihadist terrorism or right-wing terrorism. Anti-institutional extremists willing to use violence are older than individuals willing to use violence in other extremist movements: they are often over 45 years old and radicalise at a later age. The lack of teenagers being radicalised is also a notable difference in comparison to recent developments within other forms of extremism.

Another important difference is that the extremists willing to use violence relatively often have knowledge about and are skilled in using weapons. Many of them have a fascination for weapons and practice with using these weapons. A small group tries to purchase illegal firearms, but most have access to legal weapons such as crossbows and knives or powerful HPA guns (a more powerful variant of the more well-known air gun). As a result of various innovations the fire power of these air guns has strongly increased in the past years. Because of this many of the more powerful air guns have more fire power than a regular firearm.

Social challenge

The AIVD emphasises that anti-institutional extremism is not just a security issue, but mostly a broader, social problem. The breeding ground for this type of extremism includes increasing dissatisfaction and distrust with institutions such as the government. There are roles here for science and the government, but also for politicians. Only a broader approach of the causes could in time reduce the threat of anti-institutional extremism.

The broader anti-institutional extremist movement

During and shortly after the Covid pandemic the anti-institutional movement grew. Over time the number of supporters has not decreased. Within this movement there are dozens of inciters who actively propagate the narrative.

The arrests in 2024 and 2025 do not seem to have had a deterring effect on the group of anti-institutional extremists and the active inciters. Some of them view the arrests as a confirmation of their own beliefs or as a new plot within the conspiracy.

The detainees are seen as 'political prisoners' who 'came too close to the truth' and were then 'arrested by the evil elite'. These detainees receive support from other anti-institutional extremists. There are fundraising campaigns for some. Many thousands of people appear willing to donate.

Although some of the inciters and supporters consider themselves to be part of a movement, there is no properly organised scene. There is no consensus on what should be done about the supposed evil elite.

Dissemination of the ideology

The inciters regularly organise in-person meetings, such as lectures and conferences. They also spread the narrative on social media, in podcasts, and on alternative media platforms. On many of these platforms, the evil elite narrative is alternated with government criticism. Sometimes there are also voices which weaken or counter the narrative.

Pro-Russian disinformation on some alternative media channels

For many inciters and adherents of the ideology, alternative media has become an important source for receiving news. These online channels often have a large reach and can sometimes look very professional. Some of these media channels spread pro-Russian disinformation. The visitors of these channels may be susceptible to such undemocratic messages; these often fit in perfectly with their own beliefs.

> **For more information, go to: aivd.nl/extremisme**

2.1.3 Right-wing extremism

> **In 2025 the AIVD issued official reports on 8 persons in order to remove a right-wing extremist threat of violence.**

> **Not all right-wing extremists want to use violence to achieve their goals. A broader, non-violent movement makes opportunistic use of the political-administrative situation and developments.**

> **The AIVD has seen the emergence of a new form of extremism: nihilistic violent extremism.**

The threat posed by right-wing extremism is twofold. In part, the threat consists of the spread of right-wing extremist ideology in society. Additionally to some this spread may legitimise the use of violence. The AIVD sees roughly two groups within the right-wing extremist landscape: a broader, non-violent movement, and a smaller, violent movement.

Both groups largely share the same principles and goals. As such there is no clear division. Right-wing extremists from both groups believe in an enemy narrative. They view minority groups or those with different beliefs as a threat. Both groups centralise the threat against 'the white race' and strive for 'a white ethnostate'.

There are, however, different subideologies. The AIVD also sees that subgroups and individuals have different priorities. Although some individuals are explicitly for or against the use of violence, this dividing line cannot always be drawn so clearly.

Right-wing extremist violence

In 2025 the AIVD issued a number of official reports on persons involved with (online) groups which propagate non-violent methods, but also gather and construct weapons and ammunition. It is highly likely they wanted to use these weapons.

For some years we have seen that young persons, young men in particular, radicalise in online chat groups. In these online environments violence and attackers are glorified and ideologies are spread. These ideologies are not always clear-cut. In many cases grievances, occult ideas, or a fascination with death, pain, and violence play a role.

For persons with these ideas who further radicalise to be willing to use violence, it is therefore not always clear how concrete their goals and motives are. And if, in light of their young age, they will actually progress to carrying out violence. Various cases from abroad show that this cannot be ruled out.

Nihilistic violent extremism

Long-term investigation into the right-wing terrorist movement points to a new extremist phenomenon which has arisen in the past few years: nihilistic violent extremism. This extremist phenomenon largely happens in a broader online environment of crime, in which some persons purposefully want to cause damage which is disruptive to society. In these specific cases, this phenomenon comes under the remit of the AIVD.

In 2025 on the basis of police investigation various persons were arrested who were moved to (incite) violence because of this nihilistic ideology. These arrested individuals radicalised in an online environment with shocking and violent footage, animal and child abuse, and child sexual abuse material (CSAM). Individuals in this online network incite each other and others to the use of violence, such as self-harm, suicide, or deadly violence towards others. Some groups or persons also want to incite terrorism. Carrying out acts of violence and sharing this online increases someone's status within the community.

Normalisation of the ideology

Within the right-wing extremist movement there are many persons and subgroups which want to normalise and try to ensure the broad acceptance of right-wing extremist opinions. In 2025 too normalisation remained one of the most important strategies of the movement. They often present their ideas in a milder form to make them appear more acceptable, while behind the scenes they strive for the right-wing extremist goal of a 'white ethnostate'. A good example is the frequent use of the term 'remigration', which in itself is neutral, but in the right-wing extremist narrative means the mass departure from Europe of persons with a migration background. Dutch right-wing extremists cooperate with like-minded persons in other European countries, for whom normalisation is also an important strategy. In May 2025 European right-wing extremists organised a well-attended conference on 'remigration' in Italy, which also saw a number of Dutch participants. At the conference there were a mix of European right-wing extremists and members of radical right-wing parties. Right-wing extremists seek rapprochement with such parties at these meetings.

The right-wing extremist movement makes opportunistic use of the political-administrative situation and developments. To increase support for the movement, they capitalise on the fears and insecurities amongst part of the population. Multiple right-wing extremist groups were present at the asylum protest on the Malieveld in September 2025 ('Elsfest'). Some of them exhibited Nazi behaviour, committed violence against the police, moved from the Malieveld into the city and attempted to commit arson at the office of political party D66.

In 2025 the AIVD furthermore saw that the right-wing extremist movement continues to have an interest in 'entryism'. This is the process in which extremists attempt to exert influence and work on their extremist policy goals through fulfilling influential political-administrative positions. This interest in the political playing field by right-wing extremists is not new, although the approach seems to be more efficient than before. Part of this is the fact that right-wing extremists feel bolstered because of similar movements in other countries.

> **For more information, go to: aivd.nl/extremisme**

2.1.4 Left-wing extremism

> **As in 2024 the war in Gaza was one of the most important topics for the left-wing extremist movement.**

> **The threat posed by this movement was small. Much of the left-wing protest was activist in nature. Although these actions could be disruptive, they generally did not threaten the democratic legal order.**

Traditionally, the left-wing extremist movement in the Netherlands has consisted largely of anarchists and to a lesser extent of Marxist-Leninists. Both the anarchist movement and various Marxist-Leninist organisations showed strong pro-Palestinian sentiments. They turned against Israel and the support Israel received from e.g. Europe and the United States.

At the pro-Palestine and anti-Israel protests the attendance showed a very diverse composition of groups and individuals. They protested together out of various ideological motives, but also out of personal connectedness and shared emotions. Representatives from the Palestinian and Islamic communities, climate activists, anti-imperialists, and students all found each other. Like in 2024, the demonstrations were generally activist in nature. Only rarely did they result in disturbance of the public order.

Defacement and destruction

The left-wing extremist movement did not carry out actions which explicitly targeted Jewish institutions or persons. There were, however, a large amount of defacements and destructions of properties of companies (allegedly) involved in weapons supplies to the Israeli armed forces or activities of Jewish settlers on the West Bank. Government locations, such as army barracks, the Ministry of Foreign Affairs, and universities were targets of such actions. There were protests in front of the entrances, or the locations were visited at night and defaced using fire extinguishers with paint. Often windows of such properties were destroyed. Often these actions were claimed online and the reason(s) for the actions were given.

Samidoun Nederland

One of the organisations actively involved in the pro-Palestine and anti-Israel protests is the Dutch branch of the internationally established Marxist-Leninist organisation Samidoun. *Samidoun Nederland* is activist in its actions. The organisation does not call for violence, but does glorify violence against Israeli people and the Israeli state, for example by legitimising acts of terrorist organisations. Although the supporters base of Samidoun in the Netherlands is small, the extremist message resonates more broadly. This is in part due the current attention for the issue and the cross-pollination the organisation has with many other (often left-wing) organisations involved in pro-Palestine and anti-Israel protests.

The threat Samidoun poses against the national security is limited. However, some may experience the message propagated by the organisation to be threatening and it could contribute to radicalisation and increasing polarisation.

Antimilitarism

In 2025 we saw a resurgence of antimilitarism in the actions against companies which (allegedly) supply weapon components to Israel and the NATO Summit held in the Netherlands. Antimilitarist actions were limited to the aforementioned destructions of property and activist manifestations such as protests.

During the NATO Summit there were activist protests. The protests were not extremist in nature. It is possible that potential extremist plans were not feasible due to the large-scale security measures. The influx of protesters from abroad also remained limited to a few hundred activists.

Anti-fascism

Anti-fascist actions, often carried out by the anarchist movement, have been the same for years: destroying property, disrupting meetings, intimidating persons, and identifying and publishing personal details online (doxing). The AIVD considers such actions to be extremist because they undermine the proper functioning of the democratic legal order.

In 2023, a year with elections for the Dutch House of Representatives, the AIVD saw a clear increase in anti-fascist actions. These actions were focused on political parties and individual politicians, but also on other groups and persons deemed fascist. In 2025, with the exception of a few small-scale actions, it was remarkably calm around the Dutch general elections. There were a number of threats from animal rights extremists against politicians, which also received some media attention. The AIVD estimates that topics which previously caused strong polarisation between left and right played a smaller role in the 2025 election campaigns.

> **For more information, go to: aivd.nl/extremisme**

2.2

Criminal undermining of national security

- **In 2025 too the AIVD investigated criminal networks which pose a threat of violence against representatives of the democratic legal order.**
- **In late 2024 the AIVD issued an official report on the clandestine communication from the maximum security facility (*Extra Beveiligde Inrichting*, EBI) with a criminal network. In 2025 this led to the arrest of a lawyer by the police.**
- **New in 2025 is the AIVD's investigation into the connections between criminal networks and state actors.**

Interconnectedness state-sponsored actors and criminal networks

Criminal networks are active all across the world. They are specialised in operating out of the view of criminal investigation and security services. Because of this they are an attractive cooperation partner for many state actors for e.g. espionage, interference, and violence against political opponents. In 2025 the AIVD investigated the use of deadly violence carried out by criminal networks on the orders of state actors. This investigation shows that some criminal networks are structurally active in carrying out violence on behalf of state actors. The reason in part is in the possibilities the state actor has to offer the criminal networks protection in exchange for the services provided.

This protection is also the reason that (Dutch) criminal networks settle in foreign countries. They often do this in countries where the risk of prosecution or extradition is smaller, for example because they are not a priority for local authorities or because they are able to purchase protection through corrupt contacts. Some of these networks pose a threat to the Dutch national security. Protection by a state actor increases the threat against the Dutch national security, because the criminal network remains outside of the reach of law enforcement. Investigation by the AIVD shows that the connections with state actors have allowed such networks to establish a strong position in 2025.

International cooperation is of great importance for protecting the Dutch national security. And this is certainly the case when criminal networks become interconnected with state actors. Through the sharing of intelligence reports in 2025 the AIVD informed national and European partners of these connections and enabled them to act upon this.

Covert communication EBI with criminal network disrupted

AIVD investigation revealed that covert communication took place from detention in the maximum security facility (*Extra Beveiligde Inrichting*, EBI) with a criminal network. The AIVD then issued an official report to the Public Prosecution Service so that it could initiate a criminal investigation. In 2025 this investigation led to the arrest of a lawyer by the police.

The AIVD's task in relation to criminal undermining

By law, protecting the national security of the Netherlands is the AIVD's core task. When there are serious suspicions that a criminal network damages the national security, or can and wants to damage national security, the AIVD can investigate this. The AIVD has its own, clearly demarcated task. The criminal investigation (and prosecution) of criminal offences is the task of the Public Prosecution Service and the police. Because the police, Public Prosecution Service, and AIVD each investigate criminal networks following from their own duties, this gives a more complete overview of the ways in which the Netherlands can become more resilient to criminal undermining.

> **For more information, go to: aivd.nl/ondermijning**

2.3

State-sponsored interference in the Netherlands

- **Since 2025 more forms of espionage in the Netherlands have become punishable by law, such as digital espionage and espionage through using the diaspora.**
- **Various countries gather intelligence on persons from the diaspora community who criticise the regime in the country of (their family's) origin.**
- **In 2025 the AIVD and MIVD found that some countries.**

State-sponsored interference is an umbrella term for various ways in which foreign governments try to get involved in or interfere with matters in the Netherlands. State-sponsored interference is any activity which undermines the democratic legal order and which is carried out by or by order of a foreign government. This can take the form of for example covert political influencing or sabotage. The state(-sponsored) actor can also monitor and put pressure on the diaspora. This can deeply affect the personal privacy and sense of security of persons in these diaspora communities and is an infringement of the Dutch sovereignty and the fundamental rights of these persons.

Through espionage other countries try to covertly obtain information in the Netherlands and Europe. Most espionage activities, such as breaching state secrets, official secrets, and company secrets, have been against the law in the Netherlands for some time. Since 15 May 2025 more forms of espionage have become illegal, such as digital espionage and diaspora espionage. Expanding the law gives the Public Prosecution Service more opportunities to take action against espionage activities.

Expansion criminality espionage activities
If a person leaks and/or divulges sensitive information which is not state secret, or if someone carries out acts on behalf of a foreign government, this is now liable to prosecution if this can do serious damage to Dutch interests. The AIVD sees that intelligence and security services from countries such as Russia, China, and Iran, but also services from countries with a large diaspora community in the Netherlands, such as Morocco, pose a large continued threat of espionage.

Diaspora as a network of sources

The Turkish and Moroccan intelligence and security services, amongst others, gather intelligence on persons from their respective diaspora communities who criticise the regime in the country of (their family's) origin. These services often utilise a network of sources with persons from the same diaspora community. As such, persons from these communities are more susceptible to approaches for this. They often still have links to their country of origin, for example because they still have family or property there. These foreign intelligence and security services can abuse these connections, for example by providing consular favours in their country of origin in exchange for cooperation.

AIVD investigation shows that the Moroccan services have an interest in persons who work in positions with access to information that is important to Morocco. The AIVD will meet with the employers concerned in order to create greater security awareness and increase resilience. The AIVD hopes that this will also increase the willingness to file reports should something happen.

In 2024 together with the NCTV the AIVD published the analysis 'Crossing borders: State-sponsored interference in diaspora communities in the Netherlands'.

> **For more information, go to: aivd.nl/inmenging**

> **For more information, go to: aivd.nl/overdegrens**

Violence and cyberattacks against political opponents

In some extreme cases other countries can move to use violence against political opponents. Countries which use these forms of state interference try to hide their involvement in these violent activities. One way in which they can do this is through using criminal networks.

In 2025 the AIVD and MIVD in a joint cyberinvestigation concluded that some countries also use cyberattacks against critics residing in the West.

2.4

- **In 2025 the AIVD observed that the threat posed by countries with an offensive cyberprogramme is bigger than before.**
- **Notable cyberincidents and attack campaigns domestically and abroad highlighted again the scope and impact of digital threats on the (inter)national security.**
- **Technological developments enable attackers to develop and deploy increasingly advanced attack methods.**

Cyberthreat

In 2024 the AIVD already signalled that the number of countries with an offensive cyberprogramme is increasing. In 2025 the AIVD observed that the threat posed by these cyberprogrammes has grown beyond what was initially estimated. The threat of offensive cyberprogrammes from China and Russia remained unabatedly high in 2025.

The NATO Summit in The Hague

On 24 and 25 June 2025 the NATO Summit took place in The Hague. Behind the scenes the AIVD, together with many other parties, contributed to the security of this large-scale event. As expected, there were some cybersecurity incidents. The impact of these incidents was limited. This is in part due to the measures taken by those organisations responsible for the security of the event.

Cyber: unequal fight against increasing threat

The fight in the cyberdomain is an unequal fight. For ‘defenders’ such as Dutch organisations, it is often difficult to continue fending off state-sponsored actors who operate within different legal frameworks.

More attackers are using automation to successfully carry out cyberattacks. It is increasingly possible to systematically look for vulnerabilities in systems or attack multiple targets at the same time. The possibilities of artificial intelligence moreover have caused an acceleration in the development of new methods and means of attack. In order to effectively counter this, innovation and cooperation are essential.

Cybersecurity approach: the basics in order

The NCTV’s Cybersecurity Assessment Netherlands (CSBN) 2025, which the AIVD contributed to, states: ‘The conclusion that threats are becoming more unpredictable and complex does not necessarily mean that defending against them is so as well. Many digital incidents arise from a lack of proper ‘digital hygiene’. [...] For an average organisation, the message is therefore clear: do not fixate on the complex threat landscape, but first defend against it by applying the basic principles.’

Number of incidents exploiting unknown vulnerabilities increasing

The number of incidents in which attackers exploit an unknown vulnerability (a zero day) are increasing. A zero day is a vulnerability of which software providers are not yet aware. This means that there are no security measures available for these vulnerabilities. As such, these types of vulnerabilities are interesting to malicious actors. Attackers moreover succeed at exploiting these vulnerabilities more quickly and because of this make more victims within a short span of time.

In 2025 there were various incidents in the Netherlands in which attackers used unknown vulnerabilities and vulnerabilities which had only recently become known. In the summer of 2025 malicious actors abused unknown vulnerabilities in Citrix NetScaler, which is used by organisations to e.g. facilitate working from home. Amongst the targets was the Public Prosecution Service. This attack disrupted the functioning of an organisation which plays an essential role in society.

Attackers do not only use unknown vulnerabilities. As in prior years, software and hardware with older and long-since known vulnerabilities remain popular.

State-sponsored actors apply broad target selection: from (Western) politicians to dissidents

State-sponsored actors are also interested in politicians and civil servants and in critics from the diaspora community. State-sponsored actors try to gain information such as personal details through cyberattacks. In 2025 state-sponsored actors obtained communication of these persons. They were able to do this in part by hacking telecommunications providers outside of the Netherlands. With the data they obtained, state-sponsored actors can gain an insight in things like European decision-making. In more serious cases, this may also help them obtain the addresses of persons in e.g. conflict areas.

More digital attacks against mobile devices

In 2025 the AIVD and MIVD observed an increase in digital attacks against mobile devices such a mobile phones. These are vulnerable communication devices, in part because of the many frequently used messaging applications. Employers also often do not monitor these mobile devices as intensively as they do computers and servers. Furthermore people are not as aware of the risks when it comes to phone usage.

For attacks on these mobile devices and other equipment, state-sponsored actors also use commercially available spyware. They furthermore develop their own malware for this. Additionally they try to take over messages apps by means of social engineering.

Gaining access to messaging apps through social engineering

The AIVD and MIVD have established that multiple state-sponsored actors attempt to obtain personal details of their targets through social engineering. This is a technique (cyber)criminal use to coax persons into sharing sensitive information and/or get them to carry out certain actions. It happened several times in 2025 that state(-sponsored) actors impersonated employees or chatbots of a messaging app such as WhatsApp and Signal. The pretend employee or chatbot would indicate that the victim has to log in again and then has them enter a specific code. This gives the actor access to the victim's account.

Another way in which state-sponsored actors successfully approached victims was through voice phishing. The actor establishes contact with a victim and eventually calls this person. Establishing this contact can take months. During or after the phone conversation, they then send a link which allows the actor to take over the account.

Countries with offensive cyberprogrammes

The AIVD and MIVD investigate several countries with an offensive cyberprogramme. In the next sections we will elaborate on the cyberthreat from Iran and North Korea as well as on the cyberthreat from China and Russia.

Cyberthreat from Iran

The AIVD and MIVD estimate that the Iranian regime remains focused on its offensive cyberprogramme. Iranian cyberactors carry out influencing operations, digital sabotage, and digital espionage. They focus on regional opponents, such as Israel, but also on countries beyond this in Western Europe and North America.

They also target individuals. In 2025 it was found that Iran continues to carry out cyberespionage campaigns against critics of the Iranian regime in the West, including dissidents and journalists. Iranian actors use advanced malware as part of this campaign. Through this they try to gain access to the personal devices and accounts (email, social media) of these persons. This threat is thus targeting them personally. The fact that in some cases these critics are citizens of Western countries does not stop Iran.

The services also conclude that the Iranian cyberthreat targets experts on the Middle East. Lastly in 2025 Iran also showed an interest in Western government personnel.

Cyberthreat from North Korea

North Korea continues to be a significant threat to the Dutch security interests through its (nuclear) weapons programme, offensive cyberprogramme, and support to Russia in the war against Ukraine. North Korea uses its offensive cyberprogramme to keep the current regime in power.

One of the most important goals of North Korea's cyberprogramme is financial gain. The offensive cyberprogramme highly likely contributes to the funding of North Korea's (nuclear) weapons programme. Another goal is cyberespionage: the regime wants to obtain advanced (military) technology, as well as (geo)political and scientific information.

In 2025 the services observed various cyberattacks against Dutch companies and persons, which were carried out by or with the help of North Korean IT professionals. These attacks were mainly intended to steal cryptocurrency for the benefit of the North Korean regime. The attackers work in an opportunistic way. If during the attack they can obtain sensitive data as well, they will utilise this opportunity.

> **For more information, go to: aivd.nl/cyberdreiging**

2.5

Russia

- **In 2025 Russia continued to adopt a more offensive attitude towards European countries. The AIVD and MIVD carry out a joint investigation into the threat Russia poses to the Netherlands.**
- **In order to better understand this threat, it is essential to know Russia's perspective. Even if the fight in Ukraine comes to an end, what Russia believes to be a broader and existential confrontation will continue.**
- **In 2025 the AIVD and MIVD reported on a previously publicly unknown Russian cyberactor called LAUNDRY BEAR. This actor was responsible for an attack in which work-related contact details of Dutch police officers were obtained.**

As in 2024, in 2025 Russia took on a more aggressive, brazen, and provocative attitude towards European countries. Because of the West's political and military support to Ukraine, the Russian regime characterises Europe, and the European Union in particular, as an opponent. Moreover, it increasingly views this opponent with more hostility.

Russia's perspective

The AIVD and MIVD observe that Russia considers itself to be entangled in a broader and existential conflict with the West. To the Russian regime, the war in Ukraine–the biggest and most deadly conflict in Europe since the Second World War–is just a part of this.

The narrative of the Russian regime is that the West is aggressive, wants to destabilise Russia, and see it suffer defeat. They believe only one party can win (a zero-sum game). Maintaining this enemy narrative contributes to the people rallying behind the President and helps the regime stay in power. Russia is preparing for a lengthy confrontation with the West. As a result, a military conflict between Russia and the West is no longer inconceivable. Even if the fight in Ukraine comes to an end, this broader and in the eyes of the Russian regime existential confrontation will continue.

Putin's regime remained stable in 2025, even though it increasingly enforces this through repression and growing control over in particular the digital information domain. In a certain way, these initiatives are aimed at further isolating Russia from Western influences that may pose a threat to the stability of the regime. The economic issues that come with the war appear to be manageable to Russia. Since the death of Aleksey Navalny in 2024, there has been no more domestic opposition.

In the past year Russia's attitude with regard to the war in Ukraine has further hardened and become more unyielding, in spite of some Russian-Ukrainian negotiations and several substantive talks with the White House. It has become more clear than ever before that Russia is not willing to compromise on Ukraine. Russia continues the fight on the Ukrainian battlefield unabatedly.

Russian cyberactors active

As in previous years, Russian cyberactors are active in the field of offensive cyberoperations against Europe. It concerns both actors directly linked to the Russian intelligence and security services as well as pro-Russian attackers who are further removed from the Russian government, but are state-backed. Operations vary from relatively simple spearphishing attacks to advanced hacks into the systems of governments, companies, and institutions.

Russia attempts digital espionage through penetrating the systems of the Dutch government and international institutions located in the Netherlands, as well as in other EU and NATO countries. The goal: obtain information regarding, for example, the support to Ukraine. Additionally some Russian actors invest in cybercapacity so that they can carry out cybersabotage at a later stage.

The AIVD and MIVD signal that Russia's capacity to carry out cyberattacks is growing. These actors can also carry out their cyberattacks at a high speed. This is also because they can partially automate their attacks, also through means of AI.

Public attribution LAUNDRY BEAR

In 2025 the AIVD and MIVD identified a previously unknown Russian cyberactor: LAUNDRY BEAR. This actor carried out a cyberattack in which work-related contact details of Dutch police officers were obtained. In May 2025 the AIVD and MIVD made this actor known to the public. Through this they enabled other parties, domestically and abroad, to carry out their own investigations into this actor. The actor has not ceased its activities since this information has become public knowledge. LAUNDRY BEAR has been carrying out cyberattacks on Western governments, companies, and other organisations since at least 2024. The attacks of this cyberactor are often directed at targets which are relevant for Russia's war efforts in Ukraine, such as the Ministries of Defence of NATO countries, branches of the armed forces, and defence suppliers. The Dutch police appears to have been a target for opportunistic reasons.

Chat accounts Dutch government employees targeted

In 2025 the AIVD and MIVD established that a Russian cyberactor is attempting to globally gain access to a large number of Signal and WhatsApp accounts of dignitaries, members of the military, and civil servants. Within this campaign the actor also gained access to the chat accounts of multiple Dutch government employees. In addition to obtaining access to these accounts is it also possible for the actor to take over the accounts. Because of this the contact persons of the victim are under the assumption that they are sending messages to the victim themselves, when in actuality the messages end up with the actors.

Cyber on the battlefield

A large part of Russia's offensive cyberprogramme focuses on the eastern flank of Europe. As in prior years, digital espionage plays a leading role in this. The AIVD and MIVD additionally see that Russia is using the obtained information in new ways. The Russian army e.g. uses information stemming from cyberoperations, such as information on troop movements or location data of Ukrainian soldiers, in military operations.

Prioritisation in sabotage activities

Also in the case of sabotage activities in the cyberdomain, Ukraine remains the highest priority for Russian cyberactors. The targets were largely Ukraine's energy and logistics sectors. These priorities can change towards the end of the war; it is possible that Russian cyberactors will then apply their capabilities more broadly to the Netherlands and other NATO allies and EU member states.

The Netherlands remains a potential target country for both digital and physical Russian sabotage activities. This is because the Netherlands is still providing a considerable amount of support to Ukraine, and also because the Netherlands is a transport and information hub in Europe.

In 2025 Russia carried out various (attempted) digital sabotage attacks in European member states. The AIVD and MIVD did not identify successful Russian cybersabotage attacks in the Netherlands in 2025 that posed an imminent threat.

Reconnaissance activities at for example embassies in the Netherlands
Investigation by the services showed that an underage individual was mapping the digital networks of embassies and other organisations in The Hague. These reconnaissance activities were carried out at the request of a Russian state-backed hacker group. Following an official report from the MIVD the police carried out a number of arrests. Because the action was terminated in time and thanks to the cooperation between national and international partners, a worse situation could be prevented.

Russian escalation and de-escalation

With its physical sabotage activities, Russia seems to escalate and de-escalate at its own discretion. The scope of these activities varies through time. Sabotage activities which can be attributed to the Russian intelligence and security services came to a head (for now) in the summer of 2024. After this, the services saw fewer Russian sabotage activities in Europe. As yet it is unclear why Russia scaled down these activities at the time. However, a cautious increase in sabotage activities or preparations for sabotage activities has been observed since the summer of 2025. These activities often still target military and logistical goals, as well as organisations that are involved in the war in Ukraine.

In the context of the Russian hybrid threat, there has been a lot of speculation in the media regarding drones. In 2025 the AIVD and MIVD did receive an increased number of reports on drone sightings near vital infrastructures, airports, and for example military facilities. For these kinds of reports too, establishing suspected Russian involvement is complicated, and often this conceivable Russian involvement cannot be confirmed. Nor is a signalled drone always a threat.

New modus operandi: use of layered networks

It has become more difficult for the Russian intelligence and security services to develop activities in Europe. This is in part due to the large-scale expulsion of Russian intelligence officers under diplomatic cover in a large number of European countries, which followed the Russian invasion in Ukraine in 2022, and because of stricter visa rules within the Schengen area. This is why Russian intelligence and security services use a new method to carry out sabotage activities: the use of layered networks.

Layered networks consist of coordinators, facilitators, and so-called low-level agents who carry out the sabotage actions. A clear profile for these types of agents cannot be given. It does often concern persons who see sabotage activities as a way to quickly and easily make money. These, sometimes underage, low-level agents often do not seem aware that they carry out activities by order of Russia. Unlike intelligence officers they receive little to no training.

This layered construction makes it relatively easy for Russia to obfuscate its own involvement in sabotage operations.

The AIVD and MIVD deem it unlikely that an increase in these sabotage activities and the new working method will replace the already existing modi operandi of the Russian services. These existing working methods, such as the more classic forms of espionage and state interference, have already proven their worth in the past.

Russian interference

A core task of the Russian intelligence and security services continues to be espionage, a form of state interference. The Russian services try to use not only technical but also human sources to obtain strategic secrets, knowledge, and technology in order to gain a political or military advantage. Russian intelligence officers use various covers, such as scientist or journalist, in order to obtain access to this information. Furthermore they remain active under diplomatic cover both in the Netherlands and in the rest of Europe.

The Russian intelligence and security services are active in e.g. countries on the eastern border of the NATO alliance. Here they want to collect information on NATO's military capacity and try to influence the war in Ukraine to Russia's advantage.

The Russian services also play an important role in acquiring technology and dual-use goods for the Russian defence industry. This method enables Russia to partially circumvent the Western sanctions policy.

Russian approaches of European parliamentarians

The Russian services seek rapprochement with members of parliament in European member states. They do this both covertly and overtly. Moscow openly invites parliamentarians to take part in events inside and outside of Russia. It also proposes joint initiatives for resuming cooperations. At the same time, these overt rapprochement attempts seem to be less effective than Russia was aiming for. This is in part due the reticence of European politicians to show too much public affiliation with Russia. This in turn drives Russia to use more discretion in its rapprochement attempts to these politicians.

Increasing security awareness: AIVD briefs members of parliament
The AIVD has provided briefings to members of the Dutch parliament and Dutch members of the European Parliament regarding the threat posed by Russian covert influencing.

Spread of narratives favourable to Russia

In spite of various Western countermeasures, Russia continues to unabatedly carry out digital disinformation campaigns with regard to various European countries. The increasing use of artificial intelligence can be a tool for Russia to improve the quality and scope of its disinformation campaigns.

Russia uses events in e.g. the Netherlands for promoting messages favourable to Russia. These messages are often intended for the Russian population. This mainly happens through demonstrations with messages that are beneficial to Moscow. In reports on Russian state media and social media, the importance and scope of these demonstrations is exaggerated to such an extent that a (pro-)Russian audience may believe that there is considerable criticism in the West of the military support to Ukraine or of NATO.

> **For more information, go to: aivd.nl/tussen-vrede-en-oorlog**

In February 2026 the AIVD and MIVD published ***Between peace and war: The war in Ukraine and the Russian threat in Europe***.
This contains more information on e.g. Russia's perspective and hybrid activities.

2.6

China

- The threat from China is becoming more widespread and serious. The AIVD and MIVD carry out a joint investigation into the threat China poses to the Netherlands.
- China is building an international order which is favourable to China's interests.
- China is acquiring advanced technological knowledge, both in legal and covert ways.
- The AIVD and MIVD contribute to raising awareness of and countering the Chinese cyberthreat.

China is building a new world order

3 September 2025: A large military parade is taking place in Beijing to celebrate the end of the Second World War, eighty years ago. The parade shows a confident Chinese leader, as well as the outlines of the world order he envisions: a world in which China is the powerful centre. A centre which other world leaders turn to.

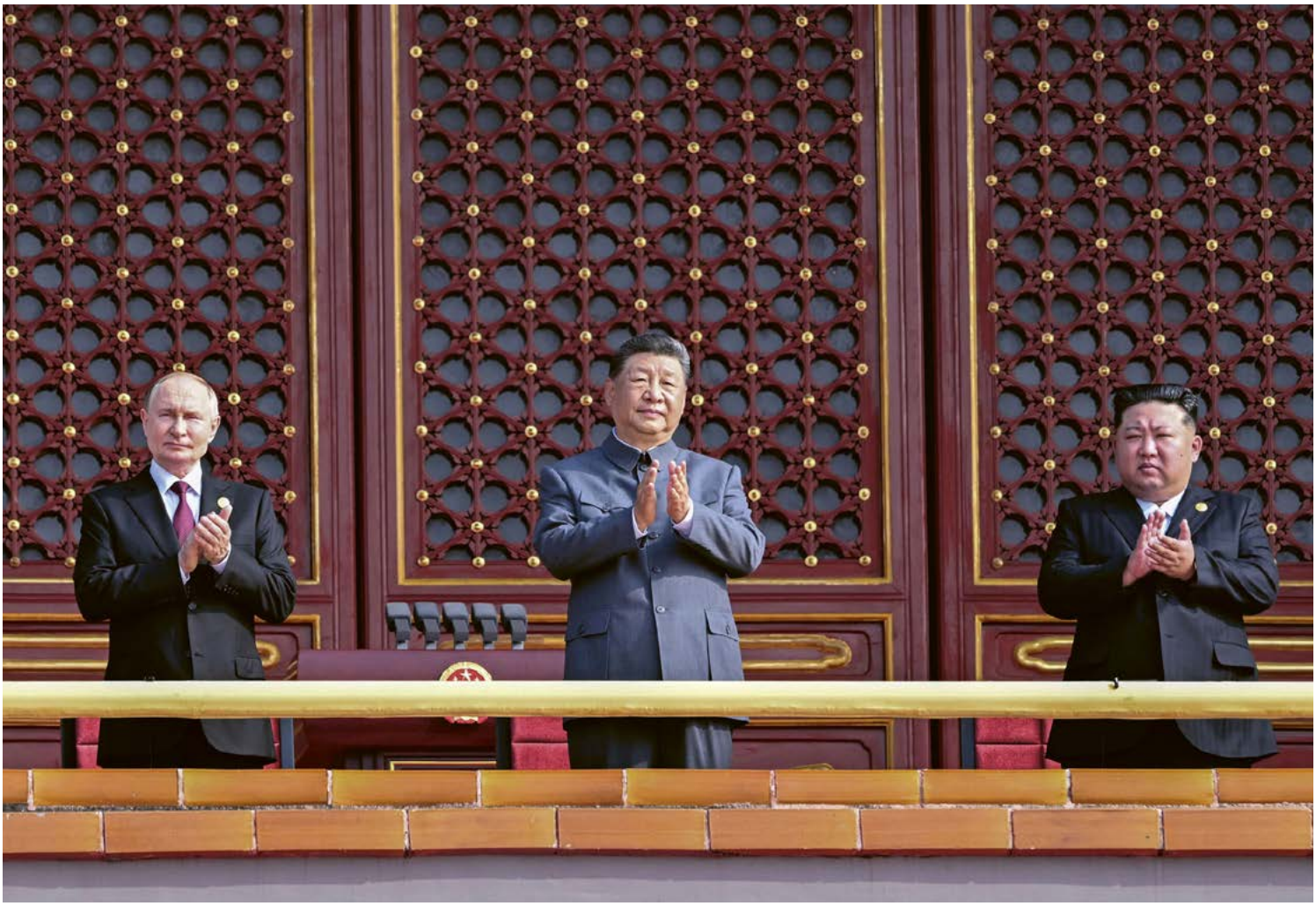
Some days before this parade, Chinese President Xi announced a new global initiative: the Global Governance Initiative (GGI). And earlier in 2025, in Hong Kong the Organization for Mediation (IOMed), initiated by China, was founded. Both initiatives are examples of how China is founding new international structures through which it can better promote its own interests than through already existing international organisations. This also enables China to further increase its own influence, in particular in countries in Latin America, Africa, and Asia. The world order China is trying to bring about in this way is aimed at decreasing the West's influence in the world, in particular that of the US but also that of Europe.

Exploiting economic dependencies

In joint AIVD and MIVD investigations, the competition between China and the West becomes clear in e.g. the area of economic ties. When the United States announced trade tariffs, China responded with trade tariffs for US products and later with restrictions on the export of rare earth metals. In doing this, China shows how dependent other countries are on China when it comes to manufacturing products which can have both a civil and a military purpose. In 2025 China also used this dependency against the US and Europe. This dependency can come with risks and threaten the European and Dutch economy and the ability to autonomously make strategic choices.

Obtaining sensitive knowledge and technology

For China's continued technological and economic development, however, it is also partially dependent on Western countries. China develops a lot of knowledge itself through advanced research. The AIVD and MIVD conclude that China also attracts Western researchers for this, and that it sends Chinese students and researchers to the West in order to gain knowledge they can later apply or further develop in China.



In September Chinese President Xi Jinping (middle), Russian President Putin (left), and North Korean leader Kim Jong Un (right) commemorated the end of the Second World War (then eighty years ago). China, Russia, North Korea, and Iran are increasingly banding together in order to increase their influence on the world. Photo: Korean News Service via AP.

In this way, China can get its hands on advanced and sometimes very sensitive knowledge and technologies. China can apply this in its own technological and economic developments and the modernisation of its armed forces. Even though China is behind on the West in some fields, such as producing highly advanced chips, this does not mean that the country is not capable of remarkable achievements. For example, the world was surprised by the AI program DeepSeek, which was on par with the most advanced Western AI programs, in spite of the fact that China was working with less advanced chips.

The fact that China wants to improve and expand in many high-grade technological fields in the coming years also becomes clear in the first outlines of the 15th Five-Year Plan, which comes into effect in 2026. These Chinese efforts pose a threat to the innovative and earning capacity of Western knowledge institutions and companies. This is in part because the Chinese researchers with whom they cooperate can be or are pressured to share the technological knowledge they have obtained. On the other hand, China can also obtain knowledge in a covert manner. Both this continued attention for high-grade knowledge and technology and the exploitation of economic dependencies broaden the threat posed by China.

Chinese cyberthreat continues to be bigger than expected

In order to obtain knowledge intended for China's economic development, China also makes use of cyberattacks. However, China's cyberactivities do not focus only on economic targets. China has a continued and considerable need for information which can be of importance to various parts of the Chinese state, decision makers, companies, and armed forces. In order to obtain this information, many Chinese advanced persistent threat (ATP) attack groups are used. The Chinese cyberthreat continues to be bigger than expected.

It cannot always be directly proven that the Chinese state is behind certain cyberoperations. The AIVD and MIVD nevertheless still conclude that there is a large ecosystem of Chinese cyberactors, companies, and state entities that plays a role in initiating, facilitating, and carrying out cyberattacks. Some Chinese cyberactors structurally focus on Europe, NATO, and also on the Netherlands. In addition, sometimes opportunism plays a role in cyberattacks, for example when the actors exploit a newly discovered vulnerability on a massive global scale. This could also cause victims in the Netherlands.

Chinese attack groups are active globally and successfully target companies, governments, and organisations in almost every country. The telecommunications sector is an important target. Not only can this yield a lot of valuable information, there are various ways in which these attacks can contribute to developing China's (sabotage) capacity which can be of benefit in case of a conflict. China's cyberprogramme is so advanced and large in scope that likely only a small part of cyberattacks on the Netherlands and its allies are identified and stopped in time. This shows that the threat posed by China is not only becoming more wide-spread, but also more serious.

Public warning SALT TYPHOON

The cyberthreat posed by China and our relatively small capacity to gain insight into and thwart this threat are concerning. The AIVD and MIVD therefore not only investigate the Chinese cyberthreat, but also actively publish information on this threat and how it can be countered. In the summer of 2025 the AIVD and MIVD together with intelligence, security, and cybersecurity services from many countries published a joint cybersecurity advisory on Chinese cyberactor SALT TYPHOON. This group was targeting telecommunications companies in the United States, but also in the Netherlands. For almost two years the group was able to carry out its actions unnoticed. In these two years, the group was able to collect information from critical and vital parts of telecommunications networks at a large scale. In publishing this information the AIVD and MIVD can warn for Chinese cyberattacks and share measures for becoming more resilient with companies and organisations they otherwise would not have reached.

> **For more information, go to: aivd.nl/cyberadvies**

The AIVD also wants to reach the broader public with its public cybersecurity advice, such as the advisory 'Risk of malware infection during travel to China'. This advice was published after the AIVD found FlowCloud malware on mobile devices of persons who travelled to China for their work. This malware was likely intended for espionage purposes: the victims work within public and private organisations on topics and issues that are relevant to China. The services also give presentations on these and other topics, for example during cybersecurity conferences.

Chinese espionage and interference

Chinese intelligence and security services actively carry out intelligence activities in the Netherlands. This was proven once again in 2025. These services approach individuals relevant to China and establish intelligence networks here. They also obtain knowledge and technology which China can use to its advantage. People can contribute to this wittingly or unwittingly. As also described in the chapter on state-sponsored inference, since 2025 intelligence activities in the Netherlands are liable to prosecution.

China uses a whole-of-society approach. This in part means that all parts of society, from individuals to companies and organisations, can be used by the Chinese government for e.g. intelligence activities. They are legally obligated to cooperate. Because this legislation has an extraterritorial effect, this can also be used to put pressure on the Chinese diaspora.

Chinese services exert control and pressure on the Chinese diaspora that is present in many countries. These services want to suppress dissident voices and mobilise Chinese citizens living in the Netherlands to counter such voices. The Chinese Communist Party (CCP) considers divergent ideas to be a threat to its continued existence.

China additionally tries to covertly exert political influence abroad. This became visible in various Western countries in 2025. The United Kingdom deported a Chinese businessman on suspicion of being involved in political influencing in the highest social circles. Also for exerting political influence outside of their own borders, China uses the Chinese diaspora in foreign countries, such as in the Netherlands, either through force or not.

2.7

Political intelligence

- **In 2025 the developments in Venezuela and the increasing tensions between the United States and Venezuela led to concerns in and about the Caribbean part of the Kingdom of the Netherlands.**
- **The war in Gaza impacted the Dutch national security in multiple ways.**

Events and developments abroad can have a strong influence on the security of the Netherlands or the Caribbean part of the Kingdom. That is why the AIVD, in some investigations together with the MIVD, investigates the threat these may pose. In this way the services gather political intelligence. It is important to the Dutch government to have independent political intelligence. On the basis of this intelligence

the government can determine the Dutch stance in e.g. international negotiations, or make well-considered decisions for the Netherlands' foreign policy. Two of the areas of investigation are highlighted below.

Venezuela

The events in Venezuela in 2025 and the increasing tensions between the United States and Venezuela are cause for concern in and about the Caribbean part of the Kingdom. The AIVD and MIVD jointly investigate the political and military developments in Venezuela and the possible indirect effects on the Kingdom of the Netherlands, and therefore closely monitor the situation.

From January 2025 the United States increased the pressure on Venezuela. From the summer of 2025 there was a large-scale deployment of US troops in the Caribbean. According to the US, the goal was to combat the drugs trade, but in Venezuela there were fears of a military action against the country. Venezuela received international support from a number of partners, including Russia, China, and Iran.

At the end of 2025 the Venezuelan regime appeared to have effectively sidelined the Venezuelan opposition.

On 3 January 2026 the United States carried out a military operation in Venezuela during which Maduro and his wife, Cilia Flores, were arrested and transferred to the United States. Former Vice President Delcy Rodriguez assumed interim leadership in Venezuela. This has eased tensions between the US and Venezuela, for now. In spite of this the situation remains volatile. This also has an effect on the Caribbean part of the Kingdom.

Consequences for the Caribbean part of the Kingdom of the Netherlands

The Netherlands is not involved in the US' nationally directed operations in Venezuela and the Caribbean. However, a further escalation could have consequences for Aruba, Curaçao and Bonaire. Additional military activity could again lead to a temporary closure of the airspace. It may also hinder the supply of goods, including daily essentials, delivered via sea. It also cannot be ruled out that a further escalation may cause a refugee flow towards the Leeward Antilles.

Middle East

At the end of 2025 there was a ceasefire between Israel and Hamas. The AIVD estimates that it will still take a long time before there is a stable government in Gaza. In 2025 there was also no prospect of a two-state solution.

The humanitarian and logistical challenges regarding the reconstruction of Gaza are considerable. The Palestinian sovereignty is under intense pressure – not just in Gaza but also on the West Bank. The AIVD takes in account that a possible annexation of the West Bank could cause more instability in the region.

The situation in the Palestinian Territories has an effect on the Dutch national security. First, combat between the parties may pose a physical threat to Dutch persons and objects in the region. At the same time the war has consequences for the Dutch social stability. The war may also be a catalyst for some individual jihadists and the left-wing extremist movement. Moreover, the threat of violence to Jewish and Israeli targets in the Netherlands has increased. Lastly, the situation requires more effort from security partners to provide for the proper functioning of the International Criminal Court and the International Court of Justice, of which the Netherlands is the host country, also on the topic of Gaza.

In 2025 too the changing regional power balance had a considerable impact on other countries in the Middle East, including Syria. In December 2024 the regime of Bashar al-Assad was driven out, led by Hay'at Tahrir al-Sham. The leader of this group, Ahmed al-Sharaa, has been interim president of Syria since March 2025. This year the political situation in Syria has developed into a tense status quo, in which changes happen in quick succession.

The current interim government has managed to stay in power, but does have to withstand a small ISIS resurgence. There is no stable unitary state yet. In spite of the relative increased stability and security, as yet it does not seem as though various regional and ethnic groups are willing to relinquish their agenda of autonomy: Kurdish groups in the north-east, the Druze in the south-west, and the Alawites in the north-west. The reconstruction of the economy and infrastructure remains a challenge, in part because various foreign actors are trying to assert their influence.

Instability in Syria also puts pressure on Dutch security interests. It offers terrorist groups an opportunity for (further) resurgence. At this point in time, many ISIS fighters who were in prison have also regained their freedom.

2.8 Contraproliferatie

- **Together with the German intelligence service BND in 2025 the AIVD and MIVD published the news that Russia intensified its use of chemical weapons in Ukraine.**
- **During the Twelve-Day War considerable damage was done to Iran's nuclear and missile programmes.**
- **The AIVD and MIVD disrupted a number of undesirable procurement attempts. In doing so, the services prevented equipment from reaching countries of concern which would use it in programmes for the development of weapons of mass destruction.**

The development, production, and dissemination of weapons of mass destruction and means of delivery (usually ballistic missiles) are globally considered a real threat to the international security. The AIVD and MIVD carry out joint investigation into the countries which (may) develop weapons of mass destruction. The services inform the Dutch government of relevant developments in these so-called countries of concern. In 2025 the services investigated the activities of countries including Iran, Russia, and North Korea.

The AIVD and MIVD also make efforts to prevent Dutch companies from (unwittingly) contributing to the proliferation of weapons of mass destruction.

Iran

In June 2025 Israel and the United States carried out attacks on the nuclear and missile facilities of Iran, with the goal of crippling Iran's nuclear programme. These attacks have become known as the 'Twelve-Day War'. Both countries wanted to remove Iran's capacity for developing nuclear weapons.

In order to be able to develop a nuclear weapon, a country must have enough highly enriched uranium, as well as the political will and technical capacity to actually turn this into a weapon. During the Twelve-Day War Iran would have been able to acquire enough highly enriched uranium in a very short time to manufacture several nuclear weapons. The AIVD and MIVD had no indications that Iran was taking the other steps necessary to make a nuclear weapon.

In the Twelve-Day War important Iranian leaders of both the nuclear and missile programmes were eliminated. Although there are various claims about the exact extent of the damage, it is clear that this is considerable. Iran responded with multiple missile attacks on Israel, in which it launched hundreds of ballistic missiles. Iran will have to invest a lot of time and means to get its nuclear programme back to the level it was at before the attacks. The ballistic missile programme also sustained considerable damage. Iran is taking large steps to repair the sustained damage. In order to do this, Iran attempts to obtain materials and equipment from other countries. Iran also provides materials to other countries. In 2025 Iran again supplied short-range missiles to Russia. The services suspect that Russia wants to use these missiles in Ukraine.

The United Nations have denied Iran the right to uranium enrichment because Iran did not adhere to the nuclear deal from 2015. However, Iran keeps holding on to its right to a civilian nuclear programme and considers uranium enrichment to be an indisputable part of this. According to another international treaty, the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), Iran is obligated to show its uranium storage and enrichment facilities to the International Atomic Energy Agency (IAEA). This has not happened since the attacks in June 2025. Within these international contexts Iran is supported by Russia and China. The cooperation between these countries has increased over the past years.

Russia

In July 2025 the AIVD and MIVD together with German intelligence service BND published the news that Russia intensified its use of chemical weapons in Ukraine. Investigation by the services has shown that in 2025 Russia continued the use of chemical weapons in this war. The services consider the use of chloropicrin to be confirmed. In this Russia shows an escalation in its willingness to use chemical weapons.

Chloropicrin has a similar effect to tear gas, but is stronger. According to the Chemical Weapons Convention, which Russia is a party to, these means are never to be used in a military conflict. Additionally, Russia continues to invest in chemical and biological weapons programmes.

North Korea

In 2025 North Korea further focused on expanding its nuclear arsenal. After the country showed photos of the known uranium enrichment halls in 2024, in 2025 it built a new facility which is very similar to the existing enrichment facilities. North Korea additionally continued with the development of new intercontinental ballistic missiles, such as the new Hwasong-20. This was presented by North Korea as the most powerful nuclear strategic weapons system in the world. The country also continues working on the development of hypersonic glide vehicles: warheads which upon returning to the atmosphere can manoeuvre at very high speed.

In 2025 North Korea prominently showed its presence on the world stage. For example, North Korean troops walked in a military parade in Moscow. Kim Jong Un himself visited Beijing to attend a parade. In the background North Korea continues to intensify its cooperation with Russia, in order to modernise their own North Korean weapons industry. It also continues to supply short-range missiles which Russia uses to attack targets in Ukraine.

Undesirable acquisition

Countries such as Iran, Russia, and North Korea are partially dependent on knowledge and resources from the West for the (further) development and production of their weapons of mass destruction. That is why the AIVD and MIVD investigate the acquisition of knowledge and goods from e.g. the Netherlands which these countries can use for their programmes in which they produce weapons of mass destruction. In light of the current geopolitical situation the investigation into Iranian and Russian acquisition has priority.

In 2025 too Russia and Iran continued their activities to acquire strategic goods in the Netherlands and Europe. As a result of imposing and expanding the international sanctions against Russia and Iran, their trade networks have shifted. They now use alternative routes, through e.g. the United Arab Emirates, Türkiye, Kazakhstan, and China. The AIVD and MIVD furthermore signal that countries like Russia, Iran, China, and North Korea are cooperating more intensively in the acquisition of goods and knowledge which can be used in the manufacturing and further development of weapons of mass destruction.

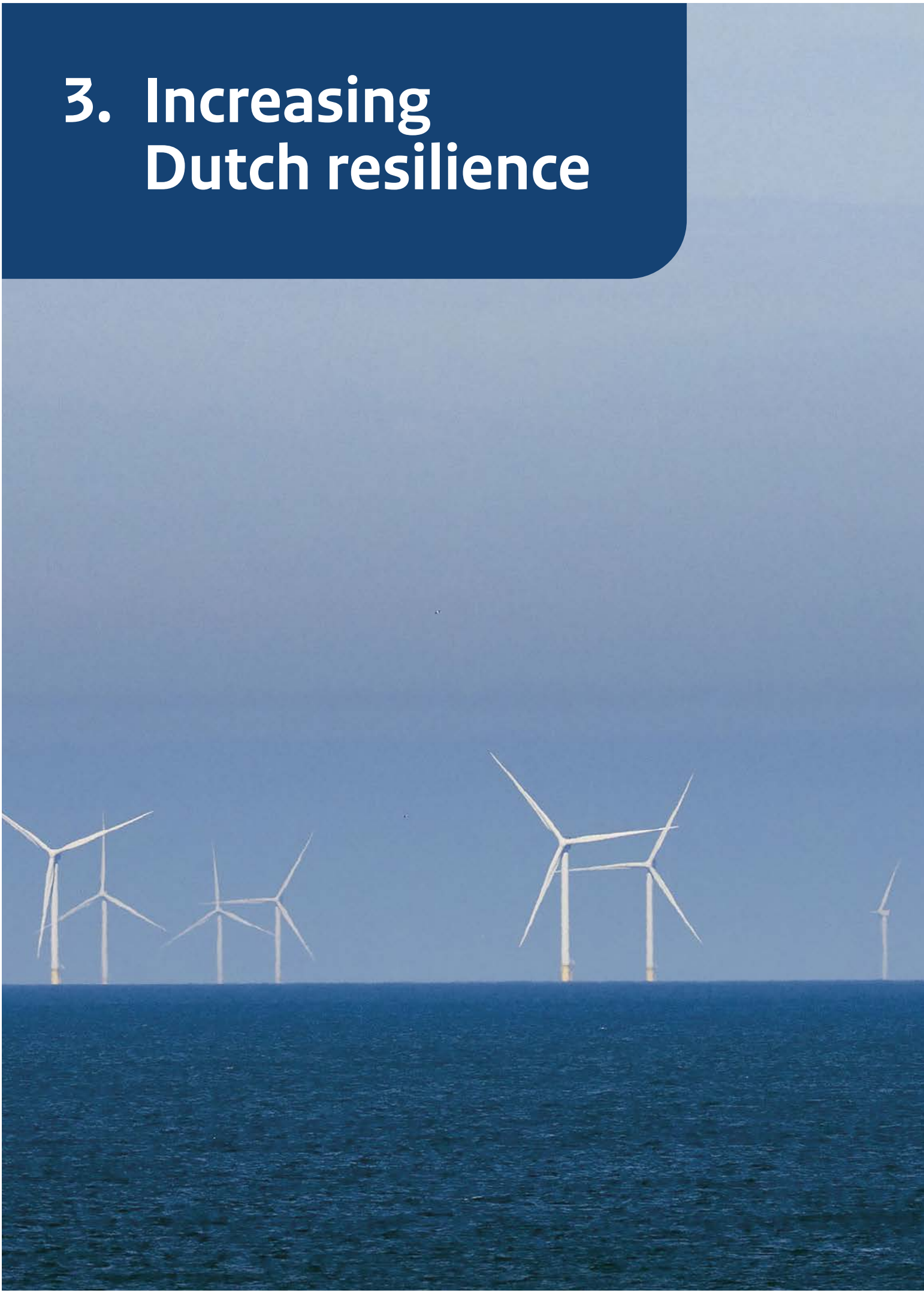
When companies supply sensitive goods, knowledge, or technology to foreign countries, there is therefore the risk that they directly or indirectly contribute to programmes which are aimed at the development of weapons of mass destruction and their means of delivery. For most companies, this risk is particularly clear when they receive a request from a country of concern. The risk is less clear when the requested supply is done via an alternative route through one of the above-mentioned countries.

The AIVD and MIVD see that both larger and smaller companies are approached by state actors who want to use their goods, knowledge, and technology for weapons of mass destruction and their means of delivery. Undesirable knowledge and technology transfer do not just have consequences for individual companies, e.g. in the form of negative publicity when the supply comes to light. Above all, they pose a threat to the national and international security.

In 2025 the AIVD and MIVD prevented such equipment from reaching countries of concern a number of times. It concerned equipment which would enable these countries to carry out technical research relating to weapons of mass destruction. The AIVD and MIVD cooperate with many different organisations domestically and abroad, such as customs organisations and intelligence services.

> **For more information, go to aivd.nl/massavernietigingswapens**

3. Increasing Dutch resilience



Wind turbines off the coast of the Netherlands. AIVD advice also contributes to the security of new wind turbine parks and the maritime sector.
Photo: ANP

3.1

Ways in which the AIVD contributes to the resilience of the Netherlands

> **A resilient society is better capable of dealing with threats. This requires society to be informed of these threats.**

> **The AIVD contributes to this resilience in various ways. This is done on the basis of intelligence and the service's expertise on resilience. The service contributed to a secure and uninterrupted NATO Summit in The Hague.**

The AIVD is a driver for boosting resilience of the Netherlands on the basis of intelligence and the service's expertise in resilience. A resilient society is better capable of handling the threats highlighted in the previous chapters.

Resilience is created through effective cooperation between government institutions, companies, knowledge institutions, and citizens, among others. Only together we can ensure that the Netherlands becomes more resilient. This chapter describes in which ways the AIVD contributes to this.

In 2025 the AIVD again published specific advice with insight into the threats and with explanations on which measures can be taken. These reports with advice and assessments regard technical matters as well as policy matters. Some of these are specifically about digital resilience. In 2025 the advisories related to e.g. the NATO Summit in The Hague, risks of travelling abroad, sovereignty, offshore wind power, dealing with software vulnerabilities, and messaging apps.

The AIVD also guides the development of information security products. Before these products can be used with confidential information, the AIVD has to approve them. The service moreover contributes to the further development of public-private cooperation. This cooperation is crucial for increasing resilience.

A resilient government

In 2025 the AIVD worked on increasing the resilience of the government itself – in particular with the central government, the National Police, the Public Prosecution Service, the Dutch Senate and the Dutch House of Representatives. With targeted advice the AIVD contributed to increasing threat awareness and improving security measures. In 2025 for the second year in a row the AIVD published the 'threat analysis central government'. With this analysis the service informed the Security Authorities and Chief Information Security Officers (CISO) of the ministries of the most relevant physical and digital threats, and the working methods of attacks. This analysis is updated annually.

> **For more information, go to: aivd.nl/weerbaarheid**

Protection of persons, objects, services, and events against (terrorist) attacks

The AIVD also provides information to the NCTV and Public Prosecution Service so they can adjust or take security measures in relation to persons, objects, services, and events. The service does this through providing so-called threat products. In 2025 the AIVD issued over 50% more of these products than in 2024.

More threat products for protection and security

The field of protection and security has the purpose of protecting persons, objects, services, and events against (terrorist) attacks. For example politicians, embassies, members of the Royal House, and international organisations. For this, the AIVD issues threat products: threat assessments, threat analyses, risk analysis, and reports. On the basis of these products the NCTV and the Public Prosecution Service can adjust or implement security measures.

In 2025 the AIVD issued 108 threat products, which is over 50% more than in 2024. This increase is partially the result of an increased demand from the National Coordinator for Counterterrorism and Security (NCTV) and the Public Prosecution Service, and new cases which came up in 2025. The AIVD also invested in additional capacity for the field. There were furthermore developments in the threats against the Dutch national security which led to more threat products.

For example, the threat of state-sponsored actors against persons in the Netherlands increased in the past years. This includes persons who are or were active on behalf of opposition or separatist movements and persons who publicly speak critically about the regime in their countries of origin (such as activists, journalists, and dissidents). The threat against the police, the judiciary, and other parties involved in the criminal justice chain has also increased in the past years.

In 2025 the AIVD also published threat analyses on the NATO Summit which was held in The Hague in June 2025 and the threat against national politicians and the elections for the Dutch House of Representatives in October 2025.

Over the past years, the AIVD has been closely involved in the reform of this field and shaping a new system for the security of persons. These changes will largely be implemented in 2026. This contributes to a proper functioning of a large number of officials who play a crucial role in our democratic legal order.

> **For more information, go to: aivd.nl/bewakenenbeveiligen**

Resilience in vital sectors

The AIVD maintains close ties with companies from vital sectors and gives priority to the energy, maritime, digital infrastructure, and civil aviation sectors. In 2025 the AIVD was also in contact with companies from other sectors which play an important role in the national security.

To illustrate: the energy sector and the maritime domain

The energy sector is essential for the proper functioning of Dutch society. The Dutch ports play an important role in job opportunities, energy supply, trade of daily supplies, and the security of the Netherlands. A shutdown or disruption of the energy sector or (parts of) ports could seriously disrupt the logistics chains in society. During times of international tensions these sectors are the targets of e.g. (economic) espionage or of disruption of processes in the ports. In the extreme case of a large-scale conflict, these sectors may be attractive targets.

Resilience through knowledge and economic security

Together with the MIVD, the AIVD also contributes to resilience against undesirable knowledge and technology transfer. The Netherlands is a small but highly developed country with a large knowledge-based economy, e.g. in the field of semiconductors and quantum technology. Various state-sponsored actors are interested in this knowledge and expertise and carry out concrete intelligence activities in order to obtain it.

In 2025 the AIVD concluded that high-tech companies and prominent knowledge institutions were adequately or well aware of the threat. This showed an increase with regard to previous years. Awareness is the first crucial step.

The companies and institutions that are aware of the threat would prefer to take risk-oriented measures. However, the AIVD sees that they struggle to identify what exactly the risks to the organisation are.

In order to identify the risks, the answers to the following questions must be clear: 'what are the interests that are to be protected?' and 'what is the threat?'. Information on the threat is shared by the AIVD, MIVD, and other security partners in classified reports as well as publications, such as this annual report. But the interests must be identified by the company or organisation itself: which specific aspects are so important that people should take protective measures to secure these? The complexity of this question sometimes results in broad and unfocused measures, the feasibility and costs of which are not realistic. It is necessary to make hard decisions about what the to be protected interests are and where fewer or more risks are acceptable.

Resilience through industry security

Together with the MIVD the AIVD also assists in industry security. Industry security relates to the oversight on the security demands companies have to adhere to when they carry out tasks for the central government, Ministry of Defence, and the Police, which can be of influence on the national security. This oversight was previously carried out by two separate departments at the AIVD and MIVD respectively. In 2025 these departments were absorbed into a new, joint unit: the National Bureau of Industry Security (Nationaal Bureau Industrieveiligheid, NBIV) which was further developed and strengthened this year.

Resilience through treaty obligations

In addition, internationally the AIVD also fulfils a number of tasks which are recorded by treaty. As National Security Authority, the service oversees the way in which the Dutch government handles the protection of confidential information from the EU, NATO, and European space programme ESA.

The AIVD is also responsible for negotiations regarding the General Security Agreements (GSAs) between the Netherlands and other countries which exist in order to safely share classified information with each other. These negotiations happen in cooperation with the Ministries of Foreign Affairs, Defence, and Economic Affairs. In 2025 the GSAs with Latvia, Norway, Ukraine, Portugal, Slovakia, and Sweden were ratified and came into effect. The AIVD also took part in a number of council working groups within the EU and NATO to contribute to the regulation of information security for EU entities. The execution of these tasks recorded in the treaties are only becoming more important in light of the threats and developments described in this annual report.

Resilience through electronic security sweeps

In good cooperation and coordination with the MIVD and police, the AIVD swept 124 spaces in 2025. Sweeping ensures that the confidential information which is discussed in these spaces remains safe: with unique knowledge and means, the space in question is searched for monitoring equipment, hidden cameras, and other sensors. The AIVD did this at the request of e.g. the Ministry of General Affairs and also during the NATO Summit in The Hague.

During the NATO Summit the AIVD, together with the police, carried out a successful search into a malicious network. This action was carried out when a Wi-Fi network became visible which had the same name as the legitimate NATO guest network.

3.2

Security screenings

> **The threats mentioned in previous sections have an influence on the security screenings carried out by the service. In 2025 the Unit Security Screenings (Unit Veiligheidsonderzoeken, UVO) saw a shift in the type of security screenings that was requested: the UVO carried out 17% more A and B screenings than in 2024.**

> **Security screenings contribute to the resilience of the Netherlands.**

The threats highlighted in previous sections are directly visible to the Unit Security Screenings (Unit Veiligheidsonderzoeken, UVO), a joint unit of AIVD and MIVD. In 2025 the Ministry of Defence employed more staff than in previous years and therefore also applied for more security screenings with UVO. This increase can also be seen in applications from other related (vital) sectors.

The UVO carries out security screenings into people who in their work (will) have access to secret information or who are or will be in a position in which they could damage the national security. Examples are people working for the central government, the Ministry of Defence, in civil aviation, or companies responsible for vital processes. The UVO also carries out security screenings for Dutch persons who require a NATO or EU clearance.

In total the UVO took 85,637 decisions in 2025. This is a light increase compared to 2024. Of this total, for civil aviation 32,862 decisions were taken by the mandated party, the Royal Netherlands Marechaussee. In spite of the continued demand for security screenings, the UVO completed 92,6% of the security screenings within eight weeks.

More A and B screenings

Depending on the nature of the position and the potential harm the (candidate) official in this position could cause to national security, a level A, B, C, or Civil Aviation (CA) screening will be initiated. The level A screening is the most thorough and intended for the most vulnerable of positions involving confidentiality. The higher the security level, the more extensive the UVO's screening is. In 2025 the UVO carried out 17% more A and B level screenings than in 2024, in particular due to the larger number of security screenings with the Ministry of Defence.

NATO Summit: over 500 additional security screenings
Prior to the NATO Summit the UVO carried out over 500 security screenings. These were screenings of persons selected to work within various secured zones during the NATO Summit. In eleven of the screenings the UVO issued a negative decision. The persons in question therefore did not work within these secured zones.

A temporary AIVD and MIVD project team, in addition to the UVO, moreover carried out many additional checks for the NATO Summit.These checks are a fundamentally different and lighter procedure than a security screening: in this case it is checking whether (and if so, in which way) someone is present in the AIVD's systems. Prior to the NATO Summit the AIVD, at the request of the Ministry of Foreign Affairs and NATO, carried out checks for 6,430 persons visiting the Summit in a short time. An immediate answer could be given with regard to 4,090 of them. The other 2,340 persons required further assessment. Based on these checks, the AIVD issued an official report on one person.

Meet the growing demand

The Ministry of Defence's intended growth, as well as the intensification of the cooperation with companies and specifically the defence industry, are expected to lead to a growing demand for security screenings. In order to meet this demand, the MIVD will hire additional staff for the UVO. It is expected that this can be financed through allocated budget related to the growth of Defence. In 2024 UVO already implemented a number of structural measures in order to meet the growing demand. In 2025 these measures were further developed and implemented. Systems and processes are being further automated. An example of this is the process for electronically applying for security screenings for the civil aviation sector This process will be further expanded in 2026.

With the publication in the Bulletin of Acts and Decrees on 30 October 2025 the final step was taken for the implementation of the reviewed Security Screening Act (Wvo). The reviewed Act will come into effect in 2026.

> **For more information, go to: aivd.nl/veiligheidsonderzoek**

Table 1

Key figures security screenings (including mandated parties)

Screenings	Positive decisions	Negative decisions	Total number of decisions
Level A, by UVO	7,136	46	7,182
Level B, by UVO	27,485	269	27,754
Level C, by UVO	6,627	55	6,682
Level CA, taken over by UVO from KMar	7,279	1,570	8,849
The NATO Summit in The Hague	516	10	526
E-CA level[2]	1,774	8	1,782
Total by UVO	50,817	1,958	52,775
Level CA, by KMar	32,862	0[3]	32,862
Total number of screenings	**83,679**	**1,958**	**85,637**

Table 2

Security screenings: results of objections and appeals

Status	Objection	Appeal	Second appeal	Provisional ruling
Submitted (in 2025)	206	11	64	2
Completed (in 2025)	167	11	3	2
Unfounded	121	9	0	0
Upheld	16	2	0	1
Inadmissible	7	1	0	0
Withdrawn	24	0	0	0
Dismissed	0	0	0	0

Notes on the results of objections and appeals

Following decisions to refuse or withdraw a certificate of no objection, the affected persons can file an objection. If this objection is deemed unfounded, they may appeal this.

[2] E-CA security screenings are submitted to UVO directly and digitally through the electronic statement of personal details (*elektronische Opgave Persoonlijke Gegevens*, eOPG).

[3] The Kmar does not issue negative decisions. In case of doubt in a Level CA security screening, the security screening is handed over to the UVO. Negative decisions are added to the number of negative decisions made by the AIVD. This explains the 0 here.

4. Organisation and key figures

The AIVD's office in Zoetermeer. Because the amount of investigations is increasing, the service has grown further over the past year. Photo: AIVD

4.1

The legal framework in which the AIVD operates

- **In 2025 the AIVD was able to make more use of the powers from the Temporary Act on investigations by the AIVD and MIVD into countries with offensive cyberprogrammes, bulk data, and other specific provisions.**
- **The AIVD continued with preparations for the new Intelligence and Security Services Act (Wiv). This is a broad revision of the Wiv 2017 and is necessary for the service to effectively and flexibly carry out its tasks in the future.**
- **In September 2025 the Dutch Senate adopted the bill for the improvement execution Security Screening Act.**

In order to effectively carry out our tasks in the framework of the national security, the AIVD sometimes has to infringe on the fundamental rights of citizens. What the AIVD is allowed to do and which frameworks are in place for that is stipulated in the Dutch law. The AIVD always has to adhere to the law.

At this moment there are three laws which together form the legal framework: the Intelligence and Security Services Act (*Wet op de Inlichtingen- en Veiligheidsdiensten*, Wiv 2017), the Temporary Act on investigations by the AIVD and MIVD into countries with offensive cyberprogrammes, bulk data, and other specific provisions (*Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkgegevens en overige specifieke voorzieningen*, Temporary Act), and the Security Screening Act (*Wet veiligheidsonderzoeken*, Wvo). The Temporary Act came into effect on 1 July 2024. In 2025 the services were able to use more investigatory powers from the Temporary Act.

For the execution of our tasks, it is important that in the future too the services can act effectively and flexibly when the threat demands this, with sufficient fitting safeguards. That is why there is currently an ongoing process for a new Wiv, which will amend the Wiv 2017. This section therefore not only talks about the Temporary Act, but also the new Wiv. It will also talk about the amendment of the Wvo.

Implementation Temporary Act

Countries with an offensive cyberprogramme are carrying out more digital attacks on the Netherlands and its allies. In order to carry out intelligence investigations into the various threats posed by these countries with greater speed and more flexibility, it was necessary to quickly adjust the legal framework for the services. These changes have been recorded in the Temporary Act and are valid in addition to the Wiv 2017.

The CTIVD stated that since 1 October 2025 they have been ready for an as full implementation of the Temporary Act as possible. Since then the AIVD and MIVD have been able to gradually put this act into use. Because of the limited extent to which the Temporary Act was implemented before then, there is currently not yet a complete picture of the effects of the implementation.

- **For more information, go to: aivd.nl/wiv**

Results implementation assessment Temporary Act
In 2025 an implementation assessment of the Temporary Act was carried out. The parts which the services were able to make use of had a positive effect on the speed and flexibility of the services – and with that on the protection of the national security.
The services assess the possibilities for use of cable interception and the regulations surrounding bulk data sets as positive.

The services also deem the possibility included in the Temporary Act to appeal with the Administrative Jurisdiction Division of the Council of State to be positive. Because of this a dispute can be quickly put before the highest administrative judge. In 2025 the services made use of this possibility to appeal in the Temporary Act one time. On 9 May 2025 the Administrative Jurisdiction Division of the Council of State ruled in an appeal case. The Administrative Jurisdiction Division upheld the appeal and reversed the TIB's decision.

The implementation assessment also showed that no consequences for the AIVD and MIVD's management were found. It was concluded that carrying out cable interception under the combination of the Temporary Act and the Wiv 2017 is not feasible. Out of operational necessity, it was therefore proposed to adjust practical execution on that front to fall under one regime, as was done for the investigations which fall under the Temporary Act.

Also after this implementation assessment, the services will continue to evaluate and monitor the Temporary Act. If the outcome of the monitoring gives reason for this, it will be taken into account in the various phases of the drafting process for the new Wiv.

New Wiv

A new Wiv is currently in development. In 2025 together with many partners and other experts, the AIVD contributed to the preparations for the draft legislative proposal. They have taken into account the experiences with the Temporary Act. The draft bill is currently being reviewed by the services for the feasibility of the proposed changes. The goal is for the bill to move into consultation in the first half of 2026.

> **For more information, go to: aivd.nl/nieuwewiv**

The new Wiv has a strong focus on a technologically neutral and more threat-oriented act, and with that a focus on practicability, being future-proof, and a more clear regime for data processing. Also true for the new Wiv: sufficient fitting safeguards. Proper review and oversight remain crucial. Furthermore a good cooperation with partners, other governments, companies, and knowledge institutions remain a priority.

Act improvement execution Security Screening Act

At the end of September 2025 the Dutch Senate adopted the proposal for improving the execution of the Security Screening Act (Wvo). This adjustment should ensure fewer administrative burdens surrounding security screenings. This act will gradually come into effect in 2026.

The most important change with regard to the current Wvo is the implementation of a site-specific certificate of no objection (*verklaring van geen bezwaar*, VGB). This VGB remains valid when someone transfers to a different position at the same location with the same security level – for example for a person who works in aviation and switches employers. There will also be a register of persons in a position involving confidentiality.

4.2

Review and oversight of the work of the AIVD

- **Strong review and oversight of the AIVD fits within the democratic legal order. In 2025 the AIVD, TIB, and CTIVD had constructive contact about the AIVD investigation into the threat posed to the national security by criminal networks.**
- **In anticipation of the new Wiv, new policy regulations are being developed for public-private cooperation. This type of cooperation is only becoming more important – especially in the cyberdomain.**
- **The internal oversight positions will be recorded in the revision of the Wiv 2017.**

Our work is strictly monitored. The safeguards of the Wiv 2017 and the amendments from the Temporary Act result in an effective oversight system on the working practice of the AIVD and MIVD.

Internally these checks are carried out by compliance and audit officials with the AIVD. Externally they are carried out by the parliament. Where necessary this can also be done confidentially. Additionally there are the Investigatory Powers Commission (*Toetsingscommissie inzet bevoegdheden*, TIB) and the Oversight Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheids-diensten*, CTIVD). The TIB is an independent commission which reviews in advance whether the use of the most intrusive special investigatory powers by the AIVD is lawful. The decision of the TIB is binding. The CTIVD checks and assesses during and after investigations whether the AIVD is adhering to the law. Citizens and organisations that believe their interests have been harmed can file a complaint with the Complaints Handling Department of the CTIVD.

Criminal undermining of national security

In March 2025 a critical letter by the CTVID and TIB to the Dutch House of Representatives about the AIVD's investigation into the threat posed against the national security by criminal networks gained some attention amongst the media and parliament. After this letter the AIVD provided a technical briefing to the Dutch House of Representatives regarding this investigation. Following the parliamentary debate, there have been multiple constructive conversations with the TIB and CTIVD on the investigation into the threat posed against the national security by criminal networks. Clear agreements have been made with the CTIVD.

Public-private cooperation and public policy regulations

The cooperation with private parties is of great importance to the AIVD and the MIVD, in particular when it comes to the cyberdomain. This public-private cooperation will only become more important in the future. By for example exchanging analyses of malware files and domain names, of which it is known that they stem from a state(-sponsored) actor, the services can get a better overview of the digital threats, and companies can better counter these.

In February 2025 the CTIVD sent a letter to the Dutch House of Representatives regarding this type of cooperation by the services. The CTIVD has expressed concerns about the lack of a legal basis and has called for drawing up a legal framework in order to increase the foreseeability.

On the basis of this there will be public policy regulations for public-private cooperation. These policy regulations will be published in early 2026. In the ongoing revision of the Wiv 2017 too the legal framework for this type of cooperation will be further outlined.

Internal oversight

In addition to external oversight the AIVD also has an internal oversight system. The Compliance department is one of the departments part of this (independent) internal oversight system. This department's main task is to ensure permanent and systemic compliance of the AIVD's activities with the framework of the relevant laws and regulations, internal (policy) rules, and ethical norms. This is done by carrying out periodical checks, providing advice on compliance matters, and by actively monitoring how the organisation is implementing CTIVD recommendations.

In 2025 the Compliance department developed a digital dashboard which provides the organisation with more clear insight into this implementation and allows it to aim for this. Over the past years the department has additionally focused on improving the internal oversight system. The internal oversight positions will be recorded in the new Wiv.

4.3

People and organisation

> **With over 2800 employees the AIVD dedicates itself to the protection of the national security and democratic legal order.**

> **With regard to operational management in 2025, business continuity and attractive employment practice were points of attention.**

Over 2800 AIVD employees dedicate themselves to the protection of the national security and democratic legal order every day. Always keeping in mind the public interest. Our people understand that security is not a given and work hard in their varying positions to keep the Netherlands as safe as possible.

Because of the threats described in this annual report, we work on increasing the resilience and robustness of our operational management. We strengthen our business continuity by realising alternate locations. If the organisation has a solid and future-proof base, we are better prepared for changes and risks. We additionally pay attention to sustainability in our operational management. This fits within our broader ambition to not only fulfil our role in the security chain, but also do this in a responsible, future-proof, and just way.

This year the growth of the organisation was once more a priority. In order to make this growth possible, we invested in the expansion of the number of workstations.

We look after our employees. In 2025 we established an onboarding programme with new digital learning programmes for new employees. In this way, they can quickly become familiar with the AIVD's work.

We also made sure there were opportunities for all employees to develop their knowledge and we organised social activities, for example in relation to the AIVD's 80th Anniversary.

In the past year we expressly paid attention to diversity and inclusivity. We appointed a coordinator for diversity, equality, and inclusion. Managers and HR employees were trained in 'inclusive recruitment'. Managers are offered trainings in Workplace Guidance relating to working with persons with a distance from the labour market. Different perspectives and backgrounds strengthen our organisation and help us to remain flexible and future-oriented in working towards a safe Netherlands.

Simone Smit has been Director General of the AIVD since 1 March 2026. Photo: AIVD

Key figures

87
notifications issued

93
official reports issued of which 30 together with the MIVD

96
written threat reports issued

363
intelligence reports issued

1,434
taps on the basis of Art 47(1) Wiv 2017

Table 3

Number of access requests to inspect information held by the AIVD, per type

Requests	Submitted	Completed	Inspection file	Still pending
Information concerning applicant	234	292	140	68
Information concerning deceased relative	48	58	23	4
Information concerning administrative matters	82	80	49	43
Information concerning a third party	-	6	-	1
Total	**364**	**436**	**212**	**116**

Table 4

Results of objections and appeals against decisions access requests

Status	Objection	Appeal	Second appeal
Completed	**34**	**3**	**0**
Dismissed	29	2	0
Well-founded (in part)	4	1	-
Inadmissible	1	-	-
Withdrawn	-	-	-

Table 5

Complaints about the AIVD to the Minister of the Interior and Kingdom Relations

Still under consideration as of 1 January 2025	19
Submitted in 2025	15
Dismissed	2
Partially upheld	3
Upheld	6
Handled informally to the satisfaction of the complainant	11
Not taken up for consideration	0
Withdrawn	0
Redirected	6
Still under consideration as of 31 December 2025	6

Table 6

Complaints about the AIVD to the CTIVD

Still under consideration as of 1 January 2025	7
Submitted in 2025	28
Dismissed	0
Partially upheld	3
Upheld	0
Handled informally to the satisfaction of the complainant	5
Not taken up for consideration	22
Withdrawn	0
Redirected	0
Still under consideration as of 31 December 2025	5

Colophon

Ministry of the Interior and Kingdom Relations
General Intelligence and Security Service
aivd.nl

PO Box 20010
2500 EA The Hague

April 2026