



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



2021

Annual Report AIVD

Foreword

This annual report describes the threats to the national security of the Netherlands in 2021. But before we can talk about this, we have to take a moment to reflect upon what has happened since the start of 2022. The Russian invasion in Ukraine has brought war into Europe on a scale that is unprecedented for many people. Other threats might pale in comparison.

At the same time, the war sometimes throws already existing threats into sharp relief. For years, the AIVD, MIVD, and intelligence and security services of other countries have warned against cyber-attacks, espionage, the steady development of weapons of mass destructions, and the intentions of state-sponsored actors with aggressive goals. All of these points now coalesced into an armed conflict in Ukraine which has shaken Europe to its foundation and has enormous humanitarian and economic consequences. It is a sad reality that underscores the necessity of the work of the AIVD and MIVD.

In the Netherlands many of 2021's threats were linked to increasing disagreement and a hardening of society. Last year, the AIVD gained better insight into 'accelerationists': a new generation of young, right-wing extremists that glorify terrorist violence in online groups with the goal of unleashing chaos and race war in the Netherlands. The AIVD also saw how some anti-government protest escalated to violent extremism. This was demonstrated by acts of sometimes public intimidation and people taking the law into their own hands, as well as (death) threats made against prominent politicians and others.

In 2021 Dutch citizens, companies, and authorities were continuously exposed to the threat of cyber-attacks by other countries. China and Russia are the forerunners in this. They have offensive cyber-programmes using large numbers of hackers to spy, steal knowledge, or prepare or carry out acts of sabotage.

Many threats in 2021 were a combination of national and international, digital and physical, and state-sponsored and non-state actors. This, carried by technology and digitalisation, raises new questions for society and for the AIVD. Such as the question whether the AIVD could play a role when crime has a harmful effect on the democratic legal order; in 2021 the AIVD started an exploratory investigation into this topic. Or the question when and how the AIVD could help combat the issue of large-scale ransomware cyber-attacks.

The current times require extensive cooperation with partners, on both a national and an international level. A good example of this is the close cooperation with the MIVD, including on the topic of Russia. It also requires the (technical) means to maintain a good intelligence position. Virtual agents, hacking operations, and cable interception played a large role in 2021.

A new, temporary law should enable the AIVD and MIVD to respond more effectively to cyber-threats, paired with adequate oversight and on a level with the dynamic nature of cyber-investigation. This law is currently in preparation. The Dutch people can rest assured that in this way the AIVD keeps guard over the national security of the Netherlands. This also involves publicly reporting what we investigated for that purpose. In particular when war casts a shadow over free countries, it is important that within the democratic legal order a secret service is, wherever possible, an open service.



Erik Akerboom
Director General
General Intelligence and Security Service

Contents

1	National threats	
	Right-wing extremism	4
	Right-wing terrorism	6
	Anti-government extremism	8
	Left-wing extremism	9
	Jihadist terrorism	10
	Radical Islam	12
2	International threats and political security interests	
	Political security interests	14
	Cyberthreats	15
	Espionage and covert influencing	18
	Economic security	20
	Jihadist terrorism in an international perspective	22
3	Eliminate and help prevent threats	
	Security screenings	23
	Counterproliferation	25
	Resilience	27
	The AIVD's role in the Dutch Safety and Security System	29
4	Organisation and facts and figures	
	Cooperation with the MIVD	31
	Oversight and the AIVD	30
	The AIVD's compliance with the Security and Intelligence Services Act ..	30
	Facts and figures	32

1 National threats

Right-wing extremism

- In 2021 right-wing extremist groups attracted more followers. Impetus came from, amongst other things, conspiracy thinking.
- Right-wing extremists try to make their world view seem normal to a larger audience.
- The normalisation of right-wing extremist views in society could threaten to undermine the democratic legal order.
- Right-wing extremists welcome chaos, exclude minorities, and justify violence, in the hopes of an actual, violent revolution in the Netherlands.

In 2021 the AIVD saw the number of right-wing extremist groups go up. Online — in particularly created by young people — and also offline. Increasingly often, groups manage to hang out together. In spite of their differences, national socialist, ethnonationalist, *alt-right*, and neo-Nazi groups share a world view in which the white population of the Netherlands (amongst other places) is structurally prejudiced against, even their very existence being under threat from ‘Umvolkung’ or even genocide.

Until recently, the main threat in this regard was immigration, in particular from Muslim countries. Around 2015, with the rise of ISIS and tens of thousands of Syrian refugees fleeing to the West, there was also the rise of many new, extremist, anti-Islam groups. They believed they had to take action to defend the Netherlands and its traditions against violent jihadists and against what they viewed as the government-sanctioned import of Islamic values intended to destroy their own race and culture.

Right-wing extremists still view immigration as a danger, in particular where it concerns Muslims. Currently, however, the threat mainly consists of conspiracies involving a powerful Jewish elite which is out to

oppress the people. In the view of right-wing extremists, Jews are able to do this through international networks and influential positions in many sectors, including the worlds of finance and culture.

The idea that Jewish people have an existing plan to dominate the world is an old one in right-wing extremism. Now it is the *alt-right* in particular breathing new life into this notion. The conspiracy theories of anti-government extremists regarding restrictive measures provide another impetus. Right-wing extremists actively try to recruit amongst anti-government extremists, playing into their dissatisfaction. Because of this, right-wing extremist concepts become mixed with the views of some anti-government extremists, and as such sometimes the lines between the different groups get blurred.

From there it is but a small step to explain the COVID-19 measures as a new way to push white Westerners into a corner. Or come up with new-fangled conspiracy theories. Think, for example, of the idea that Bill Gates, whether or not in consultation with a (Jewish) shadow elite, is using the COVID-19 vaccination programme in order to microchip and monitor, or even weaken and kill, part of the population.

Many right-wing extremists believe that within five to ten years, that cultural clash will lead to actual, violent combat in the Netherlands – a race war.

Right-wing extremists also feel threatened on a cultural level, namely by the emancipation of women, gay, or transgender persons, as well as by the 'woke' movement. These allegedly use the media, education, and the cultural sector to attack traditional values and role patterns. Many right-wing extremists believe that within five to ten years, that cultural clash will lead to actual, violent combat in the Netherlands – a race war. They believe that this war will create the space they need to found a fascist, white ethnostate.

Nevertheless, most right-wing extremist groups are careful not to be too confrontational in propagating their violent world view. Although they do not shrink from explicit hatred online, they seem to have learned from the past that public shows of aggression – as the skinheads of old used to display – are more likely to drive away rather than attract potential supporters.

Most groups seem to focus mostly on discrediting the current rule of law and dominating the cultural debate in order to increase their following and groom people for their (political) agenda.

An exception to this is formed by terrorist spin-offs and loners, for whom chaos, violence, and the collapse of society cannot come soon enough. For more information on this, go to '*right-wing terrorism*' on [page 6](#).

Many right-wing extremist groups make sure that they do not stand out too much from the rest of the population in their vocabulary or clothing, for example. No combat boots or tattoos here – the dress code for many right-wing extremist groups is suit and tie.

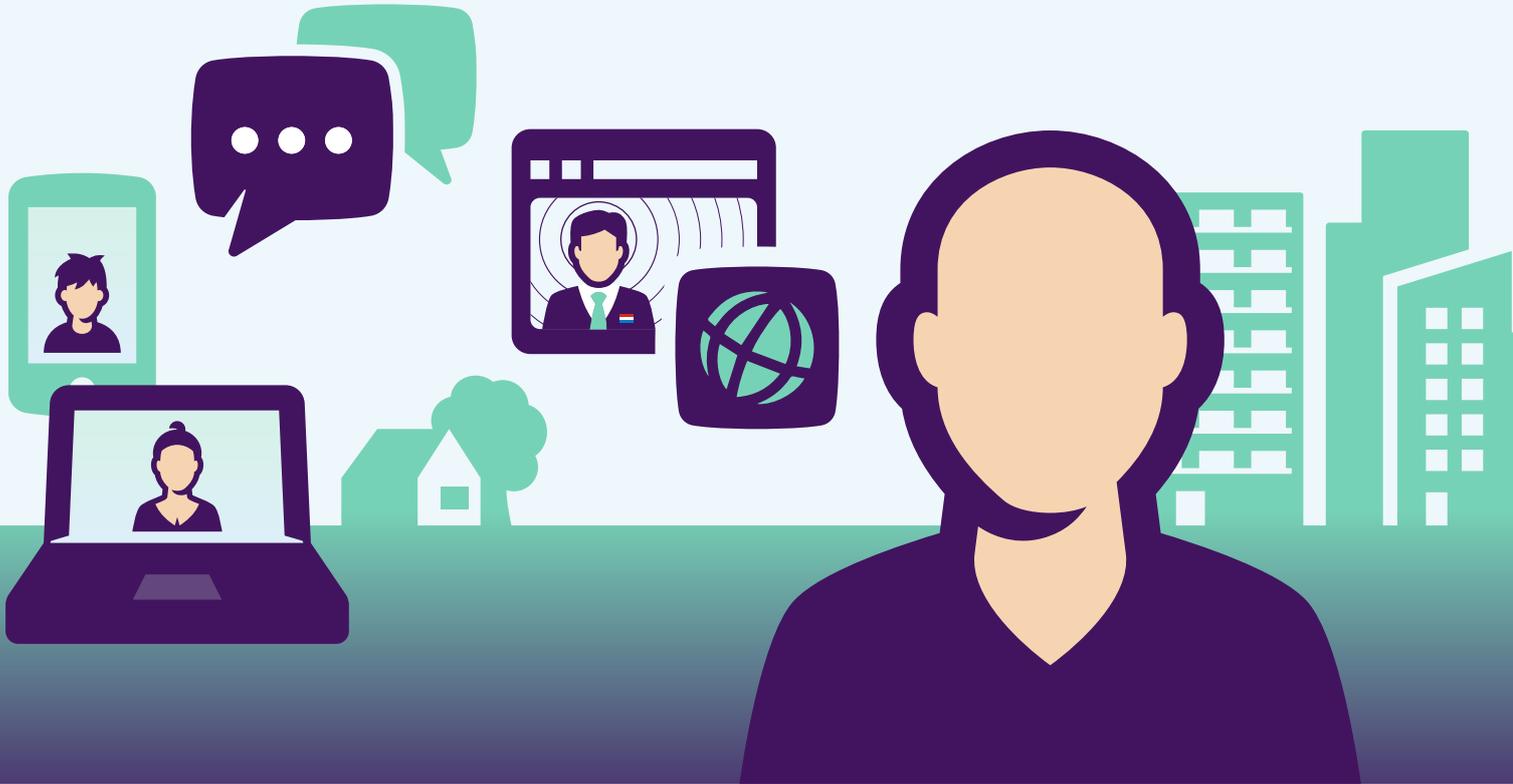
Furthermore, many extremists publicly distance themselves from violence. Even though they actually do see violence as a justified means to pursue their agenda. They consciously discuss this only in their own (private) circles.

By denying others their rights, they threaten to slowly undermine the rule of law. This lays the foundation for the chaos, hatred, and violence that they desire.

In their utterances, right-wing extremists are hitching a ride with already present dissatisfaction. With anti-government activists, as stated before. But also with, for example, people who cannot find affordable housing. (An excellent opening for extremists to bring up immigration.) The growth of the woke movement (a movement concerned with social inequality, in particular racism) is exaggerated, so that they can play into irritation about this. By far most of the right-wing extremist groups in the Netherlands do not pose a terrorist threat at the moment. They do, however, pose a danger to the democratic legal order. By denying others their rights, they threaten to slowly undermine the rule of law. This lays the foundation for the chaos, hatred, and violence that they desire. Such insidious undermining already occurs when more people accept their extremist ideas as normal and factual. In order to achieve this, some extremists make use of (pseudo) scientific jargon.

Right-wing extremists succeed in their aims when it becomes normal to see coexistence exclusively in terms of constant conflict, as us vs them. When (veiled) anti-Semitism and hatred against cultural minorities, women, and gay and transgender persons are no longer perceived as such. And when many people lose faith that the best way to serve everyone's interests is a shared rule of law.

Right-wing terrorism



- ‘Accelerationism’ – a violent current within right-wing extremism – posed a growing problem in 2021.
- In private online chat groups, accelerationists glorify terrorist violence. Young men, often the more vulnerable ones in particular, can get sucked into this and radicalise quickly.
- An attack by right-wing terrorist actors, individually or as a group, is conceivable.

Over the past year, the AIVD has gained a clearer view of a new generation of young, right-wing extremists who in private online groups glorify terrorist violence and fantasise about carrying out acts of violence. In total, these groups have several hundred adherents, and new groups continue to pop up. Like other right-wing extremists, they anticipate a future race war, which will give them the opportunity to establish a white ethnostate. Unlike most right-wing extremists, this movement wants to see the fighting break out as soon as possible. If necessary, they want to set this in motion by carrying out terrorist attacks and (through this) pit different population groups against each other. It is expected that only a small minority will want to use terrorist violence, but it is difficult to predict who will take this step.

Because of this desire to accelerate chaos and race war, this movement is called ‘accelerationism’. The term was coined by American national socialist James Mason, who is a source of inspiration to this movement.

Mason believes that right-wing extremists will never rise to power through politics – the government allegedly stands in their way. That is why incumbent governments and existing power structures have to be wiped out. Only violence and chaos can do that.

So far as is known, mainly (young) men participate in accelerationist groups. Most are between 13 and 30 years old. This is a generation which has grown up with the internet and that is where they look for contacts and information. It is their main meeting place. Out of sight of those around them, which means that radicalisation can stay hidden for a long time.

Accelerationist ideology catches on mainly with young people who are extra susceptible to radicalisation due to their background. Many struggle with psychopathological disorders which make linear, black-and-white thinking attractive to them. To a certain extent, this is true for all extremists.

Unlike most right-wing extremists, this movement wants to see the fighting break out as soon as possible. If necessary, they want to set this in motion by carrying out terrorist attacks and (through this) pit different population groups against each other.

Often times accelerationists come from broken homes and have no social safety net. Some were bullied and struggling at school. The right-wing extremist emphasis on white superiority, masculinity, and violence and is attractive compensation for some. Having a weapon means having power, which is why these individuals are interested in knives and guns, and in joining the armed forces. They moreover see this as preparation for what they believe is the inevitable race war.

Accelerationist groups have sophisticated ways of recruiting vulnerable young people. This is done through online gaming platforms and social media. Potential members are eventually asked to join private groups.

The groups do have inciters (usually the administrator of a chat group) and some form of internal hierarchy, but that does not mean there is a real leadership. The groups are more like groups of loners who inspire each other. Groups are flexible. They can pop up and disappear, and then reappear in another form in another place.

Once in such an online chat group, these young persons become part of a world in which enemy stereotypes, hatred, racism, and violence are shared constantly. And in which these fancied enemies are spoken of in a very disparaging fashion.

Members talk to each other about buying weapons, manufacturing bombs, and carrying out attacks. They share manifestos which attackers (from other countries) published as inspiration to others, as well as live streams of attacks. They also idolise attackers as saints. Some groups have notions of a kind of Valhalla which awaits white martyrs who have died for the cause.

There are some who actually help each other prepare and carry out an attack. To this end they share weapon manuals, military training videos, and guerrilla tactics.

Globally, accelerationism has led to terrorist violence resulting in deadly casualties. None of these occurred in the Netherlands, although in 2021 the AIVD sent out six official reports on accelerationists. This allowed the Public Prosecution Service and the National Police to act and arrest several persons.

Following an official report by the AIVD, in December 2021 two Dutch nationals were sentenced for incitement to a terrorist crime and for participation in the right-wing extremist and terrorist organisation 'The Base'.

Supporters of accelerationism pose a difficult threat to society. As these are largely vulnerable loners who constantly incite each other, the step to violence is quickly made and may be difficult for their surroundings to notice. This requires alertness and resolute action.

Following an official report by the AIVD, in December 2021 two Dutch nationals were sentenced for incitement to a terrorist crime.

In order to prevent further radicalisation, resulting in violence, the AIVD takes a tailored approach wherever possible. To that end, the AIVD utilises partners inside and outside of the criminal justice chain, in health care and social services. If AIVD intelligence can contribute in such a tailored approach to an intervention, this also contributes to national security.

Anti-government extremism

- In 2021 the AIVD observed how some of the anti-government protests, in particular against COVID-19 measures, radicalised.
- This has given rise to violent anti-government extremism. A terrorist attack from this direction is conceivable at this point.
- Moreover, a growing group of people is losing faith in the democratic legal order and turning their back on it.

The fact that part of the anti-government activists radicalised in the course of last year is illustrated by the worrying increase in threats directed at ministers, members of parliament, scientists, medical professionals, police officers, and journalists.

Counts by the police in The Hague, the Public Prosecution Service, and the complaints office *Persveilig* (Press Safety) show the number of reports has doubled (600 reports by politicians, 272 by journalists). Some of these threats will have been visible and intrusive to many Dutch nationals, for example the threats against Prime Minister Rutte and other members of government who symbolised the Dutch COVID-19 policy.

Anti-government extremists view and treat them (and any others they consider 'the elite') as hated enemies of the people. In often very coarsely worded e-mails, tweets, videos, and posts, they announce that they will use violence against them, wish death onto the recipient, or call upon others to harm them.

In some threats, there was the actual intention to carry out the threats, and preparations were made in order to do this. One anti-government extremist in 2021, for example, was arrested on suspicion of preparing an assassination attempt on (amongst others) Prime Minister Rutte. Another was sentenced for threatening to use terrorist violence. On his arrest he was found to be carrying a firearm. This year, between five and ten anti-government extremists were in detention, one of whom on the terrorist ward. They were sentenced on grounds of (serious) threat or incitement. In preceding years, this was rarely, if ever, seen.

Anti-government extremists view and treat them (and any others they consider 'the elite') as hated enemies of the people.

In its 2020 Annual Report, the AIVD warned of the development of a breeding ground for anti-government extremism. The protest against the government, in particular against the COVID-19 measures, was at that time mainly activist in nature, although there were already some extremist elements present. These elements have since taken flight.

Part of the reason that anti-government extremists have started to think and act more radically is because they are spurred on by inciters: popular conspiracy thinkers and critics of, amongst other things, the government's COVID-19 policy, who use their own media channels to reach tens of thousands of people.

In broadcasts, on websites, and in magazines they paint politicians and scientists as the new 'evil' ('Satanists' or 'paedophiles'), which uses its premeditated plans to harm the general population ('oppress' or 'decimate'). And they make it sound as though it would be understandable or even correct if people used violence in response to this. Be it spontaneous ('lynching'), or be it through organised 'tribunals'. They often choose their words in such a way, that they are not punishable by law.

On their media channels, these inciters profile themselves as experts. They are often eloquent and well-educated, which makes them seem credible. They talk not just about COVID-19, but about all kinds of topics in the news in order to keep repeating the same messages and increase their support base (so-called trigger events, for example the implementation of 5G). They share disinformation on a structural basis: stories which fit their world view, but which they often know are incorrect.

Their messages resonate more with those who feel uncertain about their income or their future and blame the government for this. And with those who believe the government is acting unfairly. Some of their supporters actually suffered as a result of government errors or witnessed others being affected by this.

The anger can also focus on one specific topic, such as asylum, climate, or nitrogen emissions policies or the fact that they are unable to find suitable housing. This can make them susceptible to the ideas of inciters. The same goes for groups who already believe that society is moving in the wrong direction. It is easy for anyone to join the movement, as the anti-government protest does not have a fixed, ideological programme.

The hardening amongst anti-government extremists seems to be exacerbated by (social) isolation. Many of these people spend a lot of time online, where one-sided information sources and algorithms lead them to ever more extreme messages.

They are also hearing fewer opposing opinions in the outside world. Discussions on, for example, the corona virus can sometimes drive a wedge between friends and family. This could lead people to not only lose faith in institutions, but also in those around them, causing to seek out mostly like-minded people.

This hardening is partially driven by the involvement of right-wing extremist groups. Right-wing extremists sometimes hijack anti-government protest in order to sell their own (violent) message and recruit people. On some topics, right-wing extremists and anti-government extremists are growing closer together. They also share their conspiracy thinking. Both can be opportunistic in their cooperation: together they have more mass.

All of these developments make anti-government extremism tougher and more dangerous. In the first place there is the danger that extreme ideas could lead to violence. A terrorist attack by an anti-government extremist is quite conceivable, therefore.



At the same time, there is a more insidious and serious danger: that mistrust, disinformation, and polarisation will harm democracy. That it becomes normal to have hostile thoughts about politicians, scientists, journalists, police officers, judges, and people with a different opinion that the Netherlands becomes even more divided and that faith in the democratic legal order crumbles away.

Dealing with such undemocratic goals or with the use of undemocratic means is a difficult but necessary task. It is important here that we differentiate between extremism and the legitimate right to protest. People who do not trust the government will simply view additional action taken by the authorities as a confirmation of their beliefs.

At the same time, there is a more insidious and serious danger: that mistrust, disinformation, and polarisation will harm democracy.

Meanwhile, some anti-government extremists and activists withdraw more and more into their own parallel society. Several extremists have set up their own 'police force' or so-called defence groups, who do not acknowledge the monopoly of violence held by the state. They challenge this monopoly, claiming that they have to protect protesters from police violence.

There are activists who only follow their own media, and home school their children and do not let them attend school. Hundreds of people have asked to be struck from the electoral register because they no longer have any faith in fair governance. They are slowly but surely turning away from the rest of society.

Left-wing extremism

- After a period of COVID-19 measures, left-wing activism received a new impulse, with a greater number of, and more visible demonstrations.
- Although those actions were sometimes intense for those involved, AIVD hardly witnessed any extremism amongst left-wing action groups in 2021.
- The violence shown by a group of anarchists during the housing protest in Rotterdam was, as yet, an exception.

In 2021 there was an increase in protests by anarchist groups. On top of that, there was also a growing number of participants. This seemed almost like a catch-up effort following 2020, a year in which most left-wing action groups had to cancel campaigns and demonstrations due to COVID-19.

With these new actions, the left-wing activist scene seems to have received a new impetus. In 2020, activist left-wing protests were mainly about current topics which are wider concerns within society:

lack of affordable housing, climate, racism. As such, groups were often able to join large protest marches or demonstrations in which other organisation were also participating.

Left-wing groups also protested against some of the government's COVID-19 measures (such as government aid for Schiphol, which they view as a way of maintaining the capitalist system). But in these cases, they had their own demonstrations, and stayed away from large, collective actions. They did not want to associate with right-wing extremists and conspiracy thinkers, who also came to these demonstrations.

Groups are also starting campaigns again without an end date, aimed against e.g. companies which supply materiel to the armed forces and border control. These protracted campaigns in particular become harsher the longer they go on and can result in threats, destruction of property, and intimidation.

Some actions by left-wing activists in 2021 were very visible in society. Examples are the eviction of a well-known Amsterdam squat in November; their presence at the housing protest in Rotterdam in October, where a small group of anarchists got into a fight with the police; and the long-lasting protest against slaughter company VION in Boxtel. In the campaign 'Close down Vion!' (*Sluit VION!*) various groups of activists and people living in the neighbourhood worked together. Each party had different concerns or grievances: climate, animal rights, a recent COVID-19 outbreak within the company.

Nevertheless, in 2021 AIVD hardly saw any extremist activities within the left-wing activist scene. This does not mean that there were no actions perceived as serious or disturbing by the organisations or companies they were aimed against. It just means that these actions did not threaten the democratic legal order.

Some actions by left-wing activists in 2021 were very visible in society.

The AIVD investigates left-wing extremism in order to be able to properly assess the risks to the organisations, companies, and person who are the target of such campaigns. The service also guards against radicalisation within left-wing activism, for example under the influence of ideologies that are contrary to our democratic legal order. Or through activities by extremist leaders from the past, who may not be active anymore but who – can still encourage the new generation of left-wing activists behind the scenes to carry out more radical actions. Sometimes a small spark is enough for activism to flare up into extremism.

For more information, go to: english.aivd.nl



Jihadist terrorism



- While the jihadist movement in the Netherlands seems to have stagnated, the threat remains considerable. The movement is characterised by its unpredictability.
- The AIVD assesses it eliminated a terrorist threat posed by a group in Eindhoven.
- A terrorist attack by jihadists in the Netherlands remains a real possibility.

The jihadist movement in the Netherlands is stagnating in some ways. The size of this group is still somewhere between 500 to 600 people in the Netherlands and about one hundred and fifty known Dutch citizens abroad. The movement has seen little to no growth since 2018.

The movement is fragmented into separate groups and individuals. Supporters share the convictions of global jihadist Salafism (jihadism for short) and consider themselves to be at war with the West. But they have differing opinions on what their contribution to this fight should be, in particular since travelling to Syria or Iraq is no longer a realistic option.

To some, this contribution means joining the armed struggle of jihadist militias in foreign conflict areas. But for most people, this fight can also be carried out without violence. For example by raising money, spreading propaganda (online), supporting detainees, or increasing their knowledge of the ideology.

Neither charismatic inciters nor a common goal, such as a new foreign conflict area, have been able to bridge this and other sometimes fundamental differences in interpretation.

Furthermore, support for international jihadist organisations seems to have fallen. Al-Qaeda and in particular ISIS wanted and still want to inspire jihadists in the West to carry out attacks. As such they profile themselves as strong 'brands' within the movement.

ISIS was successful at this for years. Most of the terrorist attacks in the West are planned and carried out by people (often inspired by others) who already live in these Western countries. Not directly by networks from abroad.

However, since the fall of the so-called caliphate in 2019, the ISIS brand seems to have lost its shine to jihadists worldwide. Within the Dutch movement, too, the virtually unconditional support for ISIS may not have disappeared entirely, but it has become less self-evident and connective than it was several years ago.

In spite of this, the threat of violence from the jihadist movement has not diminished. In 2021 we again saw that the movement does not need a common goal, mobilising issue, or immediate direction to pose a significant threat to national security and democratic legal order.

The arrest of a group of jihadists in Eindhoven shows this. The men were arrested at the end of September 2021 on suspicion of preparing a terrorist crime, membership of a terrorist organisation, and participating in training for terrorism. The men from Eindhoven sympathise with ISIS' jihadist ideology and (some of them) spoke about killing the prime minister and several party leaders. The AIVD assesses that the Eindhoven arrests resulted in the elimination of a terrorist threat. The case is still with the court.

In 2021 we again saw that the movement does not need a common goal, mobilising issue, or immediate direction to pose a significant threat to national security and democratic legal order.

At first sight, the Eindhoven group seems atypical for the jihadist scene in the Netherlands. The nine men are mostly well-educated and most of them had good jobs. As such, they are different from many other Dutch jihadist groups from the recent past, even if this is not uncommon within the global jihadist movement.

In other aspects, the Eindhoven network is typical for the jihadist movement in the Netherlands at this moment in time. Although there are no new issues that may provide an impetus to the movement as a whole, almost every year serious threats are identified and prevented, or attacks take place in the Netherlands.

The movement is characterised by this unpredictability. In the jihadist world view, participating in the fight is a duty. And within the movement in general, carrying out attacks is not only justified, but also encouraged. This makes it so that loners can quickly take the step to violence if they believe the situation calls for this. To those around them, this can be seemingly sudden.

What provokes such violence from small groups is therefore often difficult to see or predict. Most jihadist groups in the Netherlands are about brother- or sisterhood, studying, or playing video games together. Violence might not come up in conversations for a long time.

Terrorist violence carried out by small jihadist groups or lone perpetrators in the Netherlands is a realistic possibility right now. The service also investigates the threat posed by Dutch jihadists who travelled to conflict areas in Syria and Iraq and the threat posed by sentenced jihadists who are detained on the Terrorist Ward (Terroristenafdeling, TA) of the Custodial Institutions Agency.

For more information about *jihadism in an international perspective*, see [page 22](#), or go to english.aivd.nl

Radical Islam

- Second and third generation Wahhabi Salafi inciters in the Netherlands are gradually taking up influential positions.
- Inciters preach a message which can cause supporters to hate people with other (religious) beliefs and reject the rule of law.
- The first victims of these groups are other Muslims, for whom it is made impossible to fully participate in Dutch society.
- This message is also taught to young children through extracurricular education.
- In 2021 the AIVD received additional budget in order to investigate to what extent the work of inciters is enabled by undesirable foreign financing and interference.

In the past few years a new generation of leaders has come forward within the Wahhabi Salafism current in the Netherlands. Unlike their predecessors, they are rooted in the Netherlands. They speak the language, know the society, and are more pragmatic where it concerns practical matters such as voting or shaking hands with women.

This more pragmatic course, however, does not constitute a change in ideology and as such no change in the threat to the democratic system. It appears that the packaging of the message of this new generation of inciters stays within the boundaries of the law, which they know very well. They state, for example, that you should hate 'unbelief' rather than 'unbelievers'. The first is problematic, but not illegal. The second is hate-mongering, for which charges can be brought against you. The question moreover is whether the support base can tell the difference.

Characteristic for what the AIVD describes as Wahhabi Salafism is the absolute loyalty to their own religious community. And by extension turning away and sometimes even hating that which deviates from this. Often these are first of all Muslims with dissenting opinions, but also unbelievers, and Dutch society as a whole. In some cases Wahhabi Salafists do not acknowledge the legitimacy of e.g. the constitution, government, police, and other democratic institutions.

This is a message that inciters teach to children sometimes as young as four years old through extracurricular Islamic education. There is a lot of demand for such education within the Islamic community. Parents want their children to become acquainted with the Quran and Arab culture and learn Arabic. Extracurricular education provides this. This type of education is not problematic by definition. However, if this type of education is taught by inciters, their message may imbue children with a polarising ideology.

This ideology is taught to children first in a more moderate form and becomes stricter as they grow older. The education often consists of old-fashioned revision. The instructor is considered to be an absolute authority and critical questions are not tolerated.

The message propagated by these inciters is worrying because of what it teaches these children: black-and-white thinking, aversion to Western values, and exclusion of people with different beliefs. It can also cause

children to be excluded from participating in society. At worst, it can contribute to radicalisation.

Moreover, it can confuse children. What they learn in their extracurricular lessons and how they learn this is often contrary to what they learn during their weekdays in mainstream education, where critical thinking and asking questions are encouraged.

In the past year, the AIVD saw how some inciters were increasingly aiming their messages at the parents. This seems to be a consciously chosen strategy. By teaching children the Wahhabi Salafi interpretation of the Islam through extracurricular education and including their parents in this, the children learn more quickly. It also decreases chances of a moderate parent having a curbing influence on the ideological teachings.

The message propagated by these inciters is worrying because of what it teaches these children: black-and-white thinking, aversion to Western values, and exclusion of people with different beliefs.

Reaching parents is done in various ways. In some cases, parents have to take an ideological test before their children are admitted. Some inciters also provide parents with (ideological) homework and pedagogic advice. In some cases they even publish pedagogic books for parents, written from their interpretation of the correct creed.

The first generation of Muslims in the Netherlands held a more moderate interpretation of the faith from their country of origin. With this background, they could sometimes go against the inciters, also in educational matters. Parents from the second and third generation do not have this background and seem more vulnerable to a strict imposition of Islam. If an inciter has a lot of theological knowledge and charisma, parents are sometimes too insecure to go against this.

In the past year, the AIVD saw that inciters sometimes seize upon the opportunity to home-school children (keeping them from attending school). In some cases they call upon parents to do this.

In general, it is unclear what children are taught or not taught when they are being home-schooled. Nor what this means for their well-being and their opportunities in society. The biggest concern here is that the government has limited insight – and is therefore also not in a good position to observe signs of radicalisation – once children are exempted from compulsory education.

In the past, clear legislation sometimes helped prevent the spread of extremist messages through education. This impression is based on several cases of inciters who also teach religion in mainstream education. The government-provided framework for mainstream education has a dampening effect.

Because of this legislation, mainstream education is thus more resilient against the influence of these inciters.

In the past, the work of inciters was sometimes enabled by financing from the Middle East. This could help increase the influence of Wahhabi Salafi inciters in the Netherlands, which could undermine the democratic legal order in the Netherlands. This is not illegal, though it is undesired, as assessed by the Parliamentary Committee of Inquiry regarding undesirable influencing from unfree countries in 2020.

If an inciter has a lot of theological knowledge and charisma, parents are sometimes too insecure to go against this.

That is why in 2021 the AIVD received additional funding in order to investigate to what extent undesired foreign financing and interference pose a threat to the democratic legal order. The service wants to discover more about which foreign actors finance the spread of Wahhabi Salafism in the Netherlands, how they do it and what their intentions are.

For more information, go to: english.aivd.nl

International 2 threats and political security interests

Political security interests

- Conflicts in other countries can pose a threat to the national security of the Netherlands. In 2021 political intelligence obtained by the AIVD helped the central government make well-considered decisions.

The AIVD and MIVD investigate the political intentions, stability, and regional and global geopolitical developments of other countries. Because these things can, whether intentionally or not, harm Dutch interests.

Countries and power blocks are closely connected. Conflicts elsewhere can also pose a threat to Dutch national security, even if the Netherlands is not directly involved. These conflicts could for example affect or halt the supply of goods, raw materials, or energy.

For example, the Netherlands is partially dependent on Russian gas suppliers for its gas supply. In 2021 the long-since strained relationship with Russia led to fears of the gas and oil supply to Europe being adversely affected.

The Netherlands is a member of the EU and NATO and enjoys the benefits of this. However, this membership also comes with obligations. In order to establish an accurate picture of developments in various countries and the views of (in particular) their governments, the Netherlands has to stay well-informed. Good intelligence provides the Netherlands with a strong point of departure in international consultations and makes it possible to implement more measures to promote resilience and strengthening. the Netherlands' digital infrastructure.

Conflicts elsewhere can also pose a threat to Dutch national security, even if the Netherlands is not directly involved. These conflicts could for example affect or halt the supply of goods, raw materials, or energy.

The AIVD's political intelligence products contribute to making and adjusting government policy. These days conflicts are fought not only with weapons but also with information and intelligence. It is very important, therefore, that the Dutch government has independent access to intelligence and is able to carry out independent analysis. It is not the AIVD itself that decides which countries to investigate. The Ministers of Foreign Affairs, Justice and Security, Interior and Kingdom Relations, and Defence, as well as the Prime Minister, decide this in the so-called Integrated Order (*Geïntegreerde Aanwijzing, GA*).

Cyberthreats



- In 2021 the Dutch government, vital sectors, and companies were at greater risk of being hacked by countries with offensive cyber-programmes.
- The Netherlands is high on the list of countries whose digital infrastructure is misused in cyber-attacks.
- The current law restricts the Dutch intelligence services in speed and effectiveness.
- In 2022 a temporary arrangement should provide the services with the space required to respond effectively to cyberthreats.

In 2021 Dutch citizens, companies, and local authorities were continuously exposed to the threat of cyber-attacks by other countries. China and Russia are the forerunners in this, followed by North Korea and Iran. These countries have large, offensive cyber-programmes, which employ large numbers of hackers to spy, steal knowledge, or carry out or prepare acts of sabotage. Because of their numbers and the fact that they can act across borders and virtually unrestricted, these attackers currently have the advantage.

Every year state-sponsored actors discover more possibilities to gain access to their victims—the attack surface is expanding. The actors

not only look for vulnerabilities in the networks of targets, but also in the apps or other applications they use which are connected to the internet. Actors also break into the computer network of a supplier in order to gain access to their actual target (a so-called supply chain attack). Furthermore, in 2021 many people were working from home. As such, companies were more dependent on software that allows you to log in remotely.

In 2021 the AIVD identified several large-scale North Korean cyber-operations which were being carried out from servers rented or hacked in the Netherlands.

An important observation is that in 2021 hackers who worked for other countries exploited many unknown software vulnerabilities, also known as zero days because the developer has had zero days to patch the vulnerability. Any security implemented against unknown vulnerabilities is insufficient by definition. Hackers also make a lot of use of (sometimes newly discovered) known vulnerabilities.

That is why it is so important that organisations carry out security updates as soon as these become available.

If state-sponsored actors break into the network of a ministry, company, or knowledge institution, this is always a means to an end. In 2021 the goal of some countries was to obtain information that could help them combat COVID-19 in their own country. European (government) institutions which engage in the prevention of and fight against COVID-19 were therefore attractive targets.

Many cyber-attacks are carried out in order to spy, to influence processes in other countries, or to spread disinformation. In 2021 an actor who likely has ties to the Iranian intelligence service was able to gain access to several networks of an international organisation. It is unknown whether the Iranian actor was able to steal any data, and if so, how much.

The Netherlands is high on the list of countries whose infrastructure is misused in cyber-attacks. Many state-sponsored actors with an offensive cyber-programme prefer to carry out their attacks via Dutch connections and hired servers in the Netherlands. They do this because these servers are of a high quality and the internet connections are fast and reliable. In 2021 the AIVD identified several large-scale North Korean cyber-operations which were being carried out from servers rented or hacked in the Netherlands. One of these operations was directed against Western cyber-security investigators. The aim was likely to gain insight into how much these investigators knew of the cyber-capabilities and activities of North Korea.

State-sponsored actors also attempted to steal unique Dutch knowledge and innovations in 2021. One of the ways they did, or tried to do this, was by breaking into the networks of companies and knowledge institutions. They do this to gain economic advantages over other countries. It is only very rarely that the actual goal is to directly harm the Netherlands, but this could certainly be a side effect. For more information on this, go to *Espionage* on [page 18](#) and *Economic Security* on [page 20](#).

Sabotage is potentially the biggest digital threat to Dutch society. We are in an international, digital arms race and new techniques appear all the time which make it possible to cause considerable disruption in other countries—think of shutting down power plants, water supply, or financial systems. The chances of such means being used is very slim, as most countries would view such an attack as an act of war. But if it does happen, the consequences would be dramatic.

We are in an international, digital arms race and new techniques appear all the time which make it possible to cause considerable disruption in other countries— think of shutting down power plants, water supply, or financial systems.

Digital sabotage in one country could also inadvertently cause damage to another country. This happened for example following a cyber-attack against Ukraine in 2017. This attack shut down the Maersk terminal in the Port of Rotterdam.

The AIVD saw that some ransomware attacks in 2021 had such considerable consequences for society that they pose a threat to our national security, even if they are generally carried out by criminals rather than by state-sponsored actors. Last year, the American fuel supplier Colonial Pipeline Company was hit by a ransomware attack. Other victims included several Dutch knowledge institutions (the University of Amsterdam) and businesses (VDL).

Cooperation is crucial in countering cyberthreats. Two years ago the AIVD, MIVD, National Cyber Security Centre (NCSC), Police, and Public Prosecutor's office increased their cooperation in the field of cyber with the establishment of the cyber intel/info cell (CIIC). Since one year, the organisations have also shared a working location, where their representatives physically work together.

The advantage of this is that the cooperating parties can react to cyber-incidents and threats more quickly and in better coordination. Police and intelligence investigations can be coordinated and the government will be able to issue a single clear message about cyber-threats.

This resulted in an effective information exchange between the participating organisations. They helped create better understanding of the over two hundred digital security incidents with the government and vital sectors.

In the case of cyber-attacks, the AIVD can respond effectively if it can respond quickly. This is because opponents in the cyber-domain are also becoming faster, more advanced, and more difficult to identify.

In their attacks, state-sponsored actors often hop from infrastructure to infrastructure in order to conceal from where the attack is originating. The AIVD must ask permission to follow hackers into this new infrastructure. This can be time-consuming, as such a request must be thoroughly substantiated. The AIVD may lose sight of malicious hackers if it does not get permission in time to continue to follow the trail through new infrastructure to the source.

Sometimes services have to follow an actor across public and/or commercial infrastructure too. This infrastructure may also be used by (many) other users. For technical or operational reasons it is often impossible to carry out actions on these systems. In these cases it may be necessary to obtain bulk data from the party in question (the way in which intelligence services process large sets of data records is stipulated in the Intelligence and Security Services Act 2017).

In 2021 the current Intelligence and Security Services Act limited the services in speed and effectivity required in order to trace cyber-attacks and utilise its investigatory powers.

In order to fix this in the short term, a temporary regulation was drafted in 2021 which provides the services with the ability to act more quickly and respond more assertively to cyber-attacks. This goes hand in hand with binding, real-time oversight fitting the dynamic nature of the world of cyber. The temporary act was submitted for internet consultation in April 2022.

For more information go to: english.aivd.nl

Espionage and covert influencing

- In the past year, various countries attempted use espionage to obtain technical and scientific information in the Netherlands.
- There were also countries which covertly tried to drive a wedge between Western alliances such as EU and NATO.
- Countries with a large diaspora use espionage in order to keep an eye on their (former) citizens in the Netherlands.
- The necessity to expedite espionage legislation was emphasised once more in 2021.

The AIVD considers espionage to mean the covert and/or unlawful obtaining of information or objects by, or on the instructions of another country. Espionage affects everyone in the Netherlands. When espionage causes the loss of innovative knowledge and technology, this affects the Netherlands' revenue model. It threatens the economic security of the Netherlands, and as such our national security.

The threat of espionage was as great as ever in 2021. Various state-sponsored actors may have the intention of damaging the Netherlands' national security and are capable of doing this. To that end, they use several means such as espionage (digitally and through human sources), covert influencing, and disinformation. In addition to the superpowers of China and Russia, countries such as Iran and Turkey are also involved in (cyber-)espionage.

The goal of espionage is often to strengthen a country's own economy, armed forces, and diplomacy. Countries are thus acting out of self-interest. That this may damage the Netherlands is often an unintended side effect. The obtained information may also be used in order to keep an eye on dissidents and the diaspora in the Netherlands or even put pressure on them.

China in particular attempts to acquire technological and other scientific knowledge. Often through digital attacks, but also through students and scientists who are studying or conducting research at Dutch knowledge institutions. For example, China uses (student) grants in order to make the recipients indebted to them. This does not mean that every student and scientist has the intention or was purposefully sent to the Netherlands to carry out espionage activities.

The AIVD has established that in 2021 (too) China had an interest in communication, space, and maritime technology. Over the past years, China has utilised various methods in order to attempt to obtain such technologies. For example by digital espionage, by-passing export restrictions, academic cooperation, undesired knowledge transfer, and *insider threat*.

The goal of espionage is often to strengthen a country's own economy, armed forces, and diplomacy.

Advanced technological knowledge can also leak out through investments and company takeovers. This is not espionage, but could still damage the Dutch economy. This is further discussed on [page 20](#).

In addition to China, Russia also attempted to use (digital and physical) espionage in order to extricate technological knowledge. Yet, for Russia the focal point is collecting political information. Covertly gathering political information gives countries a head start in negotiations and aids them in determining their policy. Political intelligence is also important for covert influencing.

The AIVD is increasingly cooperating with other European intelligence and security services in order to prevent espionage. Cooperating services exchange information on identified intelligence officers and coordinate the expulsion of spies.

Preparations are currently being made for a bill (which was in the consultation phase until late April) which is to expand the criminality of espionage activities. If this bill is adopted, it will provide more opportunities to act should espionage be identified.

Covert political influencing

When countries attempt to influence the Dutch political and social system without being detected, the AIVD considers this to be covert influencing. A country may, for example, attempt to influence the political debate by intensifying the existing polarisation within society. Furthermore, countries covertly attempt to win political influence or drive a wedge between the members of Western alliances such as EU or NATO. Another goal of state-sponsored actors is to change foreign perception and decision-making processes in their favour or in favour of issues which are important to them. Attempts can be made both online and physically, through (social) media or through the political-administrative system.

The Netherlands has changed, in part due to the corona pandemic. In 2021, faith in the government and institutions decreased. Consequently, other countries have had considerably more opportunities to get involved in Dutch politics or Dutch society.

The AIVD did not observe a targeted strategy to covertly influence the outcome of the March 2021 election for the House of Representatives. The Dutch electoral system and coalition formation offer only limited opportunities to do so.

Nevertheless the AIVD is aware that vigilance is called for. The Netherlands has changed, in part due to the corona pandemic. In 2021, faith in the government and institutions decreased. Consequently, other countries have had considerably more opportunities to get involved in Dutch politics or Dutch society.

Disinformation

Covert influencing can happen online through the spreading of disinformation. Disinformation posed a limited threat to the Netherlands in 2021. There are few examples of Dutch-language pieces of disinformation spread by Russia. In a number of larger European countries, there were considerable influencing activities from Russia.

In 2021 a conversation took place between the Standing Committee on Foreign Affairs of the House of Representatives and a Russian prankster pretending to be a staff member of Aleksey Navalny. This conversation was posted to YouTube. Previous activities of this prankster saw the involvement of various Russian government institutions. The AIVD deems it possible that these same government institutions were also involved in this conversation with the members of parliament.

Disinformation is not the same thing as public diplomacy or propaganda. Expressing and spreading propaganda is not done covertly. Countries publicly propagate their norms, values, or ideology. These are not always in line with Western ideas. The AIVD has the task of exposing and countering covert activities.

Diaspora

In particular countries with a large diaspora in the Netherlands carry out intelligence activities here in order to obtain insight into and grip on their diaspora. These activities may be aimed at improving the relationship with the diaspora so that they can promote the country's interests abroad. People can be rewarded for their cooperation, for example by receiving help in administrative matters or invitations to celebrations at the embassy. Intelligence activities can also focus on identifying (supposed) opponents of the regime in order to stifle any critical voices regarding the regime. They gather intelligence on people who participate in demonstrations, for example.

Information on alleged opponents of a regime may be used by that regime to intimidate them. They may be harassed or even prosecuted as soon as they travel to their country of origin. Some countries do not shy away from using violence.

If an activist does not alter their opinion, the country in question may exert pressure by, for example, making it clear that the activist's family members may also be affected by this.

Activists are sometimes already addressed while they are in the Netherlands. If an activist does not alter their opinion, the country in question may exert pressure by, for example, making it clear that the activist's family members may also be affected by this.

For more information, go to: english.aivd.nl

Economic security



- In 2021 China the greatest threat to the economic security of the Netherlands came from China.
- AIVD investigation helped prevent knowledge theft and strategic dependencies.

The AIVD is investigating actions of other countries which may pose a risk to the Dutch economy. In 2021 the government, as well as various companies and knowledge institutions turned more frequently to the service for advice. It seems that within society awareness regarding countries which are participating in an economic or technological race and which may sometimes attempt to steal knowledge and technology from the Netherlands for this purpose. As well as the fact that they could be behind company takeovers, mergers, and investments which might be detrimental to the Netherlands.

In 2021, the greatest threat to the economic security of the Netherlands came from China. China is trying to obtain high-grade knowledge and technology in the Netherlands, especially semiconductor technology. There is a lack of high-grade chips in China, needed to boost its own technology sector. This fits with the country’s public multiyear agenda. Countries such as Russia also try to steal Dutch knowledge and technology.

The AIVD investigation primarily focusses on identifying and preventing technology and knowledge theft from Dutch companies and knowledge institutions. In 2021, for example, the service was closely involved in the establishment of the knowledge security desk of the Ministry of Education, Culture, and Science. The Netherlands is an attractive target for countries which want to steal knowledge, because it is one of the most developed countries in the world when it comes to economy, science, and technology.

By investigating this, the AIVD creates insight into which sectors attract this kind of unwanted attention from countries with active espionage programmes. This helps to prevent other countries from playing too large of a role in the Dutch telecommunications infrastructure or in the Port of Rotterdam, which would make the Netherlands vulnerable to espionage, sabotage, or influencing. Our partial dependency on Russian gas also puts Europe and the Netherlands in a strategically vulnerable position.

Lastly, investigation into economic security contributes to what we call responsible end use: that Dutch technology and knowledge is not used for matters which the Netherlands does not support. The Netherlands does not want technology to be misused for military purposes or repression.

This helps to prevent other countries from playing too large of a role in the Dutch telecommunications infrastructure or in the Port of Rotterdam, which would make the Netherlands vulnerable to espionage, sabotage, or influencing.

The Netherlands' economic security may come to be at risk due to illegal acts such as espionage (either digitally or through insiders, such as foreign employees), but also through legitimate acts such as corporate takeovers and export, resulting in the loss of crucial knowledge.

In the coming year, the AIVD will increase its economic security investigations. This will provide better insight into threats and the manifestation of these threats, as well as provide the government and commercial businesses with more perspective for action. Undesirable activities by other countries can thus be recognised and prevented.

For more information go to: english.aivd.nl

Jihadist terrorism in an international perspective

- The Taliban's assumption of power in Afghanistan has, as yet, not had a direct impact on the jihadist terrorist threat against the Netherlands.
- Sub-Saharan Africa is becoming increasingly important to both ISIS and al-Qaeda. Both are searching for (symbolic) successes and a safe haven there.
- ISIS and al-Qaeda still have the desire to carry out attacks in the West. At this time they are mainly trying to inspire local networks for such actions.

Following the withdrawal of coalition forces from Afghanistan in August 2021, the Taliban assumed power there. Radical Muslims hail this as a historic victory over the United States and the West. It remains to be seen what effect this will have on global jihadism.

The Taliban itself seems mainly focussed on Afghanistan itself. The movement currently does not pose a direct threat to the Netherlands or other Western countries. An important question in this regard is how much room the Taliban will allow ISIS and al-Qaeda.

ISKP—the local ISIS branch in the area—and the Taliban are locked in a battle to the death. Al-Qaeda and the Taliban, on the other hand, have close (sometimes even familial) connections and share a long history – Osama bin Laden planned the 11 September 2001 attacks from Afghanistan.

That is why al-Qaeda may seek out a space in Afghanistan to establish training camps, rebuild an international network, and arm its fighters. In February 2020, the Taliban agreed with the US that it would not allow international terrorists to use Afghanistan as a base of operations. Whether the Taliban can and will honour this promise remains to be seen.

Al-Qaeda may seek out a space in Afghanistan to establish training camps, rebuild an international network, and arm its fighters.

Meanwhile, Sub-Saharan Africa is becoming increasingly important to both ISIS and al-Qaeda, especially since the fall of the ISIS caliphate in 2019. Since then, ISIS has been undergoing a transformation—from an organisation that was mainly focussed on a core territory in Iraq and Syria to an organisation which is increasingly having to lean on achievements of its so-called global provinces for its international standing.

Local jihadist groups in Africa and Asia are becoming ever more important for this. As 'ISIS Provinces' or affiliates of al-Qaeda, they have sworn allegiance to the leadership of these organisations. Although for such groups the local agenda is often dominant, in the past years a number of them have also carried out attacks against Western targets outside of their own region.

If such local, loyal ISIS and al-Qaeda affiliates are seeing local successes, this is symbolic for the public image of the jihadist struggle worldwide. They may also provide the parent organisations with a safe haven from which to plan attacks against the West.

Both al-Qaeda and ISIS have the ambition to carry out attacks in or against the West. However, at the moment it seems doubtful whether they have the ability to send operatives themselves. They therefore have to depend on local networks and individuals to inspire with their ideology to carry out attacks. ISIS is more successful at this than al-Qaeda.

For more information about the jihadist threat in the Netherlands, see [page 10](#) or go to: english.aivd.nl

Eliminate and help 3 prevent threats

Security screenings

- In 2021, the Security Screening Unit (Unit Veiligheidsonderzoeken, UVO) carried out 51,354 screenings into persons under consideration for or in positions involving confidentiality.
- In 2021 the AIVD and MIVD made further steps in having only one type of security screening with one type of certificate of no objection (Verklaring van Geen Bezwaar, VGB) for all its clients.
- One milestone in this process was the implementation of a system which helps safeguard the civil aviation sector against risks of *insider threat*.

The UVO carries out security screenings into persons under consideration for, or in positions involving confidentiality—people who in their work have access to secrets or are in a position in which they could harm national security. Examples are people working for the central government, in aviation, or companies responsible for vital processes.

The Security Screening Unit is a joint MIVD and AIVD unit. In 2021, the unit carried out 51,354 security screenings to decide whether or not to issue a VGB. This is an increase of about 3,500 when compared to 2020. In 2020 the Unit Security Screenings received fewer applications for the aviation sector, as this was suffering from the impact of the corona pandemic. Of the total number of screenings in 2021, 26,438 were carried out by the UVO itself (15,479 by the MIVD and 10,959 by the AIVD) and 24,919 were carried out by the National Police and the Royal Netherlands Marechaussee (KMar) under AIVD mandate.

The UVO strives for a singular uniform process, and, in the long term, one type of VGB for all clients. In order to achieve this, the UVO improved

and unified its working processes as much as possible in the past year. The AIVD and MIVD are now more and more able to carry out their security screenings in the same manner. The UVO also strengthened its customer contact centre in order to improve its accessibility and complaint handling.

The AIVD and MIVD are now more and more able to carry out their security screenings in the same manner.

2021 also saw the further realisation of the Modernising Security Screenings (*Modernisering Veiligheidsonderzoeken, MVO*) programme. This ensures a speedier application process, thanks to automated elements and adjusted processes. One particular milestone was the moment the Automatic Alert System went live. The Automatic Alert System is a system which informs the UVO if there are adjustments in the Criminal Records System of someone working in civil aviation, or if there is new intelligence on them. Where necessary, the UVO will then carry out a new security screening. This will help keep civil aviation safe. In time, the Automatic Alert System will also be applied to other security screenings.

In 2021 the UVO, together with other departments of the services, the Ministry of the Interior and Kingdom Relations, and the Ministry of Defence drafted a Bill for the amendment of the Security Screening Act (*Wet Veiligheidsonderzoeken, Wvo*). In early 2022, the proposal was submitted for internet consultation and an implementation test carried out. The submission to the House of Representatives is expected in the second half of 2022.

Furthermore, in 2021 the new policy regulation for security screenings was implemented. This went without a hitch. This policy regulation allows for more customised screenings for persons under consideration for or in positions involving confidentiality who stayed abroad for a prolonged period of time.

There are three categories of security screenings, depending on the nature of the position involving confidentiality: the A, B or C screening. The greater the damage a person under consideration for or in a position involving confidentiality could cause to national security, the more thorough the screening. The A screening is the most thorough

and is only carried out for the most vulnerable of positions involving confidentiality. When a screening results in a positive decision, the applicant receives a so-called certificate of no objection ('Verklaring van Geen Bezwaar', VGB).

In 2021, the UVO completed an average of 94 per cent of its screenings within the legal term of eight weeks. This is well over the 90 per cent norm.

For more information, go to: english.aivd.nl

Table 1: completed security screenings by AIVD and delegated partners

Screenings	Positive	Negative	Total
Level A, by UVO	4,561	30	4,591
Level B, by UVO	15,011	73	15,084
Level B, taken over by UVO from Kmar and National Police	2,070	261	2,331
Level C, by UVO	4,408	24	4,432
Total screenings by UVO	26,050	388	26,438
Level B, taken over by Kmar and National Police	24,916	0*	24,916
Total screenings	50,966	388	51,354

* The National Police and Kmar do not issue negative decisions themselves. In case of doubt in a Level B security screening, the investigation is handed over to the UVO. Negative decisions are added to the number of negative decisions made by the AIVD. This explains why the figure here is 0.

Table 2: results of objections and appeals against security screening decisions

	Objections received	Ruling on Objection	Ruling on Appeal	Ruling on Second Appeal
Dismissed	-	15	6	4
Upheld	-	10	1	1
Inadmissible	-	6	0	0
Withdrawn	-	0	1	1
Total	27	31	8	6

Counterproliferation



- A number of countries is working on new types of weapons of mass destruction which do not fall within existing arms treaties.
- For some of the weapons, the threshold to use them may be lower.

The joint Unit Counterproliferation (UCP) of the AIVD and the MIVD investigates the biological, chemical, nuclear, and ballistic weapons programmes of countries of concern, and how these countries obtain the knowledge and supplies they need in order to manufacture such weapons of mass destruction.

This is a field of investigation which has been in a state of flux for a while now. Many countries are working on the further development of existing weapons, as well as new types of weapons of mass destructions which do not fall within the existing definitions and arms treaties.

In the past year Iran tested long distance missiles with a greater range, which also pose a threat to European countries. The AIVD is also seeing the development of new types of weapons. For example for use in space, or cyber-weapons which could potentially do just as much damage as a weapon of mass destruction. This is making the world less stable, which threatens the national security of the Netherlands.

The AIVD is also seeing the development of new types of weapons. For example for use in space, or cyber-weapons which could potentially do just as much damage as a weapon of mass destruction.

Some countries develop arms in such a way that they circumvent international arms treaties. The risk of this is threefold. If a weapon is not covered by a treaty, this means that countries have not yet decided not to use such a weapon in conflicts. It is also still allowed to export the materials which are required for the manufacture of these weapons. The Netherlands, as well as other countries, cannot simply investigate weapons which are not yet classified as such.

A particular danger of some new types of weapons is that they can be used on a smaller scale. This may lower their usage threshold. The chances of chemical weapons or a strategic nuclear weapon being used on a smaller scale are minor, and in the past few decades they were

rarely used at all (with the exception of chemical weapons being used in the conflict in Syria). Employing such weapons would be considered such an escalation of a conflict, that the response to it would be extremely severe. But Novichok—in effect a small-scale chemical weapon—has already been used to carry out attacks against Russian dissidents. The fear is that countries of concern will also use other, new, tactical weapons of mass destruction more quickly in conflicts.

This fear increased by the fact that some of these countries also seem to apply the philosophy that it is not enough to simply have weapons, but that you also have to show the rest of the world you are willing to use them. They believe such an escalation actually functions as de-escalation: the purpose is to deter attacks.

The UCP's work is focussed on preventing the acquisition of supplies and knowledge to construct weapons of mass destruction. One way to do this is by informing companies and (knowledge) institutions of the risk that they may unwittingly be supplying goods or knowledge which may be used for weapons programmes. Another way is to provide the central government with intelligence. On the basis of this intelligence, the government can draw up policy, halt export, or impose sanctions on persons and organisations.

For more information go to: english.aivd.nl

Resilience



- The AIVD assists the government, vital sectors, and the Dutch economy to be more resilient against threats.
- In cyber, true security also means resilience.
- In the increased competition between countries it is more and more important that the Netherlands safeguards its state secrets with its own cryptography.

The AIVD does more than investigate threats against the Netherlands. One of the service’s duties is to use its access to intelligence to assist the government, vital sectors, and the Dutch economy to become more resilient.

The AIVD tries to make them aware of the risk that they could become the target of e.g. espionage, sabotage, and knowledge theft by other countries, and provides them with advice on adequate security measures. If they do fall victim to an attack, the service offers perspective and advice.

The demand for such advice has been growing in the past years, and no less so in 2021. In part this is because various countries are striving

to gain an (economic) advantage over other countries and are willing to acquire unique (Dutch) knowledge and innovations. For more information on this, go to *Economic security* on [page 20](#).

They are able to do this also because technology makes it easier. State-sponsored actors who want to engage in espionage, sabotage, or knowledge theft more often do this digitally (too) nowadays, which means that the threat of digital attacks to the Netherlands is increasing. For more information on this, go to *Cyber* on [page 15](#).

One new instrument to help the central government and vital sectors cope with this is cyber-advice. The AIVD has been issuing this since 2021. Cyber-advice provides organisations with concrete, technical advice on how they can deal with current cyber-campaigns by state-sponsored actors. In the past year this advice was mostly about safely working from home, compromised e-mail boxes, and the use of social media by state-sponsored actors.

Different from most of the AIVD’s intelligence products, this cyber-advice is unclassified. That means it does not contain secret information

and can therefore be made available to a wider public. The first experiences with this are positive: it provides ministries and other organisations perspective for action and helps improve their resilience.

Recently, the AIVD has been invested in showing organisations how to operate on the principle of assume breach: (on top of security measures) make realistic plans for the steps you can take if you do get hacked.

Organisations are stronger if they can not only fend off digital attacks, but also know how to act if a hacker does gain access to their network. And if, on top of that, they have the knowledge and the backups to resume normal operations, they are even stronger. The service sits down with organisations and helps them determine which vital assets need protection.

Such a realistic approach does justice to the omnipresence of cyber-attacks and the capabilities that come countries have at this point. It also fits the current reality of many organisations and institutions, for whom it is simply unaffordable or not user-friendly to implement the highest possible (digital) security for not only its primary company processes, but the entirety of its business.

Recently, the AIVD has been invested in showing organisations how to operate on the principle of assume breach: (on top of security measures) make realistic plans for the steps you can take if you do get hacked.

Good cooperation within the central government is also beneficial for digital security. This is why in 2021, the AIVD has intensified its cooperation with the National Cyber Security Centre (*Nationaal Cyber Security Centrum*, NCSC). Advice and information products are attuned to one another. In the past year, the AIVD, together with the NCSC and other partners, spoke to all ministries on how to strengthen their digital resilience. When it comes to digital resilience, the AIVD always closely cooperates with the MIVD and the NCTV. The service further cooperates closely with international partners.

With the increased competition between countries and the growing cyber-threat, it is ever more important that the Netherlands retains its digital sovereignty and that it can continue to safeguard its state secrets. This requires high-grade cryptography products, which are made in the Netherlands (and occasionally in a European framework). The AIVD's National Communications Security Agency (*Nationaal Bureau Verbindingsbeveiliging*, NBV) plays an important role in this. The NBV has always worked on protecting the confidentiality of Dutch state secrets as well as ensuring secure communications for e.g. the army and diplomatic traffic.

The AIVD looks to the future in order to ensure that the government, vital sectors, and high-grade corporate sectors become more resilient against future (digital) threats.

In 2021, the AIVD also worked on the execution of the National Cryptostrategy (drawn up in 2019). This strategy describes how the central government can obtain reliable means of security for highly sensitive information. The Ministry of the Interior and Kingdom Relations takes on a coordinating role and makes an inventory of the needs of the ministries, after which the service presents these demands to the relevant companies. The AIVD prescribes requirements and tests the constructed software and hardware. The service moreover plays a part in ensuring that universities have departments where the cryptologists of the future are trained.

The AIVD looks to the future in order to ensure that the government, vital sectors, and high-grade corporate sectors become more resilient against future (digital) threats. That is why in 2021 the AIVD published a brochure not only on how to defend computer networks, but also on the future threat posed by quantum computers, which will be able to break some kinds of cryptography. This helps organisations take better measures. The service also studies the security risks of e.g. Artificial Intelligence (AI) and the Internet of Things.

The NBV, together with the Ministry of Foreign Affairs and the Ministry of Defence, negotiates information security treaties with other countries. These provide agreements on the security and exchange of confidential and classified information. In 2021, the treaty with Spain was approved by the cabinet.

For more information go to: english.aivd.nl

The AIVD's role in the Dutch Safety and Security System

- In 2021 it was largely anti-government extremists who threatened public figures and dignitaries.
- The AIVD contributes to this security system with intelligence and analyses.

The AIVD's intelligence contributes to the system that safeguards and provides protection for politicians, members of government, and diplomatic objects. On the basis of risk analyses, threat analyses, and threat assessments by the service(s), the NCTV may decide whether politicians and members of parliament need (additional) security in order to be able to continue their work.

In the past year the AIVD witnessed many threats made against politicians and members of government, in particularly by anti-

government extremists. The willingness to carry out the threats also seems to have increased. This can be seen in the arrests and convictions. For more information about anti-government extremism, see [page 8](#).

In the past year, the AIVD wrote threat assessments for diplomats and diplomatic objects. It did the same for officials and members of the judiciary who are involved in the Dutch interstate complaint regarding the Russian involvement in the taking down of flight MH17 in 2014. The AIVD also drew up threat assessments for events: National Remembrance Day, Veterans' Day, the state opening of parliament, and the Eurovision Song Contest.

For more information, go to: english.aivd.nl

4 Organisation and facts and figures

Oversight and the AIVD

- There are two committees which check and review the AIVD's work: 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 Veiligheidsdiensten*, CTIVD).

Because the AIVD's investigations are secret, proper oversight is crucial. There are two committees which check and review the AIVD's work: the Investigatory Powers Commission (TIB) and the Oversight Committee for the Intelligence and Security Services (CTIVD).

The TIB reviews whether the service is legally permitted to use its most intrusive special investigatory powers. Think of phone taps, hacking technical equipment, and intercepting cable and satellite communications. The TIB does this prior to the exercise of the power. If the TIB does not deem the use of a means to be lawful, it is not used.

In 2021, the TIB deemed 3.30 per cent of requests for the exercise of these powers to be unlawful.

The TIB reviews whether the service is legally permitted to use its most intrusive special investigatory powers. Think of phone taps, hacking technical equipment, and intercepting cable and satellite communications.

The CTIVD checks whether the law is executed fully in accordance with its stipulations. The CTIVD has direct access to AIVD systems. Also, AIVD employees are obligated to provide the CTIVD with all the information requested. The CTIVD carries out investigations and also looks into any complaints they may receive regarding the AIVD's actions. The CTIVD reports to the House of Representatives and the Upper House.

In 2021 the CTIVD published two reports. One was on the exercise of special investigatory powers in the support of the proper performance of duties by the AIVD and the MIVD. The other report was on the provision of data to foreign services with a high-risk profile. The Ministers of the Interior and Kingdom Relations as well as Defence adopted all of the recommendations made in the report. The AIVD improved its way of working on the instructions of the CTIVD.

The AIVD's compliance with the Security and Intelligence Services Act – our licence to operate

- The AIVD worked on the further implementation of the Intelligence and Security Services Act 2017 (*Wiv*).
- In 2021 we also started on preparations for the amendment of this law.

In 2021, the AIVD worked hard on the continued implementation of the Security Services Act 2017 (*Wiv*). This law describes the service's investigatory powers, and under which circumstances the service may use them.

In 2021, the service further standardised its policies and improved its data management system. This was done together with the MIVD.

The AIVD and MIVD also worked out a system for incident management and reporting. The CTIVD is involved in an early stage.

The services have also worked on other ways to ensure proper data processing, such as automated data analysis and a relevancy system in which data is determined to be relevant or not in light of data reduction requirements. .

Since 15 July a few changes have been made to the Intelligence and Security Services Act. The changes provide for a more directed use of special investigatory powers as well as a broadening of the duty to report to the CTIVD in sharing evaluated data.

In 2021, the Evaluation Committee Wiv 2017 (*Evaluatiecommissie Wiv 2017*, ECW), led by Renée Bos-Jones, and the Netherlands Court of Audit (Algemene Rekenkamer, ARK) published reports on the implementation of the Wiv. The ECW published an early evaluation of the Wiv 2017. This had been stipulated in the coalition agreement of the Rutte III government.

The most significant conclusion was that in general, the law works as intended, but that it will have to be amended as it falls short in a number of areas. For example where review and oversight and the services' handling of bulk data sets are concerned. The ECW report therefore makes a number of recommendations for an amendment to the Wiv 2017. The ARK's report described the effect the Wiv 2017 had on the AIVD's and MIVD's operational power. The conclusion is that this power and effectiveness have come under pressure. The government has embraced ARK's and ECW's recommendations.

Following these reports, a process has been set in motion to arrive at a new, future-proof law. This will take several years. The outlines of the amendment will be submitted to the House of Representatives and the Senate in a key points memorandum. The outcome of the parliamentary exchange of ideas that follows will be included in the bill to amend the Wiv 2017. In the meantime it was decided to accelerate the amendment of a number of problem areas through an emergency act. This is required for the growing and urgent cyber-threat against the Netherlands.

The temporary act is supposed to give the services more room to manoeuvre in the short term in order to act effectively against countries with an offensive cyber-programme. A robust system of checks and oversight has been arranged which matches the dynamic nature of cyber-investigation.

For more information, go to: english.aivd.nl

Cooperation with the MIVD

- By cooperating, the AIVD helps to make the Netherlands a safer place.
- In particular the cooperation with the MIVD is close: the services have joint teams, they join forces in issuing important messages together, and are working on creating uniform processes between the two organisations.

Cooperation is at the heart of the service's work. On the basis of its access to intelligence the AIVD enables its partners to act against the threats to the Netherlands. Especially with partners in e.g. the criminal justice chain, the government, and corporate life, the service makes the Netherlands a safer place.

In particular the cooperation with the Military Intelligence and Security Service (MIVD) is intensive and solid. Although the services each have their own legal tasks, they both take action against the threats of our day, and espionage can go hand in hand with economic threat or (surreptitious) military threat. This makes cooperation obvious and necessary.

The services have joint units for counterproliferation (for more information on this, go to [page 25](#)), security screenings (for more information on this, go to [page 23](#)) and cyber-operations. The services also cooperate closely in identifying and countering threats from China and Russia.

The services issue public messages together in order to make society aware of current threats. In early 2021, the AIVD and MIVD, together with the NCTV, published the Threat Picture State-Sponsored Actors, which shows how other countries pose a threat to the Netherlands' security interests. Later in the year the Directors of the AIVD and MIVD enjoined the public to pay attention to digital espionage by Russia and China.

Although the services each have their own legal tasks, they both take action against the threats of our day, and espionage can go hand in hand with economic threat or (surreptitious) military threat.

In the past year, the cooperation with the MIVD also intensified where compliance is concerned - the AIVD and MIVD fall under the same law and the same oversight committee. More processes have been made uniform and the services are working on making data accessible in the same way for both services so that teams can work together more efficiently. In the coming years, the services will further intensify their cooperation.

Facts and figures

Table 3: intelligence reports issued in 2021

Total	555
Of which intelligence reports	410

Table 4: official reports issued in 2021

2021	57
------	----

For more information go to: english.aivd.nl

Table 5: number of written threat-related reports in 2021

2021	103
------	-----

Table 6: official reports issued in 2021

2021	34
------	----



Table 7: requests to inspect information held by the AIVD, by nature or subject

Requests	Submitted	Reviewed	Inspection File Sent	Still Under Consideration 31-12-2021
Information concerning applicant	91	56	21	35
Information concerning deceased relative	44	26	7	18
Information concerning administrative matters	35	18	12	17
Information concerning a third party	12	8	0	4
Total	182	108	40	74

Table 8: results of objections and appeals against decisions on requests to inspect information held by the AIVD

	Objection	Appeal	Second appeal
Reviewed	5	3	2
Dismissed	5	1	0
Upheld	0	2	1
Inadmissible	0	0	1
Withdrawn	0	0	0

For more information go to: english.aivd.nl

Table 9: number of wiretaps pursuant to Art. 47 of the Intelligence and Security Services Act 2017

2021	1,133
------	-------

For more information go to: english.aivd.nl



Table 10: complaints about the AIVD to the Minister of the Interior and Kingdom Relations

Still under consideration as of 01 January 2021	5
Submitted in 2021	19
Dismissed	3
Upheld in part	0
Upheld	0
Handled informally to the satisfaction of the complainant	7
Not taken up for consideration	6
Withdrawn	2
Redirected	1
Still under consideration as of 31 December 2021	5

Table 11: complaints about the AIVD to the CTIVD

Still under consideration as of 01 January 2021	3
Submitted in 2021	25
Dismissed	2
Upheld in part	1
Upheld	0
Handled informally to the satisfaction of the complainant	8
Not taken up for consideration	13
Withdrawn	0
Redirected	0
Still under consideration as of 31 December 2021	4

For more information go to: english.aivd.nl

Colofon

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

PO Box 20010
2500 EA The Hague

October 2022