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

2020

Annual Report **AIVD**

Foreword

On 1 May 2020, the day I began work as Director General of the General Intelligence and Security Service, as many as 10,854 people had been admitted to hospital in the Netherlands on account of the coronavirus. For many, the virus has been the defining event of the year. In their personal lives as well as professional lives.

The AIVD, too, felt its impact. Because it affected colleagues, because cyberespionage and the number of cyberattacks increased, because the authorities and private companies asked for tailored security advice – in relation to corona vaccines, for example – and because jihadists found themselves confined to their homes like everyone else following the lockdown and travel restrictions.

In the course of the year, extremism found fertile breeding ground, too. This cannot be seen as completely unrelated to the virus. A diverse group of people in the Netherlands protested in a democratic manner against the government's anti-corona measures. They used their basic civil right to protest. A smaller, more radical group justified the use of intimidation, threats, and violence, and even resorted to such methods.

In December, the AIVD disrupted the espionage activities of two Russian intelligence officers. One of the officers had built an extensive network in the Netherlands with the support of the second officer, with the aim of obtaining sensitive technical knowledge.

The AIVD publicly denounced these activities in order to show Russia that the Netherlands does not tolerate such activities. And to make companies and civilians more aware of the dangers of economic espionage. Because the Netherlands is an attractive target for many states that want to steal knowledge and technology.

On such occasions the men and women of the AIVD are 'working witnesses'. This term was coined by former BVD employee Cees van den Heuvel, looking back on his career. His words are recorded in a book that will be published on the occasion of our 75th anniversary – a milestone that we wanted to celebrate widely in 2020.

It is our task to provide the Dutch government with independent information on international political developments and the intentions of other countries. To investigate risks and threats in time so that our (government) partners or we ourselves can take action against them.

To that end we will, in the coming years, allocate extra resources to the effective use of technology and data where possible. But it is not just technology in and of itself that matters. We need the right people to use – or choose not to use – this technology and data in an effective manner, in ways that are in line with our democratic values.

Society can rest assured that with these capabilities and these people we will continue to protect our national security, as we have been doing for the past 75 years.

Erik Akerboom
Director General
General Intelligence and Security Service

Contents

1 National threats

The General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) protects the Netherlands by investigating (unseen) threats against our national security. This chapter examines which national threats the AIVD investigated in 2020.

In its investigations, the service can obtain its intelligence from e.g. human sources, foreign services, or open sources. If the situation warrants it, the service is allowed to follow people, wiretap telephone conversations, and hack networks. More information on the number of times the AIVD did this in 2020 and the regulations to which it is subject, are presented in the chapter 'Facts and figures' (page 21).

For those interested in learning more about the way in which the AIVD detects and investigates threats, the six-part podcast De Dienst presents a fictional case from beginning to end: aivd.nl/podcast

Right-wing extremism

More and more often right-wing extremists sought to connect with a wider audience, by presenting their ideas as respectable and by joining public protests. The online contact between extremists throughout the world was intense, and some of the propaganda that was shared was extremely violent.

In the past year, right-wing extremist groups in the Netherlands frequently presented their ideas in an intellectual light, deserving the attention of the general public. The so-called 'alt-right' borrows ideas from a hybrid of conspiracy theories; beliefs of white supremacy; and facist, National Socialist, and conversative Christian views.

Supporters want to turn the Netherlands into a 'white ethno-state' where people with different origins or cultures are not welcome. They claim that the white race is slowly vanishing because it is being mixed with other races. They blame the government and other institutions for this.

Right-wing extremist ideas also reached a wider audience because right-wing extremists managed to gain a foothold at anti-government protests. This has led to the sprouting of conspiracy theories on corona that are variations on the so-called *Umvolkung* theory – the idea that 'the Jews want to replace the rest of the population.'

Dutch right-wing extremists have had frequent contact with like-minded people abroad, mainly in Germany. Online, in particular, right-wing extremists from around the world find each other. The resulting global online movement is cause for concern. Extremists exchange ideas – racial hatred and anti-Semitism. Some also share practical knowledge of survival techniques and firearm manuals. They also share very provocative and extremely violent propaganda.

In particular (younger) men with existing social-psycho issues are vulnerable to this. In the past year, the Dutch police arrested a number of minors and young adults that participated in such extremist online groups.

Abroad, attacks have shown that right-wing extremism can turn into terrorism. For that reason there is concern that also in the Netherlands people could become radicalised to such an extent. Consequently it is conceivable at the moment that right-wing extremists might carry out attacks in the Netherlands.

Trend: anti-government protests create breeding ground for extremism

Within the broad and diverse group of people in the Netherlands who protested against the government in 2020, a smaller group justified intimidation, threats, and violence, with some even willing to resort to such methods. This can create a breeding ground for (more) extremism.

The protests against the anti-corona measures in particular became grim and intimidating at times. Some protesters called politicians 'Satanists' and 'paedophiles', they went to the homes of scientists and threatened journalists, who then felt so unsafe that they did not want to do their work without protective security.

The groups that participate in anti-government protests are diverse and motivated by different reasons. One and the same protest could attract not only entrepreneurs who faced loss of income, but also spiritual groups and anti-vaxxers, who should be seen as separate from each other and from the hooligans and right-wing extremists who sometimes also joined these protests.

One thing the protesters share is that they are hardly, if at all, driven by ideology; what drives them is the feeling that they or others are being treated unjustly or are unheard by the government.

Their anger about this is directed not only at policy, but also at the people they hold responsible, a group that some of them see as 'the elite'. For some of the protesters this latter group not only includes politicians, but also civil servants, medical doctors, scientists, and journalists. The distrust of these groups is fanned by disinformation, misinformation, and conspiracy theories. As a result of these influences, a small group of activists has retreated into their own reality.

Social media play a major part in organising protests, sharing conspiracy theories, and expressing anger. For some protesters sharing such things online is a way of venting frustration, but for others it only adds fuel to the fire. Protesters also share a lot of information with each other through their own channels, without restraint.

Within the broader group expressing their discontent with the government in democratic ways (protests, lawsuits, own information channels) there is a radical undercurrent of small groups and loners who go much further. They (threaten to) publish the home addresses of police officers and scientists online or visit them at home, in order to intimidate them. They issue threats against scientists and politicians on social media, or threaten employees of the national health authorities in the street. Some even resort to actual violence and vandalise test centres.

These actions, justified in an online environment where anger is often fuelled and directed at individuals and combined with persistent and bitter (physical) protests, lower the threshold for intimidation, threats, and violence for some protesters. This creates a breeding ground for (more) extremism, which is being monitored by the AIVD, the National Police and the National Coordinator for Security and Counterterrorism (NCTV).

Anti-government extremism and activism

The handling of the coronavirus mobilised a lot of people in 2020, some of whom are extremely distrustful of and angry with the government. Some groups were implicitly calling for the incarceration of politicians.

For some people in the Netherlands the coronavirus became a catalyst for anti-government sentiment. Extreme distrust of and resistance to the government are nothing new, but since the outbreak of the virus, this resistance has become much broader and more multiform.

There is a discernible difference between 'thinkers' and 'doers'. Thinkers are often more highly educated people who share their anti-democratic ideas in publications or from behind their podcast microphone with an ever-expanding group of followers.

Doers want public action. At times their ideology is simply limited to 'being opposed' and they are willing to take action. Groups of 'doers' seek each other out. But tension between themselves often results in failure to cooperate in a structural manner.

The anti-government movement appears to be largely activist. Activist groups organised several protests against (the anti-corona policies of) the government. Some of the protesters became violent towards the police.

Some supporters also turn to social media to call for more extreme action, often phrased as 'suggesting ideas'. It does not appear to be very likely, however, that the organisations and their leaders would carry out threats. Anti-government extremism can lead to the structural undermining of our democratic legal order.

Left-wing extremism and activism

Left-wing protest in 2020 was expressed mostly as civil disobedience and in demonstrations against racism, and climate and immigration policies. Events featured the joint participation of broad coalitions of groups.

Left-wing protest in the Netherlands has been mainly activist in nature for some time now. With the exception of a few incidents, it is mainly expressed as protests and acts of civil disobedience. Unlike in the past, actions are hardly ever directed at individuals. Left-wing extremism could easily flare up in the Netherlands in response to developments in society. The dividing line between activism and extremism is very thin, after all.

In 2020, many of the actions and protests of left-wing protest groups were about anti-racism and climate change. There were anti-racism demonstrations for *Black Lives Matter*, against '*Black Pete*' and the colonialism of the past. Left-wing and identitarian activists have come together in a broad coalition centred around this theme. Their actions sometimes elicit fierce counter-reactions and polarisation.

Left-wing activists frequently protested against climate policy, in actions staged by, among others, Extinction Rebellion. Due to the coronavirus a widely announced international campaign against Shell - *Shell must fall* - was reduced to smaller-scale activities such as protests and painting slogans on petrol stations and office buildings. This campaign also mobilised a broad coalition of activist groups.

Characteristically, such long-term campaigns begin as activism, but they can gradually get out of hand and lead to vandalism and arson, for example. An example is *Stop the war on migrants*, a campaign against defence contractors who provide border patrol equipment. In the course of the campaign, objects were vandalised and set on fire.

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

Jihadist terrorism

In the past year the AIVD has not encountered any concrete Jihadist attack plots in the Netherlands. Nevertheless, Jihadism continues to be the main threat to Dutch society. It is a movement that believes it is at war with the Netherlands and other countries in the world, and it has the know-how to carry out an attack.

The number of Dutch Jihadists remained more or less the same: five to six hundred Jihadists in the Netherlands, and some 150 abroad. The fact that the movement shows hardly any growth is the result of internal division and fragmentation and a lack of leaders. For these reasons, and because adherents have become more security-aware, the movement is less outwardly focused, consequently reaching fewer people with its message.

The (networks of individual) Jihadists in the Netherlands pose an enduring threat nonetheless. They believe they are at war with the West, including the Netherlands. Terrorist attacks are encouraged and justified, and within the Dutch movement there is knowledge on and experience in carrying out an attack.

The number of adherents that would ultimately be willing to use violence is small, but the group is unpredictable. In 2020 the movement changed very little from the way it was in 2019 and 2018. Back then several violent threats were issued in the Netherlands, the AIVD thwarted attack plans, and in Utrecht there was an attack on the passengers of a tram.

The coming years could be decisive for the Jihadist threat in the Netherlands. The international situation is a strong influence on this. A resurgence of Islamic State (ISIS) or a new front opening up could lead to the mobilisation of Dutch Jihadists and result in a significantly greater threat. The return of foreign fighters and the release of Jihadists currently imprisoned in the Netherlands could be a contributing factor.

Dutch Jihadists also take part in the fight in the conflict areas. They can contribute to the fight and the survival of the movement in non-violent ways too. For example by lending support to terrorist organisations abroad, by spreading propaganda, and by supporting kindred spirits in detention.

In order to keep abreast of these different threats, the AIVD also investigates outside of the Netherlands, focusing on al-Qaeda and ISIS – the most important driving forces behind the global movement – and on affiliated networks and groups in Europe. More on this in the chapter on international threats and political security interests (page 8).

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

Radical Islam

The AIVD investigates radical Islamist movements that could constitute a threat to the democratic legal order in the Netherlands. This year the service continued its investigation into Wahhabi Salafism. Wahhabi-Salafist inciters attempt to gain authority through education and financing. They constitute a minority whose influence is disproportionately large.

The ideas of Wahhabi-Salafist inciters are at odds with our democratic legal order. In the long run these ideas could promote hatred, intolerance, and intimidation. Muslims in the Netherlands who are in disagreement with these ideas will suffer first, as they will be limited in their freedom to choose. But also people of different faiths and non-believers are affected.

The inciters do not acknowledge the legitimacy of the constitution, the government, the police, the law, or democratic processes – in short, what we call the democratic legal order. This could provide others with a breeding ground for radicalisation towards a violent Jihadist ideology.

In its investigation into Wahhabi Salafism the AIVD paid particular attention to education and inciters, and to interference and undesirable foreign financing.

Informal Wahhabi-Salafist education

Much of the work of Wahhabi-Salafist inciters is aimed at teaching children a version of Islam that is one-sided and intolerant, also with regard to our fundamental democratic rights. These informal extracurricular educational programmes propagate aversion to democratic values and Dutch society. Investigation has revealed that the lessons are also directed at the parents.

The extracurricular educational programmes contribute to the social isolation of these mainly young children (aged 5-16). This could cause children to distance themselves from Dutch society, and there is a danger that in the long term this will affect social cohesion and undermine the democratic legal order.

The group of Wahhabi-Salafist inciters is small in number, but their attraction is great thanks to well-made programmes, attractive websites, and high-quality education – for which there are waiting lists. They receive financial contributions, both from their own circles and from abroad.

Undesirable foreign financing and interference

In 2020 the House of Representatives instructed the Parliamentary Committee of Inquiry into undesirable influencing from unfree countries to conduct an inquiry. The then Director General of the AIVD was among those heard. He told the committee that followers of Wahhabi Salafism in the Netherlands are at a competitive advantage with regard to those who hold different views in Islam.

Because financiers from the Gulf States provide them with money, they can attain top ranking as providers of informal religious education. Online, too, they have a disproportionately great influence over the Muslim community.

The financiers are often charitable institutions that also conduct missionary activities (dawah). The Netherlands asks the Gulf States for transparency in these matters, but the countries in question do not always have a good idea of the activities of charitable institutions, or do not want to curb them in their activities for other reasons.
In 2021 the AIVD will continue its investigation of foreign financing. The AIVD will also look into the nature and extent of ideological influencing.

- Henceforth the AIVD will use the term Wahhabi Salafism to indicate a specific form of Salafism that could lead to the undermining of the democratic legal order. For more information about this movement, go to aivd/radicale-islam

PKK

In 2020, as in the previous year, the Kurdistan Workers' Party (PKK) did not use any violence in the Netherlands. Violent actions in our country are not very likely in the future either, as the organisation hopes to garner support.

The PKK is active in Turkey, but the AIVD deems it unlikely that the organisation will carry out violent actions in the Netherlands and in Europe, as its goal is to be acknowledged as the main interlocutor for the Kurdish question. The PKK hopes it will eventually be taken off the EU list of terrorist organisations.

2 International threats and political security interests

The AIVD protects the Netherlands by investigating (unseen) threats against our national security. Together or in close consultation with each other, the AIVD and MIVD (Military Intelligence and Security Service) also investigate the covert political intentions of other countries that could be harmful to Dutch interests, both at home and abroad.

This political intelligence helps ministries when drafting and modifying policies. The Minister of Foreign Affairs, the Minister of the Interior, the Minister of Defence, and the Prime Minister determine together which international topics the AIVD is to investigate. This chapter looks at which international threats the AIVD investigated in 2020.

In its investigations, the AIVD receives information from foreign services, from human sources, and from open sources. If the situation warrants it, the service is allowed to follow people, wiretap telephone conversations, and hack networks. More information on the number of times the AIVD did this and the regulations to which it is subject, are presented in the chapter 'Facts and figures', on page 18.

The digital component in espionage

Espionage, whether economic or political, is becoming increasingly digital. Russia and others try to gain access to the ICT systems of others on a large scale. The security leak at Citrix illustrates the scope of this problem. Thousands of companies and government authorities were affected, and some even compromised, as a result of this leak.

In 2020 the AIVD observed more so-called supply chain attacks by state-sponsored actors. In attacks of this type, the actor forcibly gains access to the network of a supplier to a company or government organisation. By exploiting the security vulnerabilities of this often less well-protected supplier it becomes easier for the actor to gain access to the actual target.

Russia in particular engaged in this practice on a large and global scale in 2020. Government organisations were targeted the most, but in the past year also companies came under attack. The AIVD and the MIVD found that among those who exploited the Citrix software vulnerability on a large scale were Russian state-sponsored actors.

State-sponsored actors had significantly more attack options for cyberespionage in 2020. Because so many people were working from home, companies were more reliant on software that provided remote access to the company network.

Several state-sponsored actors welcomed the corona crisis as an occasion to send out (spear) phishing emails. These emails ostensibly contain information about the coronavirus, but they are in fact used by the actor to steal data or install malware. The threat of cyberespionage also increased for government organisations, knowledge institutions, and companies involved in the prevention and fight against COVID-19.

Cyberattacks, in particular when directed at vital infrastructure in the Netherlands, can also be used as preparatory actions for sabotage. The AIVD remains alert to this issue.

For more information, go to: aivd.nl/spionage

Trend: espionage is a threat to the economic security of the Netherlands

The economic security of the Netherlands is at risk because countries attempt to steal knowledge and technology. In this area, China poses the greatest threat. In 2020 the AIVD disrupted the activities of a Russian intelligence officer. In 2021 the AIVD will structurally increase its economic security investigations. This will contribute to the identification, prevention, and combating of activities that pose a threat to Dutch interests.

The Netherlands is among the most highly-developed countries in the world when it comes to economy, science, and technology. This makes it a target for states that want to steal technology and knowledge. In this area, China poses the greatest threat. Most of China's (digital) espionage is for the purpose of stimulating its national economy. Obtaining knowledge and technology is a spearhead of this approach. In 2020 the country showed a global interest in the semi-conductor industry, telecommunications, biopharmaceuticals, and biotechnology.

Russia, too, spied on technology companies in the Netherlands in 2020. In December the AIVD disrupted the work of a Russian intelligence officer. He had an extensive clandestine network of more than ten individuals who were working or had worked in the Dutch high-tech sector.

He used this network to obtain sensitive information on nanotechnology, semiconductors, artificial intelligence, dual-use technology, and other topics. He paid some of his sources for their information.

The intelligence officer operated under diplomatic cover. In reality he was working for the civil intelligence service SVR. He was declared persona non grata and he has left the country. This is also true of a second Russian intelligence officer who provided support.

The AIVD made the operation public in order to send a signal to Russia that such intelligence activities will not be tolerated. And to make companies and civilians more aware of the dangers of economic espionage. The cabinet is currently investigating how espionage can be made punishable by law.

In 2020 the AIVD observed a successful cyberattack from North Korea. Iranian hackers were also observed by the service as they attempted to steal intellectual property from Dutch universities.

When they lead to the loss of exclusive intellectual property, legitimate investments and takeovers can also be a threat to the Dutch economy. The aim of such investments and takeovers is not necessarily to harm the Dutch economy, but they can result in damage nonetheless.

Countries can also harm the Dutch economy by buying special technology and reverse engineering it to find out how it works. There is also a risk that employees of foreign branches steal proprietary information of Dutch companies. These things are not always adequately monitored.

For more information about this, go to aivd.nl/economische-veiligheid

Abuse of infrastructure

The AIVD caught several countries in the act of renting ICT infrastructure in the Netherlands for the purpose of cyberattacks.

In 2020 the service observed how North Korea rented Dutch ICT infrastructure in order to be able to carry out cyberattacks. China, Iran, Russia, and Turkey have done the same in the past. The AIVD investigated these attacks in order to gain a better understanding of the intentions and cybercapabilities of these countries and the extent of their activities. The abuse of Dutch ICT infrastructure is harmful to the sovereignty and digital autonomy of the Netherlands, and it can damage our reputation. Following the investigation, the Netherlands informed the victims of the attacks where necessary and appropriate and took the servers offline.

Political espionage

Russia looked for political intelligence in order to undermine international cooperation. China collected personal data on a large scale. The country uses this data for cyberattacks.

Countries turn to espionage for a variety of reasons; to enable them to make better choices, or to be able to influence the political decisions of other countries, for example. In 2020 Russia appeared to be predominantly looking for political intelligence for the purpose of undermining the democratic legal order of other countries. The country uses the information it obtains also for obstructing international cooperation, in particular in the EU and NATO.

In the past year the AIVD has observed how Chinese actors continued their large-scale collection of personal data. This includes information on travel, visas, passports, flights, phone records, and medical information. China also extracts personal information from social media profiles and other open sources. This was exposed when a data leak revealed that China maintains an 'overseas key influential' database, which contains the information of 2.4 million influential persons.

In their search for personal data to collect, Chinese actors also select targets in the Netherlands. They can also obtain the personal information of Dutch nationals when they infiltrate targets abroad.

China uses the personal information it obtains to create profiles of employees of companies and organisations that the country is targeting for cyberoperations, for example. For this reason, the global, large-scale collection of personal data by Chinese actors is a threat to Dutch security.

Covert political influencing and disinformation

Russia spread disinformation about the downing of flight MH17 via online media platforms and other outlets. China tried to sow doubt about the origins of the coronavirus and Europe's approach to the crisis.

When countries try to hide the fact that they use offensive methods to safeguard their political interests, the AIVD defines this as covert political influencing. One example is the spreading of disinformation. Intelligence services often play a role in this.

Russia, in particular, uses such methods in its attempts to influence political processes in the Netherlands. The country is trying to alter the popular perception of the downing of flight MH17 over Ukraine, in 2014. In March, the Dutch trial against four suspects in this case began. Russia is keeping a close eye on the proceedings.

In the course of the year, the country organised several events with the aim of demonstrating that the work of the Joint Investigation Team (JIT) has been 'flawed'. The Russian military intelligence service, GRU, spread disinformation on the MH17 inquiry, for example on the media platform Bonanza Media. This platform published several JIT documents.

Russia continues to criticise the Dutch conclusions regarding the downing of flight MH17. It often adds that Ukraine is more at fault than is made to appear, as the country should have closed its air space completely.

Sometimes, covert influencing goes hand in hand with open propaganda. In 2020 China attempted, in the Netherlands and elsewhere, to influence the public's perception of the coronavirus. The country's propaganda became increasingly antagonistic as the year moved on: there were statements that praised China's approach and that cast doubt on the origins of the virus and the way in which European countries tried to deal with the crisis.

Jihadist terrorism in an international perspective

Al-Qaeda and ISIS are under pressure (locally), but they continue their efforts to create the kind of infrastructure that would enable them to attack the West.

Jihadists carried out several attacks in Europe in the past year. There were attacks in Paris, Nice, Vienna, and Lugano. It is not likely that any of these attacks were orchestrated by al-Qaeda or ISIS directly.

Both terrorist organisations are under pressure locally. ISIS leadership is attempting to rebuild and strengthen the organisation in Syria and Iraq, and in various international provinces. The terrorist organisation is obstructed by the anti-ISIS coalition, involving the United States and European and Islamic countries. This may have created a temporary setback in capabilities for ISIS, also in the West.

Al-Qaeda is under pressure in North-West Syria, one of the organisation's most important battlegrounds. Al-Qaeda leaders and attack planners are systematically being arrested or killed. They are being targeted in local conflicts with groups that were once their allies, and in US air raids. Consequently the threat the organisation poses to the West, and thus to the Netherlands, has decreased for now.

A number of al-Qaeda leaders may have fled Syria, presumably to resume working on their plans elsewhere. There are also indications that both terrorist organisations will continue their efforts to create the kind of infrastructure that would enable them to carry out attacks against the West. Both organisations have proven themselves to be resilient. In the past year, ISIS proved itself able to inspire others to carry out attacks in the West in its name.

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

Pressure on Dutch nationals with foreign roots

Several countries sought out opponents of their regime among the diaspora communities in the Netherlands. This can cause people to feel restricted in their freedom.

Among the countries keeping a close eye on their diaspora communities in the Netherlands, are Turkey, Iran, and China. They collected intelligence on opponents of their respective regimes, using human sources and digital means.

State-sponsored actors try to obtain the personal and travel information of dissidents, for example, to keep track of what they do. They put pressure on critics of the regime and try to get the community to put pressure on them too. The fact that many members of the diaspora have relatives or possessions in their country of origin is often used against them.

This foreign influencing of communities in the Netherlands can lead to tensions here. It can also result in people feeling less free to express themselves. Moreover, some governments are willing to use violence against critics abroad. In extreme cases the members of a diaspora even have to fear for their lives.

3 Eliminate and help prevent threats

When the AIVD uncovers threats in or outside of the Netherlands, the service warns partners so that they can take action. This chapter looks at when and how this occurred in 2020. The AIVD also has a number of unique departments that work on preventing and limiting threats to our country. This chapter describes their activities in 2020 as well.

Enabling others to act against threats

The AIVD can act autonomously against threats by using disruption, by dismantling networks or by making things public. In most cases, however, the service warns partners who are more specifically equipped to take action against potential threats.

Such a warning can be urgent and specific, for example in case of an imminent terrorist attack or after a hack. Warnings are issued also about more gradual processes that could result in threats to the democratic legal order and national security, however.

The service has specific methods to alert partners to a threat. This can be done in a meeting, through an official report (*ambtsbericht*), or in intelligence reports. The supplied information will enable a partner to act.

An official report from the AIVD can provide the police and the Public Prosecution Service with the information needed to open a criminal investigation, for example. Municipal authorities can revoke benefits or close buildings. The Immigration and Naturalisation Service can revoke a residence permit. A ministry can refuse to issue a permit, or a company can end its contact with questionable parties.

Table 1: **intelligence products issued in 2020**

	Total	**603**
Of which intelligence report:		500 *(134 in cooperation with the MIVD)*

Trend: the impact of the coronavirus on the AIVD's work

The coronavirus and the lockdown in response to it led to an increase in activism in the Netherlands. Jihadists were confined to their homes. Intelligence officers were restricted in their movements. The number of cyberattacks grew and at times the AIVD had to change the way it worked.

The coronavirus brought new work for the AIVD. The service was asked to think about the security aspects of stocking corona vaccines and the development of a contact tracing app (CoronaMelder). More on these topics below.

The government's policy of containing the coronavirus was a catalyst for anti-government sentiments. Various groups of activists furthermore believed that the crisis exposed the failure of the current system, and they used the outbreak to amplify the message of their ideology.

The lockdown had a subduing effect on the Jihadist terrorist threat in the Netherlands, because Jihadists at home and abroad were confined to their homes, with fewer opportunities to meet. Consequently they had fewer opportunities to spread their message.

Foreign intelligence services were similarly limited by the outbreak of the coronavirus in their options for physical action. For part of the year, travel restrictions made it difficult for intelligence officers to travel to and from our country. The services tried to compensate for this by turning to cyberespionage, which poses fewer risks in case of failure and which is generally much cheaper.

The number of cyberattacks increased in 2020 also because companies and public authorities were much more dependent on remote access software. Not all software used for working from home was secure.

The AIVD not only identifies threats, the service also advises companies, universities, and public authorities on security issues. Last year, many of these meetings had to be cancelled, though. The service has tried to fill the gap by organising several smaller meetings. The AIVD remained operational for the entire year, although some of its work had to be adjusted to the new circumstances.

Table 2: **official reports issued in 2020**

Official reports Public Prosecution Service	27 *(21 on Jihadism specifically)*
Official reports Immigration and Naturalisation Service	8
Official reports Ministry of Foreign Affairs	22
Official reports Mayors	0
Other official reports	6
Total	**63**

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

Table 3: **number of written threat-related reports**

2020	76

Security screenings

With the aviation industry hit particularly hard by the coronapandemic, the number of security screenings conducted by the Security Screening Unit fell by more than several thousand compared to previous years. The unit continued to develop, and screenings can be customised for candidates who stayed abroad.

The Security Screening Unit (Unit Veiligheidsonderzoeken – UVO) screens people who hold a position involving confidentiality or who apply for such a position to see if there are any security risks. Persons in a position involving confidentiality have access to secrets, or are in a position where they could damage 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 AIVD and MIVD unit. In 2020 the unit underwent further changes. Internal processes were improved and made identical for all the teams.

In 2020 the AIVD concluded 32,674 security screenings. This number has fallen by 13,829 when compared to 2019. This decrease is mostly due to the much reduced demand for screenings from the aviation sector. This sector was hit hard by the coronapandemic.

An average of 90 per cent of the security screenings conducted by the UVO must be concluded within the legal term of eight weeks. The AIVD met this requirement, concluding 92 per cent of screenings.

As of 1 January 2021 the UVO is able to customise its screenings for (prospective) officials holding a position involving confidentiality who spent time abroad. To this end the new policy regulation for security screenings was made public on 3 December 2020.

Under the auspices of the AIVD, the National Police and the Royal Netherlands Marechaussee (KMar) conduct security screenings as well. These are included separately in the overview below.

There are three categories for security screenings, depending on the nature of the position involving confidentiality: A, B and C. A-level screenings are the most thorough. When a screening results in a positive decision, the applicant receives a so-called certificate of no objection (‘verklaring van geen bezwaar’, VGB).

Table 4: **completed security screenings by AIVD and delegated partners**

Screenings	Positive	Negative	Total
Level A, by AIVD	2,122	8	2,130
Level B, by AIVD	5,695	80	5,775
Level B, taken over by AIVD from Kmar and National Police	1,276	582	1,858
Level C, by AIVD	513	3	516
Total by AIVD	**9,606**	**673**	**10,279**
Level B, by Kmar and National Police	22,395	0*	22,395
Total	**32,001**	**673**	**32,674**

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

Table 5: **results of objections and appeals against security screening decisions**

	Filed objections	Ruling on objection	Ruling on appeal	Ruling on second appeal
Dismissed	-	35	5	2
Upheld	-	13	1	1
Inadmissible	-	13	0	0
Withdrawn	-	7	0	0
Total	**42**	**68**	**6**	**3**

For more information, go to: aivd.nl/veiligheidsonderzoeken

Securing special information

The developers of the COVID-19 contact tracing app, ministries whose employees were working from home, and pharmaceutical companies working on (the distribution of) vaccines, were among those who called upon the specialist knowledge of the AIVD's National Communications Security Agency.

The National Communications Security Agency (Nationaal Bureau voor Verbindingsbeveiliging, NBV), a part of the AIVD, is the national authority responsible for the security of digital processes and confidential and classified information. The demand for advice on information security grows annually.

In 2020 the AIVD assisted the Ministry of Health in the secure development of applications such as the COVID-19 contact tracing app 'CoronaMelder'. The AIVD also helped the pharmaceutical industry to become more resilient. The service also assessed the various technical solutions used by the central government for working from home.

The AIVD investigates the security of the telecommunications infrastructure of the Netherlands, which includes future 5G infrastructure. In the past year, the service has updated its threat assessment on this topic and continued to work on security improvement measures for this infrastructure. The service also assisted in resolving several cyberincidents. One of these was a vulnerability in some Citrix applications, which was discovered in January.

The coronapandemic caused a delay in the implementation of the National Cryptostrategy (Nationale Cryptostrategie, NCS). This strategy, which was formulated in 2019, describes how the NBV can see to the development of reliable security solutions for highly sensitive information and how to deal with the vulnerable supplier base for security solutions.

The NBV, together with the Ministry of Foreign Affairs and the Ministry of Defence, is negotiating information security treaties with other countries. These are to provide agreements on the security and exchange of confidential and classified information. In 2020, agreements were negotiated with Spain and Estonia. The AIVD is also preparing agreements with other countries. The AIVD published new assessment criteria (NEC2020) for the development of secure information security products for the Dutch government.

For more information, go to: aivd.nl/informatiebeveiliging

Watching over the security of dignitaries and organisations

Anti-government activists posed a potential threat to politicians. State-sponsored actors were a potential threat to the MH17 trial and the Organisation for the Prohibition of Chemical Weapons.

The national safety and security system was devised to remove threats to dignitaries and organisations. These include politicians, members of the Royal Family, diplomats, and international organisations.

To this end the AIVD produces risk assessments, threat assessments, and threat analyses. The NCTV uses these to decide whether (additional) protection is needed.

The AIVD assessed that in 2020 anti-government activists more often posed a potential threat to politicians, at the state opening of parliament, and – to a lesser degree – to diplomatic objects in the Netherlands.

State-sponsored actors (countries, or organisations operating on behalf of a country, such as an intelligence service) played a greater part in the general threat assessment. They posed a potential threat to diplomats and diplomatic objects and to international organisations. Actors focused in particular on the MH17 trial and the Organisation for the Prohibition of Chemical Weapons (OPCW).

The national safety and security system is currently being made future-proof under the guidance of the NCTV. A proposal for this review will be presented by an independent commission. In 2020 the AIVD emphasised that it is essential that the system also focus on digital threats and cyberespionage.

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

Advising companies and the authorities about security

AIVD experts examined the security of the locations where corona vaccines are kept. The service also spoke with universities about the securing of scientific knowledge.

The AIVD provides authorities and companies with advice on how to work securely, in particular when processes that are vital to our country are involved. In 2020 the service played a major part in facilitating the security of the pharmaceutical industry. With the ongoing coronapandemic, this was needed urgently. The services provided information and concrete advice on threats.

At the request of the NCTV, AIVD experts were involved in examining the security of locations where vaccines are kept. When the government was working on a vaccination strategy, the AIVD contributed to the threat assessment.

The service advises Dutch universities about the securing of scientific knowledge, for example through a series of knowledge security dialogues. As 2020 drew to a close, the AIVD and the Ministry of Education, Culture and Science had met at an administrative level with nearly all universities in the Netherlands. The service will continue these dialogues in 2021.

A joint response to cyberattacks

In order to react quickly and in coordination to cyberthreats and cyberincidents, the intelligence services and the police will be sharing information on cyberthreats from a centralised location.

The AIVD, the MIVD, the National Police, the Public Prosecution Service, and the National Cyber Security Centre have been cooperating in the cyber intel/info cell for some time. As of 2020, they also share a physical location. The advantage of this is that the cooperating parties can react to threats more quickly and in better coordination. Police and intelligence investigations can be coordinated, and the government will be able to issue a unified message about cyberthreats.

Preventing countries from obtaining weapons of mass destruction

The AIVD and the MIVD investigated networks attempting to obtain knowledge on and materials for the development of weapons of mass destruction. As a result of the services' intervening, several procurement attempts have been thwarted.

The Unit Counterproliferation (UCP), a joint AIVD and MIVD unit, investigates the ways in which countries attempt to acquire the knowledge and materials they need to make weapons of mass destruction. Countries like Syria, Pakistan, Iran, and North Korea tried also in the past year to acquire such materials and technology in Europe and in the Netherlands.

In 2020, the unit carried out in-depth investigations into several networks playing a role in this. These networks are very active, and they make use of various intermediaries and transporters in European countries. The UCP's investigations assist the Ministry of Foreign Affairs when deciding to issue export permits for goods. Thanks to the intervention of the MIVD and AIVD several procurement attempts could be frustrated and stopped in the past year.

For more information, go to: aivd.nl/massavernietigingswapens

4 Oversight and organisation

The AIVD does extraordinary work, which requires special oversight. This chapter describes how the AIVD worked to meet the most recent legal requirements, how the Oversight Committee and the Investigatory Powers Commission reviewed our work, and how we handled bulk data in 2020. Also included are facts and figures and some important events.

Oversight and the AIVD

Two independent bodies review and oversee the work of the AIVD. This is important to the legitimacy of our work. In 2020, this oversight occurred increasingly in real time.

The Investigatory Powers Commission (Toetsingscommissie Inzet Bevoegdheden, TIB) assesses before the use or renewal of a special investigatory power, whether the minister was justified in authorising the use of these powers.

The commission assesses, for example, whether in case of an espionage investigation it is really necessary to hack into a computer, or whether less-invasive means might do, too. If the TIB decides that the authorisation is not legally justified, then the AIVD cannot use that special investigatory power in that instance.

The TIB publishes an annual report with its findings. In its annual report for 2020 the TIB came to the conclusion that, in terms of percentage, the AIVD was slightly more frequently authorised without proper justification to use a special investigatory power: in 1.9 percent of all cases, up from 1.7 percent.

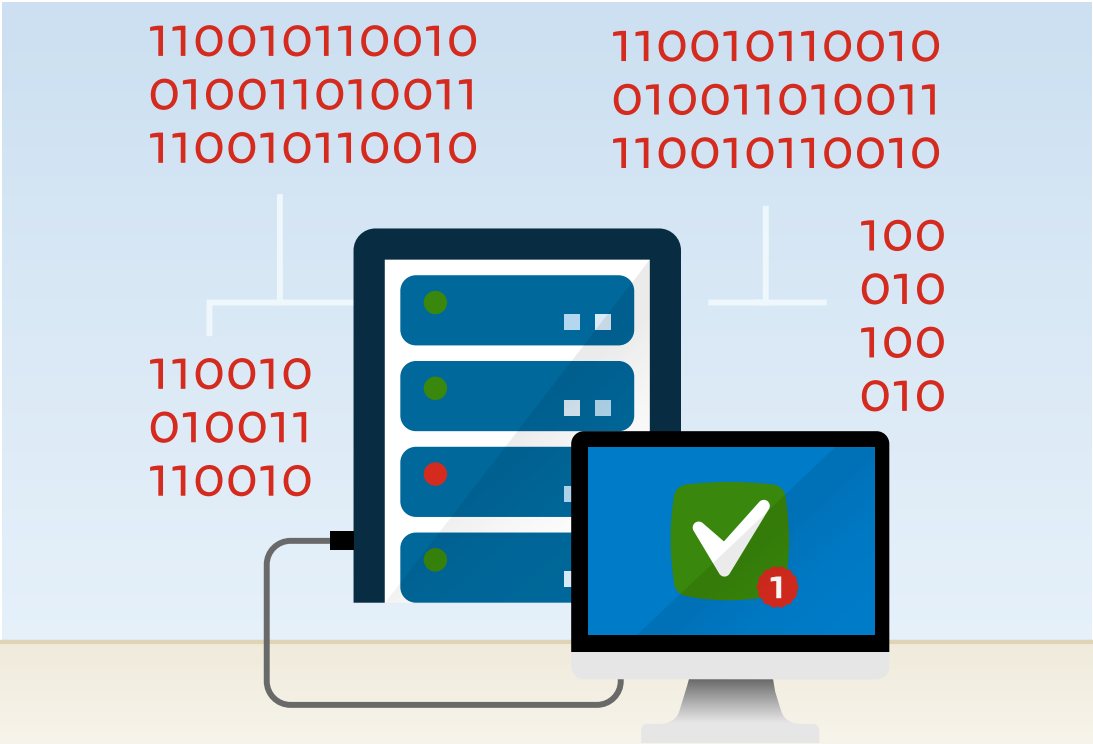
The AIVD's prime consideration is to meet all legal requirements. It is important to view the 0.2 percent increase in its proper context: in 2020 the service filed more requests than in 2019; moreover, these requests were more complex than previously and the questions about the requests went into much greater detail.

When a request was denied because it did not meet legal requirements, the reason was generally because it lacked proper substantiation. After making the necessary changes, the TIB found the requests legitimate in 69 percent of these cases.

In its annual report the TIB also writes that the AIVD continued on its previous course of qualitative improvement of the requests. To the AIVD this is the result of the time, effort, and capacity that have been dedicated to improvement. The review and assessment by the TIB provided a valuable contribution to this result and the qualitative consolidation.

The Oversight Committee for the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD) checks whether the service operates within the requirements of the law. This varies from reviewing whether an operation was conducted lawfully and checking to see if data was destroyed within the legal time limit, to the implementation of the Intelligence and Security Services Act 2017.

To carry out its task, the CTIVD has access to all AIVD systems, and more and more often it is able to oversee in real time how we operate. As a result the CTIVD's oversight will be more effective. The work of both the TIB and the CTIVD is essential to the legitimacy of the AIVD's work.



Trend: new way of handling bulk data

In 2020, the Minister of the Interior and the Minister of Defence announced new policy for handling bulk data. It is important to the AIVD that society can trust in how the service handles (personal) information. This means that the regulations have to be clear, and that we explain when and how we use data sets in general. In 2020 we used such data sets in our investigation of a group of Jihadists, for example.

As society's use of (digital) information increases, the AIVD has to look for threats in an ever-expanding pool of data. In order to gain an understanding of the actions of a single individual or a small group, it is sometimes necessary to examine an entire set of data.

This set also contains data related to people that the AIVD is not investigating, and never will investigate. In 2020, the Minister of the Interior and the Minister of Defence introduced new regulations that explain more clearly how we protect the privacy of these people.

For example, there are stricter requirements for being authorised to have access to the data set. We also assess more frequently whether the data should be deleted. The Minister of the Interior and the Minister of Defence determine in advance how the services are to handle a data set. The Oversight Committee (CTIVD) is also involved more actively in the process.

In 2020, bulk data was vital to the AIVD's work. It gave the service the means to locate the meeting place of a group of jihadists. There were indications that this group made Jihadist plans at regular meetings at this location.

By locating the telephones of one of these Jihadists, the service obtained an essential clue: during the meetings he could always be found between the same two cell phone towers. Still, those two towers covered a fairly wide area.

That is why the service decided to look into the registry of the Chamber of Commerce, a bulk data set that contains current and historical company information. The registry revealed that one of the members involved in the group rented a property in precisely this area. Further investigation then confirmed that this property was, in fact, the group's meeting location. Without the bulk data set – the Chamber of Commerce registry – this location would never have been found. The investigation into the group is still ongoing.

Compliance with the Security and Intelligence Services Act – our 'licence to operate'

In 2020 the AIVD and the MIVD continued their work on implementing the Intelligence and Security Services Act 2017. Furthermore, an independent commission reviewed the act to see whether it met the legislator's intentions: to provide the intelligence and security services with modern investigatory powers, combined with better oversight.

The Intelligence and Security Services Act 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017, Wiv 2017) describes the AIVD's investigatory powers, and which means the service may use in which instance. These regulations and safeguards are important because the means at the disposal of the service can infringe on people's privacy. The act is our 'licence to operate'.

In 2020, the service continued to work on implementing the new law. These efforts resulted in significant improvements. There is more (internal) control over the handling of data and technical data systems have been improved. In 2021 we will work on improving the quality of our systems, and we will be invested in the development of a shared data management system together with the MIVD.

In May 2020 an independent commission began its evaluation of the law. This evaluation gives effect to the coalition agreement, which stipulated that the law would be evaluated two years after it came into effect. The commission examined whether the law meets the goals for which it has been proposed, namely to provide modern investigatory powers and to enhance safeguards. The commission also examined whether the law is practicable and whether there are any practical obstacles.

The conclusion is that the law succeeds largely in what it is intended to do. The AIVD does not lack any investigatory powers and safeguards have been strengthened. In relation to this aspect, the commission also refers to the important roles of the Oversight Committee and the Investigatory Powers Commission. The evaluation mainly provides recommendations intended to improve the practical applicability of the law to investigations.

There are also some shortcomings in the new law. The AIVD and the MIVD have indicated that they are currently unable to carry out a small but essential part of its investigations. These shortcomings will have to be addressed by an amendment of the law. For example, the law should provide a single description of the use of bulk data. Both the collection and the use of bulk data should come with more safeguards. The commission also advises to use more safeguards to strengthen international cooperation. Both of these topics are cause for concern in our society.

Lastly, the commission recommends involving the Administrative Jurisdiction Division of the Council of State in case of differences of interpretation regarding legal concepts and open standards. In the first quarter of 2021 the cabinet responded to the report by evaluation commission's report.

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

Playing our part in securing 75 years of freedom

The AIVD, including its predecessors, celebrated its 75th anniversary in 2020. Due to the coronapandemic, celebrations were limited. Now the service hopes to celebrate this anniversary in 2021. A book and an exhibition are in the works.

On 29 May 1945 the National Security Bureau (Bureau Nationale Veiligheid, BNV) was founded. Its main task was to track and apprehend German spies and wartime collaborators. Its successors, the Central Security Service (Centrale Veiligheidsdienst, CVD) and the Domestic Security Service (Binnenlandse Veiligheidsdienst , BVD) initially concentrated on fighting Communism, later also focusing on extremism and terrorism.

In 2002 the BVD's tasks were expanded to include foreign intelligence and its name was changed to General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD). For those who are interested in the history of the service, go to our website aivd.nl to look at the timeline or watch a brief video with an impression of the service's colourful history.

New leadership

As of 1 May 2021, the AIVD has a new Director General at its helm: Erik Akerboom. In 2021 Simone Smit took office as Deputy Director General.

Between 2016 and 2020 Erik Akerboom headed the National Police. Before that he was Secretary General with the Ministry of Defence, and National Coordinator for Security and Counterterrorism. Erik Akerboom succeeded Dick Schoof.

As of 15 February 2021 Simone Smit is the new Deputy Director General. Between 2017 and 2021 she was Director for Counterterrorism with the NCTV. She started out with the NCTV in 2014 as Head of the Surveillance and Protection Unit. Before that she held various senior management positions with the police for nineteen years. Simone Smit succeeded Marja Horstman.

Facts and figures

In 2020 the AIVD received

2,225

notices from partner services, civilians, and public and private organisations.

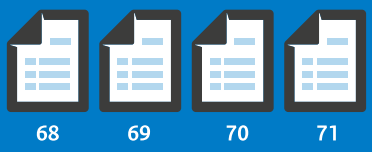
After initial assessment, **90 per cent** of these notices were considered closed as they required no further investigation.

Intelligence reports issued

Intelligence reports issued by the AIVD: 500, of which 366 by the AIVD alone and 134 in cooperation with the MIVD.

4

CTIVD reports on the work of the AIVD in 2020:4



41

Number of notifications

2,088

Wiretaps pursuant to Art. 47 of the Intelligence and Security Services Act 2017

Table 6: requests to inspect information held by the AIVD, by nature or subject

Requests	Submitted	Reviewed	Inspection file sent	Under consideration as of 31-12-2020
Information concerning applicant	85	81	31	29
Information concerning deceased relative	30	28	12	9
Information concerning administrative matters	18	28	14	17
Information concerning a third party	7	3	0	2
Total	**140**	**140**	**57**	**57**

Table 7: results of objections and appeals against decisions on requests to inspect information held by the AIVD

	Objection	Appeal	Second appeal
Reviewed	26	14	12
Dismissed	16	2	11
Upheld	5	12	1
Inadmissible	4	0	0
Withdrawn	1	0	0

For more information, go to: aivd.nl/inzageverzoeken

Table 8: **complaints about the AIVD to the Minister of the Interior and Kingdom Relations**

Under consideration as of 1 January 2020	**7**
Submitted	**25**
Dismissed	**3**
Partially upheld	**1**
Upheld	**0**
Handled informally to the satisfaction of the complainant	**3**
Not taken up for consideration	**20**
Withdrawn	**1**
Redirected	**2**
Still under consideration as of 31 December 2020	**2**

Table 9: **complaints about the AIVD to the CTIVD**

Under consideration as of 1 January 2020	**3**
Submitted	**30**
Dismissed	**4**
Partially upheld	**0**
Upheld	**0**
Handled informally to the satisfaction of the complainant	**1**
Not taken up for consideration	**24**
Withdrawn	**1**
Redirected	**0**
Still under consideration as of 31 December 2020	**3**

For more information, go to: aivd.nl/klachten

Colofon

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

PO Box 20010
2500 EA The Hague

May 2021