General Intelligence and Security Service
aivd.nl

Postbus 20010
2500 EA Den Haag

May 2019

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

AIVD
Annual Report 2018

Foreword

This is the AIVD's public annual report for the year 2018. This yearly report offers us a rare opportunity to give some insight into the day-to-day activities of the 2,000 men and women of the AIVD. The report is an account of our work and it offers members of the government, the press, and the public, a view of our activities and areas of operation.

In a constitutional state like the Netherlands it is essential that after rigorous internal control there is also thorough external oversight over a service that has far-reaching powers at its disposal.

When our service is the topic of debate in parliament or in the media, these discussions often follow from reports by the Oversight Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* – CTIVD). This committee was implemented as part of the previous Intelligence and Security Services Act 2002. In the past seventeen years, the oversight committee conducted around fifty enquiries on various topics into the AIVD and reported its findings in frank and largely public reports.

With the coming into effect of the new Intelligence and Security Services Act 2017 this past year, another oversight instrument was added to our work. Under the new act, the exercise of special investigatory powers requires not only the authorisation of the Minister, but also the review of that decision by the independent Investigatory Powers Commission (*Toetsingscommissie Inzet Bevoegdheden* – TIB) before we can proceed.

The TIB and the CTIVD are strict and critical, and rightfully so. This may sometimes complicate our work, but we know that oversight is of the utmost importance to us and to society.

We are also subject to parliamentary control, of course. The Parliamentary Standing Committee on Home Affairs oversees the activities of the AIVD, insofar as this is possible in a public setting. Where confidential and operational information is concerned, the Minister gives account of our activities to the Netherlands Committee for the Intelligence and Security Services.

The nature of our work and the letter of the law do not permit us to discuss our activities openly. This is also true of this annual report. Nevertheless, we are not a secret service – if we were, you would not have heard of us – but rather a service with secrets.

Only in this way will we be able to detect threats in time. The fact that two bodies oversee our work and report on our activities, provides us with our license to operate. This oversight provides the AIVD with the legitimacy to operate in a democracy. Because of this oversight, democratic society can trust that we are doing the right thing, in the interest of national security and our democratic legal order.

Dick Schoof
Director-General
General Intelligence and Security Service

Contents

Introduction

Not often has the AIVD been as conspicuously in the news as in the year 2018. This attention was mainly due to the public interest in the new Intelligence and Security Services Act 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*). In March of this year, Dutch voters were given the chance to express their opinion on the new act in a referendum.

The new act, which came into effect on 1 May 2018, is needed to deal with present-day threats at a time when society in all its facets is pervaded by and dependent on internet technology.

The new act also provides civilians with the security that data is collected in a targeted manner and only retained when it is significant to our work. All other data must be destroyed immediately. Furthermore an independent commission reviews all proposed uses of special investigatory powers before we can take action.

We worked hard to prepare our organisation for the arrival of the new act on 1 May. Nevertheless, the implementation of the new regulations has had a greater impact on our organisation than previously estimated. It took more time and effort to introduce and properly set up all the new safeguards for civilians, such as the independent review and the treatment of data, because these safeguards are linked in a profound way to the core of our work: the acquisition and processing of data. This has permanently changed our work.

At the same time the threats faced by the Netherlands are complex and aggressive, and almost always accompanied by a significant digital component.

States try to uncover and influence policy decisions, steal trade secrets, or intimidate and influence (former) fellow nationals. They also try to gain access to and hide out in software systems responsible for vital processes in our country, to be able to sabotage these in the future.

The arrest of seven persons on suspicion of planning a terrorist attack and a number of other incidents show that our country may also still feature as a target for jihadist or radical Islamic terrorism.

Meanwhile, as the population becomes increasingly polarized, the national debate is becoming harsher. Distrust of the government is growing, also as a result of extremist expressions. Some radical figureheads also try to disengage young Muslims by making them distance themselves from Dutch society.

All these developments occur against an ever-changing international backdrop.

The situation in the Middle East remains tense and unstable. Iraq and Syria are still in the grip of violence and unrest, and even though the so-called caliphate of the Islamic State in Iraq and al-Sham (ISIS) has lost practically all of its territory, the threat of terrorism persists. ISIS has gone underground and its attacks disrupt life in the region on an almost daily basis. Al-Qaeda too is still active and manifesting itself more and more.

The fighting in Syria in 2018 also saw the use of chemical weapons. In April dozens of civilians lost their lives in a chlorine gas attack on the town of Douma.

The historical antagonism between Iran and Saudi Arabia continues to determine the geopolitical stage. Saudi Crown Prince Bin Salman's public image as a progressive modernizer suffered a serious blow after the critical journalist Jamal Khashoggi was killed in the Saudi consulate in Turkey.

Iran is facing a more uncertain future now that the United States have withdrawn from the nuclear deal. The European Union continues to support the deal with Iran. The non-proliferation treaty, which saw its 50th anniversary last year, is under pressure as a result of rising tensions between superpowers, falling support for international cooperations, and the protectionism of various leaders.

In 2018 the direct nuclear threat posed by North Korea appeared to wane when the heads of state Donald Trump and Kim Jong-un shook hands and North Korea declared itself willing to dismantle its nuclear installations. The results of the talks are as yet inconclusive.

Tensions between Russia and the West remain high. President Putin tries to position Russia as a world power, thereby also strengthening his own position in the country. He attempts to cause division within NATO and the EU in order to weaken his opponents, and he is acting belligerently towards the Baltic States.

The attempt by the Russian military intelligence service GRU to poison a former intelligence officer in the United Kingdom and their attempt to hack the network of the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague are evidence of the insolent methods of this service.

On the other side of the world our Kingdom's largest neighbour, Venezuela, is in a deep crisis. The deplorable state of the country, both in political and economic terms, means that the population suffers greatly. This has led to millions of refugees and adversely affected the stability of the region and the areas of our Kingdom there – Aruba, Bonaire and Curacao.
In 2018 we produced over 300 intelligence reports on all these worldwide developments, reports used by the Dutch government for its foreign policy. A significant number of these reports was used in support of our membership of the United Nations Security Council during the first six months of that year.

Within the context of our investigations we produced over 900 written documents, including official reports, intelligence reports and analyses, risk analyses, threat assessments, and information security advice. More and more often we also inform interested parties orally of our findings.

In 2018 the Prime Minister, together with the Minister of the Interior and Kingdom Relations and the Minister of Defence set the priorities of the AIVD and the Military Intelligence and Security Service (MIVD) for the coming years. This is done in close consultation with the Minister of Justice and Security and the Minister of Foreign Affairs.

These agreements are recorded in the Integrated Intelligence and Security Order (*Geïntegreerde Aanwijzing Inlichtingen en Veiligheid*). The order describes which information agencies and organisations need from the AIVD and MIVD in order to be able to take responsibility for their own areas of interest and focus. The Integrated Intelligence and Security Order is evaluated every year.

These national and international developments show how important our work is. That is why the government has allocated additional funds to allow the AIVD to grow in 2018 and 2019. In the past year we welcomed over 190 new colleagues, and we hope to welcome 200 more in 2019.

Espionage and undesirable foreign interference

When other countries engage in covert activities in order to collect information in and on the Netherlands, thus harming our national interests, we call this espionage. Espionage can be digital (hacking computer systems, for example) or physical, involving persons. It could concern important political intelligence, such as policy making processes and government viewpoints, but other countries can also use espionage to steal (trade) secrets in order to boost the national economy.

Countries can also attempt to harm Dutch interests in another way, namely by interfering with national processes. For us this is undesirable foreign interference: covert political influencing, influencing and intimidating emigrated (former) fellow nationals, sabotage and abuse of Dutch ICT infrastructure. Such interference is undesirable because in this manner other countries undermine the political, economic and societal bedrock of the Netherlands.

When states use digital means for espionage and sabotage purposes in order to obtain their own political, military, economic and/or ideological goals at the expense of Dutch interests, we categorise this as an offensive cyberprogramme. Our investigations have revealed that countries like China, Iran, and Russia run such cyberprogrammes, directed also at the Netherlands.

Espionage

Anyone with specific or specialist knowledge could become the target of espionage, but not everyone is aware of this. The aim of our investigations is to protect the political and economic security of the Netherlands by identifying threats in time to alert the relevant individuals and authorities.

The year 2018 was notable in particular for the brazenness with which intelligence officers conducted their espionage activities. The attempt by the Russian military intelligence service GRU to gain access to the network of the OPCW in The Hague shows how far this service is willing to go.

Our investigations also revealed that cyberespionage is becoming more and more complex. State actors increasingly make use of methods and techniques that have been used before, which complicates the attribution of an attack. State actors also increasingly exploit internet service providers and managed service providers as a springboard to gain access to a target, because these service providers often have far- and wide-reaching structural access to the information of organisations or individuals. Methods like these make it more difficult to detect, analyse, and attribute cyberattacks.

We note that China, Iran, and Russia are at the vanguard of political and/or economic espionage, but the list of countries engaging in such practices continues to grow.

Political espionage

To Russia, our country is an interesting espionage target. Dutch politics and the judiciary have become more important to strategic Russian interests since the downing of flight MH17 in July 2014. Information about the proceedings and the results of the enquiries into the disaster are and will continue to be of interest to the country. Now that the Netherlands has held Russia responsible for its role in the downing of the airplane, this interest will only increase.

The Netherlands has been in the Russian eye for much longer, because of our membership of NATO and the EU. Russia would like to learn what our position is in these international cooperative frameworks.

To gain insight into this, Russian intelligence services not only use digital means, but also return to traditional espionage, for example the recruitment of human sources.

It may be interesting for other countries to have access to the communications traffic between a diplomatic post abroad and the Ministry of Foreign Affairs. We have observed that in 2017 and 2018 a number of Dutch embassies in the Middle East and Central Asia have been targeted in cyberattacks by a foreign intelligence service. The cyberattacks on these embassies confirm that there is structural interest in intelligence from the Ministry of Foreign Affairs.

Economic espionage

In terms of economic espionage, the largest threat by far is posed by China. This espionage is fed by Chinese plans for its economic policy, such as 'Made in China 2025' and the 'New Silk Roads', by which the country intends to expand its economic and geopolitical influence.

These plans not only lead to economic opportunities, but also to increased competition with Western – and therefore also Dutch – companies. In this competitive race China uses a wide range of (covert) means that undermine the earning potential of Dutch companies, which could in the long run result in economic and political dependencies. One of these means is economic (cyber) espionage.

China is interested in Dutch companies that are active in the fields of high tech, energy, maritime tech and life sciences and health.

Another threat to national security is related to globalisation, which brings with it growing economic interaction, digitisation, internationalisation of the labour market and production processes, and the liberalisation of establishment and investment policies for companies.

Globalisation offers further opportunities for the (covert) acquisition of Dutch technology and companies. Businesses can be acquired by foreign companies that are under state influence or able to obtain state support at lower costs, which means that the economic playing field is no longer level.

Also within the context of legitimate collaborations between academic and other knowledge institutes, research is being stolen. In this way Dutch scientific research disappears across our national borders.

The security awareness and resilience of Dutch businesses and knowledge institutes against these risks appears to fall short, which constitutes a threat to the economic security of our country.

Covert political influencing

It is entirely legitimate that a country is open about protecting its own interests with regard to other countries. However, when looking after one's interests goes beyond regular diplomatic or political lobbying because it is done under a false flag, we see this as covert political influencing.

Covert influencing can target political decision-making directly, but it can also be more indirect, when it focuses on the manipulation of public perceptions. Spreading disinformation is one of the means used in this process, and intelligence services often play a role in such covert influencing.

One of the countries mentioned continuously these past years with regard to interfering in the political processes of other countries, is Russia. Of old, this country has been most adept at covertly influencing perceptions and public opinion in other countries, which can have a disruptive effect on policy-making processes. One example of Russian interference is the dissemination of disinformation by spreading various speculations about the MH17 disaster, which obfuscated the investigation. We have also observed largely unsuccessful attempts at online influencing in Dutch which originated in Russia.

We also note how states, such as China, attempt to influence opinions and publications on their country using institutions for education and knowledge, for example in countries with which there is a fairly productive exchange of scientific knowledge. The risk here is that it could create a dependency on the government in question, for example when research is being financed by China, or the research focuses on developments in the country in question and necessitates travel to this country. This position of power would lend itself to abuse. Journalists also have to deal with a similar kind of obstructionism, for example when unwelcome publications lead to threats of revocation of work permits.

Among the countries we have observed as engaging in covert political influencing are China and Russia.

Influencing and intimidation of the diaspora

States attempt to hold sway for their own national political gain over people who left their country (diaspora) and emigrated to the Netherlands. In some cases these emigrants still hold a passport of their native country, or they still have relatives there but have been living in the Netherlands for some time. This sometimes also pertains to people who have fled the country of their birth for political reasons, only to become the victim of intimidation in our country.

Such intelligence and interference activities lead to a permanent sense of insecurity among the targeted communities, and they could also transplant external tensions to our own country. This influence can be so intrusive that people feel restricted in their civil rights, such as their freedom of expression. The security services of these states also do not shy away from pressuring the family members of emigrants in their country of origin.

Iran is interested in persons and organisations that are known opponents of the current regime. The AIVD has come across strong indications that point toward Iran's involvement in two assassinations in the Netherlands, one in Almere in 2015 and the other in 2017 in The Hague. Both victims had been opponents of the Iranian regime. As a result of the AIVD's investigations, the Netherlands took steps against two Iranian diplomats.

Among the countries we have observed as being prepared to influence and pressure emigrated (former) fellow nationals are China, Iran, Russia, and Turkey.

Sabotage and abuse of infrastructure

States can also pose a threat to the independence and autonomy of the Netherlands because they enable cybersabotage of vital infrastructure. They do this by gaining access to and then hiding out in the ICT systems for vital processes. The AIVD has detected attempts to this end.

As yet no details have been uncovered of any intentions to actually sabotage the vital infrastructure of the Netherlands, but disruptions of the power supply of one of our neighbours would also have an impact on the Netherlands. With the geopolitical unrest in today's world, sabotage is certainly more conceivable. Russia, for example, runs an offensive cyberprogramme for the disruption and even sabotage of vital infrastructure.

The Netherlands also carries a certain responsibility because it is an ICT traffic hub: just as air traffic passes through Schiphol airport and cargo ships put in at the Port of Rotterdam, a large chunk of the world's internet traffic passes through the ICT infrastructure of our country. Some countries abuse this infrastructure for cyberespionage, influencing,

or sabotage activities against other countries, which cause great damage to the international legal order and the interests of other countries, our allies in particular.

Among the countries we have observed as being guilty of sabotage and/or the abuse of ICT infrastructure are Iran, North Korea, and Russia.

Activities and results

Our investigations have allowed us to assess the risks of espionage and foreign interference for the Netherlands and for businesses. To that end we visited various organisations, gave hundreds of (awareness) presentations, and informed government partners such as the National Coordinator for Security and Counterterrorism (NCTV) and government ministries about our findings. The intelligence services' account managers with the police also play an important role in this.

We issued approximately 40 intelligence reports on espionage and undesirable foreign interference. The number of questions received by the AIVD that concerned the continuity and integrity of vital systems both within and outside of central government has grown in the past year. Partly for that reason we expedited the development and installation of detection means so that attacks can be detected in time. In 2018 the AIVD received additional funding for this.

We also provided advice on the risks to national security with regard to the implementation of a modernized closed communications network for authorities and emergency services (C2000). The AIVD deems it undesirable that where vital processes and the exchange of sensitive information are concerned, the Netherlands would come to depend on hardware and software from companies in countries that are known to engage in offensive cyberoperations against Dutch interests. We provide the government ministries and other involved parties with information on the relations between such companies and their governments, so that they can assess the risks. It is important to look at the possibilities, intentions, and interests as well as national laws of the states involved. It is also important that Dutch users see to it that they always have control over their own data.

In 2018 the AIVD and MIVD presented their joint report on cyberintelligence (*Cyber Inlichtingenbeeld*). This is a secret report intended for the national government which provides an overview of current threats and expected developments.

Additional allocated funding allowed us to focus strongly on hiring new employees and technical experts for our investigations into cyberthreats. Recruiting top-level technical staff and intelligence officers with technical expertise requires a lot of effort, in particular in view of today's labour market.

Internationally we have been cooperating closely with foreign partner services, sharing our knowledge on developments related to foreign interference. In a number of cases we provided relevant intelligence.

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

(Jihadist) terrorism and radical Islam

Where terrorism is concerned, the AIVD's prime area of interest is jihadist terrorism, but not all terrorists are jihadists. Radical Islam can provide the breeding ground for jihadist terrorist violence, and Salafism is the best known variant of Islamic fundamentalism.

Jihadist terrorism

The number of incidents in the Netherlands with a jihadist, terrorist, or radical Islamist background increased in the past year. In the previous years the Netherlands was fortunate enough not to have suffered any terrorist attacks, when terrorist incidents took place in the countries around us. The victims of these knife attacks were chosen at random, in quotidian and freely accessible locations, ostensibly with little preparation.

Incidents and arrests

Since the murder of Theo van Gogh in 2004 there had been no incidents in our country involving extremist and terrorist jihadists, until last year. In a number of incidents in 2018 the perpetrators likely had jihadist or radical Islamist motives for their (intended) actions.

On 5 May 2018 a Syrian man stabbed three people in The Hague. The Public Prosecution Service suspects the man – who suffers from serious mental illness – of attempted murder with terrorist motive.

On 31 August a stabbing incident occurred at Amsterdam Central Station, in which a 19-year-old Afghan man coming from Germany seriously injured two people. The man declared he wanted to avenge the fact that in spring PVV leader Geert Wilders had announced a cartoon contest on the prophet Mohammed.

A few days before that, at The Hague Central Station, a Pakistani man had been arrested, who had intended to attack the PVV leader for the same reason. The suspect targeted Geert Wilders because he believed the contest was an affront to the prophet. The Public Prosecution Service has charged him with preparation of an attack with a terrorist objective.

In addition there were several arrests of jihadists in the Netherlands. A cooperation between the AIVD and various international and national partners resulted in the arrest of three individuals in Rotterdam on 17 June. Two of them are suspected of preparing a terrorist attack in France. It is possible that they were also considering Dutch targets.

Perhaps the most notable incident in the Netherlands was the arrest on 27 September of seven jihadists. Our investigations had revealed that they were members of a jihadist network that originated in Arnhem, and that they were preparing a large-scale terrorist attack against a public event in our country.

The AIVD had been investigating persons involved with a jihadist network in Arnhem for some time already. These members were part of the core of the jihadist movement in the Netherlands. On 25 April 2018 we issued a first official report to the national public prosecutor for counter-terrorism on preparations by the group for an attack against a sizeable event. Their goal was to kill as many people as possible. It is a matter of grave concern that a segment of the jihadist movement in the Netherlands harbours the intention of carrying out a large attack against soft targets. The cell was apparently inspired by ISIS, but it seems very likely that it operated autonomously. The members were in touch with other jihadists in the Netherlands and abroad, but they never shared their attack plans with anyone outside of their own group.

Jihadist threat against the West

Today's jihadist menace is characterised by a constant threat of attack, ranging from fairly basic to more complex, in and against the West. Behind the attacks are global jihadist organisations like ISIS and al-Qaeda, smaller jihadist networks, and individuals. The incidents of the past year and the many arrests show that there is still a clear jihadist threat in Western Europe.

Threat posed by ISIS and al-Qaeda

Despite the collapse of the so-called caliphate and the loss of its territory, ISIS continues to be a threat. In 2018 the group claimed responsibility in Europe for attacks in Liège (Belgium) and in Trèbes, Paris, and Strasbourg (France). As a result of the caliphate's downfall and ISIS' diminishing military power, the group has become less attractive to jihadists.

Al-Qaeda too still desires to attack the West. In the past years the group has been able to work on strengthening its organisation in the shadow of ISIS. Networks and branches that are considered to be part of al-Qaeda are still focusing on attack planning against the West.

Threat of foreign terrorist fighters

There are two sides to the threat posed by foreign terrorist fighters. On the one hand there are those who still choose to remain with terrorist groups like al-Qaeda and ISIS in Syria and/or Iraq. They are in touch with their 'home base' in the West fairly regularly, thus contributing to the further assimilation of jihadist ideology in Western communities. They use these contacts to stimulate others to carry out or assist in attacks.

On the other hand we have seen significant numbers of fighters return from Syria and Iraq to Europe, including the Netherlands. Towards the end of 2018 their number was approximately 55. Their return is gradual, and concerns women, sometimes with children, as well as men. For each returnee, the Dutch authorities assess what kind of threat they pose. In late 2018 some 135 jihadists with a Dutch background were still with terrorist groups in Syria and Iraq.

The challenge faced by the AIVD – and the Dutch government as a whole – is how to establish the reason for someone's return. Are they disillusioned as a result of their difficult life there and did they flee because they yearned for the freedom of Dutch society? Were they traumatized by confrontations with, or their own participation in acts of violence? Will they get in touch with jihadists in the Netherlands and bring new impetus to the movement? Were they sent by the organisation there in order to provide support for or carry out an attack in the West?

Identified returnees are arrested and put on trial. We estimate that some of these jihadists will not renounce their ideology either during their incarceration or after their release. They could rejoin the jihadist networks that produced them or create new networks.

The Dutch detention system in which those suspected and convicted of terrorism are isolated from other detainees largely prevents that non-extremist prisoners could become radicalised and recruited by jihadists, which is something that has been seen to occur in other European countries. The Dutch system could, however, result in unwanted influencing within the group and the shaping of new networks. Furthermore, Europe will see the release of many detained jihadists in the coming years. The AIVD expects that detained and released (ex-)jihadists will constitute an important aspect of the threat picture.

The Dutch jihadist movement has over 500 members

The jihadist movement in the Netherlands is a dynamic whole of individuals and groups that adhere to the jihadist ideology. The movement does not have a hierarchy or a strictly defined structure.

Many jihadists are in touch with each other both online and in the real world. Many participate in activities as a group. Several groups are in contact with each other or with jihadist groups and individuals abroad. There are also jihadists that live their lives isolated from kindred spirits.

We include over 500 individuals in the group making up the jihadist movement in the Netherlands. Several thousand persons in our country sympathise with the jihadist ideology without actually being part of the movement.

The jihadist movement in the Netherlands is mainly pro-ISIS, but there are also jihadists that identify with al-Qaeda's line. In the past couple of years the movement focused mostly on the war in Syria and ISIS' caliphate. Over 300 jihadists left our country to go to the region. Now that the physical caliphate has ceased to exist, this particular focus has faded away. The movement has entered a reorientation phase, and now jihadists focus more on spreading their creed or ideology and extending their networks.

Whether the movement will grow or become more powerful, depends on several factors, such as the rise of new leaders, new sources of inspiration, or issues that could become a rallying cause reuniting the movement. It was the war in Syria that provided this momentum at the beginning of this decade. Even though the jihadist movement in the Netherlands has entered a reorientation phase, it still poses a threat, as evidenced by the arrests of the members of the network in Arnhem.

Unconventional attack means

In the past year the West saw a few instances of attacks in which unconventional attack means in the form of biological substances may have been involved, for example in Germany and Italy. We see that such knowledge is spread by including manuals for the manufacturing and use of chemical agents and biological poisons in propaganda material.

Activities and results

In 2018 we issued over 100 intelligence reports on developments in jihadist and radical Islamist terrorism. The public prosecution service received 35 official reports containing information pertinent to their criminal investigations. In addition the Immigration and Naturalisation Service (*Immigratie- en Naturalisatiedienst* – IND) received 8 reports, the Ministry of Foreign Affairs received 3 reports, and mayors received 2 reports on this topic. In 2018 we also published a report on ISIS and al-Qaeda in relation to the legacy of Syria.[1]

International threats demand an international response. International cooperation between partner services proved crucial in the fight against terrorism also in 2018.

Some of this cooperation is consolidated in the Counter Terrorism Group (CTG), a cooperation between the security services of the members of the EU, plus those of Norway and Switzerland. Our country is host to a platform where information on jihadist fighters is shared between the partners directly, which facilitates cooperation and contributes to gaining a better understanding of transnational and international connections. The cooperation strengthens our – and our partners' – access to intelligence. More concretely the cooperation has led to results in the early detection, identification, and arrest of potential jihadist attackers in Europe.

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

Radical Islam

The AIVD's investigation into radical Islam focuses on two types of threat. On the one hand there is the threat of further radicalisation towards (violent) jihadist ideology. On the other hand there is the threat an intolerant religious ideology poses to our

[1] 'Syria's Legacy. Global jihadism remains a threat to Europe,' AIVD, November 2018.

democratic legal order. As a phenomenon, the relationship between this ideology and our democracy is strained, but it remains (just) within national legal boundaries. Our investigation focuses mainly on certain key drivers within the Salafist spectrum.

Unwanted financial support from abroad

The AIVD investigates the financial support that Islamic institutes in our country receive from foreign countries, such as the Gulf States. This support can entail interference with ideological matters. If such foreign interference constitutes a threat to our democratic legal order, we follow it carefully, also cooperating in a European context.

Radical influences in education

The AIVD observes that radical Islamist inciters manage to create a very strong representation for themselves within the educational opportunities available to young Muslims. Examples are after-school classes in Arabic and Islam. Such school programmes are attractive also to students from more moderate backgrounds, as there are often very few or no alternatives for after-school Islamic education.

At first glance, such educational initiatives may appear fairly low-key and innocent. We believe, however, that such educational approaches can lead to children and young people becoming estranged from society or inhibited from participating in it, as a result of the intolerant and antidemocratic views represented by those who organize such initiatives. In the long run this could cause social cohesion to unravel, which would undermine our democratic legal order.

In the past, only a few established mosques and institutes were responsible for spreading such views, but today a much broader choice is on offer. A new generation of eloquent preachers has been schooled and begun to develop initiatives to spread their message. Also online we see that the target audience is within easy reach. Our investigation has revealed how some individuals have a dangerous influence in that they do not directly condemn the (violent) jihadist ideology. This could create a breeding ground for jihadism.

Activities and results

We issued 6 official reports and 12 intelligence reports on developments with regard to radical Islam.

In this area the AIVD cooperates with the NCTV, several ministries and local government. We use concrete examples to provide support for national and regional authorities in how to deal with this phenomenon, which has a strained relationship with our democracy but largely remains within the limitations of what is allowed by our legal system. In the past year we gave presentations on this topic to various municipal and other government partners.

For more information, go to aivd.nl/radicalisering.

Non-jihadist terrorist organisations

The AIVD notes that in 2018 the Kurdistan Workers' Party PKK did not have any intention to carry out attacks in Europe. The PKK's primary goal is to be taken off the EU's list of terrorist organisations, and use of violence would not be conducive to that plan. The organisation does have access to means for violent action, and it is able to mobilise PKK supporters in a very short time frame.

The PKK organised solidarity protests in Europe, including in the Netherlands, for the victims of Turkish military action in Afrin, Syria. Under the heading *#fightforAfrin*, arson attacks directed at Turkish targets in several European countries, Germany in particular, resulted in material damage.

The call for the attacks originated with a youth group that is not officially part of the PKK but that may have ties to the party.

Activities and results

Within the context of our investigations into non-jihadist terrorist organisations we issued 4 intelligence reports and 2 official reports in 2018.

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

Extremism

Extremism can be defined as actively striving for or supporting profound changes in society, changes that could endanger the (continued survival) of our democratic legal order. This could be through the use of undemocratic methods such as violence and intimidation, with detrimental effects for our democracy.

Although in general the central tenets of extremism are still largely aligned along a 'left' and 'right' divide, in practice this distinction is a lot harder to make. Certain convictions are rallying points that 'left' as well as 'right' find important. These often stem from a sense of discontent with or distrust of the government.

Public manifestations usually feature nothing more serious than civil disobedience, for example the protests against nature conservancy policies in natural park Oostvaardersplassen, and the extraction of natural gas in Groningen. Generally these protests do not go beyond activism, and as such they do not constitute a threat.

We do consider it conceivable that splinter groups or lone actors could become inspired by their activism to such an extent that they seek recourse in extremism. One of the tasks of the AIVD is to alert other authorities when activist anger turns into extremist action.

Hatred of the other, preference for own race

To some right-wing extremists, immigration is still equal to Islamisation, and both are threats to the survival of the Dutch national identity. These right-wing extremists perceive the influx of refugees from Islamic countries as a selling-out of Dutch culture by the government. A visible representative of such views is, for example, the Dutch identitarian group *Identitair Verzet*.

There are many who support this anti-Islam viewpoint, and it is no longer the exclusively male domain it used to be. The anti-government sentiments that are prevalent within this group also attract sympathisers that have no historical links to right-wing extremism. These discontents also harbour feelings of distrust towards (European) politics, and occasionally also towards science and the media.

It goes without saying that the AIVD does not consider criticism of Islam, immigration or the government as manifestations of right-wing extremism. Such things are, after all, within the limits of freedom of expression. We only consider such expressions as extremist if they cross over into hatemongering, intimidation, and threats.

Some extremists even advocate the prevention of racial mixing. This ethnic-nationalist ideology finds an audience among the supporters of the alt-right, such as the Erkenbrand Study Association (*Studiegenootschap Erkenbrand*). They state that they are not against the fact that there are many races in the world per se, but they believe the Netherlands is for the Dutch.

There are also extremists that are convinced of white supremacy. These persons have anti-democratic views and they strive for a racist society in which not all people are considered equal. This goes against national democratic principles.

Resistance to the 'causes' of migration

Traditionally also the left has resisted migration and asylum policies, but in their case because they consider these policies to be too strict.

Within the context of resisting migration and asylum policies we can see that the focus is shifting to defence contractors, companies that supply goods to the Ministry of Defence. The reasoning

behind this is: no defence contractors means less war, and less war means fewer refugees and with that fewer migration streams. Companies that provide materials to the EU's border and coast guard agency that is responsible for halting migration on Europe's exterior border are also considered beyond the pale. The left-wing group Anti-Fascist Action (*Anti-Fascistische Actie*, AFA) joined some of the non-violent protests against such companies.

More 'traditional' targets also continue to draw their share of attention, such as the people who draft and implement migration and asylum policies, the Immigration and Naturalisation Service, the Custodial Institutions Agency (*Dienst Justitiële Inrichtingen*, DJI) and building contractors responsible for detention centres. Compared to the previous years, protests against asylum policy have become less intense in the past year.

Identity-based ideology
A remarkable development in the world of activism and extremism is the fragmentation of ideologies, which leads people to fall back on personal identity. We find, for example, anti-racism activists that are organised on the basis of their own identity. They resist what they see as the Netherlands' colonial heritage and refuse the support of 'whites'.

Activities and results

On the basis of official reports by the AIVD, the Public Prosecution Service launched an investigation into an extremist who had plans to use violence against Muslims. The investigation resulted in a court conviction in early December 2018.

Within the context of our investigations into the area of extremism, we issued a total of 21 official reports and 8 intelligence reports. In October we published a public report on right-wing extremism, entitled 'Right-wing extremism in the Netherlands. A phenomenon in flux'.[2]

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

[2] 'Right-wing extremism in the Netherlands. A phenomenon in flux,' AIVD, October 2018.

Making the Netherlands a safer place

The previous chapters looked at threats to our national security and risks to national interests. We inform our partners with bespoke reports based on relevant information from our investigations. In doing so, we enable them to take responsibility for national security. We offer them perspective for action.

The AIVD itself only has limited possibilities for action. But an official report can offer the Public Prosecution Service enough information to launch its own investigation into activities that pose a threat to national security and that are liable to criminal proceedings.

Our information is also intended for ministries, executive agencies, mayors, educational institutes, as well as companies. In the latter case the information is particularly important when the companies play a vital role in our society, for example when they are active in energy supply or civil aviation. We want to advance the Netherlands' resilience by informing all of these organisations and, where possible, providing them with advice on threats that could affect them and consequently the Netherlands as a whole.

Countering the acquisition of knowledge and goods

Countries like Iran, Pakistan, and Syria target the Netherlands and other Western countries to obtain the knowledge and goods they need to further their weapons of mass destruction development programmes. In a joint AIVD and MIVD unit we investigate the ways in which these countries attempt to acquire such knowledge and materials and try to prevent this from happening. Also in the past year we extensively exchanged knowledge and information with our foreign partner services to achieve that goal.

We also cooperate frequently with Dutch parties that play a role in export control, such as Customs and the Ministry of Foreign Affairs, and we regularly receive requests for advice regarding export permits. On several occasions we informed the Ministry of Foreign Affairs of our own accord when we came across attempts to acquire goods or knowledge, usually in relation to the development or production of weapons of mass destruction or their means of delivery.

In addition we provide information to relevant parties regarding the risks of becoming involved in the acquisition of knowledge and goods that could be used for weapons of mass destruction (proliferation). By providing these parties with advice on how to identify suspect transactions, we have been able to detect and prevent several acquisition attempts.

In 2018 we issued 32 official reports to the Ministry of Foreign Affairs regarding proliferation and export control.

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

'Secure' people in essential positions

There are various areas and positions within our society where someone could be in a position to cause damage to our national security. These positions can be found with the government, the national police, and companies that are involved in vital processes, and the minister involved designates these as positions involving confidentiality.

We carry out security screenings to assess whether someone who has applied for or holds a position that is designated a position involving confidentiality can be issued a certificate of no objection (*Verklaring van geen bezwaar* – VGB).

These security screenings also enable the organisations in question to take responsibility for national security.

On 1 October 2018 the ministerial order on the Unit Security Screenings came into effect, creating the framework for the merger of the security screening departments of the AIVD and MIVD in a single unit (*Unit Veiligheidsonderzoeken* – UVO).[3] In anticipation of this cooperation, the MIVD and the AIVD coordinated their security screening policies as of March 2018.[4] That year also saw the first steps towards unifying the work processes of both organisations. The idea behind the merger is: one policy, one system, one location.

Also in 2018 the online service for filing personal information in relation to requests for security screenings (*elektronisch Opgave Persoonlijke Gegevens* – eOPG) became operational for part of the participating employers. For now this system only handles screenings by the AIVD, and for this group the process has become entirely digital. The system processes requests for security screenings by employers and the personal information provided in that regard by the prospective employees, who log into the secure environment using their national ID.

In 2018 the AIVD and delegated partners (the National Police Service and the Royal Netherlands Marechaussee) carried out almost 44,000 security screenings of persons who have applied for or hold a position involving confidentiality. This number is almost the same as 2017's number of screenings (over 45,000).

The AIVD operates on the premise that 90 per cent of all security screenings by the AIVD should be completed within the maximum statutory period of 8 weeks.

With a completion rate of 89 per cent, we all but reached our stated goal. The main reason for not quite obtaining the 90 per cent is the substantial increase in requests for security screenings. In 2018 the AIVD completed almost 20 per cent more screenings than in 2017. The increase is almost entirely due to demand from the civil aviation sector.

Additionally our preparations for the arrival of the joint Unit Security Screenings required manpower.

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

Reporting at the request of others

In addition to security screenings, we also perform another kind of screening as part of our official tasks, namely reporting on the information we hold on a particular person. This is done, for example, at the request of the Prime Minister when a new member of government is to be appointed.

This reporting on information in our own systems was not an explicit task in the Intelligence and Security Services Act of 2002; with the adoption of the 2017 Act, this has become a separate task.

In 2018 we carried out 31 checks and reported on the results in official reports to the authorities involved.

For more information, go to aivd.nl/naslag.

Role in the Dutch Safety and Security System

Like the MIVD, the National Police Service, and the NCTV, the AIVD plays a role in the Dutch Safety and Security System. This system aims to ensure that public figures such as politicians, members of the Royal Family, diplomatic representatives, and international organisations can perform their

[3] Ministerial order concerning the tasks of the Unit Security Screenings, *Staatscourant*, no. 53581, 28 September 2018.

[4] Policy rule Security Screenings, *Staatscourant*, no. 10266, 21 February 2018.

duties without being intimidated or obstructed. The essence of this system is that it not only looks at concrete threats posed by jihadist terrorists or right-wing and left-wing extremists, but that it also focuses on conceivable threats. We provide the NCTV with risk and threat analyses and threat assessments to enable them to decide on implementing security measures where needed.

In the past year we provided 1 risk analysis, 10 threat analyses, and 51 threat assessments within the Safety and Security System.

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

Information security

Part of the AIVD's expertise is advising the government on the security of confidential and secret information. We also develop means to keep such information secure.

One of our contributions to improved information security is to draw up a national cryptography vision and strategy, which found a start in 2018 in cooperation with other departments. This programme also involves input from the corporate world and knowledge institutes. This cryptography vision and strategy also describes how cryptographic security measures for the protection of sensitive information will be made available in the future.

The AIVD's National Communications Security Agency (*Nationaal Bureau voor Verbindingsbeveiliging* – NBV) provided many oral presentations to interested parties in the past year. In addition, 44 written threat information products were issued in 2018.

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

A new Act

On 1 May 2018 the new Intelligence and Security Services Act came into effect. The new act is an outcome of the 2013 Dessens report, in which one of the conclusions was that the old act, dating back to 2002, needed to be brought up to date.[5] Modern powers were needed if the service was to be able to continue to fulfil its tasks. The act also provides improved privacy safeguards.

Modern powers

The 2002 Intelligence and Security Services Act did not factor in the speed of development in the world of technology. These days everyone uses internet applications for most of their communication and data exchanges. This immense amount of data crosses the world at amazing speeds. The old Act only provided us with access to this cable data traffic on the basis of a selector for a specific person or organisation.

The essence of the AIVD's work is to make unknown threats visible. Without access to digital data streams it would not be possible to detect new threats. For example: when we know that the Netherlands is regularly subject to cyberattacks from a particular part of the world, and we find out the route these attacks take, we can investigate that data stream for the known features or characteristics of the attack. That way we can establish the target of the attack much sooner, without having to wait for the malicious software to reach the target and cause damage.

The technical preparations for this kind of investigation-specific interception are extensive and ongoing, so that in 2018 we did not yet make use of this new investigatory power.

Fitting safeguards

Internet technology has also greatly boosted data traffic quantities, and resulted in many concurrent and intertwined data streams. This could potentially cause a greater invasion of more people's privacy.

In case of investigation-specific interception and investigation of particular data streams there is a risk, for example, that we may intercept traffic from persons that have no nefarious intentions whatsoever. Intercepted data that is not relevant to our investigations is destroyed immediately. This applies to approximately 98 per cent of acquired data.

Under the previous act from 2002, many special investigatory powers required the authorisation of the Minister of the Interior and Kingdom Relations. Under the new act, the exercise of special investigatory powers requires not only the authorisation of the Minister, but also an independent prior review by the Investigatory Powers Commission (*Toetsingscommissie Inzet Bevoegdheden* – TIB). Furthermore the new act also prescribes stricter data retention limits than its predecessor.

At the advisory referendum on the new act, held on 21 March 2018, 49.4 per cent of voters voted against the law, and 46.5 per cent were in favour.

Following the referendum, the government decided there should be additional guarantees to honour the outcome of the vote. One promise was that the assessment memorandums underlying international cooperation with foreign partners were to be finished before the term stipulated in the Act (1 May 2020), namely before 1 January 2019. This pledge was fulfilled and now there is an assessment memorandum for each of the services we cooperate with. The memorandum provides reasoned discussion on the extent to which a foreign partner service and foreign country meet the legal criteria for cooperation and what this means for our cooperation with them.

[5] 'Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002', 3 December 2013.

We will also renew our request for ministerial authorisation annually where extending data retention for data acquired by investigation-specific interception is concerned. The original act did not stipulate any such interim assessment. We will now have to provide reasoned arguments why we want to retain the data in order to assess its relevance at a later date. The data will in any case be destroyed after three years, with the exception of data that has been found relevant to our investigations.

A policy regulation is being drafted that requires that any request for the exercise of a special investigatory power not only discusses the requirements of necessity, proportionality, and subsidiarity, but also explicitly states how we intend to exercise this power in a manner that is 'as directed as possible'.

The government believes that for the coming years investigation-specific cable interception can mostly be ruled out where communications originating in and destined for the Netherlands are concerned. The exception here is any investigation into cyberattacks that exploit and abuse Dutch digital infrastructure. In that case investigation-specific interception could be necessary to detect and identify such a threat.

The processing of medical data is only allowed supplementary to other data processing, i.e. when someone is already the subject of an ongoing investigation and medical records provide the final piece of information needed by the AIVD to perfect its threat assessment. Should the AIVD come across medical information that we are not allowed to consult, we will delete that information immediately.

Sharing data concerning a journalist with foreign services always requires thorough consideration, also taking into account an individual's function and the protection of that person's privacy and safety. In case information on a journalist is found to be included in the acquired data, the services will not share that data, unless absolutely necessary for national security.[6]

Impact on our work

The acquisition and processing of data are at the core of our work. The new act and the additional safeguards for citizens, in the form of independent oversight and stricter data retention limits, meant that more effort was required.

As this annual report shows, geopolitical developments and national threats also asked for a great deal of effort on the part of our employees. Combining the implementation of the new act with the unabated necessities of our operational obligations has proven to be a difficult task. The impact of the implementation has turned out to be greater than originally estimated. It took some time to get used to the new procedures for prior approval from the TIB. In a progress report issued by the TIB in November, it stated that the commission had to turn down approximately 5 per cent of our requests for authorisation.[7]

Moreover, after the new act had come into effect, the Oversight Committee for the Intelligence and Security Services carried out and issued a benchmark report at the request of the government. This critical progress report came out at the beginning of December 2018, and it provided a first insight into the implementation of the new act.[8]

The CTIVD enquiry focused on elements related to the updated special investigatory powers, such as duty of care, responsible data reduction, and investigation-specific interception (including automated data analysis). The committee also looked at the other parts of the new law that

[6] Letter to parliament with reaction to advisory referendum on the Intelligence and Security Services Act, dossier 34588, no. 70.

[7] Progress report by Commission for the Review of the Exercise of Investigatory Powers; TIB, 1 November 2018.

[8] Progress report by the Oversight Committee for the Intelligence and Security Services on the implementation of the new Intelligence and Security Services Act 2017; CTIVD, 4 December 2018.

concentrate on protection for citizens. In that regard the CTIVD looked into the possibilities for filing a complaint or reporting wrongs.

In its progress report the CTIVD indicated on which topics the services risked running afoul of legal requirements. The opinion was based on the policies and procedures as planned and implemented at that time, and no actual unlawful operations were reported.

In its report the committee also described that many parts of the new act are highly complex, for example the principle of data reduction, i.e. the destruction of data that has been found irrelevant. The data reduction principle requires a systematic approach and its technical implementation needs modifications.

The TIB and CTIVD reports were a signal that prompted us to set the implementation of all aspects of the act as our priority for 2019, in addition to our primary tasks. Our goal is to see significantly fewer risks being signalled in future reports.

For more information, go to aivd.nl/nieuwewiv.

Appendix: Facts and figures

Table 1: Number of completed security screenings by the AIVD and delegated partners

Screening	Positive	Negative	Total
Level A, by AIVD	2003	17	2020
Level B, by AIVD	4294	65	4359
Level C, by AIVD	723	10	733
Level B, taken over by UVO from KMar, National Police, Surveillance and Protection Department	2484	942	3426
Screenings by the AIVD	9504	1034	10538
Level B, delegated to KMar, National Police, Surveillance and Protection Department	33096	-	33096

Table 2: Results of objections and appeals against security screening decisions.

	Dismissed	Upheld	Inadmissable	Total
Filed objections	-	-	-	103
Ruling on objection	30	24	4	58
Ruling on appeal	1	2	0	3
Ruling on second appeal	4	2	0	6

Table 3: Complaints about the AIVD to the Minister of the Interior and Kingdom Relations.

Under consideration as of 1 January 2018	4
Received	18
Dismissed	6
Upheld in part	0
Inadmissible	3
Withdrawn	1
Handled informally to the satisfaction of the complainant	8
Still under consideration as of 31 December 2018	4

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

Table 4: Reports of suspicions of wrongdoing on the part of the AIVD.

2018	0

For more information, go to aivd.nl/misstanden.

Table 5: Requests to inspect information held by the AIVD, by nature or subject.

	Under consideration as of 1 January 2018	Submitted	Reviewed	Granted	Under consideration as of 31 December 2018
Information concerning applicant	109	130	102	37	137
Information concerning deceased relative	20	52	31	19	41
Information concerning a third party	13	16	27	2	2
Information concerning administrative matters	13	39	31	5	21
Totaal	**155**	**237**	**191**	**63**	**201**

Table 6: Results of objections and appeals against decisions on requests to inspect information held by the AIVD.

	Reviewed	Dismissed	Upheld	Inadmissible	Withdrawn
Objection	126	104	22	0	0
Appeal	27	2	3	22	0
Second appeal	14	0	3	11	0

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

Table 7: Number of notifications.

2018	29

For more information, go to aivd.nl/notificatieplicht.

Table 8: Number of CTIVD reports on the work of the AIVD.

2018	5 (nos. 55, 56, 57, 58 and 59)

For more information, go to aivd.nl/toezicht.

Table 9: Number of wiretaps pursuant to Art. 25 of the Intelligence and Security Services Act 2002, and Art. 47 of the Intelligence and Security Services Act 2017.

2018	3517

For more information, go to aivd.nl/taps.