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

ANNUAL REPORT
2012

Per undas adversas

Louis Einthoven, the first head of the National Security Service (Binnenlandse Veiligheidsdienst, BVD), the predecessor of today's General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD), was responsible for the service's motto and shield. He believed that citizens in a democracy such as ours must play an active role in society, and not just passively drift along on the waves of history.

The motto he chose was *Per undas adversas*; against the current. Living fish swim against the current; only the dead ones are carried along. This saying symbolises the service's mentality; it is an active organisation, working against the current if necessary, watching out for threats to national security.

The Cabinet has been in office for six months now, and this is also the period of time for which I have had political responsibility for the AIVD. This annual report describes the activities carried out by the service. On reading previous annual reports, I realised that the service is much more open about its activities than I had thought; in this report you can read about several countries that the AIVD is focusing on, the activities that are being developed, and – without going into technical details – the resources that are being deployed for these activities.

The information obtained serves to increase national security, and is in principle confidential, as is all the operational information regarding the activities pursued to obtain this information. For this reason I cannot give an account in this foreword of everything that has come to light during the previous year, as I would for other government services. However, on the basis of the reports that I receive several times a week, I can say this: the existence of the AIVD is crucial to national security, and as a result of its activities, many serious problems and crises can be prevented. You can read more about this in general terms further on in this report. And some cases have indeed been made public, such as the recent arrest of three terrorists in possession of explosives, weapons and farewell videos, and the recent sharp increase in the flow of jihadist travellers to Syria.

These results can only be obtained through the commitment and expertise of those who work for the AIVD. These people deserve special attention. For those who do other kinds of work, it is difficult to understand what it is like not to be able to tell anyone other than your colleagues what you do. Everything is on a strict need-to-know basis, and therefore it is better that even your partner does not know in detail what you do every day, let alone friends at the café or the sports centre. Whenever I pay a working visit to the AIVD, I am always struck by the high level of motivation of the people who work for the service. I myself have worked in the international scientific community for 25 years, and the general atmosphere at the AIVD

reminds me of that community; I would describe the AIVD as: intrinsically motivated people, experts in their field, enthusiastic about their work, dedicated colleagues, and utterly convinced of the importance of their work. Since access to the AIVD's premises is highly restricted, the public cannot express its interest and appreciation to these people, so on behalf of everyone, and through this channel, I offer my respect!

In conclusion, the government has decided not to proceed with the proposed cessation of foreign intelligence gathering in the coalition agreement, since this activity is an integral part of national security. This has again been illustrated recently by the information gained about the rapid increase in people travelling to the conflict in Syria, as mentioned earlier. Intelligence work is carried out partly at home and partly abroad, and partly in close co-operation with foreign services.

Sometimes these activities lead to the detainment of travellers; however, if young people return to the Netherlands, possibly traumatised by their participation in – or witnessing of - extreme violence, or if they have been trained to carry out violent actions and have become ideologically hardened and strengthened, they can form a real threat to security in the Netherlands or elsewhere in Europe. Without its foreign intelligence activities the service would not be able to promote and protect the national security of the Netherlands to the extent that is now possible.

I wish to thank the whole staff of the AIVD for their huge commitment during the past year, and on this occasion I do so on behalf of all Dutch people who can feel safe, or at least safer, as a result of their efforts.

dr. Ronald Plasterk
Minister van Binnenlandse Zaken en Koninkrijksrelaties

foreword

AIVD: INTELLIGENCE AND SECURITY ON THE MOVE

To the untrained eye, the threats and risks in today's world are not always visible, even though they could have serious consequences for society and the economy. In the next few years, they will become increasingly diffuse and unpredictable as a result of internationalisation and advancing technology. With its knowledge and expertise – in other words, with a trained eye – the AIVD strives to identify and draw attention to these threats in good time, so that policymakers at the various levels can take appropriate action.

For these reasons, the AIVD continues to be one of the key players who are making efforts to ensure the security of Dutch society and Dutch interests at home and abroad. We do this by exercising our special powers, by the application of technical resources, and by using our access to information from a network of international co-operation between foreign intelligence and security services. The combination of a security service and an intelligence service not only gives the service a special position in this international network, it also enables information from various sources to be linked more rapidly, increasing the strength of our analysis and interpretation. In this way, the AIVD can continue to be effective and work more efficiently in its role of protecting national security. As has also become evident from the Davids Committee report, the ability to conduct our own investigations and make independent assessments is essential for our ability to determine national policy and the political stance of the Netherlands.

The area of operation of the AIVD appears to be continually expanding. We are seeing the progressive development of a stronger interrelationship between threats originating abroad and domestic threats. We are also seeing how the division between internal and external security is becoming blurred by the ever-growing internationalisation of politics, social affairs and the economy. New technological applications are being developed at a rapid rate, and form a significant driving force behind new and more diffuse threats.

In addition to jihadist terrorism and radicalisation in groups, there is still the risk of violent lone individuals who apparently strike out of nowhere. Cyber attacks and cyber espionage are occurring regularly, and are becoming even more complex and ingenious. The nature, scale and form of the threats are changing very rapidly and unpredictably.

In order to deal with these trends and developments, it is important to maintain the co-operation between partners, themes and instruments at a high level, nationally but also internationally. In accordance the AIVD continued and intensi-fied its co-operation with the Military Intelligence and Security Service (*Militaire Inlichtingen en Veiligheidsdienst*, MIVD) in 2012. The collective unit focusing on cyber and Signals intelligence has now taken shape. This unit combines the strengths of both services in this area. It also forms a strong basis under our commitment with the various partners in the National Cyber Security Centre (NCSC) for the purpose of dealing with digital attacks in all forms.

With regard to terrorism and radicalisation, we work closely with the National Coordinator for Security and Counterterrorism (*Nationaal Coördinator Terrorismebestrijding en Veiligheid*, NCTV) and the National Police, especially with the Regional Intelligence Services (*Regionale Inlichtingen Dienst*, RID).

At the same time, an obvious dilemma has become visible. While the economic situation requires cuts in spending, developments in the threat level require investments that will enable the government to strengthen its ability to anticipate threats.

In 2012 the AIVD also faced a difficult mandate in the coalition agreement. The service's budget is to be reduced at a rate rising to a permanent 38% from 2018 onwards. The implementation of this reduction is still being developed, but it should be clear that this will have radical consequences for the service's effectiveness.

Intelligence work involves, above all, the work of individuals: it requires knowledge, expertise and skills. Our officers are well trained and equipped. The Netherlands has to be able to rely on the AIVD. For this reason, our staff conducted investigations on terrorism, extremism and radicalisation, espionage and proliferation in 2012. We produced countless official reports and intelligence briefings to ensure that the Public Prosecution Service, the police and local and national government were well informed and could take action where necessary, which enabled them to avert risks and threats.

We gathered intelligence in and on foreign countries to provide the Dutch government access to information it cannot obtain by other means. We performed thousands of security scree-nings, completed dozens of threat assessments and advised the government in the field of information security. We also worked to increase security awareness within the government and in the vital sectors.

And we will continue to do so!

Rob Bertholee
Head of the General Intelligence and Security Service

contents

2012 IN BRIEF

At first sight, the Netherlands would appear to be a safe place, with only limited manifestation of physical threats and risks.

There are, however, new threats that are occurring, and due to its international orientation the Netherlands is as dependent as ever on global and regional developments, including those in the field of security. The Netherlands strives to pursue an effective and sustainable security policy by means of an improved combination of partners, themes and instruments.

An accurate understanding of developments in the context of national and international security is therefore needed. Based on the collective studies by the AIVD (*Multi-year outlook by the AIVD, Meerjarenperspectief AIVD*), Defence (*Defence Surveys, Defensieverkenningen*), Foreign Affairs (*International Security Strategy, Ministry of Foreign Affairs, Internationale Veiligheidstrategie BZ*) and Security and Justice (*CT strategy VenJ, CT-strategie VenJ*) one can state that there are actually three major trends that are occurring. These are the advance of technology, internationali-sation, and the growing diffuse nature of the threat picture. These trends are closely interrelated.

The most important trend concerns the development taking place in the fields of information, communication and techno-logy. This development is enabling both state and non-state actors to exercise influence without requiring their physical presence. The removal of physical barriers leads to continuing internationalisation of the security area, since those of like mind throughout the world can easily make contact with each other. This leads to an increasingly diffuse and more unpredic-table threat picture.

Because of their diffuse nature, the response to the develop-ments mentioned in 2012 requires intensive collaboration between the various players in the security field. This collabora-tion will be pursued with national partners such as the NCTV, the Ministry of Foreign Affairs, the MIVD, the Public Prosecution Service, the national police force and local government.

In an international context, the AIVD continues to cooperate closely with the intelligence and security services in other countries.

In order to be able to anticipate and understand this diffuse threat picture, a combination of traditional methods, such as the use of human sources, with newer techniques such as the random interception of information flows, including those that are cable-linked, is an absolute necessity for the AIVD.

Cyber threat

The AIVD has been observing an increase in cyber attacks that form a threat to national security.
Until now, these threats have mainly consisted of cyber espionage by foreign powers. The Netherlands is one of the world's top five most competitive knowledge-based economies, and has the ambition to strengthen this position. For this reason, and due to its open society and excellent ICT infrastructure, our country is an attractive target for economic and technical-scientific espionage. Adequate protection against this cyber threat is of the utmost importance.

In 2012 the AIVD identified many electronic espionage attacks, originating from countries such as China, Russia and Iran. In future, these digital attacks will increase, and become more effective. Cyber security is essential to keep our economy and society running. In order to avert the threat of cyber attacks, co-operation between government organisations is needed. In 2012, the AIVD further extended its cooperative relationships with the Military Intelligence and Security Service (MIVD) and the National Cyber Security Centre (NCSC).

The AIVD supports government organisations in the detection of complex digital attacks against the ICT network. The AIVD has also given presentations for policymakers in government and in business to raise their awareness of the risks that are present. The AIVD has been advising the national government regarding the security aspects of using personal smartphones and tablet computers for work purposes.

Jihadist terrorism

In the latter months of 2012 the AIVD noted a large increase in the number of jihadists travelling to Syria. Extensive media and internet attention for the conflict in Syria and the easy accessibility of the country explain the large numbers of jihadist fighters that have travelled from the Netherlands to Syria. Dutch jihadists who travel to foreign conflict areas constitute a risk on their return to the Netherlands. They will, after all, have acquired skills, including combat skills, and contacts while abroad, and they may also have been traumatised.

In 2012 the AIVD also disrupted plans of suspected jihadists to undertake travels abroad. For these operations the AIVD cooperated with and provided information to a number of strategic partners, including the Public Prosecution Service, the National Investigation Service (*Nationale Recherche,* NR) and the Immigration and Naturalisation Service (*Immigratie- en Naturalisatiedienst,* IND). A number of persons were detained, based on official reports submitted to the Public Prosecution Service. Internet is playing an increasingly important role in jihadist terrorism. Professional propaganda and the exchange of views between jihadists on the Internet are progressively inspiring jihadists around the world to take action, whether

violent or otherwise. This dynamic interaction can be compared to a virtual marketplace where jihadist supply and demand meet each other. A significant proportion of the frustrated plots to attack Western targets in the last four years feature a prominent virtual component. With the publication of '*Jihadism on the Web, A breeding ground for Jihad in the modern age*' in 2012, the AIVD explains how the Internet is used by jihadists.

Furthermore, jihadist terrorism includes the intention of conducting a cyber jihad in which digital tools can be deployed against opponents of Islam. The AIVD currently estimates the jihadist movement's potential in digital terms as being limited.

Radicalism and extremism

In recent years a number of radical-Islamic activist movements have attracted attention in the Netherlands. These movements can have a polarising effect, because they encourage anti-democratic and intolerant views. Through these views and the ambivalent attitude of these movements towards violence, they also create a climate in which the use of violence becomes more acceptable. The readiness for action and the organisational abilities of the movements in the Netherlands are subject to change. For instance, in the latter months of 2012 Shariah4Holland more or less ceased to organise publicly visible activities. However, behind the scenes, individual key members of Shariah4Holland were involved in jihad travel to Syria.

Opposition to the Dutch and European policy on asylum and immigration in left-wing extremist circles increased in 2012.

This is mainly due to the definitive start of the No Border Network, in which activists and extremists have joined forces in order to encourage co-operation and coordination. Besides the familiar action groups, there were other - including some new - groups active, which for example offered direct aid to refugees on the street. Some anti-fascist groups also focused on opposition to the asylum and immigration policy.

A study by the AIVD into right-wing extremism shows that the splintering, fragmentation and general disunity among Dutch right-wing extremists increased further in 2012. There are still a few active right-wing extremists, although most of these people participate in social activities without any immediate ideological purpose.

Clandestine activities by foreign powers

Technological developments are lowering the threshold of access to sensitive and valuable information. The cyber espionage threat to national and economic security is serious and is continually increasing. In order to address this threat, the AIVD invests in international co-operation with its counterparts and in expansion of its capacity and expertise in research into cyber espionage.

In addition, foreign intelligence and security services also use classic forms of espionage.

The recruitment and deployment of human sources is a crucial element in the activities of foreign intelligence services, not only to aid in information gathering, but also to influence migrants in our country.

In early 2012, a Dutch man, accused of passing state secrets to the Russian secret service, was arrested on the basis of an official report from the AIVD . In addition, Visa applications by known intelligence officers were refused, on the advice of the AIVD. To support the government and vital sectors in dealing with espionage risks and in strengthening their defences against these risks, an e-learning module has been developed, in co-operation with the NCTV, which is based on the Vulnerability Analysis on Espionage in the Netherlands, KWAS (*Kwetsbaarheidsanalyse Spionage*, KWAS) conducted in 2010.

Security promotion

The AIVD promotes the deployment of security measures for persons, objects, services and events for which the national government has special responsibility. Diplomatic representations were confronted with incidents in the form of telephone threats, vandalism or attempted vandalism, and demonstrations. By providing specific information regarding known and conceivable threats, the AIVD enabled the National Safety and Security Coordinator (*Coördinator Bewaking en Beveiliging*, CBB) to take appropriate security measures for diplomatic representations in our country that were confronted with violent and non-violent actions.

The AIVD also promotes measures to protect confidential data vital to national security. In view of the growing threat of cyber

attacks on targets within the public administration, the Dutch government needs to protect its sensitive information against attacks by hostile parties and foreign state actors. The AIVD advises the government regarding preventive measures - secure products and security architectures - and on detection and response.

Thanks to advice from the AIVD, ministries and government-wide ICT service centres are better equipped to protect their territorial, physical, economic and political interests.

Intelligence gathering abroad

International relations are changing due to the rise of new political and/or economic powers. New powers sometimes protect their interests in an aggressive manner, particularly with regard to the security of energy provision and the acquisition of scarce commodities and high-level technology and expertise. These developments cause tensions between states and within regions, which can in turn influence and destabilise other countries or regions (for instance, due to migration or political pressure). In particular the regions on Europe's borders - North Africa and the Middle East - are progressively characterised by unstable regimes and a growing threat of terrorism.

The direct power and influence of the Netherlands in the world is limited, so a stable and well-functioning international legal system is very important to our country. The Netherlands is indeed a country with a strong international orientation and is therefore dependent on developments in other countries, which have a direct and an indirect effect on security in the Netherlands.

The Dutch vital infrastructure functions only as part of global networks, and our economy runs on raw materials that are not available in our country.

To be able to follow and identify the complex and interrelated developments in the world, the use of an intelligence service like the AIVD is one of the instruments available to the Dutch government in the formulation of its foreign policy. The AIVD provides information that was not available through normal diplomatic channels. In 2012, this included information on developments in the Arab world, especially Egypt and Syria, and changes in the political landscape in that region. Together with the MIVD, the AIVD also informed the government regarding the proliferation and production of weapons of mass destruction. The Dutch government is supported in the proper fulfilment of its duties regarding export controls by means of official reports. The AIVD produced several intelligence reports on developments affecting the security of energy provision in the Netherlands. The AIVD/MIVD furthermore informed the government on developments in the security situation in the Dutch Caribbean.

Organisational development

The AIVD's organisation must continue to develop in order to closely monitor today's trends of technological advance and internationalisation. In addition, the AIVD faces a progressively diffuse threat picture in the areas of its investigations. In this context, an intelligence and security service must have a complete range of tasks, powers and resources: a unique mix of capacities. The formation and maintenance of such a combination of capacities and the intelligence position obtained requires much time and long-term investment.

Governments need to be able to take advantage of the rapid changes in the digital infrastructure and the continuing addition of new communication channels: discussion forums, social media, cloud computing. Terrorists, extremists and intelligence services in other countries make use of these communication channels, and protect their communication with ever more sophisticated encryption. This makes it easier to hide activities from the eyes of investigative agencies and intelligence and security services.

These developments in digital technologies and the increasing volume of data flows ('big data') require permanent investments in materials as well as in knowledge and expertise. In 2012 the funding drive undertaken in recent years was continued. Expenditures made included those for the interception, management, processing and editing of large information flows. With these investments, the AIVD's intention is to initiate and expand strategic co-operation with national and international partners.

As a result of these expenditures, the costs of managing the ICT facilities have risen, and will continue to account for a substantial proportion of the budget in future. Since the entire process of gathering and processing intelligence by the AIVD is a state secret, the highest standards apply where information security is concerned.

Security screenings

In 2012 the AIVD completed 94% of all directly requested A-, B- and C-screenings within the statutory processing period of 8 weeks.

With regard to the conducting of security screenings for positions involving confidentiality, in 2012 the AIVD established a more selective policy in this area, so that only those positions involving a potentially serious and conceivable threat to national security are subject to investigation.

National and international co-operation

The ever-increasing level of internationalisation and the speed of technological developments demand good co-operation with national partners and foreign intelligence, security and Sigint services.

In 2012 the AIVD devoted efforts towards the extension and deepening of its co-operation with a number of trusted foreign services. These efforts have resulted in an increase in volume and added value with regard to the exchange of intelligence, operational collaboration and co-operation in the field of technology development, and in the exchange with foreign services.

The existing cooperative relationship with the MIVD in the field of counter-proliferation and with respect to the Caribbean region were continued. There was also close co-operation and collective reporting on specific developments in the Arab region.

In addition, the AIVD and the MIVD made essential progress on the formation of the collective unit Symbolon, which focuses on Sigint and cyber-related intelligence.

The strengthening of cyber security is a shared responsibility of many parties in society, since it is a complex and sizeable task. For this reason, this is an area in which government, business and science work together. This co-operation has led to the formulation of the National Cyber Security Strategy, and the collaboration has taken practical form within the NCSC. The AIVD and the NCSC support each other in such areas as knowledge, detection of digital attacks and situational awareness.

During 2012, the more intensive co-operation with partners in the security field involved the strengthening of relations with the RID and Special Services (*Bijzondere Diensten*, BD). The RIDs and BDs (such as the BD of the Royal Military Constabulary (*Koninklijke Marechaussee*, Kmar), the Intelligence Assistance Team of Customs and the Fiscal Information and InvestigationService (*Fiscale inlichtingen- en opsporingsdienst*, FIOD) are the eyes and ears of the AIVD in the Netherlands. Moreover, the AIVD has also made a substantial contribution to the composition of the National Terrorist Threat Assessment (*Dreigingsbeeld Terrorisme Nederland*, DTN) that the NCTV publishes three or four times a year.

AIVD operating area versus budget

Since 2002 the AIVD has been given new tasks, existing tasks have been significantly expanded, and expectations with regard to its results have grown. The intelligence and security domain of the AIVD has substantially increased, and the budget has grown accordingly. The creation of such a multi-source service and the related intelligence position requires much time, but the investments are now beginning to pay off.

The trends mentioned, such as technological development, internationalisation and the increasingly diffuse threat picture are broadening the AIVD's domain. The budgets available, however,are subject to demanding cuts. The Minister of the Interior and Kingdom Relations (*Minister van Binnenlandse Zaken en Koninkrijksrelaties*, BZK) has undertaken to inform the House of Representatives in the spring of 2013 with regard to the practical implications of the budget cuts.

CYBER THREAT

More and more frequently, threats to national security involve a digital component. Internet technology is being used in various ways to undermine national security. Vulnerabilities in computer systems are being exploited. Digital attacks are becoming more numerous, more complex and more effective.

The Internet has been used for espionage activities by other countries for some time. Jihadists can also form a cyber threat to national security. In 2012 there were no digital attacks by jihadists in the Netherlands that could be identified by the AIVD as constituting a threat to national security . The AIVD currently estimates that the digital potential of these jihadists is limited. Increased ambitions, and the possibility that jihadists may develop additional capacity, are, however, a reason for the AIVD to keep a close watch on developments in cyber-jihadism.

Economic and social interaction in our private lives and in business and government is increasingly dependent on Internet-linked systems and networks that enable the exchange of information, goods and services worldwide. In addition, the Internet is – to an even greater extent than before - supporting the management processes of vital infrastructure, such as banking, the electricity network and water and sewage management. These systems are all essential for daily social life. Dependency on Internet creates opportunities, but also threats.

The effect of digital attacks on national security and the economic wellbeing of society can be very serious. The continuity of essential processes can be interrupted, or vulnerable information can be siphoned off without this being noticed. It is difficult to state the damage caused by digital attacks, but it amounts to approximately several billions of Euros.

The role of the AIVD in the strengthening of cyber security

Basic principle:
National security is the first priority

Areas of attention for the AIVD
- *social disruption*
- *espionage*
- *terrorism and extremism*

Our cyber activities
- *investigating digital attacks*
- *gathering intelligence*
- *detecting digital attacks*
- *increasing resilience*

Implementation by means of
- *a special combination of duties and powers:*
  - *special powers*
  - *unique information from foreign partner services*
  - *protection of sources, methodology and knowledge level*
  - *combination of substantive knowledge and technical expertise*

- *co-operation*
  - *MIVD*
  - *National Cyber Security Centre*

Strengthening the digital security in our country is one of the biggest challenges facing government and business today. Cyber security (digital security), is essential in ensuring that the Dutch society and economy is able to continue to function.

The growing use of online services for the creation, exchange or storage of data (cloud computing) increases the risk of cyber espionage by other states, which can intercept large amounts of data at many different locations in the digital infrastructure in a short period of time.

It is often difficult to identify attackers, because they can successfully camouflage their actions, operate anonymously and encrypt data. The involvement of other states in these types of attacks is often difficult to prove, resulting in a lower risk for the attackers. Furthermore, technical developments are proceeding at a rapid pace. In 2012 the AIVD invested heavily in order to keep pace with the frontrunners in this race. The result is that capacity for digital investigations has been increased, in manpower and expertise as well as technical resources.

2.1   Activities of the AIVD

The strengthening of cyber security is a shared responsibility of many parties in society, since it is a complex and sizeable task. For this reason, government, business and science work together in this area within the National Cyber Security Strategy. This collaboration has taken practical form in the National Cyber Security Centre. The service and the NCSC support each other in areas that include knowledge, detection of digital attacks and situational awareness. This last term means that effective decisions can be taken because an

adequate description of an existing situation, the surroundings and potential developments can be provided.

In addition, the AIVD collaborates closely with the MIVD in the established unit which focusses on Sigint and cyber-related intelligence. Both services take the view that the level of cyber security in the Netherlands can only be strengthened through a concentration of technical know-how and specialist resources.

The AIVD makes its own specific contribution in the fight against cyber threats.
- Under the Intelligence and Security Services Act (*Wet op de inlichtingen- en veiligheidsdiensten*, Wiv) 2002 the AIVD has special powers at its disposal. This allows information regarding a certain threat to be gathered through the deployment of technical tools or human sources.
- The AIVD has extensive expertise in the area of ICT, with respect to both the application of digital intelligence tools in its own investigations and the detection of threats. This increases it's resilience to these threats.
- Due to the areas in which it operates, including espionage, terrorism and extremism, the AIVD possesses extensive knowledge regarding these phenomena, enabling it to quickly identify the intentions and originators of cyber attacks.
- The AIVD has a large network of foreign partner services at its disposal with which specific features of cyber attacks can be exchanged. The fact that the AIVD is both an intelligence and a security service, and also has access to Signals intelligence, means that we can exchange information with a large number of parties.

ICT specialist:

"Foreign intelligence services deploy very advanced digital attacks. These are so complex that they can exist in ICT systems for years without being detected by normal security software. This allows sensitive information to be siphoned off over a long period and on a large scale.

We have technical knowledge of digital attacks that are not or very little known within usual security circles. These are shared exclusively within the international community of intelligence and security services. Furthermore, the AIVD possesses knowledge of vulnerabilities in systems, and with its years of experience in counter-intelligence, the service understands how foreign intelligence services operate. By combining knowledge and experience of attacks with a knowledge of vulnerabilities, the service is able to assist both government and the business sector in the fight against cyber espionage."

Investigating digital attacks

The AIVD investigates reports from government, from its partner services or from companies regarding suspected incidents that could indicate espionage. For instance, in 2012 we investigated espionage malware found in e-mails of civil servants. Where possible, we share the results of these investigations with the MIVD, the NCSC and our foreign partner services.

Gathering intelligence

Technological developments present opportunities as well as risks. The AIVD has invested heavily in the application of digital intelligence tools in order to be able to gather, specify and analyse reliable information on its own initiative. The AIVD has progressively developed the ability to process large data flows, which is related to this activity. In addition, knowledge of the use of digital intelligence tools strengthens the knowledge of how to protect oneself against such tools. Furthermore, the knowledge in this area is strengthened by the AIVD's ability to gather unique information, for instance through human sources.

Detecting digital attacks

The AIVD assists companies and government institutions that could be targets by helping them to recognise cyber espionage and to prevent or limit damage resulting from it. In 2012 the service invested in the support of certain elements of government and the business sector in the detection of complex digital attacks on their ICT networks in 2012.

The service conducts such detection operations only if requested to do so. On several occasions we have already been able to alert ministries at the moment that we identified suspected malware in their networks.

Increasing resilience

In support of the government's information strategy, the National Communications Security Agency (*Nationaal Bureau Verbindingsbeveiliging*, NBV) of the AIVD conducted an investigation into the security aspects of the 'Bring Your Own Device' (BYOD) concept for tablets and smartphones. This describes the possibilities for using such self-chosen devices at work without affecting network security.

The reactions to the publication ('Bring your own device. Choose your own device.') were positive, both inside and outside the Civil Service. In particular, the advice not to accept any tablet or smartphone device at the user's wish but to allow only a limited number of securely configured devices to access the internal network was appreciated. The advice was also used within government institutions in the development of policy in this respect.

The publication was accompanied by an inventory of current BYOD projects within the government, and the most common security architectures and commercial security solutions were listed. At the request of various departments, the AIVD is investigating the security value of various security products for tablets and smartphones. The results of this investigation will be used by the BYOD taskforce within the government in the *Rijks Application Store* and in the *Rijkscloud projects*, among other areas. In connection with the publication of the policy document, the AIVD gave presentations at several levels inside and outside government to raise awareness of this issue.

Espionage analyst:

"Dutch civil servants have been the target of espionage. They became co-victims of a large-scale international espionage attack as a result of their contacts with a number of international organisations.

Employees of these organisations and their contacts were sent e-mails containing malware. The e-mails were formulated so as to appear trustworthy to the recipient, for example by imitating the formats used by trusted government institutions or other institutions. The malware was activated by clicking on the e-mail; this ensured that data from the infected computer was copied and sent to the attacker without this being noticed. The computers of the Dutch civil servants were not infected by the malware used in the attack and therefore no information was leaked.

The methodology used shows that the attackers were well informed regarding the activities and interests of the persons and organisations involved. The scale of the attack and the intention of retrieving information from computers indicate that this was an attempt at espionage by a foreign power.

The technical features of the malware and a substantive analysis of the targeted information led us to the conclusion that the malware originated from China, or that the attacker wished us to believe that this was the origin of the attack."

The AIVD also contributed to the nation-wide campaign 'Alert Online'. This campaign was designed to make citizens, businesses and government aware of the potential risks of Internet and smartphones.
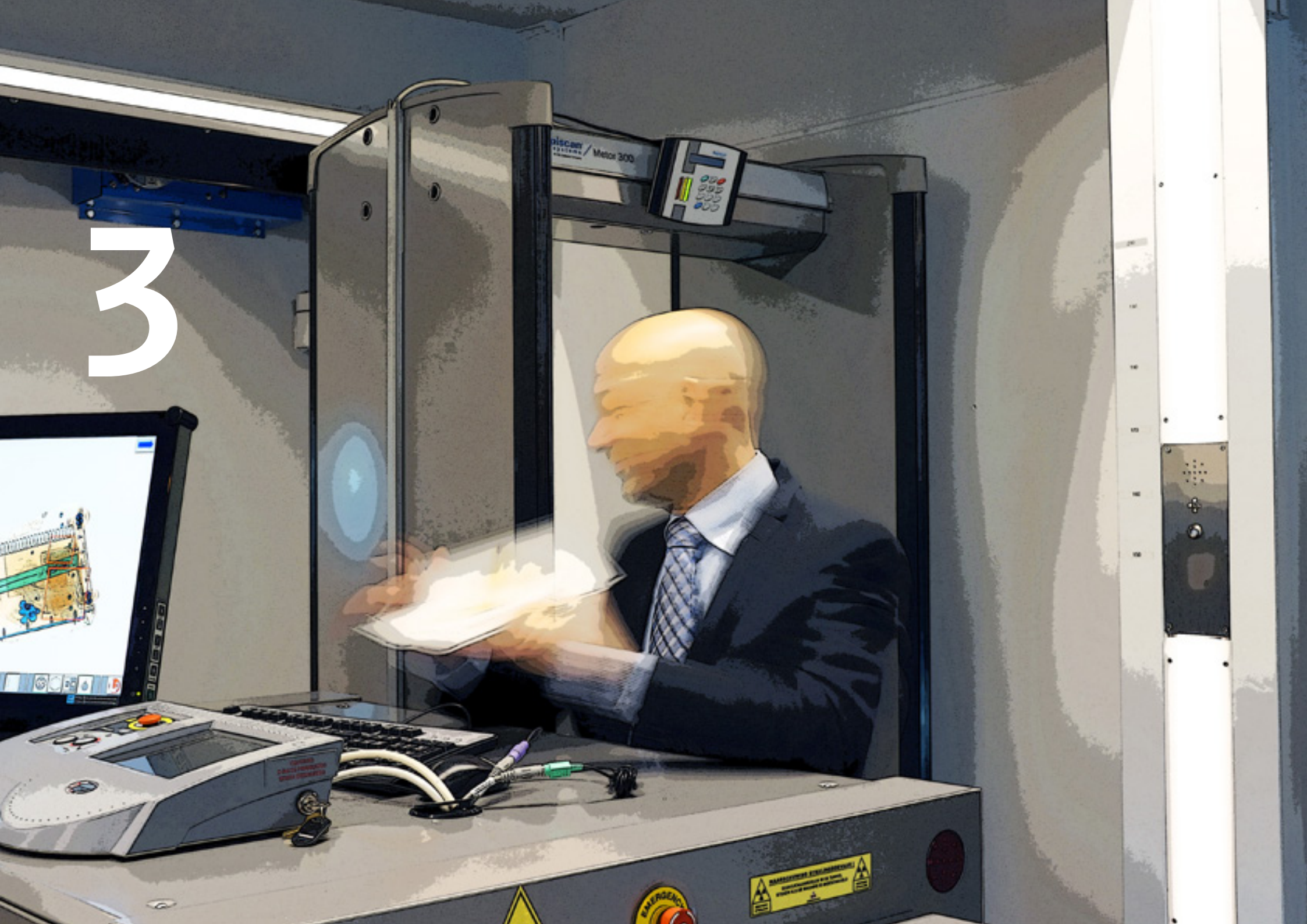
TERRORISM

Terrorism remains a threat, both to the physical security of our country and to the democratic system in general. For this reason, the fight against terrorism is an important task for the AIVD. Organisations, networks and lone individuals can constitute a terrorist threat.

The AIVD is seeing a sharp increase in the number of jihadists travelling from the Netherlands to conflict areas. This is a source of concern, especially because when abroad these jihadists acquire combat and other skills and contacts, and may also return in a traumatised condition. The attacks by Mohamed Merah in Toulouse show that a combination of focused training by an organisation and personally chosen actions and targets can lead to violent actions in the West.

In addition, the arrests made during a PKK meeting in Zeeland in December 2012 show that terrorism is not only a distant phenomenon, but can also occur close to home: terrorist organisations can use our country for their activities.

3.1   Jihadist terrorism

Travelling jihadists
For a number of years already, the AIVD has seen that the main focus of radical Muslims with jihadist aspirations in the Netherlands is primarily directed at participating in jihad outside the Netherlands. Dutch jihadists who travel to conflict areas abroad constitute a risk on their return to the Netherlands. They will have acquired skills, including combat skills, and contacts while abroad, and may also have become traumatised.

The repeated calls by core Al Qaida and Al Qaida in the Arabian Peninsula to Muslims around the world, urging them to focus on committing attacks at their own opportunity, and in their own environment, have so far not been followed up in the Netherlands. However, such attacks cannot be ruled out for the

future. Therefore the AIVD continues to identify risks to physical safety and security in the Netherlands that are related to the return of trained jihadists from conflict areas.

Many of the AIVD's efforts are focussed on identifying travels to areas of conflict, and the intention of jihadists to leave the Netherlands. The AIVD also studies travel movements from jihad areas to the Netherlands and, more generally, to Europe. Mapping the relevant travel routes used by jihadists from and to the West and monitoring these routes is one of the main elements in the investigation of terrorism. In addition to its own resources, the AIVD works with national and international partners in this area. In 2012, significant investment was made in the inventory and analysis of travel data, in the context of Travel intelligence. This allows us to identify the travel data of jihadists, among other things. Furthermore, on the basis of these travel data the AIVD can act quickly when a jihadist is planning to travel to the Netherlands.

In 2012 the AIVD was once again able to disrupt attempts of jihadists travel to conflict areas. These actions included cooperating with – and providing information to – a number of strategic partners, including the Public Prosecution Service, the National Investigation Service and the Immigration and Naturalisation Service.   On the basis of official reports submitted to the Public Prosecution Service, a number of detentions took place .

Jihadist conflict areas
Syria
At the end of 2012, in particular, the AIVD noted a large increase in the number of jihadists travelling to Syria. The large numbers of jihadist fighters that have travelled from the Netherlands to Syria are explained by the extensive media and internet

attention to the conflict in Syria, and the easy accessibility of the country.

In addition, some members of activist radical Islamist movements, such as Shariah4Holland and Behind Bars, have departed to Syria to participate in the jihad. It is clear that the dividing line between radicalism and jihadism is blurred. These movements have created an environment in which people of like mind can meet each other and in which radical ideas have been able to develop into jihadist views. Group dynamics have led to rapid radicalisation of many individuals and actual attempts to participate in the jihad in Syria. Based on information provided by the AIVD, the National Investigation Service arrested three young men who were about to leave for Syria in November 2012.

Afghanistan-Pakistan
Core Al Qaida, the jihadist network located in the border area between Afghanistan and Pakistan, still has the intention of carrying out attacks in the West. The network has suffered serious damage in recent years from attacks by unmanned aircrafts - or drones -. Despite the loss of a number of leading figures, core Al Qaida is still in a position to develop plans for attacks in the West from the border area between Afghanistan and Pakistan. In 2012, the AIVD established that core Al Qaida is actually able to train and instruct people for this purpose.

Due to the drone attacks, the Afghanistan-Pakistan region is less attractive for Western jihadists. Although Westerners are still present there, there seems to be little interest among European jihadists to go to this region. The rise of Syria as an alternative jihad region is mainly responsible for this. People with a Western background, however, continue to be important recruits for Al Qaida, since they are often able to return to

Europe from the Afghanistan-Pakistan border area without being noticed. These jihadists, some of whom have been trained and given an assignment to carry out an attack in the West, constitute a serious threat.

Mali, Sahara and Sahel
In early 2012, new life was given to the long-slumbering fight for independence by Tuareg rebels in Mali under the influence of fighters from Libya and the easy availability of weapons in that country. Initially the secular rebels were fighting in an opportunistic alliance with various jihadist groups, which soon however took control. A jihadist alliance dominated by Al Qaida in the Islamist Maghreb (AQIM) has been in control of the northern half of the country since the end of June 2012. The 'proto-caliphate' Azawad that the alliance has proclaimed is attractive to European jihadists. AQIM is not only focusing on the conflict in the region, where it constitutes a threat to Western interests, it also has the intention of committing attacks in the West.

Yemen
Al Qaida on the Arabian Peninsula (AQAS) is another organisation that still has the intention of committing attacks in the West. In 2012, however, this group came under heavy pressure, including military pressure, and after a large-scale military offensive in South Yemen, the group has withdrawn from the areas it had occupied in 2011. Furthermore, the AQAS has lost various key figures as a result of intensive air attacks, most of which have been attributed to the United States.

Mohamed Merah

Mohamed Merah is an example of a Western jihadist who has been in the Afghanistan-Pakistan region, where he was trained by Al Qaida. In mid-March this French citizen of Algerian origin killed seven people in and around the French city of Toulouse, including French soldiers and children from a Jewish school. He said that he had killed the children in revenge for the deaths of Palestinian children. He also stated that he had killed the French soldiers in revenge for their role in Afghanistan. Later he barricaded himself in his apartment, which was subsequently besieged by the French police; this ultimately led to his death. The radical Islamist web forums praised Merah as a great hero who should be emulated. It is difficult for intelligence and security services to detect a lone individual like Merah.

In the spring of 2012 plans were frustrated for an attack outside Yemen with an improved version of the 'underwear bomb' attack that had occurred in 2009 [1]. During the rest of the year, AQAS concentrated mainly on carrying out suicide bombings. The primary targets were the local police, military targets and security targets in Yemen in the capital city of Sana'a, among other places. However, the risk of attacks against Western interests in Yemen, such as diplomatic objects and the US military presence, has also increased. Furthermore, in 2012 there was a rise in the number of kidnappings of – and attacks on – persons of Western origin.

There is still interest among radical Muslims in Europe to participate in jihadist activities in Yemen.

Somalia
In 2012 the military pressure on the jihadist movement Al Shabaab (AS) strongly increased, forcing AS to effect a strategic withdrawal to the rural areas of central and southern Somalia. Pressure on AS has also grown as a result of the deployment of American drones. The victims of these drone attacks include prominent jihadists affiliated to Al Qaida East Africa and Al Shabaab. AS is fragmented, and the recent setbacks have strengthened divisions between the various factions within AS. The fact that one of the leaders of AS has formally joined core Al Qaida would appear to mean that this group - or an element thereof - is progressively orienting itself against the West. There has been no manifestation of this so far, apart from some rhetoric that was specifically directed against the Netherlands.

The risk of an attack on Western interests in the region remains present. The threat posed by AS to the West and in particular to the Netherlands remains low. The AIVD has, however, established that supportive activities for AS are being carried out in the Netherlands, including secret funding and the dissemination of jihadist propaganda material.

The popularity of Somalia as a jihadist travel destination has waned somewhat. This is also due to the rise of Syria as a conflict zone.

The jihadist Internet
Jihadist Internet plays an important part in ensuring that ideas and perceptions regarding the hostility of Western countries towards Islam are kept alive. This also became evident when the anti-Islam film 'Innocence of Muslims' was released in the autumn of 2012. Various jihadists in the Middle East and North Africa pointed to the Netherlands as the driving force behind this American film. Even though this was actually incorrect, the AIVD notes that this perception of the Netherlands as the driving force is still given credence. Such intractable misconceptions regarding the role and position of the Netherlands are often fuelled and strengthened by jihadist Internet and can have consequences for the threat to the Netherlands and/or Dutch interests abroad.

To jihadists worldwide, and certainly to those active in the jihadist Internet, the Netherlands is still one of the 'enemies of Islam'. The service sees the wish to avenge perceived defamations of Islam, the Koran or the Prophet as one of the constants in the jihadist threat to the West. The long afterlife of the Danish cartoon issue shows that such perceptions among jihadist networks, groups and individuals can have a long-lasting effect on national security.

---

1 On 25 December 2009, Umar Farouk Abdulmutallab attempted to blow up a scheduled flight from Amsterdam to Detroit with a bomb hidden in his underpants.

Aftermath of the 'Arab Spring'

In 2012, salafist jihadists took advantage of the vacuum created by changing political circumstances and the partial removal of a repressive security apparatus as a result of revolutions in Tunisia, Egypt and Libya, mostly referred to as the Arab Spring. Jihadist groups, networks and individuals played no significant part in the events of 2011.

In 2012, new salafist-jihadist networks and cells were formed in a number of countries in North Africa and the Middle East, involving people who in many cases have both a national and an international agenda. Nationally, their aim is to establish an Islamic state based on Sharia law. Internationally, they are in contact with or belong to jihadist networks that, for instance, support the conflict in Syria or the preparation of attacks outside their region. The attack on the US consulate in Benghazi (Libya) in September 2012 shows what these new networks are capable of. Clearly they focus their aggression on a Western target and there are mutual connections between these networks in the countries mentioned.

The ease with which contacts can be made between young, radical Muslims from the West and these salafist-jihadist networks is a cause for concern. They are active in countries that are relatively close to Europe and easy to travel to. Once they arrive there, it is not difficult for Western radical Muslims to get in touch with these networks.

Various large and influential jihadist web forums continued to function as feeder, market place and breeding ground for jihad. As described by the AIVD in the publication '*Jihadism on the Web, A breeding ground for Jihad in the modern age*', this phenomenon has increased the attractiveness of the jihad in Syria, for example. It has also narrowed the geographical distance between radical Muslims in Europe and the emerging networks in the Middle East and North Africa. Last year the service was able to successfully identify or differentiate various threats around the world in a timely manner, for both its national and its international partners.

Social media have also become an essential tool among jihadists. The use of Facebook, Twitter, or YouTube by jihadist networks, groups and individuals has intensified. This was partly due to the temporary absence of some of the classical jihadist web forums in 2012. Jihadists around the world accordingly sought new channels for disseminating their propaganda. So far the radical Muslims outside the Netherlands are leading the way with these new media, but the AIVD expects those in the Netherlands to catch up in the coming year.

Cyber jihad

Jihadists can form a cyber threat to national security. Their potential is currently not sufficient to realise their cyber-terrorist ambitions. In 2012 no digital attacks by jihadists in the Netherlands were identified by the AIVD that were considered a threat to national security. Abroad, jihadists have carried out some small-scale and simple digital attacks whereby Internet services were temporarily disrupted. These actions are an indication of the cyber capacities of the jihadists. The increased intentions and the possibility that jihadists will develop additional capacity are cause for us to continue to closely monitor cyber-jihadism.

3.2   Other terrorism

PKK

The Kurdish separatist organisation PKK (Partiya Karkarên Kurdistan) is secretly developing activities in the Netherlands designed to support the - armed - conflict of the organisation in Turkey. These activities are sizeable and professional, and international in nature.

One of the activities of the PKK in the Netherlands is the recruitment of young Kurds for the organisation. In co-operation with its national and international partners, the AIVD devoted its efforts towards the disruption of this activity. In this context, in December a raid was carried out by the National Investigation Service during a PKK meeting in Ellemeet, Zeeland on the basis of official reports by the AIVD. 55 people were arrested during this raid, including a PKK leader. The AIVD estimates that the disruption in Zeeland could lead to a - temporary - reduction in the organisation's effectiveness.

The PKK has no intention of using violence or launching attacks in the Netherlands. The PKK has succeeded in drawing attention to the Kurdish question by means of demonstrations and lobbying activities.

The AIVD has observed that readiness to take action appears to have increased last year, mainly among the younger members of the PKK.

European Championship Football and the Olympic Games in 2012

Together with others, the AIVD focused its efforts on ensuring the safe progression of events at the European football championships in Poland and Ukraine, and at the Olympic Games in London. In addition to its normal activities, the AIVD collaborated more closely and exchanged information more intensively with its foreign partner services in order to prevent attacks and ensure the safety of Dutch and foreign athletes and supporters. One of the measures we took for both these sporting events was to designate a liaison officer to act as a contact.

RADICALISM AND EXTREMISM

4.1 Islamist extremism

In recent years, a number of activist radical Islamist movements have attracted attention in the Netherlands. These movements use names like Behind Bars, Street Dawah and Shariah4Holland. Despite differences in views between these movements, the common factor is that they actively promote anti-democratic and jihadist views. These movements were also active in 2012. For example, supporters of Behind Bars took part in a demonstration in Amsterdam against the film 'Innocence of Muslims' which is critical of Islam. Supporters of Shariah4Holland and Shariah4Belgium openly showed their support for Mohammed B. at the penitential institution in Vught on Liberation Day. The leader of Shariah4Holland was sentenced by the court for making threats against Geert Wilders during a demonstration in Amsterdam.

These movements can have a polarising effect because they encourage anti-democratic and intolerant attitudes. In addition these convictions and their ambivalent attitude towards violence, they create a climate in which the use of violence becomes more acceptable. Similar movements in our neighbouring countries have become more militant. For instance, the Millatu Ibrahim movement is threatening attacks against Germany. Due to their mutual beliefs, the possibility that supporters of these movements in the Netherlands will adopt a similar attitude cannot be ruled out.

The readiness for action and the organisational abilities of the movements in the Netherlands are fickle. For instance, in the latter months of 2012 Shariah4Holland more or less ceased to organise publicly visible activities. This is partly due to the fact that the movement depends heavily on Shariah4Belgium, which was affected by the investigation and conviction of its leaders by the Belgian judiciary.

However behind the scenes individual key members of Shariah4Holland were involved in jihadist travel to Syria, as stated in the section on Terrorism.

The fact that in 2012 key members of Shariah4Holland participated in violent jihad abroad is more or less a direct consequence of the ideology embraced by this movement since its inception, in which 'support' for jihadists in conflict areas plays an important part. Jihad travel can have a radicalising effect on the activist radical Islamist groups in the Netherlands. With their experience of combat and enhanced status, jihad travellers can heighten the readiness to take action and harden the orientation of these groups in the Netherlands.

The AIVD has, where possible, informed local governments regarding the activities of radical Islamist movements.

4.2   Left-wing extremism

Anti-fascism
There was little activity from the national movement Antifascistische Actie (AFA). Regionally, the AFA chapter in The Hague has switched the focus of almost all its activities towards resistance to the asylum and immigration policy. In the course of 2012 the AFA working group *Laat Ze Niet Lopen* (LZNL) stopped its direct interventions against manifestations by the extreme right, mainly the Dutch Volks-Unie (NVU). Anti-fascists did however appear at protests against extreme right-wing manifestations in Germany. Dutch anti-fascists were present in Dresden, Aken/Stolberg and Münster. A number of Dutch activists were arrested in Stolberg.

Anarchist extremism
In 2012 the activities conducted by extreme anarchists that were observed by the AIVD mainly concerned vandalism against various types of property. Anarchist extremists undertook various activities in 2012 in the context of their 'international solidarity'. For instance the *Vrije Bond*, together with the '*Kritische Studenten*' among others, was involved in the organisation of the International Day against Capitalism on 31 March in Utrecht. In May 2012 some of the extremists were also present In Frankfurt where the international 'Blockupy' protests - resistance against the troika of the EU, the IMF and the European Central Bank - resulted in several arrests. In addition, unidentified perpetrators set fire to offices of Generali, an Italian insurance company, as a demonstration of international solidarity with their Italian comrades imprisoned in Diemen.

Animal rights extremism
In 2012 the partly anarchist *Respect voor Dieren* (RvD) intensified its campaign against Air France/KLM and other airlines transporting primates. The actions are in opposition to the transport of primates for the European animal testing industry. In addition to intimidating noise campaigns at various offices of KLM and other companies, in some cases the action group disrupted the work of KLM employees.

The RvD's campaign was disrupted by a court ruling during 2012. Two leaders were extradited to the United Kingdom in connection with an international investigation into home visits, arson and blackmail in neighbouring countries.

RvD activists calling themselves Stop Huntingdon Animal Cruelty- Nederland (SHAC-NL) have carried out hit-and-run-

actions [2] at pharmaceutical companies in protest against animal testing.

Last year the AIVD passed on information to the security organisations of the various institutions that are targets – or potential targets – for animal rights extremists, in order to enable them to strengthen their defences.

Intimidating and/or violent opposition to the asylum and immigration policy
In 2012, opposition to the Dutch and European policy on asylum and immigration increased. This was mainly due to the definitive start of the so-called No Border Network, in which activists and extremists - such as the Anarchist Anti-Deportation Group in Utrecht and the Stop the Deportations Working Group - have joined forces - while retaining their own principles and action methods - to promote co-operation and coordination. The annual 'No Border Camp' activities, where activists discuss matters such as international campaigns, took place in Sweden and Germany this year.

Actions taken in 2012 by opponents to the asylum and immigration policy included graffiti at the residence of the then Minister for Immigration, Integration and Asylum, Mr Leers, and the training centre of the IND in Utrecht. In addition, Dutch people were involved in blockading detention centres for asylum seekers in Belgium (Merksem and Brugge), during which several people were arrested.

---

2   Protests in the form of secretly prepared actions involving graffiti and vandalism, which where carried out unannounced.

In addition to the familiar action groups (the Working Group Stop the Deportations and the Anarchist Anti-Deportation Group in Utrecht), in 2012 other - to some extent new - groups were active, which for instance provided direct aid to homeless refugees. Some anti-fascist groups (AFA-Fryslan, AFA The Hague) also changed the focus to the opposition to the asylum and immigration policy.

Among the groups opposed to the asylum and immigration policy there is much interest with respect to Frontex, the European Union (EU) agency that coordinates the monitoring of Europe's borders. The left-wing activist Campaign Against Arms Dealing published a brochure on the 'militarisation of Frontex', containing a list of Dutch defence contractors. The AIVD sees this as a possible call to take action.

Regional groups were especially active in the organisation and maintenance of various tent camps belonging to Somali and Iraqi asylum seekers who have exhausted all legal procedures. The Anarchist Group Amsterdam (AGA) was involved at the camp on Notweg in Osdorp, and AFA-Fryslan at the tent camp and deportation centre in Ter Apel. In addition, AFA The Hague was heavily involved in the organisation of the tent camp at the Koekamp in The Hague, and played a part in preventing this camp from being cleared. The AIVD maintained contacts with the local authorities regarding the actions of these groups.

4.3   Moluccan activism

Activism is declining in the Moluccan community, but the risk remains that public order may be disrupted around the comme-moration dates in the Moluccan calendar and also in the event of visits by Indonesian dignitaries. The investigation by the AIVD into Moluccan activism in the Netherlands shows that the RMS government in exile (Republic of Maluku Selatan, Republic of the South Moluccan Islands) is continuing to engage in peaceful confrontations with a high political and media profile. An example of this is an open letter to the Prime Minister regarding the proposal to decorate the soldiers who participated in the termination of the train hijack at *De Punt* in 1977.

In 2012, the AIVD also informed its partners with respect to Moluccan activism. This involved large companies being informed regarding the nature of and developments in Moluccan activism in the Netherlands.

4.4   Right-wing extremism

A study by the AIVD into right-wing extremism shows that splintering, fragmentation and general disunity among Dutch right-wing extremists increased further in 2012. There are still a few active right-wing extremists, although most of these people participate in social activities without any immediate ideological purpose.

The actions by the German authorities against various German extreme right-wing groups, such as the Kameradschaft Aachener Land (KAL), led to very little reaction among Dutch right-wing extremists. This is notable, since many of them maintain close and friendly contacts with their German comrades and have participated in activities organised by the KAL.

The Dutch Volks-Unie
One of the findings of the AIVD is that the Dutch Volks-Unie (NVU) has little remaining ability to mobilise support. Whereas the NVU used to be able to marshal around 100 right-wing extremists at previous demonstrations, since September 2011 the presence of around a score of demonstrators - coming only from its own supporters - has been the rule rather than the exception.

Right-wing anti-capitalism
The National & Socialist Action, previously known as the National Socialist Action/Autonomous National Socialists, is poised to form the Dutch section of the Anti-Capitalist NetWork (ACN). The ACN is a European network of right-wing anti-capitalists.

The social-revolutionary right-wing extremists want to start a right-wing anti-capitalist movement in the Netherlands. Some Dutch social revolutionaries have attended anti-capitalist demonstrations in France and Italy. Furthermore, the National & Socialist Action has introduced itself on the Facebook page of the ACN, where it put forward an ideological programme.

Blood & Honour and Ulfhednar
Last year various Dutch Blood & Honour activists attended European demonstrations and concerts. The Ulfhednar (or Vanguard) group, against which the police took action in October 2011 on the basis of information from the AIVD regarding possession of firearms, now appears to no longer be a significant force in Dutch right-wing extremism.

Voorpost (Outpost)
In the second half of 2012 the extreme right-wing nationalist action group Voorpost became more active, and organised various demonstrations and actions. This increased activity by Voorpost appears to be linked to the unemployment of several members of the group, who for this reason had more time at their disposal for preparing and carrying out actions. The AIVD is in close contact with the police regarding this kind of demonstration.

Anti-Islamist activism/Anti-Islam
After a more intensive investigation of the threat from anti-Islamist, anti-multiculturalist and anti-left-wing groups in 2012, the conclusion is that this threat is not currently significant. The AIVD continues to be alert to any increase in activity in this area and any developments in this threat.

CLANDESTINE ACTIVITIES BY FOREIGN POWERS

Intelligence activities by foreign intelligence services not only infringe the sovereignty of the Netherlands, they also cause serious economic harm.

Foreign intelligence services conduct clandestine activities in the Netherlands for the purpose of strengthening their own country's geopolitical and economic position. They attempt to gather sensitive and valuable information, for example to ascertain the standpoint of the Netherlands in negotiations with another country in advance. The future policy of international joint ventures in which the Netherlands participates, such as the European Union, the United Nations or NATO, is also of interest to them.

Espionage activities are designed to obtain governmental, economic, military and scientific information. The Netherlands is an attractive target for state actors - nations and their government agencies - due to its knowledge-intensive and internationally oriented economy. For many countries, the obtaining of innovative ideas and knowledge by means of espionage is a part of their economic and foreign policy. They protect their own interests, in some cases aggressively, mainly with regard to scarce commodities, the security of energy provision and the acquisition of high-level technology and expertise.

The powerful ICT infrastructure in the Netherlands is also very attractive to other countries. In addition, some countries attempt to exercise influence and carry out espionage within migrant groups in the Netherlands.

5.1 Government and administration

The gathering of political information continues to be an important objective for many foreign intelligence services. Dutch government organisations and international organisations located in the Netherlands are therefore targets for the intelligence operations of foreign powers.

The foreign intelligence services use both digital and more traditional methods to obtain political information. The usage of digital means such as malware, viruses and hacking is growing exponentially. Information is more or less always stored in digital form, often at a central location, which makes such a location an attractive target for digital attacks by foreign services.

During the past year, the AIVD identified espionage attacks on the Netherlands originating from several countries, including China, Russia and Iran. Given the worldwide volume of incidents of cyber espionage, the number of incidents in the Netherlands is probably much higher.

Tracing the origin of cyber attacks is often complicated, since all kinds of methods are used to cover the tracks of such attacks. It is also difficult to identify the actual originator, since these attacks are usually deployed indirectly, via many detours. Nevertheless the AIVD's investigations of digital attacks on Dutch targets have produced very strong evidence of foreign state involvement and also definite indications of the country of origin.

The threat to national security is at least as great in cases where intelligence officers attempt to gather information by more traditional means, by approaching persons who can access sensitive and valuable information. The AIVD has seen that this activity has continued unabated in 2012. Partly for this reason the Ministry of Foreign Affairs has been advised on several occasions to refuse visa applications from intelligence officers applying to travel to the Netherlands under cover.

One well-known approach used by intelligence officers for the recruitment of government and other officials is to offer money in exchange for information. Prior to attempting to recruit these people, they try as far as possible to gather information on the employee's position, his access to valuable information and his personal situation. The fact that people nowadays post a lot of information about their personal lives on the Internet makes the identification of potential starting points a simple matter. Any vulnerabilities such as financial problems or frustration in connection with career development can be used to recruit people as agents.

The AIVD has organised presentations in order to raise awareness of the risks of espionage among government officials and organisations. For this purpose we used the e-learning module set up together with the NCTV that is based on the Vulnerability Analysis on Espionage in the Netherlands (*Kwetsbaarheidsanalyse Spionage*, KWAS) and assists government agencies and businesses in the vital sectors to recognise signs of espionage in good time.

In addition to Dutch institutions, international institutions – of which there are many in the Netherlands – can also be the victim of espionage. In these cases, as well, the AIVD has a responsibility to fulfil.

5.2 ICT infrastructure

The Netherlands is a hub in the international ICT infrastructure. Digital methods are therefore not only used against persons and institutions within our borders, but also for cyber espionage against persons or institutions outside the Netherlands. Although the Netherlands is not the attacker's intended target in these cases, these abuses can lead to harmful side-effects for the Netherlands. Where we have observed these activities, we have informed the institutions concerned.

In order to continue to be able to detect such attacks on the ICT infrastructure, it is important that we can continue to conduct random interception of cable-linked telecommunications. A parliamentary bill is in preparation to ensure that this power, subject to safeguards, is anchored within the Wiv 2002.

5.3 Migrants in the Netherlands

The attention of foreign intelligence services to various migrant communities and opposition groups in the Netherlands is expressed partly through more or less open diplomatic efforts to exercise influence, but it also involves espionage within these communities and groups. Because this also infringes the rights of Dutch citizens, the AIVD strives to identify and frustrate these intelligence activities.

Foreign intelligence services search for personal information on migrants and dissidents and make efforts to infiltrate their organisations. This enables public protests and activism by these groups against the regime in their country of origin to be disrupted.

The AIVD has ascertained that the Chinese government has been guilty of espionage, intimidation and practices designed to influence the Uighur community. The AIVD has developed various activities during the past year designed to disrupt these practices that were designed to exercise influence. In addition to tackling these disruptive measures, we have also drawn attention to this form of espionage in the media.

The AIVD also noted that the Iranian government is still fully active in its fight against the opposition movement Mujahedin-e-Khalq (MKO). It has emerged that the Iranian intelligence service is directing a European network that is also active in the Netherlands. This network consists of former MKO members who have been recruited by the Iranian intelligence service. They have been tasked with negatively influencing the public opinion regarding the MKO by means of lobbying, publications and anti-MKO meetings. They also gather information on the MKO and its members or suspected members for the Iranian intelligence service.

FOREIGN INTELLIGENCE

The intelligence-gathering that the AIVD carries out in foreign countries focuses on political intentions, activities and opinions of governments, institutions and citizens of specifically named countries or regions. The AIVD gathers information - political intelligence - that cannot be obtained through diplomatic channels, or can only be obtained with difficulty. Developments in these countries and regions affect Dutch foreign policy, trading interests and the security of energy provision. They can also have direct consequences for our national security. The countries investigated by the AIVD are listed in the 'Foreign countries designation order' (*Aanwijzingsbesluit Buitenland*). This list is regularly established by the Prime Minister. The names of the countries listed are a state secret.

The analysis and interpretation of the intelligence obtained by the AIVD enables the Dutch government to make its own independent considerations of policy options and positions to adopt in an international context.

The intelligence is gathered by means of both human and technical sources. In 2012 the use of the technical method Sigint was given a new boost by the far-reaching cooperating with the MIVD. This will take shape in the unit that will focus on Sigint and cyber intelligence. Lastly, the AIVD's foreign partner services are an important source of information. In 2012 links were forged with various services, exchange of information with these services has been expanded, and operational co-operation with a limited number of them has been extended to include additional areas.

The information on the areas of investigation and the results achieved provided in this annual report is limited, since it concerns confidential information. The ministries in question and the Intelligence and Security Services Committee (*Commissie voor de Inlichtingen- en Veiligheidsdiensten*, CIVD) of the House of Representatives however, do receive this information.

6.1 Results

In 2012 the AIVD produced more than 370 reports arising from the investigations conducted by the service in the context of its foreign intelligence duties. These include official reports, responses to requests for information originating from the European Union, intelligence reports and intelligence analyses. In addition, in 2012 we also regularly provided briefings and presentations on foreign political developments for the Intelligence and Security Services Committee, the Council for the Intelligence and Security Services, cabinet members and civil servants.

The existing cooperative relationships with the MIVD in the field of counter-proliferation and with respect to the Caribbean region were continued. There was also close co-operation and collective reporting on specific developments in the Arab region.

6.2 The Arab region and Iran

Developments in the countries bordering the European Union (EU), and especially in North Africa and the Middle East, affect Dutch foreign policy, trade interests, the security of energy provision and the migrant communities living in the EU. In 2012 the instability in this region increased. This meant that the threats to the national security of the Netherlands increased as well. For these reasons, the AIVD closely follows developments in this region.

The Arab region

In 2012 the crisis in Syria and the effects of this on the political and security situation in neighbouring countries was the central issue in this region. The greatest concern is the power of this crisis to attract foreign, including Dutch, jihadists. This development is directly relevant to Dutch national security. The conflict between the Syrian opposition and regime of President Bashar al-Assad continued at full force in 2012. Partly as a result of foreign support, the opposition was able to increase the pressure on the Syrian regime. Despite continuing rivalries, both the political opposition groups and the armed combatant groups have managed to increase their cohesion. The continuing crisis in Syria has negative consequences for the political and security situation in Lebanon. At the end of 2012 Dutch interests in the region increased, with the stationing of Dutch Patriot anti-missile batteries in Turkey.

In 2012 a number of countries in this region – in which the Arab Spring had resulted in a change in the regime – made vain attempts to regain a measure of economic and political stability. In many of these countries the Muslim Brotherhood played an important part in these efforts. President Morsi accordingly came to power in Egypt, and the influence of the Muslim Brotherhood increased significantly. In 2012 the economic situation in Egypt deteriorated further, and the jihadist threat increased. In other countries, such as Tunisia and Jordan, the political contrasts between the Muslim Brotherhood and other political movements increased. In the Gulf region, particularly Saudi Arabia, the United Arab Emirates and Oman, fears of increased influence of the Muslim Brotherhood became much stronger, while Qatar, contrary to this development, expressed its support for the Muslim Brotherhood.

Iran

In 2012 the developments in Iran, with respect to both political and nuclear issues, were important items on the international political agenda. The elections to the Iranian parliament in March 2012, and also the period thereafter, featured a conflict between (ultra)conservative factions and political groups allied to President Ahmadinejad. The position of Supreme Leader Ali Khamenei continued to be dominant, and the Iranian Revolutionary Guard (IRG) maintained its strong position. The economic situation underwent a serious deterioration in 2012. The EU sanction on oil imports that took effect on 1 July 2012 and the sanctions against the Iranian financial sector have heavily affected the economy. This did not, however, bring about any change in the country's nuclear policy.

In 2012 Iran also held discussions with both the International Atomic Energy Agency (IAEA) and the permanent members of the United Nations Security Council plus Germany (P5+1 countries). The IAEA wants to obtain clear information regarding the potential military aspects of the nuclear programme.

The P5+1 countries want Iran to comply with UN Security Council resolutions regarding the Iranian nuclear enrichment programme and to reach a solution with the international community.

Iran wants to strengthen its position as an influential player in the region. An important part of this effort was the political, diplomatic and material support given by Iran to the regime of its Syrian ally Bashar al-Assad. The Iranian ambition of strengthening its regional position has encountered political opposition from other regional players such as Turkey and Saudi Arabia, which observe Iran's actions with suspicion.

6.3   Asia

The situation in Pakistan forms an ideal breeding ground for further radicalisation of the population and for growth of the terrorism problem, which is also of importance for Dutch national security. Pakistan has nuclear weapons, a weak central government and large parts of the country are actually controlled by terrorist groups. Furthermore, Pakistan faces a worsened economic situation. After the relationship between Pakistan and the United States cooled markedly in 2011, both countries have slowly attempted to restore the relationship in 2012. At the same time, Pakistan tried to improve relations with other countries in the region, such as China, Iran, Russia, Saudi Arabia and the Gulf States in order to reduce its dependence on the US. In the light of the announced withdrawal of Western troops from Afghanistan in 2014, Pakistan is currently proclaiming its support for the Afghani Taliban, in order to be able to influence the formation of a more pro-Pakistani government in Kabul.

The developments in China – which became the world's second largest economy in 2012 – are relevant to Dutch politics and particularly to Dutch economic interests. The long-expected change of leadership was effected in 2012 whereby nearly all the top leaders of the Chinese Communist Party were replaced. Xi Jinping has been appointed as Secretary-General of the Communist Party and Chairman of the Central Military Committee. His appointment as president will follow in March 2013. The effects of the change of leadership were not especially noticeable at the end of the year, but the domestic policy priorities appear, for the time being, to be focused on the fight against corruption, and on economic reforms. In 2012 China's economic growth slowed somewhat, mainly due to falling exports to Europe. The Communist Party has made extensive efforts to promote growth in order to safeguard the country's stability.

6.4   Latin America and the Caribbean

With the islands of St. Eustace, Saba and Bonaire as special Dutch communities in the Caribbean, the national borders of the Netherlands now extend to Latin America. Developments and events in this region can therefore affect Dutch interests. The AIVD and the MIVD have joined forces in order to provide the Dutch government with intelligence on this region. For the MIVD, the permanent military presence of Dutch armed forces in the Caribbean parts of the Kingdom is reason to monitor developments in general terms, to the extent that these can affect the Dutch armed forces.

In October 2012 Hugo Chavez was re-elected as President of Venezuela. In the regional elections in mid December, his party, the PSUV, won in 20 of the 23 Venezuelan regions. Despite the president's illness, the 'Bolivarian Revolution' proceeded unabated, which has led to further political polarisation of the country. Judicial, legislative and executive powers came under the control of Chavez and his party to an even greater extent. As in previous years, in 2012 further restrictions were imposed on private ownership and freedom of the press. The regime's links with like-minded countries like Cuba and Bolivia are very strong. These countries are increasingly pursuing a foreign policy that is focused on the region and more specifically on regional economic co-operation.

Progress was made in 2012 on modernising the Venezuelan armed forces. With the avowed intention of protecting Venezuela's national raw materials, Venezuela has the ambition of making its armed forces the leading power in the region from 2015 onwards. In addition to deliveries of material mainly from Russia and China, attention was also devoted to improving logistical capacity and the maintenance of military material.

6.5   Russian Federation

Developments in Russia can affect Dutch political and economic interests and the security of energy supply to Europe. Russian politics were dominated by the presidential election in 2012. This was won by Vladimir Putin, who appointed Dimitri Medvedev as prime minister. Indications of electoral fraud led to widespread protests from the opposition in Russia after the election, mainly manifesting in the large cities. During the course of the year the Russian authorities discouraged the organisation of and participation in demonstrations by raising the penalty for these activities. And successfully, it would appear: demonstrations from the broad opposition attracted far fewer demonstrators at the end of 2012 than at the beginning of that year.

The Russian Federation's position as an energy superpower continues to be an important element in the Russian political agenda, partly due to the importance of energy to the Russian economy and therefore also to the political stability in that country.

This means that, to a greater extent than before, the Russian Federation must deal with developments that are beyond its control and that could negatively affect demand for Russian energy. These include technological developments in the field of extraction and transport of energy, European competition legislation and an assertive European energy policy. These developments mean that Russia's position as an energy superpower can no longer be taken for granted.

PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

The spread - or proliferation - of weapons of mass destruction (WMD)and its means of delivery forms a threat to international security. A legally binding system of international treaties exists, in order to counteract the proliferation of nuclear weapons and nuclear weapons technology, the conduct of nuclear tests and the development and possession of biological and chemical weapons. The Netherlands is affiliated with this system, and this entails obligations. Due to these obligations and the national and international security implications associated with proliferation, the AIVD and the MIVD have a duty to investigate relevant activities of so-called countries of concern. These are countries that are suspected of working on the development of weapons of mass destruction or possessing such weapons in contravention of international treaties.

7.1 Co-operation between AIVD and MIVD

The AIVD and the MIVD cooperate closely in the area of counter-proliferation in the joint Counter-Proliferation Unit (Unit Contraproliferatie, UCP). The two services work within this unit at one location and share each other's expertise, information and contacts. In this way they have built up a pre-eminent position with respect to intelligence. The UCP has an intelligence task as well as a security task. The intelligence task consists of informing the government with respect to developments of WMD in countries of concern. The security task consists of activities designed to thwart recruitment activities by or on behalf of countries of concern in or via the Netherlands.

7.2   Results

The UCP has produced several intelligence reports and special briefings. These were mainly intended for the Ministers of the following ministries: Interior and Kingdom Relations, Defence, General Affairs, Foreign Affairs, and Economic Affairs.

To raise awareness and promote security, specific companies and institutions were visited to inform them of the risks associated with proliferation. The AIVD and the MIVD provided information to the Ministry of Economic Affairs, Agriculture and Innovation - and to the Ministry of Foreign Affairs later in 2012 - with reference to export controls.

The UCP actively participated in innovative international co-operation projects and analytical exchanges with foreign intelligence and security services. The UCP was therefore a valued partner for various foreign partner services in 2012.

7.3   Nuclear weapons and means of delivery

Iran
Iran is working on a nuclear programme and states that its actions are purely for civil purposes. There are doubts within the international community regarding this claim, and suspicions that the nuclear programme also has a military dimension.

The nuclear installations in Iran are regularly inspected by the International Atomic Energy Agency (IAEA). One of the most notable findings of the IAEA in 2012 was that the speed with which Iran could produce 20% enriched uranium had substantially increased. The stock of 20% enriched uranium that Iran possesses has also grown. In itself, 20% enriched uranium is not suitable for use in a nuclear weapon3, but the next step to an enrichment percentage that is suitable for such use is relatively small. The acceleration in the Iranian enrichment programme continues to feed concerns regarding the nature of the Iranian nuclear programme. This is certainly the case in combination with the fact that the Iran continues to deny the IAEA access to the Parchin military complex, where research relating to nuclear weapons may have been conducted.

The UCP assesses the IAEA reports on this matter as authoritative and reliable, and therefore as reports that may serve as an important frame of reference. The UCP is following developments in relation to the Iranian nuclear programme closely, and is thereby in a position to understand the progress and potential future developments of the programme and explain the significance of these developments to the government.

Iran has an active civil space programme, which in recent years has shown steady progress. The activities taking place include, among other things, work on rockets for the launch of satellites.

The knowledge and experience gained in this respect can however also be applied in the Iranian ballistic missile programme, which is military in nature. In 2012 Iran launched a so-called Space Launch Vehicle (SLV) for the fourth time, thus successfully placing a satellite in orbit.

North Korea
The North Korean nuclear programme, its associated means of delivery and the role that this country is playing in the proliferation of related knowledge and resources continued to be a cause for concern in 2012. In December 2012 North Korea successfully launched an SLV putting a satellite in orbit around the earth. This was the first successful launch by North Korea. The SLV that was launched used missile technology. With this action, North Korea breached UN Security Council resolution 1874, which calls on the country to cease all activities relating to missiles and the nuclear programme. Partly as a result of these launches, a resumption of the Six-Party Talks was postponed

The fact that North Korea does not attach much importance to the Security Council resolution was also confirmed earlier in 2012 when a new ballistic missile was displayed during a large military parade in honour of the 100th birthday of Kim il Sung.

7.4   Chemical and biological weapons

Syria
Syria possesses chemical weapons that are stored at various sites in the country. Due to the chaotic situation in Syria that began in 2011 and has continued in 2012, there is a risk that these weapons will fall into the hands of third parties. A further risk is that in an extreme situation the Syrian regime will use - or attempt to use - its arsenal of chemical weapons. There would appear to be a serious obstacle to this because deployment of these weapons by the regime would probably lead to foreign intervention, a situation which the regime is devoting all its efforts to avoid.

Libya

The new authorities in Libya discovered 'undeclared' chemical weapons at the end of 2011 that in view of its admission to the Chemical Weapons Convention (CWC) in 2004 should have been reported to the Organisation for the Prohibition of Chemical Weapons (OPCW). The weapons had been kept secret until that time, but have now been declared. They were inspected by the OPCW in January 2012.

7.5 Acquisition of relevant knowledge, equipment and materials

The UCP investigates the open or secret acquisition of relevant knowledge, equipment, materials and commodities for or by countries of concern in or via the Netherlands.

These investigations arise from in-house research and notifications from the Dutch government and foreign partner services. There is close co-operation in this area with the ministry responsible for the issuing of export licences [3] and with executive bodies such as the Customs Administration and the Fiscal Intelligence and Investigation Service (FIOD). In 2012 this also led to situations where, in a number of cases, the shipment of proliferation-related goods were prevented. As and when necessary, policymaking bodies and other investigative agencies were notified of the outcome.

Export controls

The UCP supports the implementation of the Dutch export control policy relating to dual-use goods [4] by means of investigating applications for export licences for these goods to countries of concern. The UCP investigates what is known about the purchaser and the end user, and any intermediate destinations. The UCP also provides an opinion or estimate regarding the usability of knowledge and goods in programmes for WMD when such cases arise. The UCP explains its findings to the ministry with responsibility for issuing export licences. The ministry in question considers this information, together with information it has obtained from its own sources and other parties, and then makes a decision regarding the application.

---

3   At the end of 2012 the Directorate-General responsible for issuing export licences was transferred from the Ministry of Economic Affairs (formerly the Ministry of Economic Affairs, Agriculture and Innovation) to the Ministry of Foreign Affairs.

---

4   Goods or materials that can be used for both military and civil purposes.

8

SECURITY PROMOTION

For the proper and uninterrupted functioning of the democratic legal system, it is important that certain elements within society are protected. The AIVD promotes the deployment of security measures for persons, objects, services and events for which the national government has special responsibility. The AIVD also encourages the taking of measures to protect information that should be kept secret for reasons of national security, and vital elements in the government and trade and industry.

8.1   Safety and Security System

The AIVD provides information on known and conceivable threats to the National Safety and Security Coordinator (*Coördinator Bewaking en Beveiliging*, or CBB), part of the NCTV, who then decides on the security measures to be taken. We do this in the context of the Safety and Security System.

In 2012, in the context of the Safety and Security System, the AIVD submitted 115 threat assessments, 27 threat analyses, 29 notifications and 4 risk analyses. In this manner the AIVD's contribution to the Safety and Security System clearly increased in comparison to 2011.

The AIVD plays an important part in the Safety and Security System, which was set up after the murder of Pim Fortuyn in 2002. The system is designed to protect the physical safety and uninterrupted functioning of political officials, the government, diplomatic premises and international organisations, and to ensure the unobstructed holding of large-scale events. These matters concern people, premises, services and events for which the government bears a special responsibility because of their importance to the Dutch state and Dutch society (known as the national security domain).

Threats against individuals in the public domain

People who play a prominent part in public debate and politicians such as ministers and members of the House of Representatives are regularly confronted with threats. These often come from people venting their anger and frustration through letters, e-mails or tweets formulated in menacing terms. The easy access to the new forms of media makes this easy to accomplish. Usually there is no actual threat to the person concerned in such cases, although these messages could potentially affect the uninterrupted functioning of the addressee.

Two-thirds of the threat assessments produced by the AIVD in 2012 concerned people in the national security domain, compared to half of the assessments in 2011. In 2012 threat assessments were prepared for politicians, including the members of the new Cabinet, and for state visits, conferences and ceremonial activities in which members of the Royal Family were involved.

Diplomatic premises

The Netherlands bears responsibility for the safe and uninterrupted functioning of diplomatic representations in the Netherlands. These are regularly confronted with various actions, whether violent or non-violent. Each year the AIVD accordingly prepares many threat assessments with regard to embassies and consulates. In addition, in 2012 the AIVD also issued a threat analysis which presented an overall description of the threat against diplomatic premises in the Netherlands and abroad. Last year, the threat picture was, broadly speaking, the same as in the year before.

The fact that diplomatic representations in the Netherlands could be the target of actions was confirmed in 2012 by a fire

bomb attack on the Turkish consulate in Rotterdam. Other diplomatic representations were also confronted with incidents in the form of telephone threats, vandalism or attempted vandalism, and demonstrations. In many cases the AIVD was able to inform the relevant authorities in advance, so that measures could be taken in good time. In other cases we were able to further specify whether there was an additional threat as a result of an incident.

Consequences of events abroad

Events abroad can have repercussions for the safety of people and organisations in the Netherlands. For instance, in 2012 demonstrations and/or violent actions took place in various countries in response to the anti-Islam film 'Innocence of Muslims'. The AIVD informed the CBB on any potential associated effects for people and/or property in the Dutch national security domain.

International tribunals and courts

As the host country, the Netherlands has to ensure the safe and uninterrupted functioning of international tribunals and courts located on its territory. These include the Special Tribunal for Lebanon (STL), the International Criminal Tribunal for the former Yugoslavia (ICTY) and the International Criminal Court (ICC). The proceedings of these tribunals and courts may cause unrest in the countries concerned, and may therefore have consequences for the security situation in the Netherlands. In 2012 the AIVD prepared threat and risk analyses for organisations located in the Netherlands, in which these developments are specified and information is provided on the threat to these international tribunals and courts. In addition, in order to promote security, the AIVD provided specific information to the international tribunals and courts regarding actual and potential threats as a result of the intelligence activities of other countries.

Elections and other events of national importance

The events designated as nationally important are Queen's Day, Remembrance Day, Veterans' Day and Budget Day (Prinsjesdag). The AIVD produced threat analyses for these events. The elections to the House of Representatives in 2012 were also an event of national importance. In this connection the AIVD was able to inform the local authorities in Amsterdam in good time regarding plans by radical Muslims to disrupt an election debate.

Preparations for the Nuclear Security Summit (NSS)

The third Nuclear Security Summit (NSS) will be held in the Netherlands in 2014. This event, which is an initiative of US President Obama dating from 2010, is intended to improve global nuclear security. It is important that the AIVD identifies and reports on threats in good time, in order to ensure that the NSS can proceed without interruption. The summit is being organised by the Ministry of Foreign Affairs, and will be attended by a large number of high-ranking delegations from other countries and from international organisations. In 2012 the AIVD had already begun work on the preparations for the summit.

8.2   Vital sectors

The safe and uninterrupted functioning of the vital infrastructure is primarily the responsibility of the companies concerned. The government however also has a responsibility to prevent failure of facilities, such as the supply of energy and drinking water. The AIVD accordingly provides companies in the vital sectors with information on actual and potential threats, and in this way enables them to take measures to reduce their

vulnerability. In 2012 the efforts of the AIVD were focused on both permanent increases in resilience, or prevention, and urgent responses to immediate known or suspected threats. For this purpose the AIVD issued threat analyses and specific recommendations and information designed to increase awareness of particular threats.

Counter-Terrorism Alert System

The purpose of the Counter-Terrorism Alert System (*Alertingssysteem Terrorismebestrijding*, Atb) is to provide companies involved in the vital infrastructure with specific information regarding conceivable or known terrorist threats. For a number of years the AIVD's assessment of the jihadist threat to the sectors concerned has been low. A higher threat level applies only to the civil aviation sector, as a result of international incidents.

8.3   Focused information

Since the citizens, companies and organisations themselves bear the primary responsibility for their own safety, the AIVD provides focused information in the context of security promotion and the Safety and Security System. In 2012 we organised more than a hundred such informative meetings for companies and organisations. This is more than a 25% increase compared to 2011. In this manner the AIVD contributes to raising awareness of the risks of cyber or other espionage and terrorism at these companies and organisations. We also suggest options for actions whereby they themselves can put adequate measures in place to increase their ability to withstand potential threats.

Civil aviation is one of the sectors for which the AIVD began to organise informative meetings in 2012. We want people working in the air travel industry, for example at airlines and flying schools, to be aware of the terrorist threats with which they could be confronted.

8.4   Security of special information

The threat of cyber attacks on government targets is rising. The Dutch government has to be able to protect sensitive information from falling into the hands of hostile parties and other countries (foreign state actors). A unit of the AIVD, the National Communications Security Agency (*Nationaal Bureau voor Verbindingsbeveiliging*, NBV), provides independent and reliable advice to the government regarding the protection of state secrets by means of ICT security solutions. The NBV applies its unique knowledge and expertise and uses information from an extensive international network.

The AIVD advises the government regarding preventive measures - secure products and security architectures - and on detection and response. On request, the AIVD also assesses security products before they are taken into use by government. In this way the AIVD helps to increase the government's digital resilience, and supports risk management within the government. Thanks to our advice, ministries and government-wide ICT service centres are better equipped to protect their territorial, physical, economic and political interests.

Advice and evaluation

The AIVD has completed various evaluations of hardware and software with positive results and given recommendations. The

TG4 (Tiger 7401) secure telephones have been approved for secure telephony up to the Secret (*Stg. Geheim*) classification level. The AIVD also gave a positive assessment of the use of Microsoft BitLocker for the Ministerial Restricted (*Dep. Vertrouwelijk*) level. BitLocker is a security product delivered as standard with various versions of Microsoft Windows.

The AIVD made recommendations with reference to the implementation of the wireless network in the new premises occupied by the Ministry of Security and Justice. In support of the government's information strategy, the AIVD conducted an investigation into the security aspects of the 'Bring Your Own Device' (BYOD) concept for tablet computers and smartphones.

The central government uses the Government Digital Working Environment (*Digitale Werkomgeving Rijk*, DWR). Together with the Shared Service Centre for ICT (*Gemeenschappelijk Dienstencentrum ICT*, GDI) the AIVD has laid the basis for the Government Digital Working Environment (Secret) (*Digitale Werkomgeving Rijk-Geheim*, DWR-G). The GDI, a unit of the Ministry of Security and Justice, will provide workstation and computer centre environments for the processing of information classified as Confidential and Secret.

The AIVD advises on the security requirements, architecture, technical design and management of the DWR-G infrastructure. The standards and requirements developed for DWR-G can also be applied in other government-wide projects such as the Data Centre Consolidation project.

The AIVD has assessed the equipment for the central part of the government's Public Key Infrastructure. By means of the exchange of digital certification, this infrastructure safeguards the reliability of information exchange via e-mail, websites or

other exchange of data. The equipment for the signature of certificates has now been replaced, and the current implementation meets the AIVD's criteria for information classified as Confidential. This is a necessary precondition to ensure that PKI solutions under the infrastructure can attain the classification of Ministerial Restricted. Certain recommendations were made to ensure that the central part of Public Key Infrastructure continues to meet the criteria in the longer term.

Public campaign 'Alert Online'
With the 'Alert Online' campaign, government and business want to make people more aware of the risks associated with the use of Internet and smartphones. Among other things, the AIVD has compiled a cyber challenge for this campaign. The primary objective of the challenge was to draw the attention of members of both the public and private sector in the Netherlands to the threat of cyber espionage (see also the section entitled Cyber threats).

Production of encryption keys
The AIVD produces encryption keys for encryption equipment for the government institutions. The implementation of a digital system for production of encryption keys for national communications traffic was started in 2012.

9

SECURITY SCREENINGS

In the Netherlands, there are positions which, as a result of their potential to affect national security, are designated as positions involving confidentiality. People holding such positions could potentially harm national security to a greater or lesser extent. Positions involving confidentiality are designated as such by the relevant government minister in consultation with the Minister of Internal Affairs and Kingdom Relations. Positions involving confidentiality may only be designated as such after other reasonable security measures have actually been put in place - as a final measure.

In the context of protecting national security, the AIVD conducts security screenings of people wishing to take up positions involving confidentiality. A person can only take up such a position after the AIVD has issued a Security Clearance (*Verklaring van geen bezwaar*, VGB) for the person in question. A VGB means that there is no objection to this person taking up a position involving confidentiality on national security grounds.

Depending on the sensitivity of the position involving confidentiality, the level of the security screening is set at A, B, or C, with category A being the deepest screening used for the most sensitive positions. The AIVD conducts screenings at all three levels. Some category B screenings are conducted by the Royal Netherlands Military Constabulary (*Koninklijke Marechaussee*, KMar) and the police, on the instructions of the AIVD.

9.1   Developments in 2012

New requirements for the conduct of security screenings
The AIVD has reformulated the requirements that must be met by Task B, the conduct of security screenings.

Among other things, the revision is intended to apply greater selectivity in the designation of positions involving confidentia-

lity. Greater attention will also be given to the concept of the finality of the measure with regard to this process. It is important that employers have first instituted a cohesive package of security measures.

New guideline
The AIVD has revised its guideline with regard to the process of designation of positions involving confidentiality, in which the requirements for the designation of such positions are formulated in more detail. The focus is on national security, with reference to the seriousness and probability of a potential threat to national security. From now on, when making these designations the AIVD will apply greater differentiation, and a risk profile will be formulated for each position. The concept of the finality of the measure will also be involved in the designation process at an earlier stage.

A narrower definition of positions involving confidentiality is needed because there is a greater need in society for wider screenings in areas other than that of the protection of national security. These areas mainly concern social and private interests. This increased need for screening has stretched the limits of Task B, while actually Task B exclusively concerns the protection of national security. This is the only purpose for which justification can be found for the intrusion into a person's private life that a security screening involves. By being more selective in the designation of positions involving confidentiality, the AIVD can concentrate on its core duties.

In order to meet the wishes of users, from now on it will be possible for the occupant of a position involving confidentiality to change positions without a new security screening being necessary, subject to certain conditions. This mobility is made possible by means of linking positions with equivalent levels of

sensitivity - position clustering. The important preconditions for the application of this concept concern the up-to-date registration of the occupants of positions involving confidentiality and the issue dates of VGBs. The periodic conduct of repeat screenings is also one of these preconditions. This is a responsibility of the departments concerned.

The AIVD has now enabled position clustering for the various departments, which may apply such position clustering if they consider it to be necessary, for instance due to a high level of internal mobility, once the preconditions have been met.

Recharging of the costs of conducting security screenings
The preparations for the recharging of the costs of conducting security screenings to the public sector (the charging structure) were completed in 2012. The Cabinet decided to adopt a charging structure for security screenings on 29 April 2011.

The charging structure was implemented in the public sector as of 1 January 2013. After amendment to the Security Screening Act (*Wet veiligheidsonderzoeken*, Wvo) – expected to take effect as of 1 January 2014 – security screenings for the private sector will be charged. The charging structure is based on the actual cost, the calculation of which has been tested by the National Audit Service (Auditdienst Rijk, ADR).

New policy rules
The new policy rules 'judicial data for security screenings' and 'assessment period for insufficient data' formally came into force on 1 February 2012. These describe the situations in which judicial records are incompatible with taking up a position involving confidentiality, and elaborate the cases in which the VGB will be refused due to residence in a country with which the AIVD does not cooperate with regard to security screenings.

The new policy rules contribute to consistency in the screening process, including the use of clearly defined assessment periods.

The policy rule 'security screenings for the police' (Government Gazette 2001, 241) and the policy rule 'insufficient data for security screenings' at civil airports (Government Gazette 2001, 59) no longer apply, now that the new policy rules have taken effect.

9.2 Number of security screenings and their processing time

In 2012 a total of 40,140 security screenings of persons intending to take up a position involving confidentiality were conducted and completed, either by the AIVD or on the AIVD's instructions. In 990 cases, the screening led to the refusal or withdrawal of the Security Clearance, or VGB. The AIVD completed a total of 5,684 security screenings in categories A, B and C that were requested directly. The screening was completed within the statutory processing time in 5,348 cases (94%). By category of screening, this breaks down to 1,384 category A (94%), 3,345 category B (94%) and 619 category C (96%). The AIVD met the political commitment to complete at least 90% of the category A security screenings within the statutory processing period of eight weeks.

table 1

Decisions in 2012	VGBs issued	VGBs refused or withdrawn	Total number of decisions
Category A by the AIVD directly	1,462	12	1,474
Category B by the AIVD directly	3,533	34	3,567
Category B by the AIVD via KMar, Police, DKDB	1,341	938	2,279
Category B by KMar, Police, DKDB	32,177	0	32,177
Category C by the AIVD directly	637	6	643
Total	**39,150**	**990**	**40,140**

Checks for partner services

In addition to carrying out its own security screenings, the AIVD also conducted checks screenings for its international partner services. In 2012, 1,191 such checks were completed. The AIVD also completed a total of 2,800 international checks for the mandated organisations and for the MIVD.

Number of VGBs refused or withdrawn

990 VGBs were refused or withdrawn in 2012. A refusal or a withdrawal of a previous decision occurs if there is insufficient assurance that the person concerned will carry out all the duties arising from the position of confidentiality in all circumstances, or if the security screening does not reveal sufficient information to be able to make a well-founded decision.

Objections and appeals

In the event that a VGB is refused or withdrawn, the person concerned has a right to object to and to appeal against the decision. If the person concerned objects, they will receive a copy of the screening report, abridged if necessary. In the interests of protection of the legal rights of the person concerned, the law provides that the courts and the Council of State may examine the full report on the security screening

-including the secret sections -, as long as the subject explicitly grants them permission to do so.

table 2

Total number of objections and appeals initiated in 2012

|	Submitted
Letter of notification	2
Objection	59
Appeal	11
Further appeal	2
Further appeal to minister	
Interim injunction (objection)	
Interim injunction (appeal)	1
Interim injunction (further appeal)	
Interim injunction (further appeal to minister)	
Total	**75**

table 3

Total number of objection and appeal procedures completed in 2012 (procedures started in 2012 or earlier and completed in 2012)

	Unfounded	Upheld	Inadmissible	Withdrawn	Refused	Issued	Completed	Total
Letter of notification							2	2
Objection	29	17	11	1				58
Appeal	8	1		1				10
Appeal, legal effects stand								
Further appeal by appellant	1							1
Further appeal to minister								
Interim injunction					1			1
Total	**38**	**18**	**11**	**2**	**1**	**0**	**2**	**72**

9.3 Positions involving confidentiality in the Dutch Caribbean

The Ministry of Security and Justice has designated positions involving confidentiality at Bonaire International Airport (BIA) with effect from 15 July 2011. The AIVD conducts the security screenings of the people appointed to a position involving confidentiality at this airport. Since 15 July 2011 a total of 445 of the 453 candidates for these positions have undergone a security screening.

The AIVD provided assistance to the Saint Martin Security Service (*Veiligheidsdienst Sint Maarten*, VDSM) in 2012, after a request to do so. After an information campaign conducted by the VDSM in 2011 and early 2012, the National Decree for appointments to positions involving confidentiality and the conduct of security screenings was established by the government of Saint Martin on 21 February 2012. The National Decree came into force on 26 April 2012, and the VDSM has been authorised to conduct security screenings on Saint Martin since that date. Prior to the effective date of the Decree, the AIVD provided education and training for the employees of the VDSM. As part of its request for assistance, the VDSM requested the AIVD to provide guidance during the conduct of the first security screenings.
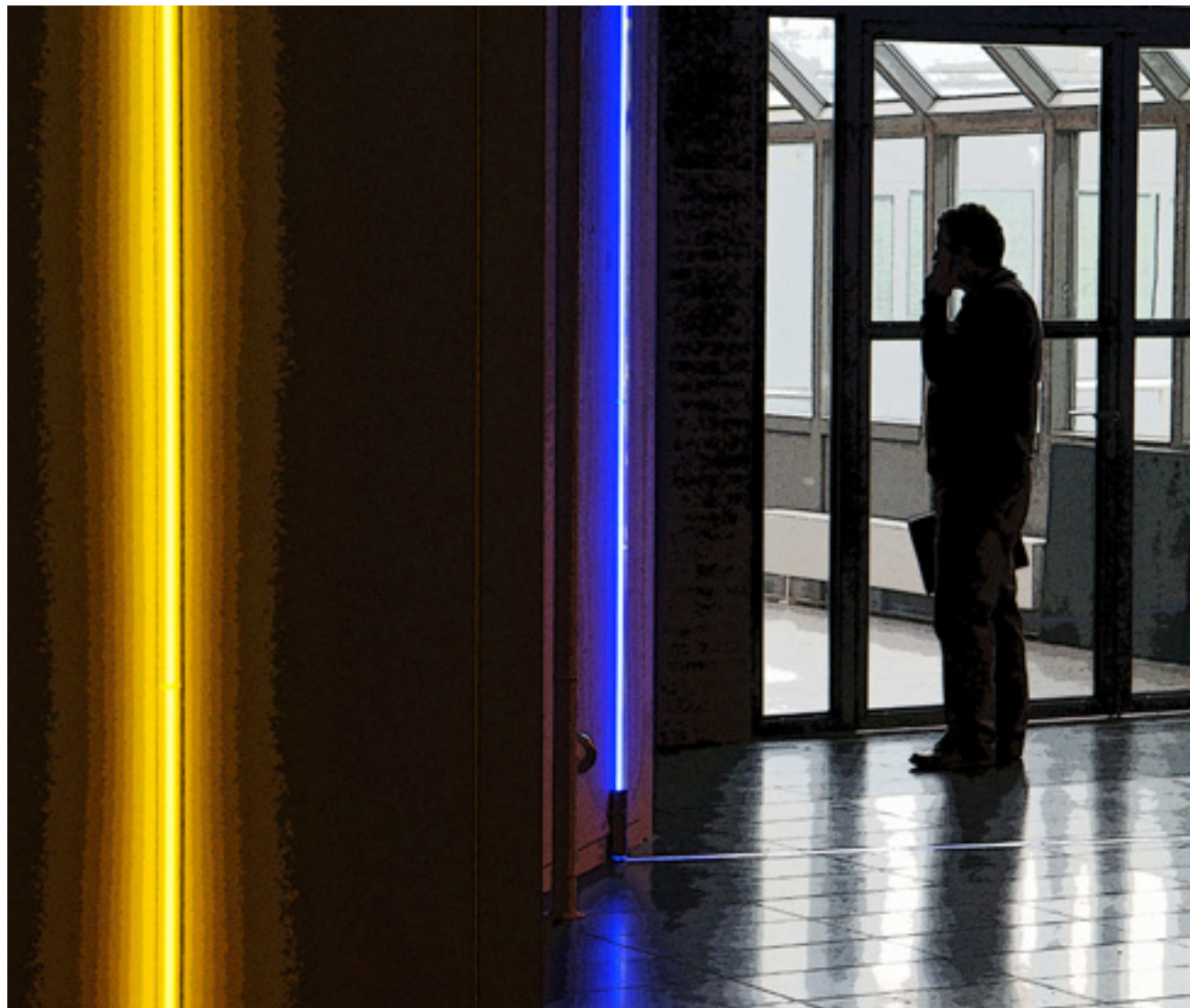
ORGANISATIONAL DEVELOPMENT AND INFORMATION MANAGEMENT

The technological advances, internationalisation and the more diffuse threat picture that the AIVD is faced with in its areas of investigation mean that the AIVD's organisation must undergo continual development. An intelligence and security service can only function if it has a complete mix of tasks, powers and resources, and therefore unique multi-source capabilities. Permanent investment is required in order to accomplish this, mainly because the creation of such a multi-source service and the related access to information takes a great deal of time.

Internationalisation and technological advances also mean, among other things, that the AIVD needs to have and to maintain access to all (very diverse) means of communication and data flows that are increasingly in use but also increasingly difficult to access. For several years the AIVD has been investing in intelli-gence resources with an international reach, such as Signals intelligence (Sigint) and Computer Network Operations (CNO).

In 2012 the AIVD made significant investments in more or less all aspects of the intelligence-gathering process. This is not restricted to expenditures for technical intelligence assets and the underlying technical infrastructure for the storage and analysis of information. It also involves the costs involved in adjusting internal working methods and implementing an associated internal education and training programme. Investment was also made in ICT resources in the area of cyber threats (including cyber espionage) and offensive technology in 2012. With these investments, the AIVD's intention is to initiate and expand strategic alliances for co-operation with national and international partners.

As a result of these expenditures, the costs of managing the ICT facilities have risen and will continue to account for a substan-tial proportion of the budget in future.

Since the processing of information by the AIVD is classified as a state secret, the requirements with regard to information security are at the highest level.

10.1 Target registration and data integration

In 2012 the AIVD adopted a new system for the processing and analysis of information flows, in which target data from various sources can be integrated. The intention is to be able to filter and select information at an early stage and to be able to analyse the behaviour of targets efficiently. In 2012 this system was used for the first time to analyse travel movements.

The use of travel information by the AIVD, also known as 'Travel Intelligence', is becoming more and more important in the fight against terrorism and in strengthening national security. We have observed that travel by jihadists to and from Middle Eastern countries has increased. In the past few years, the acquisition and analysis of travel data has continued in co-operation with other parties, and has now become an integral part of the service's operations. This makes a substantial contribution to the information available to the AIVD and enables us to respond more quickly to threats to national security.

This development underlines the importance of Travel Intelligence and justifies the heavy investment made in recent years. It also shows the need to continue to make such investment on a permanent basis.

In addition to Travel Intelligence, the AIVD participated in a joint venture with KMar, the Customs Service, IND and the Seaport Police with the objective of modernising the monitoring and supervision of the Dutch borders.

10.2 Bulk data: acquisition and analysis

The AIVD has developed a system in which new sources can be input and made searchable in an extremely rapid manner. Although the system was designed for Sigint data, its design means that it can also be used to save and search large amounts of data from other sources.

For the further analysis of these large amounts of data, the AIVD has developed applications that can generate reports and statistics on specific trends. Regarding the analysis of Sigint data, we have entered into cooperative arrangements with foreign partner services.

10.3 Digital file creation

Last year the AIVD made significant progress on improving the service's file creation and making its investigation files more easily searchable and retrievable. One of the improvements will be to introduce a system specifically adjusted for the AIVD to enable the secure processing of state secret information and the reporting of progress in investigations and the use of special powers. This process was more or less completed in 2012, and we expect to implement it in the first half of 2013.

10.4 Operational management

In 2012 the AIVD also carried out upgrades to its ICT facilities to support its operational management. Contrary to the offensive and innovative application of technology in our operational investigations, our ICT strategy with regard to operational management is conservative. Where possible, our operational management is linked to collective facilities used by central government.

In 2012 an HR management system developed together with P-Direkt was also implemented. Furthermore, we have installed a new intranet system for internal communication within the service and have implemented a new system for the digital processing of invoice flows.

10.5 Co-operation

The information processed by the AIVD in its investigations originates partly from the deployment of our own intelligence resources, but also frequently from our cooperative arrangements with partners in the security domain. In 2012 this co-operation intensified, in particular with the Regional Intelligence Services (RIS) and, with regard to Sigint and cyber security, in the Symbolon unit in co-operation with the MIVD. With regard to the conduct of security screenings, the AIVD has new access to the databases of the BES islands in the Caribbean.

These cooperative arrangements require secure network connections and a common infrastructure, in order to allow efficient exchange of investigative information. The AIVD's external infrastructure will be further expanded next year in order to strengthen our co-operation with these partners.

Topos

During 2012, the closer co-operation with partners in the security field involved the strengthening of relations with the RIS and Special Services (SS). The RIS and SS (such as the SS of the Royal Military Constabulary (KMar), the Intelligence Assistance Team of the Customs, and ID FIOD) are the detached posts: the eyes and ears of the AIVD in the Netherlands.

This closer co-operation is reflected in the institution of the Topos programme, whereby these services are prepared at a central point in the intelligence process of the AIVD. In this way they will become a fully-fledged and integral part of the AIVD. This programme will be implemented in close co-operation with the National Police.

Symbolon

The AIVD and the MIVD worked intensively in a project team on the formation of a collective Sigint/cyber unit in 2012. Both services are convinced of the need to combine and collectively develop their Signals intelligence (Sigint) and cyber intelligence capabilities. An integrated approach to the use of these technical intelligence resources will increase efficiency. The separation of substantial elements of both services and the creation of the preconditions for forming the new unit as an integral part of the intelligence-gathering process of both services have taken more time than originally expected. Nevertheless, the AIVD and the MIVD have made essential progress towards the formation of this collective unit, and have

decided to give the co-operation and input of resources a very broad scope. Decisions have also been made regarding the premises to be used by the core staff of the unit and how the unit will be managed.

At the end of 2012 a facilities coordination organisation was instituted in Zoetermeer - at the AIVD headquarters-, consisting of AIVD and MIVD employees. A facilities coordinator from the Ministry of Defence directed the formation of and further preparations for the new unit. The unit will commence operations in early 2014. With this is mind, it has already been arranged that the elements of the two services that will form part of the collective unit will be managed by the facilities coordinator with effect from 1 January 2013. Furthermore, the facilities coordination organisation includes a single point of contact for the two services, for the purpose of information exchange and co-operation with foreign partner services in the area of Sigint and cyber operations. This will directly improve our efficiency and effectiveness in the international arena.

EXPENDITURE AND DEVELOPMENT OF THE AIVD BUDGET

11.1 Income and expenditure

From almost EUR 200 million at the AIVD's disposal in 2012, approximately EUR 120 million was spent on salaries, job-related early retirement (*Functioneel Leeftijdsontslag*, FLO) and other employee-related expenses (60 percent). In addition, nearly EUR 22 million was spent on housing, EUR 35 million on ICT development and management, and around EUR 10 million on secret operations. The remaining EUR 12 million was spent on public operational duties (material expenditure).

The AIVD – in part due to its special security requirements – can only use the shared services of the Ministry of the Interior and the central government to a limited extent. For this reason the service has to provide its own supporting processes such as security, facility management, HRM and ICT, which involves high inherent costs. The fact that spending on facilities and early retirement are fixed over several years and involve legal obligations means that the service has relatively high fixed costs.

Realisation AIVD	2010	2011	2012
Expenditure	191	197.1	198.9
General expenditure	182.7	188.6	188.3
Confidential expenditure	8,3	8,6	10.6
Income	**3.2**	**1.6**	**3.1**

Analysis of expenditure by the AIVD in 2012

figure 1

Expenditure of the AIVD in 2012

- Salaries
- Early retirement
- Employee-related expenses
- Premises
- ICT
- Task budget
- Confidential expenditure
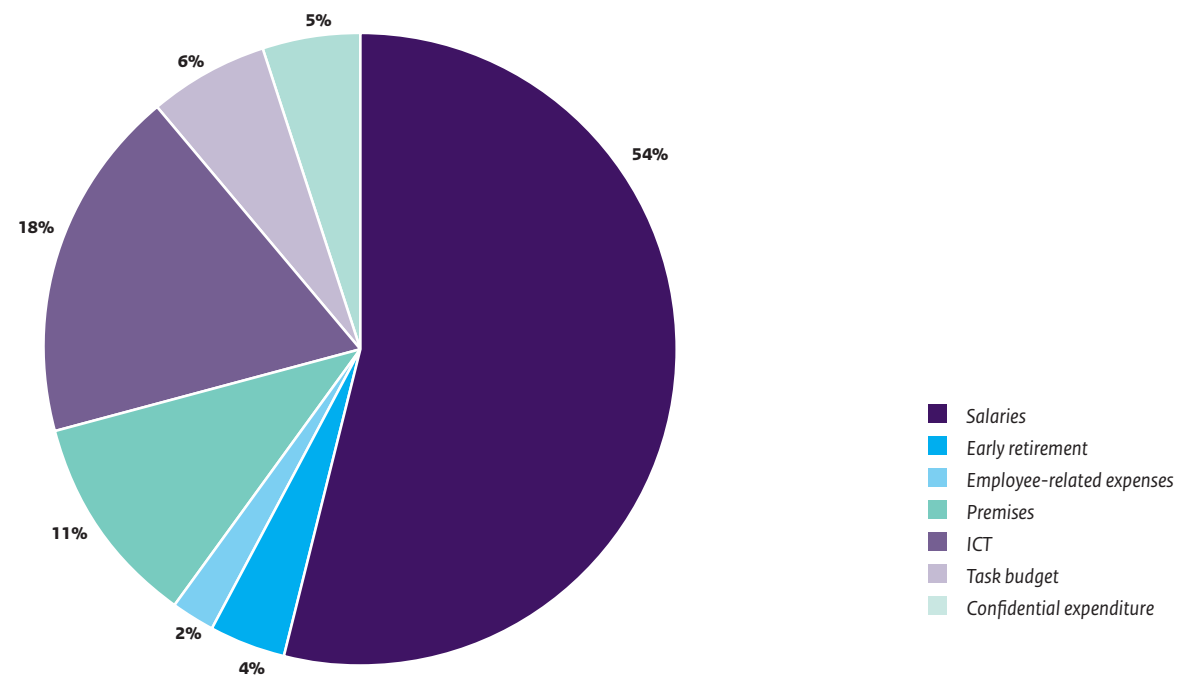
11.2 Development of the tasks and budget of the AIVD since 2000

figure 2

Development of the AIVD budget in EUR x million since 2000
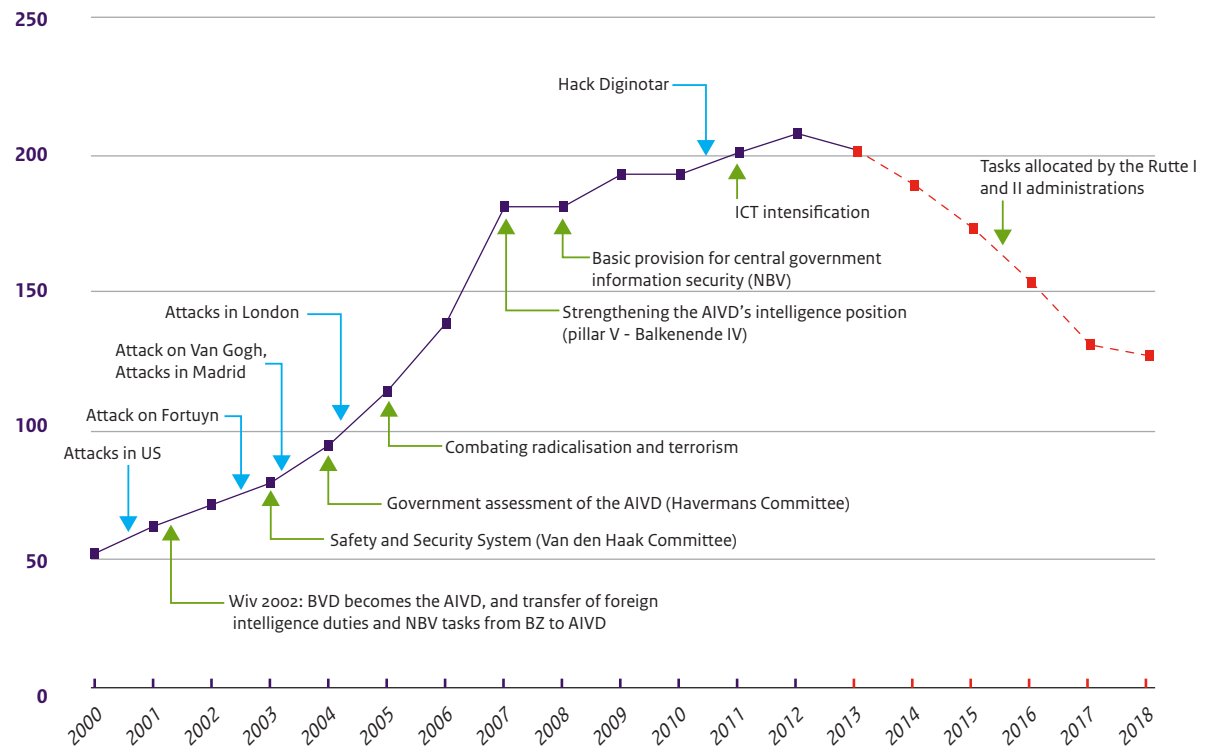
Since the year 2000, various successive cabinets have invested substantially in the AIVD, mainly in relation to developments in the international security situation. Since 2002, the AIVD has acquired new mandates, its areas of attention within its existing tasks have been significantly expanded, and expectations have increased. As a result, the AIVD's area of responsibility has expanded significantly and its budget has accordingly increased. From a small Internal Security Service (Binnenlandse Veiligheidsdienst, BVD) with a limited area of attention, we have grown into an integrated intelligence, security and Sigint service.

Apart from its wider responsibilities, the AIVD has also had to deal with mandates amounting to more than EUR 20 million, mainly from the Balkenende IV and Rutte I administrations. These are already included in the multi-year picture: partly through spending cuts and efficiency measures (amounting to approximately EUR 10 million) and partly because from 2014 onwards the AIVD should receive around EUR 11.5 million from users of security services as a result of the charging-on of the costs of carrying out security screenings. The government agreement of the Rutte II cabinet included two new tasks for the AIVD: one additional mandate and a generic mandate based on the discount percentage for BZK. Together, these mandates amount to approximately EUR 70 million on a permanent basis from 2018.

In early 2013, the Minister of the Interior and Kingdom Relations will make a proposal regarding the content of the mandates, whereby the duties of the service will be reconsidered and its priorities will be reviewed. The precise effects of this on national security will be defined as accurately as possible, as will the consequences for the AIVD's workforce, the winding down and cessation of investigations and operations, and the effects of this for the AIVD's national and international partners. The risks to national security that are considered to be acceptable will have to be defined in consultation with the House of Representatives and the users of the AIVD's services.

table 5

AIVD mandates 2014-2018

in EUR x million

	2013	2014	2015	2016	2017	2018
Multi-year expenditure (OW2013)	199.6	196.9	194.6	194.3	194.1	193.7
Additional mandate for AIVD by Rutte II		-10.0	-23.0	-35.0	-45.0	-45.0
Generic mandate BZK by Rutte II (estimate based on 13.3%				-8.9	-20.2	-24.6

ACCOUNTABILITY, SUPERVISION AND LEGAL AFFAIRS

The Minister of the Interior and Kingdom Relations has ultimate responsibility for the proper functioning and effective performance of the AIVD. The service reports to the Minister, who in turn is accountable to the House of Representatives.

Where public accountability is not possible due to the need for secrecy, reports are submitted to the Intelligence and Security Services Committee of the House of Representatives. These concern matters such as the annual plan classified as secret, the quarterly reports on the service's performance, and the secret appendix to the annual report. In addition, the external and independent Intelligence and Security Services Regulatory Commission (*Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten*, CTIVD) ensures that both the AIVD and the MIVD perform their duties lawfully.

In addition, a number of institutions oversee certain aspects of the services' activities through independent external supervi-sion. The Netherlands Court of Audit (*Algemene Rekenkamer*) checks the legitimacy of the AIVD's income and expenditure and also studies its policy efficiency and effectiveness, while the National Audit Office (*Rijksauditdienst*) scrutinises the legitimacy and financial management of the AIVD. Citizens may also submit complaints to the National Ombudsman regarding the government's performance of its duties, and therefore regarding activities carried out by the AIVD, as well. Finally, the Dutch criminal, civil and administrative courts all have jurisdiction over the service.

At parliamentary level, during 2012 various questions in the House were asked and the House of Representatives devoted extensive attention to the evaluation of the Intelligence and Security Services Act (*Wet op de inlichtingen- en veiligheidsdiensten*) 2002. The House of Representatives dealt with a total of 45 questions involving a contribution from the AIVD.

12.1 Evaluation of the Wiv 2002

The Cabinet decided to evaluate the Wiv 2002. The desire to evaluate the Wiv 2002 was expressed in the House of Representatives at the end of 2011 and ultimately was realised in the (amended) motion by Elissen/Cörüz (Parliamentary Papers II 2011/12, 29 924, no. 81) adopted by the House. This motion requested the government to conduct an evaluation of the Intelligence and Security Services Act 2002 with particular attention to the supervision of the intelligence and security services. The Minister of the Interior and Kingdom Relations (also on behalf of the Minister of Defence) outlined the general principles of the proposed evaluation in a letter to the House dated 25 June 2012 (Parliamentary Papers II 2011/12, 29 924, no. 91). The evaluation would be conducted by an independent committee formed on the basis of Section 6 sub 1 of the Advisory Bodies Framework Act (*Kaderwet adviescolleges*). The composition of the committee would be such that the necessary knowledge and expertise with regard to the evaluation of acts of parliament, human rights and the activities of the intelligence and security services - both civil and military - would be ensured. The committee was formally appointed in early 2013, and is expected to produce its evaluation report in September 2013.

12.2 Accountability and supervision

Intelligence and Security Services Committee (Commissie voor de Inlichtingen- en Veiligheidsdiensten, CIVD)
Under the Wiv 2002, the Ministers of the Interior and of Defence are empowered to inform the House of

Representatives in confidence about the methods, resources and secret sources used by the Dutch intelligence and security services, and about their current level of knowledge. They do this through the CIVD of the House of Representatives, which consists of the parliamentary leaders of all parties with elected representatives in the House of Representatives, with the exception of any group which may have split from an established party during the current session.

In 2012 the Minister of the Interior reported to the CIVD on the operational activities conducted by the AIVD by means of regular quarterly reports; these reports are the substance of the accountability process. The National Intelligence Overview (*Nationale Inlichtingenbeeld*, NIB) is the quarterly intelligence overview prepared in partnership with the MIVD. The CIVD also reviewed the AIVD's 2011 annual report, including the secret appendix and its secret annual plan.

The AIVD also provided substantive information to the committee on various aspects of its operational activities and developments in the areas of attention of the AIVD. The CIVD received a number of letters from the Minister of the Interior regarding developments in North Africa and the Middle East.

Council for the Intelligence and Security Services Committee (Raad voor de Inlichtingen- en Veiligheidsdiensten, RIV)
The RIV is a Cabinet subcommittee chaired by the Prime Minister and including the Ministers of the Interior and Kingdom Relations, Defence, Foreign Affairs, and Security and Justice.

In 2012 the responsible officials were briefed with an intelligence overview regarding countries requiring attention due to national security concerns. This enables the Dutch government to formulate its stance with regard to these countries on the basis of its own intelligence gathering. Presentations were held for the RIV, for instance on the jihadist Internet and the cyber threat to the Netherlands. The 2012 annual plan and the 2011 annual report were also discussed.

The National Intelligence Overview as discussed by the CIVD, in which the services (the AIVD and MIVD) place important current developments in an intelligence context and present their future expectations, is also a permanent agenda item.

Intelligence and Security Services Regulatory Commission (Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten, CTIVD)
The CTIVD is an independent body charged with overseeing compliance by the AIVD and MIVD with the Wiv 2002 and the Wvo.

In 2012 the CTIVD produced three regulatory reports on the AIVD. These concerned the report on previous recommendations with regard to the AIVD, the report on the legitimacy of the use of its power to effect wiretapping and the authority to select Sigint by the AIVD, and the report on the classification of state secrets by the AIVD. These reports were submitted to parliament with comments from the Minister attached. The report on the classification of state secrets by the AIVD still has to be discussed by the House of Representatives, which has already discussed the other two reports.

The CTIVD has its own website providing further information, at: www.ctivd.nl. The reports of the CTIVD and the Minister's reaction thereto are published here. The CTIVD produces its own annual report, which is also available on this website.

12.3 Legal Affairs

Amendment to the Intelligence and Security Services Act 2002
Preparatory work was carried out on the amendment of the Intelligence and Security Services Act 2002 in the area of Sigint and cyber intelligence in 2012, in particular as a result of the regulatory report of the CTIVD regarding the use of Sigint by the MIVD (CTIVD no. 28). The proposals, which mainly concern revision of the provisions in relation to the interception of telecommunications, are included in the parliamentary bill that was in preparation in 2011. In this last-mentioned bill, various proposals from the bill withdrawn in March 2011 (Parliamentary Papers 30 553; the so-called post-Madrid bill), have been included again after being updated as necessary. The bill is currently at an advanced stage of official completion. The bill will not be further processed until the results of the evaluation of the Wiv 2002 are available, which is expected to be in September 2013. The results of the evaluation, to the extent these give reason for a change to the legislation, will be included in this bill.

Amendment to the Security Screenings Act

In 2012 a proposal to amend the Security Screenings Act (Wet veiligheidsonderzoeken, Wvo) was formulated. The intention of this bill is to create a statutory basis in the Wvo for the charging-on of the costs involved in the conduct of security screenings in the private sector. The bill was accepted by the Council of Ministers at the end of 2012 in connection with the request for advice to the Council of State. The amendment to the Act should take effect on 1 January 2014.

European Court of Human Rights ruling in the Telegraaf case

On 22 November 2012, the European Court of Human Rights (ECtHR) issued its ruling in the case against the Netherlands brought by De Telegraaf and others. [5] This concerned a complaint by De Telegraaf and others regarding the application of special powers by the AIVD and the seizure of state secret documents as part of a criminal investigation into the dissemination of these documents. In its ruling, the unanimous opinion of the ECtHR was that the application of special powers by the AIVD against the journalists of De Telegraaf was in breach of Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (now known as the European Convention on Human Rights, ECHR) (the right to respect for private and family life) and Article 10 ECHR (freedom of expression).

The intention of the ruling will be included in the amendment to the Wiv 2002 for which a parliamentary bill is in preparation.

Freedom of information requests

In 2012 extensive use was made, once again, of the statutory right to inspect information held by the AIVD in 2012. This right only applies to information that is not relevant to current AIVD activities. Outdated material will also not be released if this would or might compromise the service's sources and methods. In addition, the personal data of third parties will only be released for deceased family members in the first degree.

---

5   Case of Telegraaf Media Nederland Landelijke Media B.V. and others v. The Netherlands (Application no. 3931 5/06).

The procedure and conditions applying to freedom of information requests are described further on the AIVD's website.

The number and nature of freedom of information requests and how they were dealt with are shown in the tables below.

table 6
Number of requests for information

	Submitted	Dealt with	Granted
Requests	208	221	114
Objections	26	27	3
Appeals	5	5	
Further appeals	2	1	

table 7
Number of requests

Subject of request	Submitted	Dealt with	Granted
Applicant	117	126	50
Deceased relative	25	27	17
Non-personal matters	58	60	47
Third party	8	8	
Total	**208**	**221**	**114**

table 8
Procedures conducted

	Dealt with	Unfounded	Upheld	Inadmissible	Withdrawn
Objections	27	23	3	1	
Appeals	5	4			1
Further appeals	1	1			

Notification

Section 34 sub 1 Wiv 2002 imposes a duty of notification upon the AIVD. Specifically, this requires that, five years after the completion of certain investigations involving its special powers, the service reviews whether the subjects can be notified that they have been investigated. Since this duty of notification only covers enquiries regulated under the Wiv 2002, which took effect on 29 May 2002, the duty of notification has effectively existed only since 29 May 2007.

Moreover, compliance with the duty of notification may be annulled, deferred or suspended if, for example, the subject is untraceable or an ongoing investigation might be compromised. The same applies if notification could endanger sources or damage international relations. No notifications were issued in 2012. The first notification reports will be issued in 2013. The CTIVD closely monitors the service's policy and practice in respect of the duty of notification.

Complaints

Under Chapter 9 of the General Administrative Law Act (*Algemene wet bestuursrecht*) and Sections 83 and 84 Wiv 2002, any person is entitled to submit an oral or written complaint with regard to the manner in which the AIVD or an employee of the AIVD has behaved towards him or another person. After a complaint is made, it is considered whether this can be dealt with in an informal manner. If this is not possible or successful, the matter is referred for advice to the CTIVD, which takes charge of dealing with the complaint. If the complainant is not satisfied with the handling of his complaint, he may apply to the National Ombudsman.

The AIVD received ten complaints in 2012, seven of which were referred to the CTIVD for advice. Of these complaints, in one case the CTIVD advised that part of the complaint should be upheld. This case will be dealt with by the AIVD in 2013. The committee also advised that part of one complaint submitted in 2011 should be upheld. This case was dealt with by the AIVD in 2012, and the committee's advice was followed. In the other cases referred to the CTIVD, including two complaints submitted in 2011 and dealt with in 2012, the complaints were declared to be unfounded either on the committee's advice or on the basis of the facts. In addition, two complaints were immediately dealt with, to the complainant's satisfaction, while one complaint was withdrawn by the complainant.

The National Ombudsman dealt with one complaint regarding the AIVD in 2011 that was still being dealt with in 2012. The National Ombudsman also took one complaint regarding the AIVD into consideration in 2012, and has chosen not to issue a report with regard to this case.

| 73

appendices

MISSION AND TASKS OF THE AIVD

Mission

The AIVD safeguards the national security of the Netherlands through the timely identification of threats, international political developments and risks that are not immediately visible. To this end, the AIVD conducts investigations both in the Netherlands and abroad. Where necessary, the AIVD shares knowledge and information so that partners and other interested parties can take appropriate measures.

The AIVD identifies risks and advises and mobilises third parties. And, if necessary, it works actively to reduce risks itself. Thus the service has a clear position in the network of official organisations dedicated to the protection of national and international security.

The AIVD focuses on risks and threats that might potentially have a major impact on national and international security interests of the Netherlands. From its independent intelligence position, the AIVD seeks to provide its stakeholders and partners with context, unique information and perspectives, so that threats to Dutch national security can be identified in good time and reduced as necessary.

The tasks of the AIVD
The tasks of the AIVD are defined by law in Section 6 sub 2 at items a to e of the Intelligence and Security Services Act 2002 (*Wet op de inlichtingen- en veiligheidsdiensten 2002*, Wiv 2002). For the performance of these tasks the AIVD is authorised to use special powers. The Minister of the Interior and Kingdom Relations is responsible for the AIVD's proper conduct of its assigned tasks.

As defined in the Wiv 2002, the work of the AIVD consists of "safeguarding the democratic legal order, the security of the Dutch nation and other important state interests". The service is expected to act if any of these national or international security interests are at stake and especially if the risks or threats to these interests:

- are clandestine in nature (if they are invisible or difficult to detect by parties without the AIVD's special powers);
- are prompted by undemocratic political intentions or involve an attempt to change or disrupt our society through undemocratic means;
- could have a major impact on the national or international security interests of the Dutch state or society.

In the case of Task A, the subjects for investigation are determined using risk analyses and assessments. These consider the national security interests of the Dutch state and society, the risks or threats to these interests and the present level of resilience, which includes checking whether other government agencies are already involved in identifying or attempting to reduce the threat in question.

Task B, the conduct of security screenings for persons intending to take up positions involving confidentiality, has its own statutory basis in the Security Screenings Act (*Wet veiligheidsonderzoeken*, Wvo). Such positions are designated by the responsible government ministers or employers, with the AIVD acting in an advisory capacity.

The scope of Task D is defined in the Foreign Intelligence Designation Order (*Aanwijzingsbesluit Buitenland*) which is established by the Prime Minister in consultation with the ministers of the relevant government departments. This is preceded by a process in which the end users' interests and

information needs are weighed against the threat assessments compiled by the AIVD (and the MIVD), as well as their operational capabilities and the risks involved.

For Tasks C and E, the choices as to which institutions, sectors or subjects to focus on are in part the AIVD's own responsibility, based upon its in-house expertise, and in part are made jointly with government departments or agencies.

Tasks

Under Section 6 sub 2 at items a to e Wiv 2002, the AIVD has the following tasks.

Task A: *To investigate people and organisations reasonably suspected of representing a serious danger to the democratic legal order, to national security or to other important state interests.*

Task B: *To screen candidates for positions involving confidentiality, and also to issue recommendations regarding which positions should be designated as such.*

Task C: *To promote security by interpreting information regarding threats and by sharing this information with affected parties, and also to promote the security of information and communications.*

Task D: *To conduct investigations with respect to other countries, also referred to as the foreign intelligence task.*

Task E: *As part of the national Safety and Security System, to compile risk and threat analyses with the object of protecting people, property and services in the national security domain.*

GLOSSARY

Activism
The general name for the phenomenon where people or groups operating outside of the parliamentary system, but within the limits of the law, strive to improve the rights and living conditions of individuals, groups and animals.

Counter-terrorism alert system
A warning system for the government and industry that warns operational services and business sectors in the event of a heightened threat. This enables measures to be taken quickly that can reduce the risk of an attack or limit the effects thereof.

Al-Qaeda
In current usage, this refers collectively to both core Al-Qaeda and to networks associated with it. These are allied with one another ideologically: the leaders of local jihadist groups adopt the ideology of international jihad propounded by core Al-Qaeda and swear allegiance to the leader of core Al-Qaeda.

They subsequently use the name Al-Qaeda, followed by the name of the area in which they are active. Examples of this are Al-Qaeda in the Islamic Maghreb (AQIM) and Al-Qaeda in the Arab Peninsula (AQAP). While these groups support the international jihad, they also pursue their own agenda. There is not necessarily any co-operation or control relationship between core Al-Qaeda and the affiliated organisations. Because the term 'Al-Qaeda' can refer to different groups, its use presents difficulties in practice. As a rule therefore, the specific name of the organisation in question is used.

Official report
A notification, usually in writing, to an individual or institution concerning personal or other details obtained by the AIVD that could be of interest to the recipient in discharging their responsibilities with respect to the interests they are charged with protecting.

Anarchist extremism
This refers to various overlapping forms of action, with general mutual support for each other's protests. These (often radical) protests are based on an anarchist ideology and take extremist form, including large-scale vandalism and arson in some cases. These protests may also involve personal intimidation.

Special intelligence resources
Technical and other instruments which are deployed in the exercise of a special power under the Wiv 2002 and which are usually secret in nature.

CBRNe weapons
The term for chemical, biological, radiological and nuclear weapons and home-made explosives.

Dual-use goods
Goods or materials that can be used for either civilian or military purposes. This term is used in the fight against the further proliferation of weapons of mass destruction.

Extreme
Individuals, groups or organisations are defined as extreme when their actions extend to but do not exceed the boundaries of what is acceptable within a democratic legal framework.

Extremism, extremist
The phenomenon whereby people and groups, when striving to improve the rights and living conditions of individuals, groups or animals, deliberately commit illegal and sometimes violent acts.

Violent jihad
The armed struggle against supposed enemies of Islam, legitimised by the invocation of Islamic legal doctrine.

Islamism, Islamist
A radical movement within Islam which seeks to make society a reflection of what it claims is prescribed in the original sources of the faith: the Koran and the sunnah (the sayings and practices of the Prophet). Islamism has a political agenda which may find its expression in violent or non-violent or even democratic forms, and is related to Salafism.

Jihadism
An extremist ideology based upon the glorification of violent jihad.

Jihadist network
A fluid, dynamic and vaguely delineated structure consisting of a number of radical Muslims with some form of mutual association, both individually and at collective level in the form of cells or groups. At least temporarily, they are linked by a common purpose: the pursuit of a jihadist aim. For the AIVD, a person involved in a jihadist network is classified as a member if they play an active part in it and consciously contribute towards achieving the jihadist goal.

Countries of concern
Countries suspected of developing weapons of mass destruction and their delivery systems, and which pursue objectives that may pose a threat to the international legal order and to the security and interests of the Netherlands and its allies.

Delivery systems
The means of delivery necessary for the effective use of chemical, biological, radiological and nuclear (CBRN) weapons, such as ballistic missiles, cruise missiles and unmanned aircraft.

Position involving confidentiality
A job or other appointment in which abuse of office could seriously compromise national security or other important interests of the state. This is the case when there is access to state secrets, when a lapse of integrity could endanger national security, and with respect to certain specific positions in vital sectors.

Proliferation
The (further) spread of weapons of mass destruction (chemical, biological, radiological and nuclear weapons) and of their delivery systems.

Radicalisation
A growing willingness to pursue and/or support fundamental changes in society that would endanger the democratic order, possibly by undemocratic means which are in conflict with or could pose a threat to that order.

Radicalism
The pursuit and/or support of fundamental changes in society that would endanger the democratic legal order, possibly by undemocratic means which are themselves in conflict with that order.

National security domain
People, premises, services and events for which the central government bears a responsibility because of their importance to the Dutch state and Dutch society.

Salafism
A broad ideological movement which seeks a literal return to the 'pure' Islam of the faith's early period.

Separatism
Attempts by a particular section of a population to shake off existing national ties and establish a state of its own.

Sigint (Signals intelligence)
The interception and localisation of electronic signals transmitted on radio frequencies.

Safety and Security System
A cooperative arrangement led by the Safety and Security Unit of the National Coordinator for Counter-Terrorism (the NCTV), on behalf of the central government. This cooperative system bears responsibility for the security of people, property and services within the so-called national security domain in the Netherlands. The AIVD provides threat information concerning these subjects within the Safety and Security System framework.

Terrorism
Ideologically motivated actual or threatened violence against persons, property or the fabric of society, with the aim of bringing about social change, creating fear amongst the population, or influencing the political decision-making process.

Travel Intelligence
The acquisition and analysis of travel information.

Security screening
An investigation of a person in search of facts and circumstances which on grounds of national security may be relevant to their holding a specific position involving confidentiality.

Vital sectors
Sectors and sections of the national infrastructure which are so crucial that their failure or serious disruption could cause major damage to Dutch society.