Ministry of Defence

PEACE & SECURITY THROUGH FORESIGHT

Netherlands Defence Intelligence and Security Service

Protecting that which we hold dear

2019 Annual Report

PEACE & SECURITY THROUGH FORESIGHT

Netherlands Defence Intelligence and Security Service

Protecting that which we hold dear

2019 Annual Report

CONTENTS

FOREWORD BY DIRECTOR OF DISS

The work done by the Netherlands Defence Intelligence and Security Service (DISS) is essential, every single day, since it protects the security of our military personnel and our country. I am incredibly proud of our people: the professionals with their military heart and their dedication to their exceptional and responsible work, which they often cannot even disclose at home.

In this annual report we describe the work that we carry out as an intelligence and security service. The report is an opportunity to clarify the tasks that our service shoulders. As director of DISS, I would like to highlight two points in particular.

First, the enormous range of increasingly complex threats that exist in the hazy space between war and peace – the 'grey zone' – is a factor that is requiring steadily more attention. Even as these threats become more and more concrete, in many cases they remain invisible. Undeniably, the nature of international relations and the manifestations of conflict and war are changing. Increasingly, inter-state conflicts and competition for global or regional leadership play out not only in the military domain but across all domains.

Like other countries, the Netherlands is confronted on a significant scale with undesirable and covert influencing, digital espionage and sabotage, and an intensifying intertwinement of national security and the economy. In fact, digital espionage, carried out by state actors such as the Russian Federation and China and targeting governments and businesses, cannot only potentially disrupt our vital infrastructure but is one of the greatest threats facing the Netherlands and its allies. Not only have threats to our values and interests become more complex, but it is also becoming increasingly difficult to identify those who take aim at these values and interests. If, as a country, we fail to keep sight of the threats arising in the 'grey zone', and if we fail to ensure that both our government and our society are better equipped to deflect them, then we are putting our freedom and prosperity at risk.

Second, DISS must ensure that it remains capable of monitoring these threats in its capacity as an intelligence and security service.

With the adoption of the Intelligence and Security Services Act 2017 (Wiv 2017), both DISS and the General Intelligence and Security Service (GISS) now have even more instruments with which to identify threats. And these instruments are crucial, given the significant challenges faced by intelligence services as a result of the widespread use of modern capabilities and new information technologies. At the same time, deploying them on a day-to-day basis while remaining within the limits of the law has proven complex. To an extent, this is because the Wiv 2017 is ambiguous on some points. An independent committee will therefore begin an evaluation of the legislation this year. In my view, our common objective continues to be a legal framework whose guarantees are as effective as possible with regard to both the privacy of our individual citizens and the service's ability to competently carry out the tasks intended to protect these same citizens.

Whatever the outcome of the evaluation, our service's highest priority this year is to implement the Wiv 2017. A main precondition for doing so is the modernisation of our IT infrastructure and information management, areas in which investments have been made in the past year and will continue to be made in the future.

The main pillar of reliability, integrity and decisiveness continues to be our DISS staff members, who are well aware of the exceptional responsibility they carry and deeply committed to staying ahead in a landscape of rapidly evolving threats.

I am proud of our organisation, and fully confident that in the coming year our people will continue their efforts in support of the security of the armed forces of the Netherlands. Freedom is not a given.

Major General Jan R. Swillens
Director, Netherlands Defence Intelligence and Security Service

DISS mission statement
We are DISS, the military eyes and ears of the Netherlands, whose task it is to protect that which we value. We detect and uncover that which others seek to keep hidden. We operate around the world in cooperation with our partners and allies. In this way our armed forces can do all that is necessary, both today and in the future. In our rapidly changing world, our intelligence makes a world of difference. We know who our opponents are. We predict threats, identify opportunities and safeguard our military secrets and expertise.

Our intelligence helps our politicians and military decision-makers choose the best possible path. Our assessments are arrived at independently. We enhance the security and resilience of the Netherlands.

Our people are our strength. Our team reflects the best aspects of all of our diverse backgrounds and experience. We are professional, flexible and persevering. Working in the shadows, we perform our difficult tasks both in the Netherlands and abroad, and in the physical and digital domains. We are aware of our exceptional position and act responsibly. We are ordinary people with a military heart and a special task.

The DISS mission statement was compiled in September 2019 by DISS personnel, who consist of 40% military personnel and 60% civilians.

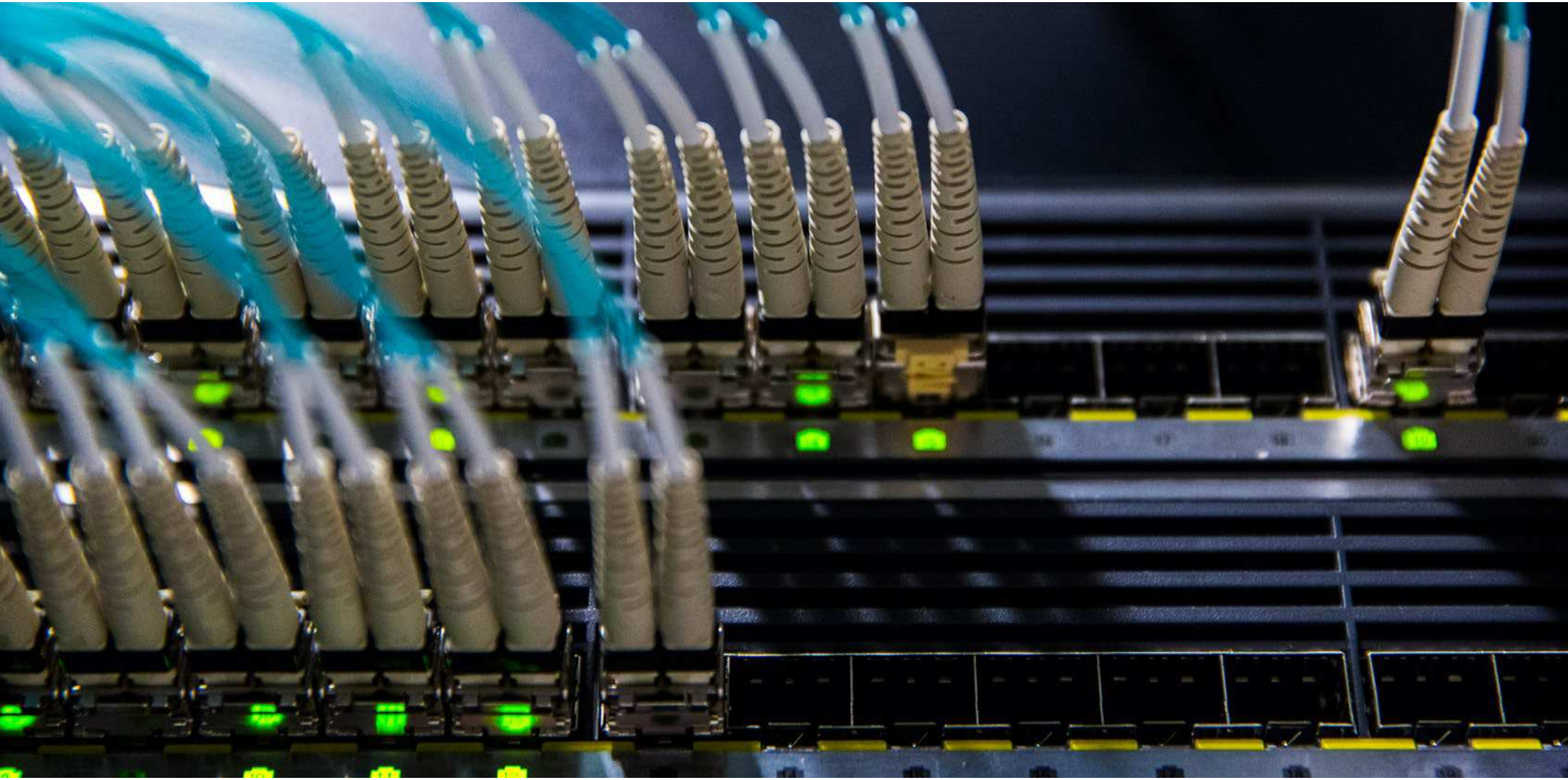
1 THREATS: HERE AND NOW

In 2019 the Dutch armed forces were once again faced with complex and multifaceted threats. Some of these threats arose from shifts in the global balance of power, and others from assertive actions by state and non-state actors deploying new technologies that have had substantial impact. These capabilities and their deployment are often invisible and difficult to signal at an early stage, while identifying perpetrators also presents challenges. With regard to the traditional arenas, the Russian Federation and China have made considerable efforts to expand and update their military capabilities in a bid to achieve more rapid effects over greater distances. Their modern air defence systems and anti-ship missiles – which they also sell to other countries – enable actors to threaten and seal off large areas. Besides traditional operations, conflicts increasingly play out in the grey area between war and peace and on a range of front lines. Cyber attacks can inflict significant political, military and economic damage. The potential digital disruption of vital infrastructure and essential operations is among the greatest cyber threats to the Netherlands, its allies and the operational readiness of the armed forces. Cyber has become a fully-fledged domain of military operations.

Besides engaging in undesired foreign political interference and influencing media and public opinion through disinformation and fake news, states also conduct economic espionage in the cyber domain and elsewhere. Such activity is often an element of a hybrid conflict. In terms of hybrid activity impacting European security, the Russian Federation is the major player and has the capability to effect an integrated deployment in Europe of every element in its arsenal. Influence campaigns are central to the Russian modus operandi. In a global trend, the Russian Federation uses targeted information operations to exploit topics intended to sow dissent among various target countries and in alliances. In this respect, social polarisation and fragmentation in the political landscapes of a large number of countries play into its hand.

A key aspect of the Russian hybrid strategy is the deployment of military and other capabilities, such as its intelligence and security services. This could include cyber units, including those linked to the Russian military intelligence service (GRU), militias such as the 'little green men' deployed during the Russian annexation of Crimea, and proxies such as non-governmental organisations (NGOs) and private military companies, for example the now familiar Wagner company. The deployment of these entities to the east of Europe, in Ukraine, in southeastern Syria and in southern Libya helps the Russian Federation to achieve its geopolitical aims while avoiding formal involvement.

Influence campaigns are also a central element of the Chinese modus operandi, and are geared to creating strategic conditions favourable to China's broader security and defence policies. China has a growing arsenal of capabilities with which to realise this, ranging from advanced cyber capabilities for espionage and misinformation campaigns that could, for example, target elections in Taiwan or influence the global perception of the resistance movement in Hong Kong, to military and paramilitary units that could be deployed in service of its territorial claims in the South China Sea.



The deployment of economic resources and the fostering of strategic and technological dependency are elements of a power politics that operates just under the threshold of warfare. For instance, China can manipulate trade, investment and tourism to exert economic pressure intended to undermine alliances and to impose its influence on international forums, not only in its own region but also in South America, Africa and Europe, including the Netherlands. Through the takeover of and investment in vital infrastructure and businesses engaging in the development of high-level technologies, states can create undesirable dependencies that entail risks to the Dutch economy and national security. Such a situation poses a threat to the continuity of our vital processes and opens the way for leaks of knowledge as well as classified and sensitive information. The defence industry is equally at risk of economic and traditional espionage. This is particularly the case as the Defence organisation becomes increasingly reliant on open-market partnerships. Strengthening the resilience of the Defence organisation and these commercial partners will require increasing capacity and attention.

New technologies and capabilities pose an even greater threat when they fall into the hands of hostile groups and individuals. One example of this is the exploitation of social media by jihadist groups, who use it to encourage 'lone wolf' attacks. The deployment of unmanned aerial systems (UASs) by opponents in mission areas has also become a commonplace threat.

In facing the task of addressing these complex, comprehensive and often invisible threats, DISS is reliant on the people and resources at its disposal and is bound by administrative and legal frameworks. The results of its efforts are described in this report.


F805
P842

2 CAPABILITIES AND SCOPE

2.1 *Legal and political scope*

Legal scope

DISS requires various powers in order to gather intelligence and counter-intelligence on the militarily relevant intentions, capabilities and activities of specific countries, groups and regions. The Wiv 2017 provides a legal framework for exercising such powers and sets out conditions for their lawful application, including the requirement to process data in a highly targeted manner and guarantee the protection of personal data. DISS complies with all these conditions. Correct application of the law is also vital to ensure the confidence of politicians and society in DISS's work. In addition, the Dutch Review Committee on the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* – CTIVD) provides continuous independent oversight, while the Review Board for the Use of Powers (*Toetsingscommissie Inzet Bevoegdheden* – TIB) assesses in advance whether the exercising of a number of specific special powers is within the law.

In 2019 the implementation of the Wiv 2017 was assigned the highest priority, with new personnel appointed and existing personnel freed up for this purpose. While important steps have been taken, the risk of unlawful action continues to exist, as concluded by the CTIVD in its third progress report. The modernisation of DISS's IT infrastructure and data management systems is a vital factor in the further implementation of the Wiv 2017, and steps have been taken to this end. The implementation of the Wiv 2017 will again be assigned the highest priority in 2020, with attention devoted to duty of care, quality of data processing and responsible data reduction. While DISS will continue to carry out its operational duties throughout this process, seeking a balance between these tasks remains a challenge.

Regulatory tasks

Review Board for the Use of Powers

The Review Board for the Use of Powers (*Toetsingscommissie Inzet Bevoegdheden* – TIB) assesses whether a number of special powers for which the minister has granted permission are exercised within the law, and its decisions in such matters are binding.

Dutch Review Committee on the Intelligence and Security Services

The Dutch Review Committee on the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* – CTIVD) is an independent body that assesses whether DISS and GISS operate within the law. The CTIVD also handles complaints concerning the actions of DISS and GISS and reports of suspected criminal actions committed by the services.

Administration

The Secretary-General of the Ministry of Defence is responsible for directing DISS, while the Minister of Defence holds ministerial accountability for DISS. The Netherlands Joint Intelligence Committee (*Commissie Veiligheids- en Inlichtingendiensten Nederland* – CVIN) is officially responsible for carrying out the ground work for decisions pertaining to security and intelligence policy. Decisions are subsequently taken by the Security and Intelligence Council (*Raad Veiligheid en Inlichtingen* - RVI), a Cabinet subcommittee, and final decisions by the Cabinet.

Accountability

The Minister of Defence is accountable before Parliament regarding DISS's activities. If information can be shared with the public, the minister gives account before the Parliamentary Standing Committee on Defence; if it must remain secret, the minister gives account before the Committee for the Intelligence and Security Services (*Commissie voor de Inlichtingen- en Veiligheidsdiensten* – CIVD) The director of DISS attends the CIVD meetings as the minister's advisor.

2.2 *Personnel and resources*

Working at DISS is no ordinary job. DISS personnel are sent to mission areas, must initiate investigations, are digitally savvy, operate covertly, work irregular hours or expose themselves to risks not faced elsewhere, and are unable to disclose information about their work to family members due to its secretive nature. Personnel are DISS's most valuable assets. DISS invests in the retention of its existing personnel, among other things by offering them loyalty premiums and improving their working environment. In 2019 DISS launched a reorganisation of its primary structure in order to boost its effectiveness and agility.

DISS grew in 2019. More effort is required to recruit some categories of military personnel and specialists such as IT and cyber experts than others, and this is an area of concern across the entire Defence organisation. But an expanding workforce also requires larger accommodation. In 2019 renovations were carried out to provide extra space, and additional rooms will become available when work is completed in 2020. A shared location for GISS and DISS (to be known as the AMF) is scheduled to be completed at the Frederikkazerne barracks in The Hague in the long term. The intention of the Minister of the Interior and Kingdom Relations and the Minister of Defence to build shared accommodation for GISS and DISS was confirmed in the Letter to Parliament of 1 July 2019 (Parliamentary Paper 30 977, No. 155). According to the current schedule, construction of the AMF will be completed in 2028 and occupation will begin in 2029. Until then, the existing accommodations will be upgraded in compliance with prevailing standards.

Information technology

Just as people are vital to DISS, so are its resources. DISS is developing into a data-driven organisation, since data is indispensable for its activities. In 2019 DISS faced the task of bringing its IT and information provision systems up to par. The Ministry of Defence will invest in DISS's IT requirements in the coming years. A multi-year, step-by-step programme has been developed to reduce the IT backlog and create platforms in a robust information domain.

DISS's current priority is to increase its IT workforce and to create a data management system in compliance with the law, which will contribute towards the overall improvement of its business processes. In 2019 a small number of additional personnel were taken on for this purpose. Technical and operational facilities are also undergoing improvement to enable IT systems to operate independently or with partners across the globe to collect, process and disseminate data around the clock.

2.3 *Cooperation*

DISS constantly seeks opportunities to engage in new, or strengthen existing, cooperative partnerships with government organisations and knowledge centres at the national and international levels, both inside and outside the Defence organisation.

Besides the Defence Intelligence and Security Network, crucial national partners include GISS and the National Coordinator for Security and Counterterrorism (*Nationaal Coördinator Terrorismebestrijding en Veiligheid* – NCTV).

The Defence organisation

The various Defence departments represented in the Defence Intelligence and Security Network work together to ensure the continued efficiency and security of the Defence organisation. DISS and the Defence Cyber Command (DCC) provide mutual support in the deployment of military personnel in the digital domain. DISS also supports the branches of the armed forces and the Special Operations Command (SOCOM). The Joint Intelligence, Surveillance, Target Acquisition and Reconnaissance Command (JISTARC) is a key operational and tactical partner in the Defence network. DISS also provides input intended to boost information-driven operations by the armed forces, and works closely with the Defence Intelligence and Security Academy and the Dutch Defence Academy in the areas of intelligence courses and innovation.

In order to conduct information-driven operations, DISS must be capable of acquiring all relevant information at any required level and processing and disseminating it in a timely manner to ensure it is present in the right place at the right time in order to achieve the desired effects.[1]

1 Netherlands Defence Doctrine, February 2019, page 91

GISS

DISS cooperates closely with GISS in a number of joint teams such as the Counter Proliferation Unit, the Caribbean Region Team, the Security Screening Unit and the Joint Sigint Cyber Unit (JSCU). The joint initiatives of the two services include frequent, constructive consultations pertaining to the intelligence process and technical support domain, which are held at all levels of their organisations, both on the work floor and between their directorates.

NCTV

The NCTV is responsible for policy, measures and coordination in the areas of counter-terrorism, cyber security, crisis management and threats posed by state actors. To this end DISS provides information and intelligence products to the NCTV and participates in NCTV consultative forums and working groups.

Cooperation between DISS and the NCTV includes strategy relating to attack capabilities; the risk and crisis management agenda; the counter-terrorism alert system; civil aviation security; surveillance and protection; chemical, biological, radiological and nuclear (CBRN) weapons; the Counter-Terrorism (CT) Infobox; the Cyber Security Assessment for the Netherlands; the Terrorist Threat Assessment for the Netherlands; misinformation; unmanned aerial systems (UASs); economic security; integrated terrorism strategy; national counter-terrorism strategy; national security strategy; the Netherlands cyber security agenda; undesirable foreign interference in the form of radicalisation; threats posed by state actors; and vital infrastructure.

International cooperation

DISS cooperates with foreign intelligence and security services. By exchanging information the services strengthen their own intelligence positions, and by organising joint training and sharing information on developments in the field they boost the quality of their intelligence products. Cooperation can also help resolve challenging issues arising from technological innovations. DISS consults with other services to discuss the impact on their procedures and organisations of artificial intelligence, information-driven operations, cyber, social media and associated security aspects, and to learn from their experiences in a process of mutual enrichment and reinforcement.

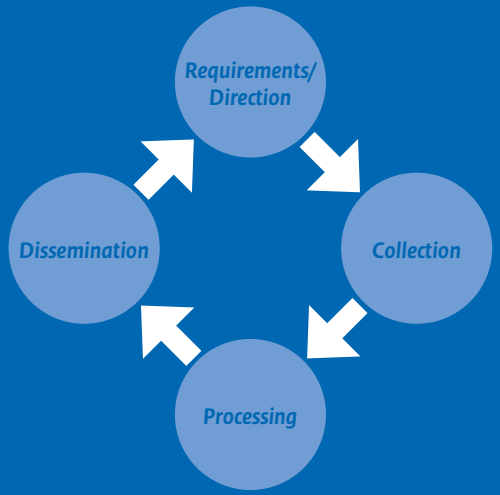
The terms under which DISS is permitted to exchange information or engage in other forms of cooperation with foreign services are laid down in the Wiv 2017. Since 2018 these terms have been detailed in partner assessments, which list the five criteria governing cooperation between services: democratic embedment, respect for human rights, professionalism and reliability, legal powers and instruments, and data protection. The risks associated with cooperation are identified for each criterion in order to prevent potential risk to Dutch civilians and DISS. No cooperation is entered into without a partner assessment. International cooperation also occurs with alliances such as the North Atlantic Treaty Organisation (NATO) and the European Union (EU).

2.4 *Intelligence process*

The Integrated Intelligence and Security Directive lays down specific agreements concerning the focus areas and depth of investigations conducted by DISS. The Directive is established for a period of four years by the Prime Minister, the Minister of the Interior and Kingdom Relations and the Minister of Defence following consultation with the Minister of Foreign Affairs and the Minister of Security and Justice, and is reviewed annually to establish whether any amendments are called for. Investigation orders are contained in the Directive and constitute the basis for DISS's annual plan and intelligence cycle.

Intelligence cycle

The intelligence cycle comprises the process and methods used to compile threat analyses and intelligence and counter-intelligence products for requisitioners and consists of four phases.



3 RESULTS: WORK IN 2019

3.1 *Russian Federation*

The European security landscape has changed fundamentally over the past decade, with a substantial increase in threats posed to Dutch, European and allied interests by Russian espionage, cyber and hybrid operations and, no less so, military capabilities. The Kremlin's ultimate aim is to inflict disruptive change on the European security architecture, thus weakening or negating the role of NATO. This aim is in line with the Russian world view in which each great power is entitled to maintain an exclusive buffer zone consisting of peripheral countries. A concerning development is the Kremlin's increasingly frequent representations of relations between itself and the West as ideological stand-offs in which opposing value systems are at odds with each other.

Also alarming is the increasing military threat that is arising as Russian military power grows strongly. Regionally, primarily but not exclusively in the Baltic Sea region, the Russian Federation has at least initial conventional and tactical nuclear dominance. It is capable of initiating a military operation with limited geographical objectives, virtually without prior warning, against NATO and, in principle, bringing such an operation to a successful conclusion. The Russian Federation has an extremely rapid decision-making chain, very rapidly deployable units, offensive long-distance precision-guided dual capable weapons systems for both conventional and nuclear payloads, and the ability to seal off operational areas (A2AD environments) for protracted periods. In these areas it has the strategic initiative in the military domain, and thus also in the political domain, since it has greater capabilities and a wider variety of deployment options.

Every crisis involving the Russian Federation entails a nuclear dimension. Tactical nuclear weapons play a fundamentally different role in the Russian mindset than in Western countries. In the perception of the Russian leadership, these weapons are an essential instrument in applying political and military pressure. Consequently, in regional crises and military conflicts their threatened deployment could be considered a means of forcing an opponent to enter into political negotiations.

The Russian Federation is also modernising its strategic nuclear forces. On 27 December 2019, Russian defence minister Sergei Shoigu reported that the first Avangard hypersonic glide vehicle (HGV) had entered service in the Russian Strategic Missile Forces. An HGV is capable of manoeuvring after entering the atmosphere. However, doubts exist concerning the current deployability of this weapons system and the technical capabilities ascribed to it by the Russians. Even so its existence is indicative of the Russian Federation's threat perception as well as the absolute importance that it attaches to strategic deterrence.

A military conflict between NATO and the Russian Federation appears improbable in the short term. The Kremlin realises that NATO ultimately has more power, but also that the US plays a crucial role in it. In the Kremlin's view the US, its military capability and its guarantees to Europe with regard to security constitute the cornerstones of the alliance. The Russian Federation would therefore only initiate a military operation against NATO if it perceived a direct threat to its vital security interests and if it did not expect NATO to respond in what the Kremlin considered to be a unified fashion.

As a demonstration of allied solidarity, and in light of the increasing threat posed by the Russian Federation, NATO stationed a defensive multinational battle group known as enhanced Forward Presence (eFP) in the three Baltic states and Poland in 2017. The Netherlands has contributed to the eFP since 2017 in the form of an infantry company stationed in Lithuania. Set to last until at least the end of 2021, this is the largest deployment of Dutch armed forces personnel on foreign soil.

Russian interference is not limited to its immediate peripheries. For a number of years there has been increasing Russian involvement in conflicts and conflict resolution outside of its traditional focus areas. This activity is mainly directed towards supporting regimes, but also parties and movements that support the Russian agenda either directly or indirectly.

Russian Federation: military technology

In 2019 DISS investigated the development and production of weapons systems, Russian scientific research into relevant military technologies, and the proliferation of weapons systems in areas in which Dutch military personnel are currently deployed or could potentially be deployed in the future. For some time the Russian focus has been on developing and updating high-level weapons systems for deployment on land and at sea, in the air and in space, and in the cyber domain. In particular, major advances have been achieved in the areas of ballistic and cruise missiles, hypersonic weapons, air defence systems, anti-satellite weapons and electronic warfare. These weapons systems are being developed with the specific aim of disrupting the Western modus operandi and thus mitigating the perceived threat posed by the West.

Advanced Russian weapons systems are not only in development for domestic use but also for export to other countries and existing and potential conflict zones. If deployed in these areas, Dutch units could potentially encounter these systems.

Russian Federation: espionage and cyber espionage

The Russian offensive cyber arsenal includes capabilities for digital espionage and sabotage as well as for information operations that can be rolled out globally, in some cases after a short preparation cycle. The Russian intelligence requirement is largely geopolitical and military-based, and in the digital domain the Russian Federation is an advanced adversary of countries everywhere in the world. The Russian Federation uses information and cyber sabotage operations as instruments in hybrid conflicts. In 2019 a DISS intelligence investigation signalled a range of cyber espionage and sabotage activities as well as information operations targeting the Netherlands, other Western countries and allied interests. DISS continues its investigation of espionage and cyber espionage activity in 2020.

DISS considers a potential digital disruption of vital infrastructure and essential sectors and business as among the greatest cyber threats facing the Netherlands and its allies.

3.2 China

China's influence will increase in every domain, not only in Asia but around the world. Chinese trade, investment and tourism and the associated roll-out of investments in connection with the digital silk route are illustrative examples of this. The lines between Chinese economic and geo-economic interests and its political, geopolitical and military aims are hazy. The same is true for its multi-year programmes such as Made in China 2025, which, besides their open and evident economic objectives, also include a less clear but still significant emphasis on the military-technological ambitions of the Chinese armed forces.

Growing Chinese influence around the globe could have repercussions for Dutch and Western interests in the long term. China is increasingly promoting its political system as an alternative to the liberal Western democratic model, and thus an attractive concept for authoritarian regimes. It relies primarily on diplomatic and economic instruments to shape its foreign policy, but as its military capabilities increase so also does regional uncertainty regarding its intentions and activities. While China poses no direct military threat to the Netherlands in the short to medium term, the Netherlands could experience negative repercussions as a result of a shift in the balance of power at regional and global levels due to China's growing influence on the world stage. DISS monitors these developments and reports on them to the Defence organisation and other Dutch ministries.

China: espionage and cyber espionage

In the Chinese system, economic, political, military, cyber, security and intelligence activities are closely intertwined. This strategy is part of China's commitment to acquiring and developing innovative technologies, which it does covertly in part through the deployment of offensive cyber programmes and economic and other espionage activity. Chinese cyber actors deploy a wide range of malware in a bid to achieve their objectives. These offensive programmes target not only suppliers of the Dutch Defence organisation and Dutch ministries, but also vital sectors, as well as personal data and the data of other organisations in the Netherlands such as telecommunications companies, universities, research institutes, medical and biotechnology facilities, high-tech industry, start-up companies, the trade sector and defence contractors. The Chinese intelligence services also engage in traditional espionage activities with the intention of gathering military intelligence in the Netherlands. DISS investigated several threats in 2019, and the importance of such investigations is set to intensify in 2020 with an eye to the growing importance of economic security.

Economic security

Through its intelligence investigations DISS contributes to a better understanding of the intentions, capabilities and activities of states such as China and the Russian Federation, including their deployment of economic and other capabilities. DISS also contributes to economic security through its activities pertaining to the monitoring of exports, industrial security, counter-espionage and cyber activity as well as through promoting awareness. In 2019 a pilot project was rolled out to generate investigative capability with regard to investment and takeovers.

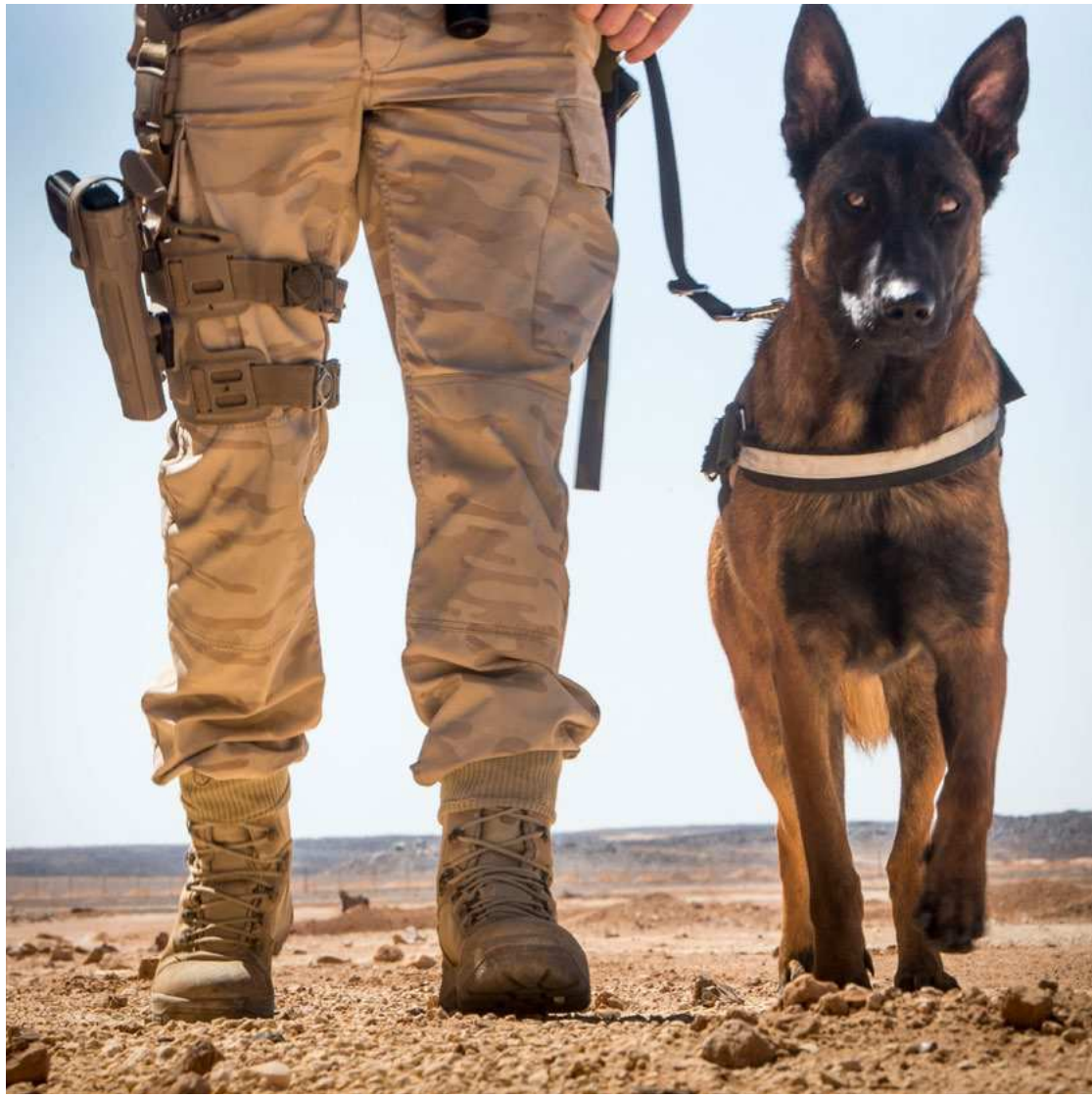
The Dutch government places great importance on economic security and protection against cyber sabotage and espionage. With closer attention being paid to economic security, and in the growing awareness that in modern warfare states are increasingly deploying additional means besides military capabilities in order to achieve politico-strategic objectives, the intelligence requirement in this area is expected to increase.

3.3 Afghanistan

DISS provides intelligence products in aid of the Resolute Support Mission (RSM) in Afghanistan. The RSM assists in the build-up of a professional Afghan security apparatus, including the armed forces and police. Dutch special forces personnel also contributed to the training and deployment of the special police unit ATF 888, which takes orders from the Afghan interior ministry.

The political intelligence analyses that DISS carried out in 2019 covered issues such as the peace talks between the US and the Taliban in Doha, Qatar. Little progress has been achieved so far. The Taliban made no serious concessions in 2019, instead clinging to their demand that an agreement be forged with the US before it would commit to a ceasefire or direct talks with the Afghan government. The year was dominated by the presidential elections held on 28 September 2019. With only 5% of the population casting their votes, turnout was extremely low. In 2020 DISS will continue to monitor political developments and their effect on the security situation in Afghanistan.

DISS issued a number of threat analyses pertaining to the security situation in northern Afghanistan in 2019. These also discussed the influence of the Taliban in the region and Taliban attacks on the Afghan Defense and Security Forces (ANDSF). Other intelligence products issued pertained to the security situation in the city of Kabul and the surrounding region, and to the intentions, capabilities and activities of the Taliban, the Haqqani network and Islamic State in Khorasan Province (ISKP) in this region.



3.4 Africa

As the large-scale Dutch military contribution to the United Nations Multidimensional Integrated Stabilisation Mission in Mali (MINUSMA) came to an end in May 2019, DISS changed its country investigation policy regarding Mali, shifting the emphasis to strategic intelligence and expanding the geographic scope of investigations to include the entire Sahel region. Dutch military personnel present in the Sahel region in connection with capacity building and training missions were provided with threat assessments and information on relevant developments.

The security situation in this region deteriorated further in 2019. Complex violent attacks by jihadist groups with ties to both al-Qaeda and Islamic State of Iraq and al-Sham (ISIS) increased in number. Jihadist groups also expanded their area of operations in 2019, particularly in the border region between Mali, Burkina Faso and Niger. Apart from jihadist violence, the security situation in the Sahel region is also under pressure due to persistent ethnic tensions between population groups there. In the first half of 2019, ethnic tensions in central Mali sparked violence that cost the lives of hundreds of civilians. Moreover, the deterioration of the security situation has worsened the already desperate humanitarian situation and further strained the limited resources of national administrations in the Sahel.

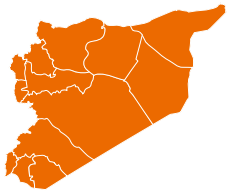
In accordance with its early warning task, in 2019 DISS reported on developments in a range of countries in Africa as well as in Yemen and the Balkan region of Eastern Europe.

Early warning
The timely observation and signalling of national or regional developments posing a potential threat to national security

3.5 Middle East

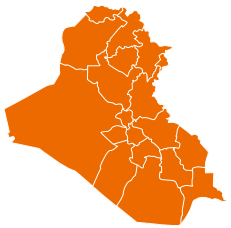
In light of the Netherlands' participation in the fight against ISIS, the primary areas of attention for DISS in the Middle East in 2019 were Syria and Iraq. The Netherlands also contributed to Operation Inherent Resolve (OIR) by providing training for Iraqi and Kurdish troops. In support of defence operations and associated decision-making pertaining to deployment, DISS provided intelligence products to Dutch and international customers.

Syria and Iraq



In light of the Syrian regime's ground operations against the armed opposition in northwestern Syria and, in the autumn of 2019, the Turkish ground operation in northeastern Syria, DISS focussed mainly on these two regions in 2019. Regional and international interference in these areas of operations had a major impact, and the shifting power balance that resulted from the Turkish operation cast serious doubt on Syrian-Kurdish autonomy.

While the Coalition dealt a major blow to ISIS in Syria, the group continues to have significant capabilities and to fuel radicalisation. ISIS continued its asymmetric attacks in Syria in 2019, mainly in the area east of the Euphrates. Its presence in northwestern Syria is small, but the presence of the now deceased ISIS leader al-Baghdadi in this area probably helped feed the perception of this opposition-held area as a terrorist stronghold.



Developments in Iraq in 2019 were mainly dominated by the resignation of Prime Minister al-Mahdi and its repercussions for regional political and security developments. Despite being a key demand of demonstrators in Iraq, the prime minister's resignation did not lead to a political breakthrough. No new government was formed and the promised early elections failed to take place, while demonstrators remained dissatisfied despite the announcement of reforms. ISIS remained capable of mounting attacks in Iraq and continues to pose a threat to security in the country.

Iran

DISS monitored Iran's involvement in Iraq and Syria in 2019 in connection with mission support provided for OIR. Iran continued its military support to the Syrian regime throughout the year, with a focus on combating ISIS (an objective that is in line with Iran's national security policy) and keeping the Assad regime in power. Tehran also continued its military support to 'strategic Shia ally' Hezbollah. Iran's involvement in Iraq also continued undiminished in 2019. Its intention in Iraq was to maintain and expand its influence in the country, since stability in Iraq is in the interests of Iranian national security.

From mid-2019 onwards, DISS provided support for political decision-making regarding Dutch participation in a mission in the Persian Gulf. Among other things, this support included analyses pertaining to the brief period of escalation in the region. This limited escalation peaked in the wake of shooting near Kirkuk on 27 December 2019, during which a US contractor was killed, and encompassed noteworthy incidents such as the US air strike that killed a military leader from Iran, Qasim Soleimani, and another from Iraq, Abu Mahdi al-Muhandis, as well as Iran's launch of ballistic missiles towards two Iraqi bases at which personnel from the US and the anti-ISIS Coalition were stationed. In 2020 DISS continues to provide support for the Dutch maritime mission in the Gulf region in the form of up-to-date threat reporting.

As part of mission support DISS also analyses technological developments pertaining to improvised weapons systems including improvised explosive devices (IEDs), homemade explosives (HMEs) and commercially available radio-controlled aircraft and helicopters (unmanned aerial systems – UASs). The role of weapons systems such as these is increasing, in part because they are cheap and readily available. Together with other sections of the Defence organisation, DISS investigates the deployment of these new technological applications both in mission areas and in the Netherlands in order to facilitate the timely development of countermeasures. It is also important to establish how these systems can be promptly detected and neutralised.

3.6 *Venezuela*

The situation in Venezuela deteriorated further in 2019. Current estimates indicate that more than four million people have left Venezuela, out of a population of 31 million. The economy is in dire straits, with basic necessities such as food, medicine, electricity and drinking water increasingly becoming luxuries that are available only to the small, elite group who dominate political power.

With the Maduro regime in a constant state of confrontation with the opposition, Venezuela's political crisis will persist, a situation that contributes to political instability in the country. Consequently, the support of the armed forces is vital for the regime. Large swathes of Venezuela have deteriorated into lawless regions in which independent armed groups engage in illicit activities for their own enrichment. Venezuelan state bodies have eroded further in the meantime.

Venezuela is expected to remain a source of instability in 2020, further endangering the security situation in the region as a whole. In light of the repercussions for neighbouring countries, including the Kingdom of the Netherlands, DISS and GISS will continue to monitor developments closely.

3.7 Counter-proliferation

Weapons of mass destruction (WMDs) pose a major threat to international peace and security. The Netherlands has signed international treaties aimed at countering the proliferation of such weapons, and in 2019 the joint DISS and GISS Counter Proliferation Unit (CPU) conducted investigations of countries suspected of developing or possessing WMDs and their delivery systems or otherwise acting in violation of these treaties.

Iran

In recent times, Iran has focussed on a gradual withdrawal from the Joint Comprehensive Plan of Action (JCPOA). With Iran-US tensions rising, Iran has ignored the technical restrictions imposed by the JCPOA, but has said it will continue to cooperate fully with the International Atomic Energy Agency (IAEA) and allow inspections to take place.

It will carry on actively developing ballistic missiles as part of its comprehensive ballistic missile programme, a major spearhead of which is to improve the accuracy and destructive capabilities of its existing ballistic missiles. Iran conducted a similar number of test launches in 2019 as it did in 2018. DISS and GISS also investigate Iran's development of WMDs.

North Korea

In 2019 US President Donald Trump and North Korean leader Kim Jong-un set forth talks on North Korea's denuclearisation, but without success. The most recent official talks between the two countries, in September 2019, were aborted, after which North Korea resumed its traditional threatening rhetoric. In 2019 North Korea conducted approximately 10 test launches of various new types of ballistic missiles.

Syria

In 2019 the CPU also investigated the deployment of chemical weapons by the Syrian regime, including its use of sarin to target opposition groups. In 2020, DISS and GISS will continue efforts to identify the threat posed by Syrian WMDs, to map their deployment and to investigate them.

Russian Federation

In 2019 the CPU followed developments surrounding the amendment of Chemical Weapon Convention (CWC) lists, which included a proposal by a consortium consisting of Canada, the US and the Netherlands, and by the Russian Federation itself, to incorporate Novichok in the lists covered by chemical weapon treaties. The CPU will continue to closely follow Russian developments in 2020.

Acquisition of information and goods by countries of concern; export control

Countries such as the Russian Federation, China, Iran, Syria, Pakistan and North Korea continually seek to acquire information and goods in the Netherlands and other Western countries that they can apply in their own arms programmes. DISS and GISS investigate the methods these countries use in their attempts to acquire knowledge and goods. Since these methods frequently involve cross-border activities, intensive national and international cooperation is of vital importance.

3.8 Counter-intelligence: radicalisation and extremism

DISS provides counter-intelligence (CI) that is used to identify and neutralise threats facing Dutch Defence personnel. DISS investigates signs of radicalisation and extremism among Defence personnel in any form in which they may appear. Actual personal behaviour is always the basis for investigation. DISS also investigates societal developments, such as polarisation and anti-democratic sentiment, and their influence on the Defence organisation in order to ensure maximum operational readiness of the armed forces.

Radicalisation

Personal behaviour inspired by Salafist religious beliefs can pose a threat to the Defence organisation and national security. In 2019 DISS conducted investigations into violent jihadism and Salafism, focussing on identifying suspected radicalisation among Defence personnel and jihadist-terrorist threats to the Ministry of Defence. It investigated several cases of suspected radicalisation within the armed forces and intensified its investigation of Salafism. None of the investigations revealed any concrete threats to the armed forces.

Extremism

DISS investigates signs of right-wing extremism and its influence on Defence personnel. Right-wing extremism within the Defence organisation has the potential to jeopardise the internal security of the armed forces. Discrimination against military personnel may spark unrest among the ranks and affect hierarchy and cooperation. It therefore remains vital that DISS promptly identifies individuals or groups within the Defence organisation that embrace extremist ideologies or actively or passively support extremist parties and organisations.

In 2019 DISS investigated two cases of suspected right-wing extremism, but uncovered no threats against the armed forces. DISS received no indications of any polarising discourse on Islam occurring within the Defence organisation, nor did its investigations yield any indications of right-wing extremist networks operating within the armed forces.

CI support in mission areas

In 2019 DISS provided CI support to Dutch units operating in mission areas. DISS experts instructed units being deployed to mission areas on the potential and actual CI threats in these regions in order to boost their ability to deflect hostile intelligence-gathering activities and increase operational security. CI support also contributes to mitigating threats against Dutch military personnel in mission areas.

DISS has adopted three criteria to estimate threats posed by state actors, non-state actors and individuals as accurately as possible:

Intentions – Capabilities – Activities

3.9 Industrial security

Companies charged with carrying out classified or vital defence contracts must comply with the General Security Requirements for Defence Contracts (*Algemene Beveiligingseisen voor Defensieopdrachten* – ABDO). DISS's Industrial Security Office monitors whether these ABDO-certified companies adhere to these requirements and advises them accordingly. Classified contracts for the Ministry of Defence are carried out exclusively by ABDO-certified companies.

In 2019 the Industrial Security Office's main task was to supervise and advise Defence contractors on the transition towards compliance with the 2017 ABDO security requirements. Defence contractors were repeatedly found to be taking risks in situations that necessitated on-the-spot measures including the suspension of work, orders and processes.

In late 2019 an amended version of the ABDO directive, ABDO 2019, was introduced in response to the current threat picture, the rising number of incident reports and developments anticipated in the defence industry. The expansion of the Industrial Security Office enabled improved identification of digital and traditional espionage, influencing and sabotage activities and an increased focus on economic security and international cooperation.

3.10 Security screening

The joint DISS and GISS Security Screening Unit conducts security investigations of individuals holding or applying for positions of trust at the Ministry of Defence. The nature of such positions is based on the potential risk that such individuals could pose to national security, and determines the rigorousness of security investigations (security authorisation level A, B or C). Security screenings at the A security authorisation level are the most comprehensive and apply to the most sensitive positions of trust. Security screenings for positions at the C security authorisation level are the least intensive. In 2019 a total of 63,386 security investigations were conducted, 16,883 of which were carried out by DISS.

Security screenings are conducted on the principle that 90% of requested investigations must be completed within the statutory period of eight weeks. The creation of a joint Security Screening Unit in October 2018 placed an enormous strain on the unit in 2019, resulting in backlogs in the first half of 2019. Measures were taken to clear these backlogs, including the temporary expansion of the unit's capacity.


FREDERIKKAZERNE

4 THE FUTURE: PRIORITIES AND OUTLOOK

4.1 Priorities in 2020

The implementation of the Wiv 2017 will continue to be a matter of the highest priority in 2020. This will require capacity, but steps will also need to be taken to bring technology up to date and improve information management.

DISS's second priority in 2020 is to ensure responsible growth and bring about prescribed changes to the service. Additional attention will therefore be directed to recruitment, selection and retention of personnel. In the coming year the initial effects of the inflow of new personnel will become noticeable. Career development, sound infrastructure and good working conditions require special attention, in part because they contribute towards the retention and well-being of personnel.

DISS will continue to fulfill requirements in 2020, with a focus on the following areas.

DISS will continue to conduct investigations in support of missions in Afghanistan, Africa and the Middle East and to support Dutch military personnel deployed in enhanced Forward Presence (eFP) mission until at least 2021. As part of its early warning task, DISS will continue to report on developments in Africa, Yemen and Eastern Europe (Balkan region) in the coming year. The Russian Federation and China exert a major influence on the global security climate, and DISS will therefore continue to monitor all potential manifestations of threats emerging from these two countries. Political and socio-economic developments in the regions surrounding the overseas areas of the Kingdom of the Netherlands will also continue to be monitored.

In 2020 DISS and GISS will set forth joint investigations of countries suspected of possessing or developing weapons of mass destruction and the means of delivery for such weapons, in cases in which this is prohibited by treaties. Other focus areas in 2020 will include developments in foreign military technology and the proliferation of advanced military technology and weapons systems in existing and potential crisis areas. In the area of counter-intelligence, investigation into various forms of radicalisation and extremism among Defence personnel will continue in 2020.

Attention will also be paid to traditional and cyber espionage, influence and sabotage. Economic security will be another area of increased focus in the coming year. States with strong geopolitical ambitions seek information they can use to modernise their armed forces, bolster their economies and influence political decision-making. Takeovers and investments are other manners in which states endeavour to acquire information or create strategic dependencies. Consequently, in the coming year DISS will continue to investigate espionage and cyber activity through which foreign powers could possibly target the defence industry. Besides supervising and monitoring the security measures of defence contractors, in 2020 and subsequent years the focus will be on businesses that are involved in the purchase and replacement cycles of defence materiel such as the F-35 fighter jet, submarines, M-frigates and air defence and command frigates. To protect the resilience of the Defence organisation, the Security Screening Unit will continue its efforts to conclude security screenings within the statutory period.

4.2 Outlook

For the long-term continuation of its work to fulfil its legal obligations in the promotion of national security, DISS has formulated a number of principles for its further development.

Human capital is central to these principles. Since our staff are our most valuable resource, we provide excellent training opportunities, career development support and employment terms. Doing so enables us to recruit the brightest, best and most creative people, building up a diverse workforce representing a wide range of specialist expertise.

Our personnel work in an organisation that increasingly runs on data. Teamwork is a given. Each day, intelligence teams work on gathering and processing data streams using the applicable tooling. We automatically distribute their products to the channels that require them.

DISS is a forward-looking organisation in a complex and ever-changing environment. We are capable of recognising contexts for strategic decision-making and taking timely countermeasures in response to potential threats both in the Netherlands and in the international arena. While we are capable of operating independently, whenever possible we cooperate at the national and international levels.

Our organisation is agile and capable of responding to constantly evolving circumstances. We take an active approach to forging connections with and building trust among our stakeholders. We are visible when possible, demonstrating what we do and why. In every respect, we adhere to the terms of the Wiv 2017. DISS information management structures are up to date, orderly and transparent.

5 ACCOUNTABILITY: STATISTICS

Industrial Security Office statistics

Agencies

Number of companies in portfolio:

- 703 Dutch companies
- 161 foreign companies

Authorisations

Number of ABDO authorisations issued:

- 327 in response to requests by the Ministry of Defence
- 62 in response to requests by foreign defence organisations
- 78 in response to requests issued by the Ministry of Defence to foreign companies

Number of ABDO authorisations withheld: 46

Audits

Number of companies audited: 10
Number of audits completed: 18

Incident reports

Incident reports: 115

Processed requests pertaining to non-Dutch nationals seeking positions of trust in ABDO-certified companies:

Number of processed requests: 33

Facility security clearances

DISS maintained contact with foreign national and designated security authorities (NSAs/DSAs) to request and finalise facility security clearances (FSCs). A foreign country may request an FSC for a Dutch company hoping to serve as a defence contractor for that country.

FSC

53 requested by foreign countries
62 issued to foreign countries
75 requested by the Netherlands
78 issued to the Netherlands

Requests for visits

The ABDO directive stipulates that besides Defence personnel, companies must also submit requests for visits to the Industrial Security Agency for employees travelling for Defence-related reasons. This makes it possible to establish a fuller picture of Defence-related travel and traveller behaviour and trends in this area.

RfV

Industry
(visits to industry sites)

355 outgoing
189 incoming

Defence
(visits to Dutch or foreign Defence organisations)

3287 outgoing
837 incoming

Security Screening Unit/DISS

Security authorisation	Positive rulings	Negative rulings	Total rulings
Level A investigations	2,358	7	2,365
Level B investigations	9,929	16	9,945
Level C investigations	4,568	4	4,572

Objections and appeals

Various individuals objected to, requested reviews of, or submitted appeals against decisions to withhold or revoke certificates of no objection. The table below shows the numbers of objections, review requests and appeals pertaining to decisions to withhold or revoke certificates of no objection.

2019	Submitted in 2019	Finalised in 2019	Unfounded	Founded	Inadmissible	Revoked	Withheld
Objections	8	3	1	-	1	1	-
Reviews	1	2	1	1	-	-	-
Appeals	1	2	-	2	-	-	-
Provisional certificates	-	-	-	-	-	-	-
Total	10	7	2	3	1	1	-

Society and media

DISS answers questions put to it by citizens and the media as quickly and fully as possible but without disclosing classified information. In 2019 over 2,000 reports and questions were submitted directly to DISS by citizens and 100 by the media. A large number of these questions concerned 5G, the Wiv, military security and espionage.

An area of tension exists between public reporting and the work performed by intelligence and security services. The fact that DISS is not permitted to reveal its current level of knowledge, sources and procedures restricts the degree to which it can reveal information. For example, DISS never reveals information concerning individual lawsuits still in progress, confidential personnel data or details that could violate an individual's privacy. In all other cases, DISS considers whether responding to a question from the general public or the media could:

- result in the disclosure of its procedures or current level of knowledge;
- contravene the statutory regulations governing source protection;
- jeopardise military operations.

Complaints and criminal actions

Complaints concerning actions (alleged or otherwise) by DISS can be submitted to the DISS complaints coordinator. Complainants who are unhappy with the way their complaint has been dealt with can turn to the CTIVD. In 2019 DISS received 15 complaints, most of which related to the duration of security investigations. This led to concrete improvements such as the creation of a direct telephone number to call the Security Screening Unit with queries regarding duration. One complaint was submitted to the CTIVD for settlement, resulting in improvements to the manner in which security investigations are handled. DISS and the CTIVD complaints department regularly engage in constructive consultations.

No reports of criminal actions were submitted in 2019.

Complaints

2019	Submitted in 2019	Finalised in 2019	Unfounded	Founded	Inadmissible	Revoked	No ruling/complaint not processed
Complaints	15	12	1	1	-	5	5

Access requests

Anyone may submit a request to inspect information recorded by DISS. Only information that is no longer relevant for DISS's work may be made available, providing it does not reveal any sources or procedures used by DISS. Objections to refusals to disclose information can be submitted to an independent committee, and reviews and appeals to the courts.

Access requests submitted in 2019	Number of requests	Finalised	Fulfilled**	Denied	Pending	Objections	Reviews	Appeals
Data on the applicant	25	23	8	15	4	-	-	-
Data on deceased family members	39	35	-	35	17	-	-	-
Data on administrative matters	8	45	17	28	4	4	1	-
Total	72	103*	25	78	25	4	1	-

* Some of these requests were submitted prior to 2019

** One or more documents were provided to the applicant

Notification

In accordance with Article 59 of the Wiv 2017, DISS is obliged to investigate whether individuals can be notified of certain special powers having been exercised against them, five years after such powers were exercised. These powers include:

- opening letters or other postal items;
- targeted interception of communications, including the tapping of telephone and internet traffic and the installation of microphones;
- entering homes without the occupants' permission.

Two such notifications were issued in 2019.

Threat analyses pertaining to individuals

DISS compiles threat assessments whenever it identifies concrete and/or conceivable threat information. It also assesses the potential effects in the event a threat is carried out and whether the party posing the threat has the intentions and capabilities to carry it out. DISS compiled no threat assessments pertaining to individuals in 2019.

DISS also produces threat analyses. These are comprehensive analyses of threats perceived by targets such as politicians and diplomats to be concrete or conceivable. DISS produced no threat analyses in 2019.

Lawful interception statistics

In 2019 DISS conducted lawful interceptions on 879 occasions, including telephone tapping and the installation of microphones. Eavesdropping on individual targets (persons or organisations) occurs in various ways and on various devices, each of which is included separately in the statistics.

Reporting of exceptional incidents

Each year DISS receives reports of exceptional incidents, most of which originate from the Defence organisation, partner organisations and private citizens. In 2019 DISS received 1,869 widely diverse reports from within the Netherlands and from mission areas. Some reported incidents involve possible threats to the security of the armed forces, and may include observations of unusual attention paid to military barracks or to Defence personnel or their families and friends. When necessary, DISS informs third parties of such threats so that appropriate action can be taken. The Security Authority and the Royal Netherlands Marechaussee are among DISS's key partners within the Defence organisation, while external partners include the National Coordinator for Security and Counterterrorism (*Nationaal Coördinator Terrorismebestrijding en Veiligheid* – NCTV), the National Police and GISS.


UN
UN

This is a public edition of the 2019 annual report of the Netherlands Defence Intelligence and Security Service.
Publication date: April 2020

Layout : Crossmedia | MediaCenter Ministry of Defense | The Hague

Photos : MediaCenter Ministry of Defense | The Hague