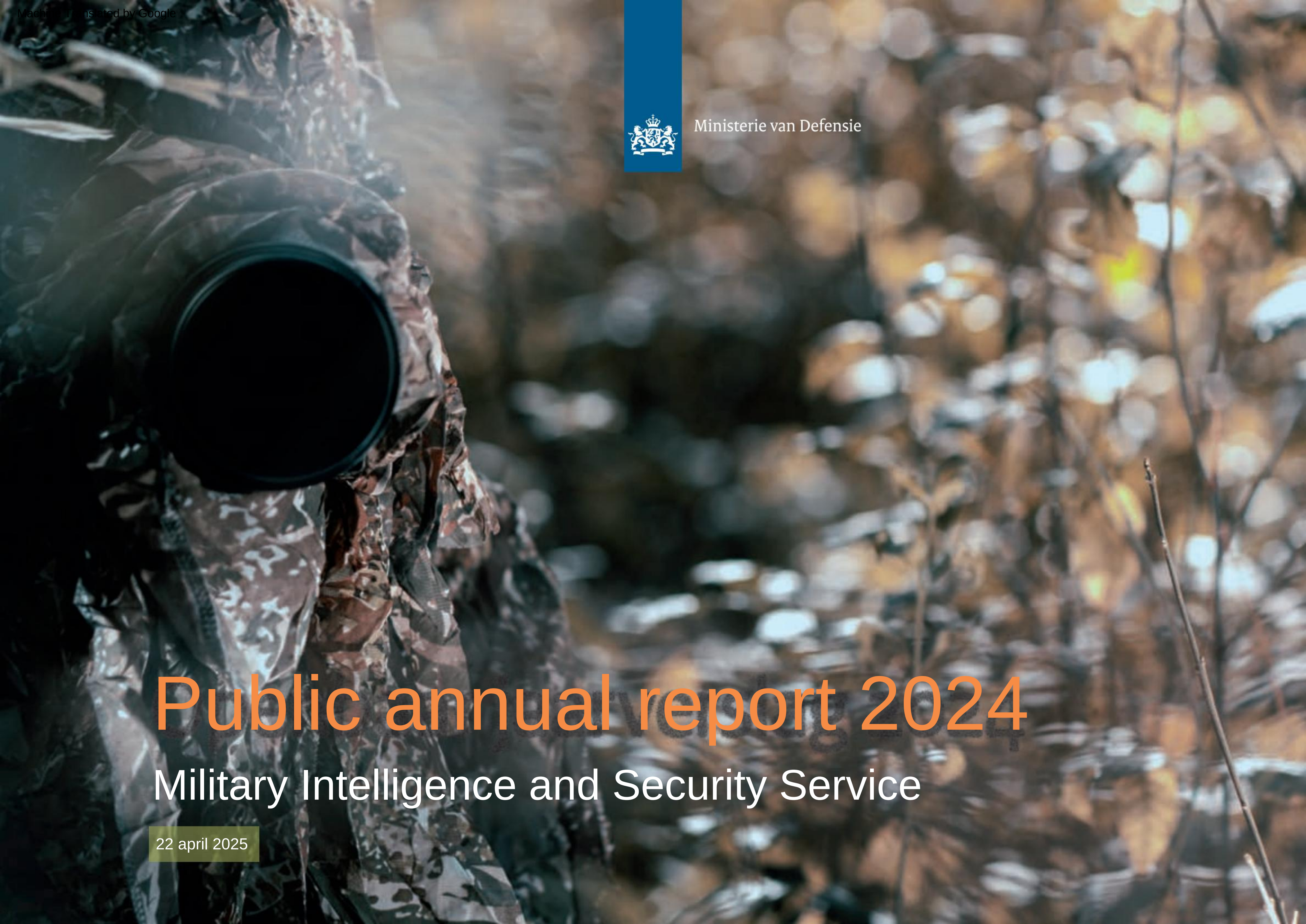


Ministerie van Defensie

Public annual report 2024

Military Intelligence and Security Service

22 april 2025

In April 2024, the 2023 Annual Report was published
by the Military Intelligence and Security Service.

Design: Studio MIVD | The Hague

Photo: Defense Media Center | The Hague

Public annual report 2024

Military Intelligence and Security Service

22 april 2025

2 Military Intelligence and Security Service

TABLE OF CONTENTS

4 Military Intelligence and Security Service

Foreword by the director of MIVD

Vice-admiraal Peter Reesink

The unrest in the world and the threat for the Netherlands and the rest of Europe are worrying. The safety of the Netherlands, our prosperity and our way of life are under pressure. The turbulent developments in geopolitics and alliances have called into question certainties on which we could build and trust until recently. The speed at which this is happening and the potential effect on our safety is unprecedented. This makes it all the more urgent that Defence and the MIVD can provide an appropriate response to these developments.

to offer.

The services do not see the Russian threat to Europe decreasing, even after a possible end to the war with Ukraine, but increasing. This underlines the importance for the Netherlands, NATO, and in particular for the European member states, to build up military power as quickly as possible. This is necessary to deter Russia and, in the worst case, to be able to defend the Netherlands and Europe against an attack by Russia.

The MIVD has the task of supporting the Dutch armed forces in this. We do this by providing timely and accurate intelligence and counter-intelligence, for example about the development and manner of operation of the Russian armed forces and Russian espionage and sabotage. We maintain the coherence between intelligence at all levels. In this way, the MIVD contributes to the strengthening of our own territorial defence and that of our allies.

The conflict in the *grey zone,* the twilight zone between peace and war, has now become a reality. Our country is increasingly confronted with state actors who try to disrupt and weaken our society with hybrid attacks. Russia in particular wants to keep their (cyber) actions below the level of an armed conflict. We see this

increase risk appetite.

In 2024, for example, the MIVD saw a Russian hacker group launch a cyber sabotage attack against the digital control system of a public facility in the Netherlands. As far as is known, this is the first time that such a sabotage attack has been carried out against such a digital control system in the Netherlands. The attack ultimately caused no damage. The MIVD also observed a Russian cyber operation against Dutch critical infrastructure, possibly in preparation for sabotage. Because the target acted quickly, the Russians did not succeed in gaining access to the network.

The MIVD has been warning about this (cyber)threat for some time. For example, last year the MIVD made public the working methods of a Russian GRU unit so that potential victims can arm themselves against these serious attacks and espionage. The focus of the hackers of this cyber unit of the Russian military secret service is to gain insight into and disrupt Western aid to Ukraine.

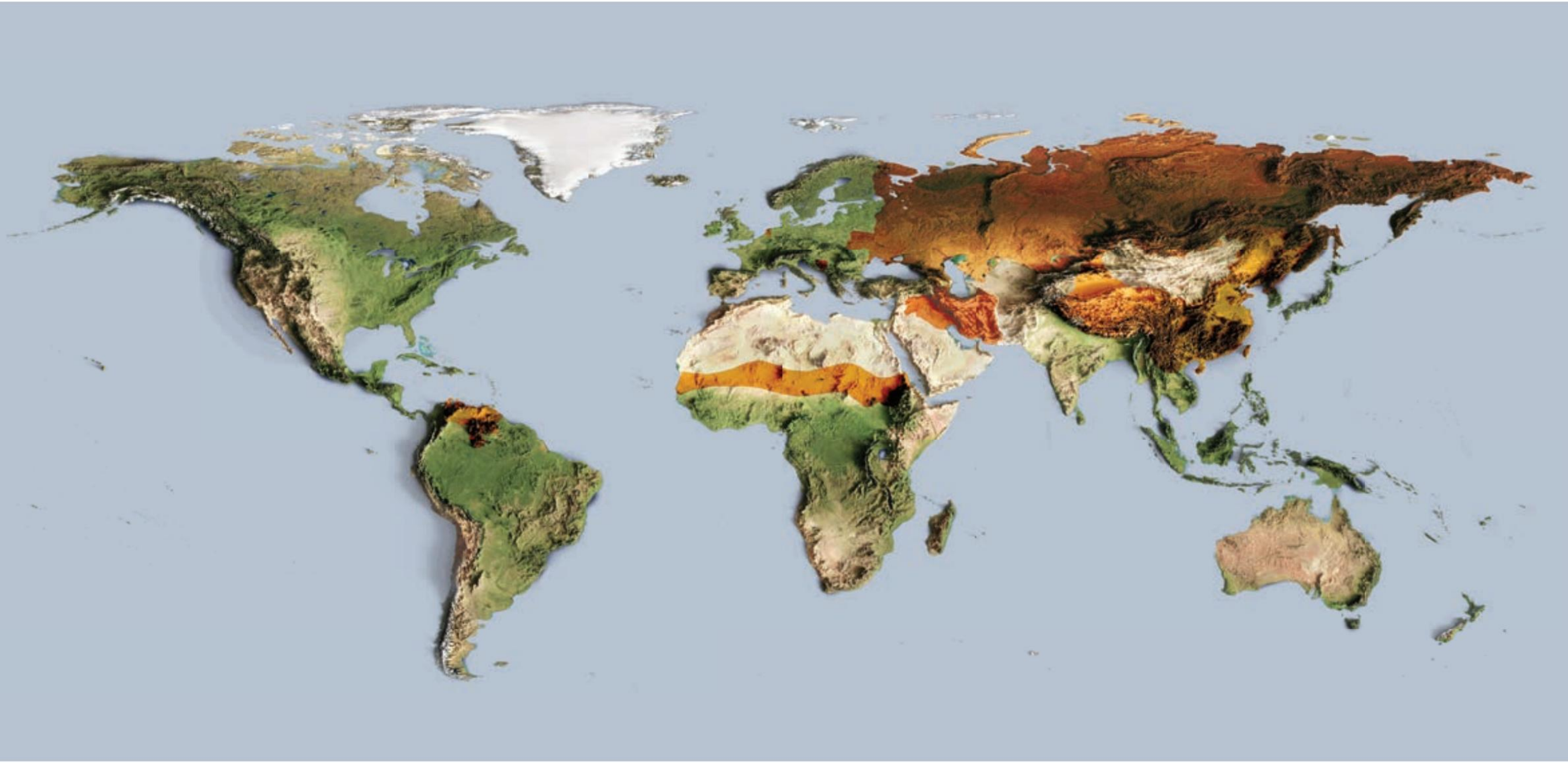
The MIVD further recognizes that several Russian units are attacking the infrastructure of the North Sea mapping and (underwater) activities that indicate espionage and preparatory actions for disruptions and sabotage. Think for example of internet cables, drinking water and energy supplies. Actual disruptions can lead to major damage and disruption in the Netherlands, Europe and the rest of the world.

The threat also comes from China and becomes visible with the support of Russian war activities and the aggressive stance against Taiwan and in the South China Sea. In the Netherlands, we have seen Chinese activities in the area of unwanted knowledge transfer of high-quality Dutch technology such as semiconductors. This can be done openly through acquisition, investments and participation in scientific research, but also illegally by evading export restrictions and (cyber) espionage. In 2024, the American intelligence and security services published about the Chinese cyber actor *Salt Typhoon.* This cyber actor had access to major American telecom providers for at least a year. Communications of politicians and civil servants were reportedly viewed and possibly also accessed secret information from investigative services. The reporting fits in with observations by the MIVD and AIVD. According to the services' assessment, it is likely that European telecom providers are also the target of advanced hacking attempts.

The Temporary Act, which entered into force in 2024, should enable us to defend the Netherlands more effectively by deploying existing powers such as cable interception and hacking. The Temporary Act will be partially applied in consultation with the Intelligence and Security Services Review Committee (CTIVD). The starting point is and remains full application of the Temporary Act under the necessary supervision, in the shortest possible time frame that is feasible for all parties.

Finally, I would like to emphasize that we can only carry out our tasks through the efforts of our employees. They have again delivered a great performance in the past year and will continue to work for the armed forces and the safety of the Netherlands in this challenging year.

6 Military Intelligence and Security Service



1

INTELLIGENCE AND SECURITY FOR THE NETHERLANDS

In 2024, the armed forces and thus the MIVD were also faced with the task of dealing with complex threats that threaten our security, stability and prosperity. These threats are partly the result of the current geopolitical relations and assertive state and non-state actors who use new technologies with a major impact. Resources and technologies that are often invisible, difficult to recognize in time and difficult to attribute to perpetrators. In addition to the classic actions, conflicts are increasingly taking place in the *grey zone,* the grey area between war and peace. Current developments are characterized by increasing unpredictability, in which traditional boundaries between war and peace, friend and foe, and international cooperation and conflict, are becoming increasingly blurred.

The war in Ukraine is still ongoing. In addition, the tension between Russia and the West is historically high, with implications that may extend beyond the European security structure alone. The world is confronted with the possibility of a new conflict, in which the strategic rivalry between the West and major powers such as Russia and China will once again be central. Even if the war were to end, the tension between Russia and the West, as well as the reconstruction of Ukraine, will continue to require a great deal of effort from the armed forces and thus the MIVD. In addition to the war in Ukraine, the tension in the Middle East is still high as a result of the conflict between Israel and Hamas. There were also conflicts or increasing tensions in other parts of the world, such as Sudan, the Democratic Republic of Congo and Kosovo. All these events underline the picture
of an uncertain, changing security context.

In this uncertain security context, the MIVD must be able to respond quickly to crises and at the same time provide sustainable strategic intelligence to be able to conduct research into, for example, the threat from China and Russia. The uncertain and changing security context places great demands on the agility of the armed forces and the services, because crises arise quickly and threats are diverse and extensive. The MIVD supports the deployment of the Dutch armed forces worldwide with intelligence that is reliable and up-to-date. The MIVD produces various intelligence products, such as threat assessments and intelligence reports, for the military deployment and the political decision-making related to this.

In addition to strategic dossiers, areas of interest and support to the armed forces, the MIVD also has security promotion tasks.
For example, the MIVD protects the military secrets and operations of Defence, detects cyber attacks and unmasks foreign intelligence officers who gather intelligence secretly and sometimes illegally.
The Dutch Defence industry, companies, knowledge institutions and scientists are a potential target of various state actors who (secretly) try to acquire high-quality, military-relevant or otherwise, technology. The MIVD contributes to the resilience and security of Defence and the Defence-related industry by, for example, conducting research into the security of companies that must comply with the safety requirements of Defence1

The great diversity of threats requires that the MIVD must also have a relevant and reliable intelligence position on a multitude of subjects, and must be able to gather, process, analyse and disseminate information quickly. To this end, the MIVD works closely with, among others, the armed forces, the AIVD, the NCTV and with foreign colleague services.

[1] *General Security Requirements for Defense Contracts 2019 (ABDO 2019)*

> **MIVD and AIVD: 'Foreign countries behind police hack'** *(October 2024)*
> It is very likely that another country is responsible for the cyber incident at the police. This is evident from research by the MIVD and AIVD, as Minister of Justice David van Weel wrote in a letter to the House of Representatives in October 2024. The services have not made public which country is involved. The MIVD and AIVD have been warning for some time in their annual reports, among other things, about the increase in offensive cyber activities by a number of countries.

Reading guide

This annual report discusses in Chapter 1 the intelligence research, mission support and areas of attention based on a geographical and thematic division and finally the security promotion tasks. Chapter 2 describes the accountability to society.

Chapter 3 then describes the MIVD as an organisation and finally Chapter 4 provides an overview of the key figures for 2024.

1.1 The Russian Federation

Relations between Russia and the West have reached a new low in 2024. Moscow perceives the war in Ukraine as part of a broader and existential conflict with the West.

In Russian eyes, this confrontation has a 'total' character. This means that, regardless of the outcome of the war in Ukraine, the conflict between Russia and the West is a long-term one. In the Russian narrative, Western support for Ukraine is aimed at inflicting a strategic defeat on Russia and destabilizing domestic politics.

The Kremlin presents Russia, both to its own people and to the outside world, as a unique civilization with its own system of norms and values, which should serve as an alternative to the one imposed by the US-dominated world order. So far, Russia is coping with the challenges posed by the war. Putin's regime is stable, although this stability is enforced by increasingly repressive means and is not anchored in functioning democratic institutions.

There is still a lot of support among the Russian population for the war, which is part of a broader conflict with the West and is seen as a war to defend against Western aggression.

Russia has taken a number of worrying escalation steps in 2024. The publication of the revised Nuclear Doctrine, in which the nuclear threshold has been lowered even further, the first ever deployment of an *Intermediate Range Ballistic Missile* (primarily a weapon with a nuclear task), and statements that Russia is ready to resume nuclear testing, are intended to create uncertainty in the United States (US) and NATO. What is worrying is not only the nuclear nature of the threats, but also the fact that the number of non-nuclear escalation possibilities is decreasing. In addition, Western countries must take into account that under the Putin regime, Russia's position towards the West will harden rather than soften.

Russian Federation: War in Ukraine

Finally, in 2024 it became clear that Russia continued to receive support from China, North Korea and Iran for the war effort. China and Russia further strengthened their bilateral ties in 2024. China provides Russia with political and diplomatic support in multilateral forums such as the United Nations (UN). Chinese companies remain important suppliers of components that are crucial to the Russian war industry. North Korea was the largest supplier of artillery shells in 2024 and the first state to officially send troops to Russia for active participation in the war. Russia and Iran continued bilateral cooperation in the political, economic, military and nuclear fields over the past year. Iranian arms deliveries to Russia (including several types of *OWA-UAS*[2] munitions and *Close Range Ballistic Missiles* (CRBMs) and the intermediate

[2] *OWA-UAS: One way attack- unmanned Aerial Systems. (including drones equipped with a camera, sensors, navigation equipment and an explosive charge, which flies 'into' the target after launch and explodes.*

military-technological cooperation has contributed to Russian sustainability in Ukraine. As a result of this cooperation, NATO is increasingly confronted with the deployment of Iranian weapons systems (and Russian improved copies thereof) on its eastern flank.

Ground-based operations

The war in Ukraine is still characterized as a war of attrition, with both sides suffering high losses in personnel and material. Although the Ukrainian invasion of Russian Kursk provided local and temporary initiative, Russia still generally has the upper hand and is carrying out offensive actions along the entire front. The numerical superiority in personnel, material and fire support is still strongly in Russia's favor, partly because the Ukrainian armed forces are faced with structural shortages of personnel and material.

In late October, the Russian armed forces launched an offensive in the Donbas, capturing a relatively large amount of territory in a short period of time, particularly in the southern part of the Donetsk Oblast. The scenario is realistic that Russia will succeed, at the cost of high personnel and material losses, in capturing cities in the Donbas in the coming six months that serve as important logistical hubs for the Ukrainian armed forces. This will limit the Ukrainian ability to defend the Donbas in the future.

Air domain

Over the past year, Ukraine's air defense and air forces have been further reinforced with Western ground-based systems and fighter jets. This has allowed Ukraine to intercept a significant portion of the ongoing Russian cruise missile, drone, and other long-range attacks. However, Ukraine still lacks the resources to adequately protect all vulnerable infrastructure, the population, and the armed forces.

In particular, the greatly increased massive Russian use of glide bombs results in significant civilian casualties on an almost daily basis in vulnerable Ukrainian cities such as Kharkiv.

In turn, Russia has also been confronted with a growing air threat behind its own lines. With increasingly sophisticated, self-produced long-range drones, Ukraine is now carrying out attacks of more than a thousand kilometres into the Russian hinterland.

These attacks not only bring the war to the heart of Russian power in terms of publicity, but also have visible disruptive effects on, among other things, Russia's petrochemical sector, defense industry, ammunition supply and air defense. In addition, with the relaxation of restrictions on the use of Western long-range weapons at the end of 2024, Ukraine gained a significant additional capacity to attack targets in Russia itself.

Maritime domain

The intensity of the war in the Black Sea region has decreased significantly in 2024, as the Russian fleet has chosen to position itself further east due to the continued threat of Ukrainian naval attacks. However, Ukraine has continued to conduct several successful strikes with increasingly sophisticated *Unmanned Surface Vessels* (USVs) against military targets in the Black Sea region this year.

This limited Russia's maritime operations.

Restoration and expansion of Russian military capabilities

The combined capacity of Russian industry to produce, overhaul and modernize military equipment is more than sufficient for Russia to quantitatively compensate for the losses suffered in Ukraine. In addition to the greatly increased domestic production, Russia also receives significant assistance from China, Iran, Belarus and North Korea. This allows Russia to continue the war in Ukraine as well as to give limited substance to the ambitious expansion plans of its own armed forces. Russia, while the war

in Ukraine, a comprehensive reform and expansion of the armed forces has been initiated with a view to a post-conflict situation.
In this, preparation for a possible military conflict with NATO is the main motivation for Russia.

Russian threat to Europe

As a result of the Russian threat assessment and increased tensions between Russia and the West, partly as a result of the war in Ukraine, the Russian threat is increasingly manifesting itself in a hybrid manner in Europe. This is expressed, for example, in the form of both physical and digital (classical)3 espionage, (covert) influencing of the public debate, the political-administrative system and diplomacy, offensive cyber attacks and campaigns, sabotage and the use of energy policy as a means of pressure.

This is done through a diffuse, opportunistic, and unpredictable interplay of Russian government entities (including the Russian intelligence and security services), a diverse group of Russian or pro-Russian individuals, organizations, and networks in Russia and the West, who are deployed or actively offer themselves to perform often lucrative activities. In addition, Russia is now showing a greater willingness to take risks, which manifests itself through more brutal, aggressive, or provocative activities in both the physical and cyber domains, sometimes with a violent component. These actions are aimed at organizations that are involved in various ways in (supporting) the war in Ukraine, but increasingly also at military and logistical locations in Europe.

The purpose of these sabotage activities is multi-fold. On the one hand, the activities are aimed at delaying Western supplies to Ukraine, on the other hand, at sowing division in the West and undermining support for Ukraine. In addition, Russia can use sabotage activities to test where the West draws red lines when it comes to Russian aggression on its own territory. Finally, these activities aimed at mapping Western response(s) to such activities, with Russia seemingly seeking a model whereby it can maximally disrupt Western support for Ukraine without provoking a full-fledged military response from the West.

MIVD director in FD: 'Russia could have a major conflict with NATO within a few years' *(December 2024)*

Despite heavy losses in Ukraine, Russia is replenishing its arms and ammunition stockpiles "many times faster" than NATO countries.

According to the director of the MIVD, Vice Admiral Peter Reesink, Moscow could be ready for an armed conflict with NATO by 2030. The director is considering a scenario in which the Russians actually attack. Reesink: 'We think it is possible that Russia will start a regional conflict when it is done with Ukraine.' The aim of this, according to him, is 'to see if the alliance can be played off against each other.'

Russian threat to the Netherlands

The Netherlands is, and remains, an interesting target country for Russia, because of its leading role in Western support for Ukraine, as home to international organizations such as the OPCW and the International Criminal Court, and the presence of companies from the high-tech sector (such as *Brainport*
Eindhoven), a main port (important transport routes including the port of Rotterdam, Schiphol Airport) and an information hub in Europe. The Russian intelligence and security services (GRU, SVR and the FSB) carry out various activities that pose an espionage and/or sabotage and influence threat to Western European countries and NATO allies. For some of the identified activities and plans, there is uncertainty about the extent of Russia's involvement. In addition to the (classic) intelligence threat through activities in both the physical and cyber domains, Russia is developing activities in the Netherlands to secretly acquire technology.

acquire.

[3] *Unlocking information from so-called human sources.*

Russian Federation: Military technology

The Russian Military-Industrial Complex (MIC) is extensive and is characterized by a focus on production, technology-oriented Research & Development and development of high-quality new weapon systems. Despite increasingly severe sanctions, Russia continues to develop, produce and export weapons and military technology. In order to meet the continuing need for weapons and ammunition as a result of the war in Ukraine, Russia has increased its production capacity. In doing so, Russia seems increasingly capable of finding alternatives for sanctioned items, for example through successful import substitution and covert acquisition. In addition, Russia uses imported components, but also complete weapon systems such as Iranian and Chinese drones.

Nevertheless, Russia strives for the greatest possible strategic independence, preferably replacing imported weapons systems with nationally developed and produced systems.

The Russian MIC focuses on (further) development of weapon technology for deterrent, defensive and offensive purposes. Examples include robust ballistic and hypersonic missiles, high-quality air defence systems and relatively cheap OWA UAVs.

The conflict in Ukraine has enabled Russia to refine proven technologies and develop new concepts aimed at Western weapon systems. In doing so, the MIC has demonstrated its great adaptive capacity to respond quickly to specific needs from the Russian armed forces. The MIC primarily produces and develops for the Russian armed forces, but traditionally also exports weapons and weapon technology on a large scale.

The MIVD conducts research into Russian military-technological developments, partly to enable the Dutch armed forces and their allies to make well-founded choices when it comes to purchasing new military systems and developing adequate tactics for now and the future. The study conducted in 2024 investigation, the MIVD has determined that the threat posed by current and future Russian military assets is and will remain significant. It is possible that the Dutch armed forces, as part of NATO, may come into direct or indirect contact with high-quality Russian weapon systems, partly due to the global proliferation (export) of these systems by Russia.

Russian Federation: (cyber)espionage

In 2024, the MIVD investigated espionage by or on behalf of various foreign intelligence services. In 2024, the MIVD, in collaboration with the AIVD, investigated (possible) activities of the Russian intelligence and security services GRU, SVR and FSB against the Netherlands and its allies. Russia is also trying to secretly obtain technology and technological knowledge in the Netherlands.

The Netherlands is also a target country for the Russian regime because of its support for Ukraine, the international organisations based here and the logistical hub that the Netherlands is.

Cyber espionage is and will remain of great importance to Russia. The war with Ukraine has increased the need for Russia to gather intelligence on political and military affairs. Since the Russian war with Ukraine, the MIVD has recognized an increase in the number of cyber actors within the Russian government that are supported or controlled by them. A large number of these cyber actors carry out cyber operations that can also directly or indirectly affect the Netherlands. Where possible, the MIVD takes steps to take action against these actors, both covertly and publicly. For example, earlier this year, the MIVD co-wrote the *Cyber Security Advisory* issued by the American government about a Russian actor that the MIVD holds responsible for carrying out various cyber operations against, among other things, the vital infrastructure4

in NATO countries.

[4] *Vital infrastructure: Processes and services that form the foundation on which the Netherlands runs, such as electricity, access to the internet and drinking water. Source: www.nctv.nl/ onderwerpen/ vitale-infrastructuur*

The Netherlands has also been the target of Russian cyber operations. Over the past year, the MIVD has observed various cyber espionage attempts against the Dutch government. In addition, the Netherlands can become an indirect victim of cyber operations, for example through operations against allies. In this way, Russian cyber actors have obtained sensitive data such as personal data of Dutch government employees and Dutch companies.

In order to recognize Russian cyber operations, the MIVD works closely with private security companies to detect and mitigate cyber operations. This collaboration is an essential part of the digital resilience of the Netherlands.

Russian Federation: cyber

The Russian government is increasingly using a *'whole-of-society' approach* to carry out Russian cyber operations [5] approach. Multiple Russian entities, from private companies to the highest levels of the Russian government, play a role in Russia's offensive cyber program deployed against the West and Ukraine, but even against Russian allies.

The services note that state-sponsored groups pose an increasing threat to the Netherlands and its allies. Over the past year, it has become apparent that several of these groups have carried out cyber sabotage attacks against vital infrastructure in Western countries and actively contribute to Russian influence campaigns. Despite the fact that the impact of these groups has remained limited, the MIVD has observed an increasing willingness of such groups to actually commit sabotage. The MIVD also sees that the technical capacities and knowledge within such groups are increasing. According to the MIVD, these developments can result in an increased risk of serious attacks with both digital and physical effects.

Ukraine: cyber

Russia is also waging war with Ukraine on a large scale via the digital domain. A significant part of Russian cyber capabilities is therefore deployed in cyber operations against Ukraine. As a result, Ukraine is continuously faced with a large number of Russian cyber operations against Ukrainian government organizations and vital sectors. Smaller companies are also targets. In the first phase of the Russian war with Ukraine, the focus of Russian efforts was on cyber sabotage, by using large numbers of *wipers*[6] against Ukrainian systems. The Russian focus is now more on obtaining intelligence, or cyber espionage.

In 2024, the MIVD identified an increase in Russian cyber actors conducting cyber operations to obtain tactical intelligence. This intelligence provides direct support to Russian military-tactical operations in Ukraine. Russia is able to quickly obtain this intelligence from the executive units within the Russian armed forces and use it for kinetic operations. For example, Russia uses vulnerabilities in applications on mobile phones to determine the locations of Ukrainian soldiers and military equipment, in order to then attack them kinetically.[7] Cyber is thus increasingly playing an important role in Russian military operations in Ukraine. In 2024, the MIVD also shared intelligence from its own cyber investigation with the Ukrainian government, in order to contribute to the physical security of people and equipment in Ukraine.

Cybersabotage

Last year, the MIVD observed an increase in cyber operations against European and NATO allied targets. These attacks were probably aimed at gaining a digital position within vital infrastructure in order to sabotage it at a later time. This year a cyber operation was observed against the Dutch vital

[5] *Whole-of-society approach: an approach that involves the entire society (government, business community, knowledge institutes and citizens).*

[6] *Malware aimed at wiping data on infected systems.*

[7] *Kinetic engagement: The use of a variety of weapon systems and/ or maneuver units with the aim of disabling the unit, object or target.*

infrastructure, possibly in preparation for cyber sabotage. Because the target acted quickly, the actor was unable to gain access to the network.

In 2024, a state-sponsored group carried out a cyber sabotage attack against the digital control system of a public facility in the Netherlands. As far as the MIVD is aware, this is the first time that a group like this has carried out a cyber sabotage attack against such a control system in the Netherlands. Although the impact of the attack has been minimal, the MIVD is concerned about the threat of cyber sabotage against the Netherlands and NATO allies, both from the Russian state and from state-sponsored hackers.

MIVD warns: Russians are targeting Western aid to Ukraine *(September 2024)*

In September 2024, the MIVD warned of Russian cyber operations by GRU unit 29155. The focus of the hackers of this Russian military intelligence service is, among other things, on visualizing and disrupting Western aid to Ukraine.

Their operations primarily target Western governments and vital infrastructure.

The MIVD, together with the US and other partner services, has issued a warning and technical advice. This states how countries and organisations can recognise these operations and arm themselves against them. According to the Western intelligence services involved, '29155' is trying to gain insight into military movements of Western arms deliveries to Ukraine. The cyber operations may also be aimed at supporting the physical sabotage for which 29155 is known.

The MIVD previously linked this unit to cyber sabotage operations against Ukraine. These took place in the run-up to the large-scale Russian invasion of Ukraine in February 2022. Furthermore, the MIVD links the hackers of 29155 to preparatory actions for destructive cyber operations against vital infrastructure and government institutions in Western countries. This GRU unit has also long been held responsible for committing physical sabotage and attempts to do so in Europe.

Several countries have linked 29155 to, among other things, the poisoning of former GRU officer Sergei Skripal in 2018, an attempted coup in Montenegro and the assassination of a Bulgarian arms dealer.

Digital influence

In 2024, the MIVD supported the US government in disrupting a Russian influence campaign that spread pro-Russian sentiments through *social media.*

The MIVD has determined that Russia is taking advanced steps to make artificial intelligence (AI) usable in digital influencing operations.

So-called Russian hacktivists[8] aim to disrupt Western support for Ukraine, undermine NATO cohesion and spread pro-Russian sentiment. In 2024, such groups launched DDoS attacks against websites of political parties and public transport companies in the Netherlands, among other things, in an attempt to make it difficult for Dutch people to vote in the European elections.

[8] *Hacktivism is a combination of activism and hacking that involves the use of hacks, computer knowledge and the Internet as an act of protest or subversive activity to attack computer systems to steal data or disable them.*

1.2 China

The past year, the People's Republic of China (hereinafter: China) celebrated its seventy-fifth anniversary. Although the Chinese Communist Party (CCP) tries to emphasize the geopolitical and economic revival that the country has experienced during this period, Xi Jinping's China is also characterized by increasing national and international tensions.

In 2024, China has shown itself increasingly willing to assertively advance its political and military-strategic interests. In many cases, this has come at the expense of other actors in the Pacific region. For example, China has taken an increasingly tough stance towards Taiwan as the year progresses. Despite ongoing tensions between the two parties, military pressure from China was relatively limited in the first months of 2024. However, this changed after the inauguration of the new Taiwanese president, Lai Ching-te, in May. In response to the inauguration, the Chinese military conducted a large-scale military exercise around Taiwan, raising tensions between the two countries to a new high. From this point on, the overall military pressure from China has increased, as can be seen, among other things, from the fact that large-scale military assets were deployed around the island twice in the remaining months of 2024.

Holding military exercises around the island is part of China's broader strategy to eventually bring the island under Beijing's control. Military intimidation is combined with economic and political pressure. China also applies lawfare9 and actively spreads disinformation.

In the South China Sea, tensions between China, which claims large parts of the area, and surrounding countries have remained high throughout 2024. Through the deployment of its naval and coast guard units, China has attempted to enforce its territorial claims, especially around the Spratly archipelago, which regularly results in incidents. For example, confrontations between the Chinese and Filipino units around the *Second Thomas Shoal10* (part of the Spratly Archipelago in the South China Sea) has led to several collisions.

Although Taiwan and the South China Sea are located on opposite sides side of the world, the increasing military tensions around these areas pose a direct threat to Dutch and allied economic and security interests. For the Netherlands, as a trading nation, the maritime trade routes that run between Asia and the rest of the world through the South China Sea and the Taiwan Strait are of great importance. Taiwanese companies are also essential in the production of semiconductors.

China and the relationship with Russia

In relations with Russia, China plays an important role on the world stage. China and Russia have continued and further intensified their economic, political and military cooperation in 2024. With the growing strategic competition between the US and China on the one hand, and between NATO and Russia on the other, Beijing and Moscow are finding each other as partners. Both countries aspire to a more multipolar world, in which the role of the US (and NATO) is reduced and in which China and Russia have a more prominent voice in regional and world politics.

China's strengthened relationship with Russia directly and indirectly contributed to maintaining Russia's war efforts in Ukraine in 2024. China is an important sales market for Russian energy products. Chinese (state) companies can supply all kinds of goods to Russia almost without restrictions, which uses them for its war efforts in Ukraine. Although China does not supply weapons and ammunition to Russia in principle, Chinese companies did supply dual-use goods for the Russian war industry and even attack drones. This goes against the export control policy that China itself advocates. This made China a direct player in the

[9] *Lawfare: the use of legal means to coerce or intimidate an opponent to achieve strategic goals.*

[10] *The Second Thomas Shoal is an underwater reef located within the Philippines' exclusive economic zone, but also claimed by China and Vietnam.*

area of European security, and indirectly a threat to the Netherlands and its allies.

It is doubtful whether Beijing can (or wants to) make a substantial contribution to peace negotiations that do justice to Ukrainian sovereignty. For example, despite repeated calls and invitations from the international community, Beijing did not participate in an international peace conference organized in Switzerland in the summer of 2024 and announced its own peace initiative with Brazil at the UN, without involving Ukraine in its design.

Sino-Russian military cooperation

The MIVD has observed that China and Russia have further intensified their military cooperation in 2024. This is reflected in joint (para)military exercises in various domains, both bilaterally and multilaterally (with South Africa and Iran). These exercises are becoming more complex and also cover new geographical areas. For example, Chinese strategic bombers were spotted above the Arctic Circle for the first time during a joint patrol with Russia, and the Chinese coast guard exercised with its Russian counterpart for the first time.

In addition, the experience of the Russian armed forces in Ukraine and Syria is potentially very important for the People's Liberation Army (PLA), which has little combat experience. Certainly with a view to preparing for a possible future military conflict in which China itself is involved. This aspect of military cooperation with Russia has become increasingly important to China since the war in Ukraine.

Despite the growing cooperation and shared interests, there is no natural alliance between China and Russia. This is strongly reflected in China's self-interested policy towards the Ukraine conflict.

The war in Ukraine and sanctions against Russia have created a new dynamic in the cooperation in which the 'unlimited partnership' is being tested. The war results in a complex dynamic in which Russia is increasingly dependent on China and Beijing successfully exploits this dependency. At the same time, Beijing tries to find a balance between its ambitions as a 'responsible great power', support for partner Russia and its trade interests, especially in Europe.

China: Economic Security

China's *whole-of-society approach* blurs the distinction between normal academic or economic exchange and espionage activities. That is why the MIVD, in the context of economic security, looks specifically at unwanted knowledge transfer. This also covers activities that are open and legal – think of investments and scientific research – but that nevertheless pose a threat to our economic security interests.

In doing so, the MIVD is looking in particular at the transfer of high-quality Dutch knowledge and technology to China. This is not only undesirable because of the risk of undesirable end use, such as military applications or the use of technology to restrict human rights. It also affects Dutch security interests because it can result in the loss of the strategic knowledge position of Dutch companies and knowledge institutions, or because it leads to a strategic dependency on China for certain raw materials, technologies or services.

The Dutch semiconductor industry has the attention of China. The Netherlands has unique knowledge on which China depends for a significant part of its production capacity. In 2024, China tried to acquire this crucial technology in the Netherlands in various ways. China uses a combination of (cyber) espionage, recruiting experts within Dutch companies, (strategic) takeovers of semiconductor companies and circumventing applicable export restrictions. As legal and overt acquisition of technology is made more difficult by, among other things, investment screening and export controls, the risk of illegal, covert acquisition increases.

With regard to strategic dependencies, the MIVD pays particular attention to the Chinese presence in vital infrastructure.
Individually, the security risks of tenders such as Chinese scanners at Dutch airports and seaports, Chinese providers in our telecom networks and Chinese cameras in public spaces seem manageable, but taken as a whole, they put the Netherlands in a position where Dutch actors are potentially vulnerable to economic pressure, espionage or even sabotage.

China: espionage

In 2024, the MIVD established Chinese espionage activities against Dutch and allied defense interests. The Netherlands is clearly in the picture and is an interesting espionage target for China.
This is due to the high-quality Dutch (defense) industry that China needs to achieve its stated political, economic and military objectives.

In addition, the Netherlands remains interesting for Chinese espionage activities as part of NATO, the EU, as a security partner of the US and because of the recent Dutch military presence in the South China Sea. The focus here is, among other things, on mapping the military intentions of NATO and the US with regard to China. Employees of the armed forces of the Netherlands and allies, including former employees, were espionage targets for China in 2024 because of their knowledge of contemporary Western military operations, personnel, processes and knowledge of high-quality equipment. The information collected by the Chinese services does not always concern targeted and specific information, but also information about individuals and defense components. All potential interesting information is in principle useful, if not now then perhaps in the future.

China: Cyber

In 2024, Chinese cyber units again conducted cyber operations against the Netherlands and allies in the EU and NATO. In order to operate more effectively, the Chinese PLA reorganized in 2024.
As part of this, most operational cyber units now fall under the *Cyber Space Force* (CSF), which is directly controlled by the *Central Military Commission* (CMC) led by Xi Jinping.
The MIVD estimates that this reorganization will further increase the threat posed by PLA cyber operations.

Intelligence from the MIVD has long indicated major Chinese efforts to achieve such strategic intelligence positions, with the aim of gathering intelligence and having options for action in the event of a possible future military conflict.

While China likely sees the US as its primary adversary in the cyber domain, it could also deploy significant cyber sabotage capabilities against European targets in the future.

In 2024, the MIVD and AIVD issued reports on the Chinese malware that the services found on the network of a Dutch defense unit11 and the broader campaign that the attack was part of12. In 2024, the services again observed that Chinese cyber actors successfully abused vulnerable edge *devices13,* such as firewalls and VPN software14. Software vulnerabilities were exploited at a rapid pace, often within hours or days of being announced. A campaign can thus victimize tens of thousands of organizations.

[11] *'Ministry of Defense of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT (MIVD & AIVD, 6 February '24)' and 'New malware highlights continuing interest in edge devices (NCSC-NL, 6 February '24) https:// www.ncsc.nl/ current/ news/ 2024/ february/ 6/ new-malware-benadrukt-continuing-interest-in-edge-devices*

[12] *Ongoing state cyber espionage campaign via vulnerable edge devices (NCSC-NL, June 10, 2024) https:// www.ncsc.nl/ actueel/ nieuws/ 2024/ juni/ 10/ aanhouden-statelijke-cyberspionagecampagne -via-vulnerable-edge-devices*

MIVD has exposed Chinese cyber espionage *(February 2024)*

The MIVD has exposed Chinese cyber espionage in the Netherlands. The service discovered advanced Chinese malware that makes this possible. Based on its own intelligence, the MIVD determines that a Chinese state actor is responsible for this malware.

China uses this type of malware for espionage on computer networks. The malware is used in systems *(FortiGate)* of the company Fortinet, with which computer users can work remotely in a protected manner. Fortinet supplies this cybersecurity worldwide.

For the first time, the MIVD has chosen to publish a technical report on the working methods of Chinese hackers. “It is important to att ribu such espionage activities by China,” responded then Minister of Defense Kajsa Ollongren. In this way, we increase international resilience against this kind of cyber espionage.

The MIVD has shared information about the incident and the characteristics of the malware on the website of the National Cyber Security Centre (NCSC). This allows users of the FortiGate system to determine whether they have become victims. They can also take measures to defend themselves.

Chinese cyber actors can tap into an ecosystem of facilitators estimated at hundreds of organizations. Chinese companies offer services to disguise the origins of state cyberattacks by routing them through vulnerable network equipment of unsuspecting individuals and organizations in third countries.

In addition, intensive cooperation with Chinese companies and knowledge institutions makes specialized knowledge accessible to Chinese state actors, such as research into vulnerabilities in hardware and software.

Notable in 2024 were publications by the US intelligence and security services about Chinese cyber units that managed to nestle themselves in critical infrastructure in an advanced way. The fact that they managed to operate undetected for at least a year indicates that Western intelligence services and cybersecurity companies have only limited control over the Chinese cyber threat.

Large-scale hack on US telecommunications providers

The Chinese cyber actor *Salt Typhoon* had access to major US telecom providers for at least a year. This would have included viewing communications from politicians and officials and possibly also gaining access to secret information from law enforcement agencies.

The reporting fits in with observations by the MIVD and AIVD. The services estimate that it is likely that European telecommunications providers are also the target of advanced hacking attempts.

Hacks on telecommunications providers are among the most valuable intelligence assets for Chinese state actors. Thus, the data stolen by *Salt Typhoon* likely contributed to the following capabilities for Chinese intelligence agencies:

- View confidential communications from American politicians and high-ranking officials.
- Identifying U.S. government officials, military personnel, and intelligence officers.

[13] *Edge devices: a device that provides an access point (gateway) to (core) networks of enterprises or service providers such as routers, routing switches, etc.*

[14] *VPN: Virtual Private Network; protects users by encrypting data and masking the IP address*

- Identifying the social and professional networks *and patterns of* life of these people.
- Gain access to classified information from US law enforcement agencies through *lawful* intercept systems.
- Discovering vulnerabilities in American networks governments, defense components, I&V services, vital sectors and top sectors.
- Performing *supply* chain operations through internet connections of telecom providers' customers.

The news about *Salt Typhoon* comes on top of earlier reporting about actor *Volt Typhoon,* who is said to have positioned himself for future sabotage of US military and civilian critical infrastructure.[15]

China: Military technology and weapons systems

With its ambition to become a world-class armed force, China is doing everything it can to acquire military trump cards: new weapon systems or existing systems that use new technologies. In its plans, China has long made considerable room for the development of technologies such as quantum technology, artificial intelligence and biotechnology, so-called key technologies. The country is doing this not only to become a civilian leader, but also to enable its armed forces to deter and dominate. These key technologies can cause such a major disruption of a society that they are strategic[16] in nature.

One of those trump cards concerns *quantum sensing.* This is a technology that makes it possible to make observations with extremely high accuracy, for example of accelerations or magnetic field strengths. *Quantum sensing* can be applied in a wide range of range of weapon systems. For example, quantum radars may be able to detect stealth aircraft, where conventional systems may have difficulty. In addition, quantum magnetometers will probably be able to detect submarines in the foreseeable future, which would negate their greatest strength, namely “invisibility”.

The MIVD notes that China will also focus on swarm technology in 2024. Swarm technology involves the deployment of a larger number of unmanned units that can work together autonomously to achieve a military objective. Autonomy is achieved on the basis of artificial intelligence. Examples of deployment include the neutralisation of air defence systems, the escorting of manned platforms or direct offensive deployment where the power largely results from operating in large numbers.

China is already a leader in swarm technology and is committed to developing systems for the air and maritime domains, among others. Furthermore, the development of swarm technology by China is seen as part of an arms race for *high* -tech warfare.

China is doing a lot to be and remain a frontrunner, including the export of knowledge from all over the world. The speed and scale of China's technological developments for military purposes pose challenges for other countries, including the Netherlands, in the field of defense and security. It is essential that the MIVD follows these developments closely and enables our armed forces to adapt their own strategies and capabilities in order to be able to respond effectively to the changes in the military landscape.

[15] *In this case, strategic key technologies are technologies intended for use as or in weapons, the weapons themselves being intended for total warfare, including against civilian targets and population centres.* [16] *In this case, strategic key technologies are technologies intended for use as or in weapons, the weapons themselves being intended for total warfare, including against civilian targets and population centres.*

LZ115

1.3 Caribbean

The MIVD and the AIVD are jointly investigating political and military developments in Venezuela and possible radiation effects on the special municipality of Bonaire and the countries of Aruba and Curaçao within the Kingdom of the Netherlands

The first months of 2024 in Venezuela were dominated by the Essequibo dispute. Following a referendum in December 2023, Venezuela declared a substantial part of neighboring Guyana as Venezuelan territory, which led to increased international tensions. Although Venezuela and Guyana both committed to finding a diplomatic solution, the Venezuelan regime nevertheless increased its military presence in the border area to underscore Venezuelan intentions. However, in the run-up to the Venezuelan presidential elections that took place in July, the Venezuelan military focus on the border with Guyana diminished. This did not fully return for the rest of 2024.

The presidential election of July 28, 2024 has been in many ways the most important event of the year for Venezuela. Although Nicolás Maduro has claimed victory, there is overwhelming evidence that his opponent Edmundo González Urrutia was the real winner of the election with a large majority of the votes. Shortly after the election, the Dutch diplomatic representation in Caracas provided refuge to presidential candidate González until he fled to Spain in September, due to the serious threat posed against him.

A significant part of the international community, including the US, the EU and several Latin American countries, do not recognize the regime's claimed victory of Maduro. The regime has subsequently broken diplomatic relations with several Latin American countries and further sharpened the discourse against the West.

While no new sanctions have been imposed on Venezuela's oil sector, both the US and the EU have announced new personnel sanctions against regime members. The Venezuelan regime has meanwhile sought to expand cooperation with its allies Russia, China and Iran, as well as other non-Western countries.

The Venezuelan armed forces have continued the upward trend in investments and development in 2024 that has been visible for several years. In cooperation with international partners such as Iran, Russia and China, Venezuela is working on making and keeping the existing equipment (re)deployable, as well as acquiring new equipment and resources. Despite this upward trend, the MIVD notes that the Venezuelan armed forces still face major challenges in 2024. For example, there are major personnel shortages, many units are only able to train to a very limited extent and there is a backlog of maintenance on many vehicles and weapon systems. On average, the readiness level of the Venezuelan armed forces therefore remains low.

1.4 Counterproliferation

The Counterproliferation Unit (UCP) is a joint unit of the MIVD and the AIVD. The unit investigates countries that could pose a threat to international security with weapons of mass destruction or develop the necessary means of delivery (usually ballistic missiles). The UCP also helps to prevent such 'countries of concern'[17] (Russian Federation, Iran, China, North Korea and Syria) from obtaining technology and knowledge to start or expand weapons programmes.

In 2024, it was again found that the use of weapons of mass destruction by countries of concern, including Russia, Iran and

[17] *Countries of concern are countries that may pose a threat to international security.*

North Korea, is a real possibility. The use of such weapon systems is not necessarily taboo for some of these countries. As explained below, Russia illegally used chemical agents in the fight against Ukraine in 2024 and Iran used ballistic missiles for the first direct attacks on Israel. In addition, both Iran and North Korea supply weapons (including ballistic missiles) to Russia for use in Ukraine, and developments in the nuclear field in Iran and North Korea are also worrying. Against this background, the services also actively took action in 2024 against the unwanted transfer of knowledge and technology from the Netherlands to such programs in (among others) the countries mentioned.

Russia

Russia is systematically violating the Chemical Weapons Convention by using chemical agents in the war in Ukraine. Already a few days after the 2022 invasion, the first reports emerged that Russia had used tear gas on Ukrainian territory. Since then, the use of chemical agents by Russia has intensified and focused on use against Ukrainian soldiers. Incidents with chloropicrin have also been documented. The Ukrainian Ministry of Defense has now reported thousands of incidents of Russian use of chemicals against Ukrainian armed forces, something that is explicitly prohibited under the Chemical Weapons Convention. The use resulted in additional sanctions against Russia by the US and the UK in 2024.

Iran

In 2024, Iranian ballistic missiles were used extensively in the Middle East. For the first time, Iran carried out direct attacks on Israel, using ballistic missiles developed by Iran itself. Iran claims that the hypersonic ballistic missile 'Fattah' was also used. However, the threat was not limited to Iran. Iranian allies such as Hezbollah and the US active in Yemen Houthis used Iranian-developed missiles in 2024. Iranian missile systems have thus played a major role in threatening shipping in the Red Sea and Persian Gulf.

Iran also delivered short-range missiles to Russia in 2024. Following this delivery, the European Union and a number of allies have imposed additional sanctions on Iran.

In the field of space travel, Iran has taken further steps in 2024. It has thus carried out several spacecraft launches. Technology from these spacecraft can also be used in the development of ballistic missiles. Furthermore, several Iranian satellites have been successfully launched into orbit by Russian spacecraft.

The MIVD also notes that Iran, if desired, could have sufficient highly enriched uranium available within a very short time for the production of several nuclear weapons. However, the MIVD and AIVD have no indications that Iran is currently performing the other necessary activities to carry out tests to develop a nuclear explosive. However, the development of nuclear weapons capacity does seem to be increasingly being discussed in the country. For example, the recent unrest in the Middle East has led to calls from certain circles within Iranian politics to revise the 2003 fatwa against nuclear weapons. Iran also threatens to withdraw from the nuclear non-proliferation treaty (NPT) if the E3[18] were to trigger the snapback mechanism[19] of the *Joint Comprehensive Plan of Action* (JCPOA). Furthermore, the International Atomic Energy Agency (IAEA) states that Iran is not enabling it to verify that Iran's nuclear programme serves exclusively civilian purposes. These developments complicate the process of reaching a new nuclear deal that would address proliferation concerns surrounding Iran's nuclear program.

[18] *E3: Germany, France and the United Kingdom.* [19] *Snapback mechanism: if Iran does not comply with the JCPOA, any JCPOA member (directly, if a member of the UN Security Council) or indirectly of the UN Security Council can initiate a procedure to impose sanctions.*

North Korea

North Korea also continued to develop both short-range and intercontinental ballistic missiles in 2024. The country conducted test launches of tactical ballistic missiles and cruise missiles with a larger explosive payload than previously demonstrated, and test launches of new hypersonic ballistic missiles and a new intercontinental ballistic missile. In addition, Kim Jong-Un issued an order to increase munitions production, in a year in which tensions between North and South Korea continued to rise. Like Iran, North Korea also delivered several short-range missiles to Russia in 2024. In the case of North Korea, these missiles were also actually deployed on the battlefield in Ukraine.

North Korea has given a unique glimpse into its nuclear weapons program in 2024. The country published photos of a uranium enrichment facility, something that has never happened before. Kim Jong-Un is thus fulfilling his intention to expand the North Korean nuclear arsenal.

Acquisition

Countries of concern (in addition to Russia, Iran and North Korea, also countries such as Pakistan and Syria) were still dependent on the West for knowledge and high-tech in 2024. The services investigate the acquisition activities for this knowledge and technology, and also in 2024 the government was able to take action against Russian and Iranian acquisition networks, among others. This action included diplomatic, administrative or criminal measures, or operational action by the services themselves.20

The services' investigation has shown that Russia is circumventing tightened sanctions on the export of "dual-use goods"21 by importing them through "conduit countries", including the United Arab Emirates, Turkey, Kazakhstan and China. This makes it more difficult to identify and counter exports at an early stage. In some cases, this also involved 'dual-use goods' from the Netherlands.

The services also note that existing trade channels within the civil nuclear sector are being used by Russia to acquire technology for the military-industrial complex. Due to dependency relationships, the West has so far refrained from imposing trade restrictions on the civil nuclear sector, which generally does not enhance the effectiveness of sanctions against Russia.

1.5 Counterintelligence (CI)

One of the tasks of the MIVD is to conduct research into threats of extremism and terrorism in particular in relation to the armed forces. In 2024, the MIVD will focus this research primarily on right-wing extremism and anti-institutional extremism. The focus of the research is on threats against Defence and on threats from (aspiring) defence employees towards the democratic and international legal order. With the findings from this research, the MIVD can enable stakeholders to take measures, both against specific individuals and in the area of policy development.

Right-wing extremism

In 2024, the MIVD launched several investigations into possible right-wing extremism among (aspiring) defense employees. Some of these investigations do not appear to involve ideologically motivated statements, but rather other forms of serious norm-blurring. When the ideological component does appear to be present, it usually involves Nazi sympathies in which anti-Semitic statements play a prominent role. The MIVD has no further indications of right-wing extremist networking within Defense, but does see that right-wing extremist (aspiring) defense employees are active in

[20] In a podcast published in 2024 on countering such acquisition attempts, the services provide a glimpse into what such operations entail.

[21] Goods are 'dual-use' if they can be used for both peaceful and military purposes, e.g. both for basic scientific research and in a weapons of mass destruction programme.

F803

right-wing extremist networks outside Defence. In 2024, the MIVD informed various stakeholders about right-wing extremist (prospective) defence employees to enable them to take measures. The MIVD currently has no indications of a right-wing extremist threat of violence towards Defence.

Anti-institutional extremism

Anti-institutional extremists believe that there is an evil elite in power that severely oppresses the people. This alleged evil elite would use institutions such as the government, the media and science to do this. Some anti-institutional extremists see Defence as part of the evil elite or call on the military to take action and protect the people against this elite. This poses a threat to the defence organisation and the democratic legal order. In 2024, the MIVD recognised that some defence employees adhered to the evil elite narrative and acted accordingly. In a number of cases, a pro-Russian sentiment was part of the ideology of these defence employees. The MIVD informed stakeholders where the behaviour of these defence employees raised serious doubts about their reliability with regard to the deployability of the armed forces and the protection of the democratic legal order.

The MIVD currently has no indications of violent anti-institutional extremism towards the armed forces.

Espionage, unwanted interference and economic security

In 2024, the MIVD conducted research into the threat of espionage (intelligence) activities from countries other than those specifically described above. These countries attempt to determine the position of the Dutch armed forces within multilateral partnerships or attempt to obtain specific knowledge about Defence or the Defence industry.

Iran

The MIVD is conducting investigations into the (covert) activities of Iranian military and civilian intelligence services aimed at acquiring knowledge and resources that pose a threat to the security, readiness and deployability of the armed forces in a national or international context, for the (Dutch) defence industry and for military alliance organisations such as NATO. Investigations in 2024 have shown that Iranian activities against Defence continue to take place on an opportunistic basis, at home and abroad.

In 2024, Iranian cyber actors focused primarily on interests related to the Israel-Gaza conflict. Through digital attacks with local and temporary impact, in some cases also targeting critical infrastructure, Iran sought to assert itself.
In this way, persons affiliated with Iran are attempting to use *hack-and-leak* operations online (through various forums such as social media) to reinforce certain messages and, in extreme cases, to enforce policy changes. This also made Iranian cyber activities more visible compared to previous years.

In addition to its more visible activities, Iran has stepped up its covert espionage activities against experts involved in the Middle East conflict in the past year. Iranian actors have sometimes used highly sophisticated social engineering techniques to compromise communications tools through *phishing*[22] and *spear phishing*[23] methods.

[22] *Phishing: A form of internet fraud in which cybercriminals attempt to steal personal information or passwords.*

[23] *Spear phishing: A targeted form of phishing that uses email, telephone, or other channels to trick a specific individual or small group of individuals into sharing confidential information or installing malicious software.*

North Korea

North Korean cyberattacks contribute significantly to North Korea's political, military and economic ambitions.
North Korea has an offensive cyber program. For example, the attacks are aimed at stealing information about political and economic positions on North Korea, international cooperation, but also about high-quality (military) technology.
North Korean cyber actors are very successful in stealing *cryptocurrency* and circumventing sanctions imposed on North Korea with their attacks. The cyber attacks contribute to the financing of the regime. For example, this finances the North Korean cyber and nuclear weapons program.

Economic security

Dutch economic and security interests are still exposed to a variety of (state) threats. These primarily concern unwanted knowledge and technology transfer and strategic dependencies.

The Dutch defense industry, companies, knowledge institutions and scientists are a potential target of various state actors who (secretly) try to acquire high-quality, military-relevant or otherwise, technology. The Netherlands has unique high-quality knowledge and technology positions, including in the field of semiconductors, quantum technology and aerospace, which are threatened by espionage attempts or (secret) takeovers by countries of concern such as Russia, China and Iran. This knowledge and technology can contribute to military capacity building in these countries.

The Dutch defence industry is largely dependent on suppliers from third countries and is therefore susceptible to risky strategic dependencies. In addition, dependencies in the Dutch vital infrastructure can pose a risk to Dutch economic security interests.

The MIVD and AIVD have assigned the investigations in the field of economic security and strategic dependencies to the joint MIVD-AIVD intelligence teams. These teams also contribute to various measures that the government has taken to counter the threat to Dutch economic security and to increase resilience, such as the Business Desk for Economic Security, the system of investment assessment and the Desk for Knowledge Security.

1.6 Mission Support and Areas of Focus

In 2024, the MIVD supported the deployment of the Dutch armed forces in mission areas. The MIVD produces intelligence products for military deployment and the political decision-making involved. The MIVD also remains involved during the deployment by conducting research into aspects that are relevant to the direct threat to Dutch military personnel in a deployment area and coalition and threats to the successful execution of the mission, such as threats to national political support in the country of deployment or factors that influence the effective performance of units.

Western Balkans

In 2024, the MIVD will conduct research into the Western Balkans in support of the deployment of the Dutch armed forces as part of *the European Union Force Bosnia and Herzegovina* (EUFOR Althea). In Bosnia and Herzegovina, despite the start of accession negotiations with the EU, strong ethno-nationalist rhetoric, particularly from the Bosnian Serb side, continued. There were also more separatist voices from the Serbian Republic, a constituent entity of Bosnia and Herzegovina. In Kosovo, unrest increased in the run-up to the 2025 election year. The tensions fitted in with the increase in activities of the often (Kosovar) Serbian nationalist groups. The

The Kosovo government has tried to deploy more police in Northern Kosovo as part of its efforts to combat corruption and organised crime. Tensions are expected to flare up periodically. The normalisation process between Serbia and Kosovo, mediated by the EU, has become more difficult due to the tough stance of both sides. Large-scale incidents and significant social unrest in the region have been prevented, partly due to the presence of EU and NATO military missions.

Africa

The MIVD's research focuses on the timely identification and reporting of strategic and security-relevant developments that pose a (potential) threat to national security, Dutch interests and/or (potential) EU missions.

Mali, Burkina Faso and Niger are among the least developed countries in the world. Due to a combination of extreme poverty, weak state capacity, climate change and strong population growth, there is an increasing shortage of basic necessities of life. In all three countries, the military has become frustrated about the poor (security)

situation seized power.

In Mali, jihadist organizations continued to expand their areas of operation. The focus of jihadist activities is in Northern and Central Mali, but there is a shift in violent incidents towards the south. Outside the capital, the jihadist threat has also increased. But jihadists also struck in the capital last year. In September, the jihadist organization Jama'at Nusrat al-Islam wal-Muslimin (JNIM) managed to attack the airport and a training institute of the gendarmerie there.

The Malian army is cooperating with Russian paramilitaries in fighting the jihadists.

The security situation in Burkina Faso has deteriorated in 2024, just as in previous years. Citizens are increasingly caught between the ruling junta of President Traoré, who came to power in a coup d'état in 2022, and jihadist groups. The jihadist attacks are also becoming increasingly large-scale and are occurring in more and more places in the country. To deal with the deteriorating security situation, the junta has, as in Mali, called in the help of Russian paramilitaries. They are responsible for the personal security of junta leader Traoré and provide training for the Burkinabe armed forces.

The situation in Niger is similar to that in Mali and Burkina Faso. This country also has a persistently poor security situation that the government that came to power in a coup in July 2023 has failed to effectively improve. Here too, attacks by jihadists pose the greatest threat and the Nigerien junta has also called in the help of Russian paramilitaries who carry out similar tasks as in Burkina Faso.

Iraq

The MIVD also conducted research into Iraq in 2024. The focus was on intelligence support for the *NATO Mission in Iraq* (NMI). The Dutch military contribution to the NMI mission includes the delivery of a Dutch commander, approximately fifteen additional staff members, a *Force Protection* element and three transport helicopters including personnel for the period from May 2024 to May 2025.

In 2024, the conflict between Israel and Hamas led to attacks by the (mostly) Shiite militias affiliated with Iran on coalition locations in Iraq and Syria. These attacks were mostly small-scale and the human and material damage remained largely limited. There have been no attacks on coalition locations in Iraq since early October.

From mid-August onwards, Iraqi militias allied with Iran shifted their focus to carrying out small-scale attacks in the direction of Israel. The number of attacks increased significantly from mid-September 2024. After the ceasefire between Israel and Hezbollah on November 27 last year, attacks on Israel were suspended.

In 2024, the MIVD conducted research into Iraqi politics. Despite the regional conflict between Israel and Iran (including its allies Hamas and Hezbollah), Iraqi politics in 2024 was characterised by relative stability. The government of Prime Minister al-Sudani has achieved various successes, including by improving infrastructure. However, large-scale structural problems remain unresolved. Persistent social discontent due to a lack of, among other things, sufficient basic facilities (such as water and electricity) and employment regularly results in demonstrations throughout Iraq.

Iran

In 2024, the MIVD will conduct an investigation into Iran's political and military influence in the Middle East. The country supports numerous pro-Iranian militias in that region, such as Hezbollah and the Houthis, with weapons, advice and intelligence. In this way, Iran tries to maintain its influence in the region and, where possible, to increase it.

But the Iranian regime suffered a number of heavy blows in 2024. First, the simmering conflict with Israel flared up. During the year, the two countries attacked each other several times with missiles and UAVs, with the Israeli attacks proving militarily much more effective than the Iranian ones.

Secondly, Iran had to watch its allies in the region come under fire. Hamas and Hezbollah were hit hard by Israeli attacks. In December, Iran saw the fall of the Assad regime in Syria, leaving a key partner behind, making Iran’s geopolitical position more vulnerable.

A notable political event in Iran was the death of President Raisi, who died in a helicopter crash on May 19. Raisi was succeeded by the relatively moderate Mahmoud Pezeshkian, who won the presidential election on July 5. President Raisi was considered the leading candidate to succeed Iran's Supreme Leader Ali Khamenei. Raisi's death has put the question of succession back on track.

open.

ISIS

In 2024, ISIS in Iraq and Syria continued to suffer personnel and material losses due to the continued pressure from the various security forces supported by the anti-ISIS coalition. In 2024, the decline in attacks by ISIS in Iraq continued. In 2024, several weeks passed without any attacks, which was exceptional. The attacks that ISIS did carry out were mostly small-scale, using simple *hit &* run tactics. Most incidents occurred in central Iraq. Given the cross-border nature of ISIS activities and (support for) the deployment of allies, ISIS activities in Syria were also examined.

1.7 Safety promoting tasks

Electronic security investigations The Defence Security Policy (DBB) sets a number of security standards that promote the exclusivity, integrity and availability of information (of all classifications). In addition to construction, organisational and security-technical standards, the DBB stipulates that a space where information is discussed or processed with the classification Stg. GEHEIM and/or higher is subject to an Electronic Security Investigation (EVO). The MIVD carries out investigations on such existing spaces and issues advice for new construction or renovation projects. This is to signal any points of attention regarding information security at an early stage. The MIVD carries out these investigations for all defence components and works, where possible, together with Dutch colleague services within the field.

Economic security

In view of the increased importance of intelligence and security-promoting measures in the field of economic security, the MIVD specifically looks at risks and security interests with regard to (economic) espionage and unwanted foreign influence in relation to defense contracting companies. It is important that the open economy and thus the earning capacity of Dutch companies, including defense contracting companies, does not come at the expense of the integrity, security and operational deployability of the Dutch armed forces.

The Dutch economic and security interests are still exposed to a variety of (state) threats, including the Dutch defense industry. This primarily concerns unwanted knowledge and technology transfer and strategic dependencies.

The Netherlands has unique high-quality knowledge and technology positions, including in the fields of semiconductors, quantum technology and aerospace, which are threatened by espionage attempts or (secret) takeovers by countries of concern such as Russia, China and Iran. This knowledge and technology can contribute to the military build-up in these countries.

Dutch industry is largely dependent on suppliers from third countries and is therefore susceptible to risky strategic dependencies. In addition, dependencies in Dutch vital infrastructure can pose a risk to Dutch (economic) security interests.

The MIVD and AIVD have assigned the investigations in the field of economic security and strategic dependencies to joint intelligence teams. These teams also contribute to various measures that the Cabinet has taken to counter the threat to Dutch economic security and to increase resilience.

Industrial Safety

The DBB, and in particular Industrial Security, prescribes the obligations that apply internally to Defence when exchanging Special Information (BI) with the business community, the defence industry or when carrying out assignments of a vital nature. The General Security Requirements for Defence Assignments (ABDO) regulation prescribes the requirements that the business community must meet before they can be authorised to come into contact with BI. At the start of an assignment, the MIVD's Industrial Safety Bureau (BIV) checks the companies to ensure that they meet the requirements set out in the ABDO. Continuous activities of BIV include routinely inspecting companies with an ABDO authorisation, carrying out integral safety checks, and advising ABDO companies and the client (Defence). In the event of an incident involving BI, BIV takes or has measures taken to prevent or limit (possible) compromise.

In view of the increased importance of intelligence and security-promoting measures in the field of economic security, the MIVD specifically looks at risks and security interests with regard to (economic) espionage and unwanted foreign influence in relation to defense contracting companies. It is important that the open economy and thus the earning capacity of Dutch companies, including defense contracting companies, does not come at the expense of the integrity, security and operational deployability of the Dutch armed forces.

In 2024, the MIVD had information about (intended) foreign takeovers and/or investments in defense orders companies involved in the delivery of exclusive services or high-quality (military) technology. In addition, an increase in incidents in the cyber domain was seen. ABDO companies are also affected by this. In 2024, the collaboration with the AIVD will be intensified in preparation for the transition from defense contracts to government-wide contracts. In the coming period, the General Security Requirements for Government Contracts (ABRO) will be completed under the leadership of an interdepartmental program. The BIV will be incorporated into the National Bureau for Industrial Safety (NBIV), a joint office of the MIVD and the AIVD.

Security Investigations

The Security Investigations Unit (UVO) of the MIVD and the AIVD looks back positively on 2024, as 93.3% of the security investigations were completed within the statutory standard of eight weeks. In 2024, the UVO, together with the mandate holder (Royal Marechaussee), completed 84,847 security investigations. The need for security investigations continues to increase. This trend was also visible in 2023. This is partly due to an increase in the number of positions of trust in the Netherlands, including at Defence.

In 2024, the UVO implemented structural measures to meet the need for security investigations. Among other things, the unit has recruited more staff and worked on digitalisation and (partial) automation of security investigations. Automation allows the UVO to deploy more employees on complex files, which allows for high-quality investigations to be delivered. In addition, automation has ensured, among other things, that the average waiting time has been reduced compared to last year.

In 2024, the Defence Mandate Regulation Intelligence and Security Services Act 2017 and the Security Investigations Act were amended. As a result of this amendment, the authority to refuse or withdraw a declaration of no objection (VGB) no longer lies with the Deputy Secretary General of Defence, but with the (deputy) director of the MIVD.

The amendment to the Security Investigations Act was submitted to the House of Representatives in January 2025. The law aims to provide more flexibility to sectors where employees holding a position of trust frequently change employers and introduces a location-based VGB. Employers are required to register and deregister if they place an employee in a position of trust or remove him from it. As a result of this obligation, an up-to-date file of confidential officers is created for the AIVD and MIVD, in the form of a register. Work is underway to develop this register.

Parliamentary consideration of the bill is expected to be completed in 2025, so that the new law can come into effect in 2026.

F803

2 RESPONSIBLE TO SOCIETY

Social support and trust of society in the actions of the MIVD are essential. The service has various powers at its disposal that enable it to perform its tasks. The Intelligence and Security Services Act 2017 (Wiv 2027) provides the basis for the use of special powers and the Temporary Act on AIVD and MIVD investigations into countries with an offensive cyber programme, bulk data sets and other specific provisions (Temporary Act) is an addition to this. The law and society place high demands on how the service acquires and processes its data. The internal system of compliance, supervision and accountability is referred to as compliance.

2.1 Working on the Wiv 2017 and the Temporary Act

The Wiv 2017 describes the tasks and powers of the MIVD and the AIVD. It has been clear for a number of years that the Wiv 2017 does not meet the requirements of the modern operational practice of the services in some areas. Independent investigations by the Wiv 2017 Evaluation Committee and the General Audit Office confirm the shortcomings: the services are not agile enough in countering foreign threats and are faced with a high administrative burden. This burden is at the expense of effectiveness and the possibility to innovate. The effectiveness through effective use of powers and the future-proofing of the services are therefore under pressure. The cabinet therefore decided in 2021 that the Wiv 2017 had to be thoroughly revised.

In September 2023, the Cabinet presented the House of Representatives with a policy statement. This contains a framework for the broad revision of the Wiv 2017.

On 23 October 2024, a committee debate was held on this matter. Based on the main points note, the input from the House of Representatives and the operation of the Temporary Act, a new future-proof Intelligence and Security Services Act will be created. The aim is to offer the bill for public consultation at the end of 2025.

The Temporary Act entered into force on 1 July 2024. This Temporary Act should enable the services, among other things, to defend the Netherlands more effectively in the short term against countries with offensive cyber programmes. This Act should enable us to defend the Netherlands more effectively by deploying existing powers such as cable interception and hacking more effectively and the possibility of using acquired data sets for a longer period of time. The Temporary Act also stipulates that the services can appeal to the Administrative Law Division of the Council of State against binding judgments of the Review Committee for the Use of Special Powers (TIB) and the Intelligence and Security Services Supervisory Committee (CTIVD).

In 2024, not all powers from the Temporary Act will have actually been used. The CTIVD has indicated that due to housing problems24 not yet be able to fully carry out all activities for binding supervision under the Temporary Act. This has resulted in, among other things, the provisions regarding the hacking authority not yet being implemented. An implementation test is being carried out on the operation of the Temporary Act in practice. The first results will be presented to the House in June 2025 and will be included in the revision of the Wiv 2017.

Even after the implementation test, the Temporary Act will be continuously monitored.

[24] Chamber letter: 'Status of CTIVD housing' 29 November 2024: Ref.4427880

2.2 Compliance and risk

The MIVD works with special data. In this respect, it is important that employees are aware of the legal frameworks. Responsibility for compliant work also includes carefully investigating compliance reports. In 2024, the MIVD invested in increasing the compliance awareness of its employees and improving the incident process. This has resulted in an increased number of compliance reports to the Compliance Office. The Compliance Office coordinates the processing of these compliance reports, which often result in measures such as improving policy, processes and/or procedures. Because employees experience that a compliance report leads to concrete improvements, the willingness to report increases.

In the past year, the MIVD informed the CTIVD several times about a compliance incident. This was in accordance with the agreements laid down in the incident protocol between the CTIVD and the services. In a number of cases, the CTIVD endorsed the measures advised by the Compliance Office in response to a compliance incident and advised the MIVD to follow them. In one case, the CTIVD informed the Lower House about the lack of progress before concluding the handling of the compliance incident.

Koninklijke
Marechaussee
stream

3AN ORGANIZATION IN MOTION

3.1 MIVD Future Perspective 2024 - 2030

In October 2024, the MIVD established an internal perspective for the period 2024-2030. This perspective is the result of a continuous process of strategy formation, involving both internal and external actors. The perspective outlines the security context, the resulting objectives for the organization and a number of operational lines along which these are realized. The objectives describe where we want to be in 2030:

- The MIVD responds quickly to geopolitical changes: The MIVD responds quickly to emerging crisis situations, anticipates geopolitical changes and investigates both known and unknown threats. To this end, we join forces with our partners, we can quickly switch between our intelligence positions and, with the help of new technological possibilities, we organize our organization in a smart and flexible way.

- The MIVD is a crucial instrument in the *grey zone:* the MIVD has a essential role in the *grey zone.* In doing so, the MIVD has unique powers, resources and expertise to protect the Netherlands and Defence and to provide deterrence. The MIVD offers options for action to others and, based on its own counter-intelligence task and the security-promoting tasks, takes proactive measures against threats in collaboration with other agencies. We work together with our (inter)national partners in this.

- The MIVD is ready for a large-scale armed conflict: the MIVD helps strengthen the armed forces and build deterrence to prevent NATO and the Netherlands from engaging in large-scale armed conflict conflict. The MIVD achieves an authoritative intelligence position and thus increases the effectiveness of the Dutch military intelligence and security system. We ensure that we are well connected to the Operational Headquarters.

- The MIVD identifies, uses and protects new technological developments for our customers and our operations: we utilise the opportunities offered by new technological developments, are aware of the implications of disruptive technologies and protect militarily relevant technology to prevent state actors from obtaining sensitive technologies.

3.2 Change and grow

Good support in the field of Human Resources (HR) is essential for the realization of the vision of the service. The MIVD is an organization with both a qualitative and quantitative growth task in which the growing military threat and the necessary knowledge that is required for this must be anticipated. Further development in the field of

The area of strategic personnel planning and strategic talent management enables the MIVD to address succession issues and invest in clearer and better career prospects.

In addition, the MIVD is continuously working to be an attractive employer for both our existing staff and future colleagues. The MIVD does this by, among other things, continuously investing in leadership and offering training and development opportunities. In particular, for the purpose of recruiting scarce capacity, the MIVD actively approaches potential candidates to introduce them to the Intelligence and Security domain. Where possible, this is done in collaboration with our partners within Defence and the AIVD.

3.3 A data-driven intelligence service

The investigation process is highly dependent on the fast and targeted processing of large amounts of data and the IT facilities that enable our analysts to do this. In order to remain relevant in the future, the MIVD is working to make the intelligence process and decision-making more data-driven. The service is continuously working on innovation and improvement of information technology for the acquisition, storage, processing, editing, analysis and dissemination of our intelligence. In addition, the MIVD invests in the necessary but scarce human capital.

The importance of continuity and operational reliability of the IV facilities only increases with increasing tension. The service therefore invests extra in strengthening the foundation.

Finally, the service invests in a number of programs and projects that enable data-driven work and increase the quality of information management. This also includes programs in the field of infrastructure, data processing and strengthening cooperation and connectivity with the armed forces. Strategies in the field of algorithms and Cloud have been further developed. Together with the AIVD, a jointly established department was completed in 2024. This department brings together knowledge and expertise in the field of IT, applications, data, information management and frameworks and architecture. This means that the MIVD is better equipped to organize strategic prioritization and implementation in the field of data and IV in such a way that a data-driven future can be given substance to for both services.

3.4 Cooperation

Connected to the armed forces

The prioritization of Main Task 1 requires enhanced cooperation between the MIVD and the armed forces. In 2024, the MIVD will have further steps have been taken to provide better and long-term support to the armed forces in the event of a large-scale conflict. The need for this has always existed, but the work and prioritisation within the framework of Main Task 1 have become even more urgent due to the continuing deterioration of the international security situation.

In order to better support the armed forces, cooperation with joint organizational units such as the Defense Cyber Command and the *Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance Command* (JISTARC) will first be consolidated in 2024. In addition, the armed forces can acquire and process data within the legal framework, for example with the MQ-9, under the mandate of the MIVD and at the same time perform their own tasks *(dual hatted).*

The processes of the MIVD and the armed forces must be well-coordinated in order to be able to work together. The MIVD now aligns itself more closely with the planning and readiness process of the armed forces and is closely involved in the development and establishment of the operational headquarters *NLD Joint Force Command.* Finally, further steps have been taken to share more intelligence with NATO and EU allies, including by giving more priority to responding to *Requests for Information* (RFIs).

Finally, in 2024, the MIVD took the lead in strengthening strategic personnel management within the intelligence and security domain of Defence. Intelligence and security personnel are scarce and it is important that personnel can be deployed optimally, especially with a view to preparing for Main Task 1.
Strategic personnel management can help to offer future employees an interesting career and development perspective, which will help retain employees for intelligence and security functions within the armed forces and the MIVD.

Collaboration with the AIVD

Last year, the collaboration between the MIVD and the AIVD was further intensified. The services investigated how to collaborate even more efficiently and effectively to jointly strengthen the resilience and security of Defence and the Netherlands. Collaboration takes place at almost all levels of the organisations, in joint organisational units or in mutual coordination.

Collaboration between private sector and academic partners

The MIVD works in an ecosystem with companies and knowledge institutions on the latest technologies, products, services and expertise. Strengthening these partnerships is an important pillar in the vision for the future.

In 2024, the MIVD became more open and sought connections with the academic world, in particular universities, colleges and knowledge institutes. The service facilitated academic research, enabled employees to publish and provided guest lectures.
An example is the first Arthur Docters van Leeuwen lecture by the director of MIVD at Leiden University on 10 December. Furthermore, *'Lifting the Fog'* by Bob de Graaff is now also available in English, for which he was given access to MIVD archives at the time. Relevant knowledge development and knowledge sharing in the field of intelligence and security keeps the MIVD *'fit for purpose'.*
Transparency also contributes to a better understanding of information within society.

Market parties are increasingly important to the MIVD. With talent, technology, data and capital present there, the innovation capacity of some companies is great. In the current information age, the access of companies to data has also increased significantly. Commercial services and information products are therefore increasingly relevant to the service. The MIVD is taking steps to increase the insight into the possibilities of the market and to use these in an effective, efficient and lawful manner.

3.5 Space

The armed forces and society are not only highly dependent on the space domain, but there is also increasing military action in space. For example, the conflict in Ukraine shows that modern warfare extends to all domains of military action, including the space domain. For example, earth observation capabilities and satellite communication, for example via Starlink, have great added value for the Ukrainian armed forces.

Over the past year, the MIVD investigated the space capabilities of countries of concern and a wide range of threats to satellite capabilities.
These threats range from activities involving satellite signal jamming to the development of a nuclear anti-satellite weapon by the Russian Federation, which has also been reported in open sources. Disabling, jamming or otherwise negatively influencing satellite infrastructure will not only have military implications, but will also have disruptive consequences for society.

An independent intelligence position on threats in and from the space domain is of great importance. By attributing and interpreting such threats, the MIVD provides a perspective for action at national and multilateral level. The Defence Memorandum 2024 emphasises the need to increase the MIVD's ability to use the space domain and the intelligence position on space as the fifth domain for military action. Since 2023, the MIVD has been intensifying its efforts on space, in close cooperation with the Defence *Space Security Centre* of the Royal Netherlands Air Force, in bilateral cooperation and in NATO and in the EU context. Investments in the space domain in the short term are necessary to be prepared for a large-scale conflict and to be able to keep up with and make use of the rapid technological developments in the space sector.

3.6 Infrastructure and housing

The Ministers of Defence and the Interior and Kingdom Relations have the joint ambition to continue to strengthen the cooperation between the MIVD and the AIVD across the full breadth of work in the security domain for the benefit of national security. This strengthened cooperation has been initiated previously and takes place on content, by means of joint teams and also by joint housing.

Joint housing will take place at three locations; the existing Zoetermeer location, the Leidschendam location to be renovated and the new construction to be realised at the Frederikkazerne location. The House of Representatives was informed about this on 28 October 2024 by means of the collective letter *'developments in real estate, living environment and spatial planning'.25* The Zoetermeer and Leidschendam locations are managed by the AIVD and the new construction to be realised at the Frederikkazerne by the MIVD. The Central Government Real Estate Agency (RVB) expects to be able to deliver the renovated Leidschendam location at the end of 2027.

In the meantime, hundreds of people are already working in joint teams at the existing locations of the AIVD and the MIVD. In anticipation of the final situation, the MIVD and the AIVD will continue to work in 2025 on joint agreements on various business management components that are helpful for the further intensification of cooperation in the primary process.

In order to accommodate the MIVD's staff growth in the coming years until the additional housing is delivered, a number of processes have been initiated to keep the housing at the Frederikkazerne available and to ensure uninterrupted business operations and a safe working environment for the service. In addition, work is being done on two interim facilities.

[25] *Collection letter on developments in real estate, living environment and spatial planning (BS2024031462) dated October 28, 2024.*

F-015

Machine Translated by Google

4KING NUMBER

Key figures from the Industrial Safety Bureau (BIV):

Companies in portfolio; 2069 of which:
1,566 Dutch companies
503 foreign companies

Intake authorization:

In 2024, a total of 968 new authorizations were requested, of which:
507 new authorization requests by a Dutch client (Defense or company) for a Dutch company
181 new authorization requests by a Dutch client (Defense or company) for a foreign company
211 new authorization requests by a foreign client (Defense or company) for a Dutch company
69 new authorization applications were not processed because the company did not meet the requirements of the quality assessment for intake.

Processing authorizations:

In 2024, a total of 1174 authorizations were processed, of which:
687 final authorizations;
101 withdrawn authorizations by the client;
92 denied authorizations;
136 FSCs issued abroad;
158 FSCs issued by foreign countries.

Context voor Facility Security Clearances (FSC)

With foreign National and Designated Security Authorities (NSA/DSA)25 has been maintained in contact to request and process FSCs. On request from a foreign country, in connection with the possible award of a foreign defense order, a Dutch company is asked to submit an FSC.

Audits

In 2024, a total of 22 audits were carried out at 22 companies.

Notifications and incidents

Incidents reported:	153
Incidents handled:	161

Assessed applications from non-Dutch nationals for positions of trust in ABDO assignments

In 2024, a total of 426 applications for Non-Dutch were submitted:
428 have been approved.
12 were rejected.

Requests for Visit

The ABDO stipulates that, in addition to Defense employees, companies must also submit their Request for Visit (RFV) to the Industrial Safety Bureau.
This makes it possible to obtain a more complete picture of (trends in) travel and traveller behaviour for defence-related trips.

In 2024, 2,413 RfVs were issued for classified visits to the Dutch defense:

For visits to foreign defenses **3042.**
209 RfVs were issued for visits to Dutch industry .
For visits to foreign industry **897.**

[26] *NSA/ DSA: Supervisor of the security of inter- (DSA) or national (NSA) classified information.*

To research	Positive decisions	Negative decisions	Total number of decisions
A-level by UVO	6.884	30	6.914
B-level by UVO	22.769	158	22.927
B-level taken over by UVO from KMar	9.244	1.607	10.851
NAVO Top 2025	92	0	92
Total by UVO	44.283	1.811	46.094
B-level by KMar	38.573	0*	38.753
Total number of studies	83.036	1.811	84.847

*The KMar does not issue negative decisions. In case of doubt in a B-level security investigation, they transfer the security investigation to the UVO. Any negative decisions are then included in the negative decisions of the AIVD. That explains the 0 here.

Safety research key figures

Box: The UVO is a joint unit of the AIVD and the MIVD. The unit conducts security investigations into (candidate) confidential officials: people who have access to secret information through their work, or are in a position in which they can harm national security. For example, in the central government, Defence, civil aviation or in companies that work on vital processes.

If the investigation is completed successfully, the candidate will receive a certificate of no objection (vgb).

Explanation of safety investigation key figures

Of the total number of investigations in 2024, 46,094 were carried out by the UVO itself and 38,753 by the mandate holder. Depending on the nature of the confidential function and the possible damage that the (candidate) confidential functionary could cause to national security, an A, B or C investigation is initiated. An A investigation is the most in-depth and intended for the most vulnerable confidential functions.

Explanation of the handling of objections and (higher) professional procedures

Following decisions to refuse or withdraw a declaration of no objection, individuals may file an objection. If the objection is declared unfounded, they may appeal (to a higher court).

2024	Submitted	Dismissed in 2023	Unfounded	Founded	Not in 2024 receptive	Withdrawn	Rejected
Objections	170	90	55	11	12	13	-
Occupations	9	2	2	-	-	-	-
Higher appeal	0	1	1	-	-	-	-
Interim provision	0	0	-	-	-	-	-

Notification

On the basis of Article 59 Wiv 2017, it must be investigated whether, five years after the end of the exercise of certain special powers, this can be reported to the person against whom the special power has been exercised.[27] This concerns the power to:

- opening letters or other postal items;
- the targeted interception of communications, such as by tapping a telephone, placing a microphone or tapping the Internet;
- entering a home without the resident's permission.

No notifications were made in 2024.

Threat assessments of individuals

If the MIVD has concrete and/or conceivable threat information that can be interpreted, the MIVD issues a threat assessment. In addition to the threat information, the effect is also assessed when the threat is carried out and whether the threatener has the will and the possibilities. The MIVD can also provide the desired information in a threat assessment or threat analysis. This is a more extensive analysis of concrete and conceivable threats from the perspective of the threatened party, such as a politician or diplomat.

Last year, 19 threat assessments were written.

Tap statistics

In 2024, the MIVD placed 5397 taps. This concerns the actual use of all forms of taps. Examples include a telephone tap, IP tap or placing a microphone. One target (person or organisation) can be listened to in different ways and on multiple devices. These are counted separately in the statistics.

Validation research

In 2024, the MIVD initiated 70 interpretation studies based on validation of reports and signals. The number of studies is therefore apparently lower than the number of validation studies (115) in 2023. A change in definition and working method[28] is the main reason for this lower number. The number of registered reports and signals increased by approximately half in 2024 compared to the previous year.[29] Some of the reports and signals received involved a possible threat to the safety or deployability of the armed forces, for which an investigation was initiated. The reports that the MIVD receives can come from both partners in the Netherlands and abroad. These can be mission areas and countries where the armed forces are exercising or represented. The reports and signals are diverse. These include concerns about individuals in relation to various forms of extremism, striking interest in equipment, complexes, industry and/or unwanted interference by state actors among Defence personnel.

[27] *See also letter from CTIVD (reference 2024/088); the MIVD has met the expectations of the CTIVD, which has resulted in the backlog being completely eliminated.*

[28] *From 2024 onwards, a validation phase will take place before an interpretation study is started. Previously, the validation phase was more quickly called a validation study.*

[29] *In 2023, this consisted of 327 reports resulting in 115 investigations. In 2024, there were 596 reports resulting in 70 investigations.*

Access requests 2024	Number	*	**	Refused	Still	Objection		Higher
Personal data	21 34 10 24 7					7 submitted 6 completed	0 submitted 1 completed*	0 submitted 0 done
To deceased family	5	9	2	7	1	4 submitted 4 completed	0 submitted 0 submitted	0 submitted 0 submitted
Administrative Affairs - 1 present		4	1	3	1 (3*)	0 submitted 3 completed*	0 submitted 1 submitted*	1 submitted 1 submitted*
Total	27 47 13 34 9 (12*)					11 submitted 13 completed*	0 submitted 2 submitted*	1 submitted 1 submitted*

* Partly requests from years before 2024.

** Honored means that the applicant has been provided with one or more documents.