Threat Assessment of State Actors 2025

Ongoing threats at a time of growing uncertainty

Cover photo: *Over two months prior to the start of the NATO Summit, the street where the event would be held in late June was closed off to traffic.*

Ongoing threats at a time of growing uncertainty

The 2025 Threat Assessment on State Actors (DBSA) is being published at a turbulent time, in which international relations are becoming more unpredictable. Over the past two years, the threat to the Netherlands and our interests posed by state actors has in many respects remained as serious as ever, and the threat of sabotage has increased. Not one of the threats described in the DBSA has decreased. However, our resilience in the face of state threats is increasingly accompanied by uncertainty about the immediate future.

Changes in global relations

The power balance in the world is shifting, and it is uncertain what the world order will ultimately look like. The era in which liberal, Western values held sway appears to be over. The countries of the 'Global South' are showing less interest in the West, and they are setting up new institutions and partnerships to serve as a counterweight to existing political spheres of influence. Changes in the world order appear to be having an ever greater impact, for example because countries are increasingly prepared to actively use their power to defend their interests within international institutions and partnerships. These changes could have major consequences for the Netherlands and our national security; the openness of our society, democracy and economy make our country vulnerable.

Threat posed by state actors is undiminished

Amid these changes in global relations, state actors pose a threat to the Netherlands' national security in various ways.[i] A direct military attack by Russia on NATO territory is unlikely, but as the rift between Russia and the West widens, there is a growing risk of further escalation (intentional or otherwise). Russia is carrying out more and more acts of sabotage to sow fear and turmoil in Europe, in the expectation that this will reduce the political and societal will to engage in conflict with it. These operations are expected to continue, as sabotage falls below the threshold of a military conflict and thus does not constitute 'an armed attack' within the meaning of Article 5 of the NATO treaty. Russia can use sabotage to continue pursuing its objectives without sparking a full-scale war with NATO. Physical and digital sabotage could lead to social upheaval, the breakdown of critical infrastructure, disruption to military operations (or operational preparations) and economic damage. Of all cyber threats, digital sabotage potentially would have the greatest impact on Dutch society.

i The six national security interests are territorial, physical, economic and ecological security; social and political stability; and the international legal order and stability.

Many other threats remain undiminished as well. The threat of espionage posed by countries such as China, Russia and Iran is as great as ever. In addition, a growing number of countries seem to be seeking to influence Dutch society and political decision-making by relatively simple means, such as digital espionage, intimidation or the dissemination of disinformation. It is possible that more countries are now employing these techniques as a result of the changing world order. Another possibility is that the Netherlands' enhanced focus on recognising state threats has made such threats easier to identify. Espionage, easy-to-mount disruption attacks, transnational repression and subversive influencing operations can stoke feelings of unease and insecurity within diaspora communities or in society more broadly. Such actions undermine social and political stability.

The economy is closely bound up with geopolitics. Strategic dependencies are used as a form of political or economic pressure. An increasing number of countries are pursuing protectionist economic policy, erecting trade barriers and imposing restrictions on the trade in technological knowledge and goods. The use of economic instruments by state actors can have major repercussions for the Netherlands. In the short term, life can become more expensive due to trade conflicts, export restrictions or higher energy prices.

Moreover, the threat of the undesirable transfer of knowledge and technology remains as high as ever. When facing sanctions, state actors seek alternative ways of obtaining technological knowledge, which makes them more likely to engage in covert forms of acquisition. If other countries acquire the same technological knowledge as the Netherlands (possibly by covert means), this could undermine our leading position in certain technological domains over the long run or structurally reduce the competitiveness of Dutch companies. What is more, it could boost other countries' military strength, thereby reducing the effectiveness of our armed forces.

Growing uncertainty about resilience

The threat posed by state actors is as great as ever, but our resilience to it has become more uncertain. The Netherlands and other European countries still heavily depend on the US for security, defence, the economy, raw materials and technology. Security-related dependencies have become more vulnerable due to the fact that European countries' threat perception and assessment of the current international legal order are increasingly diverging from those of non-European countries. Choices made by state actors have an impact on the Netherlands, even when they do not relate to the Netherlands directly. This creates major uncertainties and entails risks to our national security. Owing to the changes to the world order and our resilience, state actors may encounter less resistance and start acting more brazenly. Europe now needs to become more self-reliant and take up its responsibility for security in its own part of the world.

Contents

A Finnish pilot in an F-18. Leeuwarden Air Base hosted the international exercise Ramstein Flag. This year this NATO exercise replaced the annual exercise of the Royal Netherlands Air and Space Force, which is normally known as 'Frisian Flag'.

Introduction

The 2025 edition of the Threat Assessment on State Actors (DBSA) was drawn up by the General Intelligence and Security Service (AIVD), the Defence Intelligence and Security Service (MIVD) and the National Coordinator for Counterterrorism and Security (NCTV). DBSA 2025 reports on the main developments with regard to state threats to national security since the appearance of the previous assessment, in November 2022. The aim is to raise awareness about the nature and severity of these threats. In this way the threat assessment lays an analytical foundation for the policy response.

State actors seek to defend their interests as effectively as possible. In doing so, some unintentionally or unwittingly inflict harm on others, while others do so deliberately. Whether consciously or not, whether deliberately or not, in all cases our national interests can be harmed. The DBSA focuses specifically on this threat posed by state actors. It defines 'state threats' as follows:

> *Coercive, subversive, misleading or covert activities carried out by or on behalf of state actors which fall below the threshold of an armed conflict but which can harm the Netherlands' national security interests through a combination of the aims pursued, the means used and the associated effects.*[1]

The present DBSA comes at a turbulent time in which international relations have become more unpredictable. The most notable developments are the wars in Ukraine and Gaza, tensions around Taiwan and the Red Sea, and the strained transatlantic relationship.[2] All these circumstances affect the Netherlands and our national security interests. In some cases they affect the Netherlands directly, while in others there is an indirect or latent threat against which our country must be vigilant.

In comparison to the previous DBSA from 2022 the threat is undiminished in many areas, and the threat of sabotage has grown. Not one threat has decreased. Moreover, our resilience to state threats is increasingly accompanied by uncertainty about the immediate future, partly on account of geopolitical developments. It is therefore vital to recognise state threats in order to take the most appropriate measures in response.

Methods and targets of state actors

Our national security is under threat from state actors in various ways, as noted in the previous DBSAs from 2021 and 2022. Actors threaten national security using various methods which are not always clearly distinct from one another and indeed may be interconnected. Those methods are as follows:

- Military: this includes the development and conspicuous manifestation of both conventional and nuclear arms, and the deployment of military units or operations – possibly by proxies.[ii]
- Espionage: the gathering of intelligence, by either physical or digital means, in order to further economic, political/governmental or military objectives, or to monitor the diaspora and dissidents.
- Sabotage: deliberately damaging military and civilian targets in order to delay the delivery of war supplies, sow fear and division, or test when opponents will react.
- State-sponsored interference: this refers not only to forms of espionage but also to threats of violence or attempts to influence the diaspora and engage in subversive influencing, for example by disseminating disinformation or conducting hack-and-leak operations.[iii]
- Economic: economic instruments, such as corporate takeovers and investments, can be used legitimately or covertly, to achieve geopolitical or military goals by way of civilian companies. This category also includes the undesirable transfer (acquisition) of knowledge and technology.
- Diplomatic and political: this involves influencing or obstructing existing institutions, establishing parallel institutions and forming alliances in order to amplify one's own influence.

These methods can be used against targets in every domain of Dutch society, e.g. against democratic processes, policymakers, people or organisations involved in political decision-making and national and international bodies such as NATO, along with educational and knowledge institutions or international bodies on Dutch soil. Businesses and the Netherlands' 'top sectors' can fall victim to espionage for example, and specific diaspora and faith communities can be used by state actors to sow division. In short, the methods used by state actors and their objectives are highly varied.

ii Proxies are third parties, such as companies, hackers' collectives or local criminal groups that are being used by foreign governments because of their capabilities and because they enable the government in question to conceal its own involvement.

iii Hack-and-leak operations involve obtaining access to sensitive personal or organisational information by means of a hack, and then sharing this information, possibly in manipulated form, on social media or with certain individuals or institutions.

National security interests

If state actors threaten one or more national security interests to such an extent that there is the possibility of social disruption, national security is at risk. Threats to national security are always undesirable, regardless of their impact. Protecting national security means ensuring that individuals, organisations and communities can function without interruption. DBSA 2025 describes the main geopolitical developments, state threats against the Netherlands and the impact of these developments and threats on our national security. This impact is examined in the context of the six national security interests.[3]

These are:

- Territorial security (including digital security);
- Physical security;
- Economic security;
- Ecological security;
- Social and political stability; and
- International legal order and stability.

Structure

This DBSA begins with a background chapter on the changing world order, which deals specifically with shifts in the geopolitical balance of power and the rise of new theatres of operations. This is followed by six chapters, each devoted to one of the methods used by state actors: military, espionage, sabotage, state-sponsored interference, economic measures, and diplomatic and political measures.

The Hera space probe in a 'cleanroom' of the European Space Research and Technology Centre (ESTEC). This ESA space vehicle will conduct research on the deflection of asteroids as part of a larger planetary defence mission dubbed 'Hera'.

The Netherlands in a changing world order

The time in which liberal Western values held sway, often driven by American dominance, appears to be over. The power balance in the world is shifting, and it is uncertain what the world order will ultimately look like. What is clear is that these changes will have major consequences for the Netherlands and our national security. The openness of our society, democracy and economy make our country vulnerable. The security of the Netherlands is thus closely bound up with that of the rest of the world.

Shifts in the balance of power

The changing world order is characterised by fragmentation; this is a common thread running through DBSA 2025. 'The Netherlands in a Fragmenting World Order', a report by the Scientific Council for Government Policy (WRR), describes three axes of fragmentation: power centres, arenas where power is exercised and world views.[4]

Firstly, the unipolar world order is evolving into a multipolar world order. In such an altered world order, the dominance of the US and the West as a whole will decline in favour of countries like China, Russia, India, Iran, Saudi Arabia, Turkey and Indonesia. The world's centre of gravity – in demographic, economic and other terms – is shifting toward the East and South. Countries are showing less interest in the West, and are setting up new institutions and partnerships to serve as a counterweight to existing political spheres of influence. Every power defends its own interests, which are often at odds with the interests of others. For example, China and Russia have further deepened their partnership, even though they do not have the same goals. For now, it seems that the emergence of such a multipolar world order is inevitable.

Secondly, countries are active in more arenas, and they view these arenas from a security perspective. For example, economic activities are not undertaken for purely economic reasons; they are also seen as necessary for the country's own security. Consider the global market for computer chips, in which countries take measures to prevent the most advanced equipment from falling into the hands of systemic rivals. This is also true for the social and digital arenas, where state actors exert influence over diaspora communities in order to promote their own security interests. These arenas are not new of course, but they have acquired more importance in recent years.

Thirdly, we are witnessing a fragmentation of world views. Countries like Russia and Iran can be seen as systemic rivals of the West. Though a major trading partner with which the Netherlands shares key economic interests, China must also be considered a systemic rival at times. China believes that a change in the international legal order is necessary in order to boost its influence on the world stage and maintain its political power on the domestic front. In addition, countries are seeking to influence existing institutions and partnerships to their advantage, and they are forming alliances of their own to further their interests. It is unlikely that the stance of these systemic rivals towards the Netherlands and our interests will change in the short term.

Changing US stance has implications for our national security
For a number of years now, the centre of gravity of US security policy has been shifting away from Europe and towards America's rivalry with China. This trend has accelerated since the inauguration of President Trump, who has also clearly indicated that more is expected of Europe when it comes to its own security. This evolving, more transactional stance adopted by the US gives rise to uncertainty with regard to the Netherlands' national security, not least in view of our major dependencies on the US, both in the realm of security and in other areas. The US is a key ally, but it is clear that Europe now needs to become more self-reliant and bear greater responsibility for security in its own part of the world.

From the Arctic region to space

Physical locations have always been significant focal points of conflict, and this has remained the case in recent years. For example, President Trump has explicitly expressed his wish to acquire Greenland and the Panama Canal, and various other countries have expressed increased interest in the Arctic region, and even outer space, in the past few years. Countries are interested in the Arctic because of the reserves of natural gas and metals in the region, and new opportunities for maritime navigation.[5] Russia, in collaboration with China, is building ports on its northern coast to control the shipping lanes that are opening up as a result of climate change. Russia is also enhancing its military installations in the region, and it is engaging in military cooperation with China to a limited but increasing degree around the Arctic region. The growing tensions around the Arctic region could lead to shifts in the balance of power there, and possibly to regional instability.

Space as a disputed domain

Space has also acquired greater strategic importance. The geopolitical conflicts being fought out on earth are now finding their way into space. The space race of over half a century ago is back with a vengeance, launching a wide range of innovations. The number of players in this domain is increasing swiftly, and the major space powers are boosting their capabilities and their military and other ambitions. Space is after all a realm of vital importance to defence, security, the economy, science, research and innovation: every day, people around the world use satellites and satellite services on a large scale, for communication, financial transactions, navigation, weather forecasting and the internet.[6]

At the same time, space is increasingly a disputed domain: a growing number of countries are developing capabilities to restrict or deny access to or the use of space resources by other parties, varying from disruption and degradation to the physical destruction of satellites.[7] In particular, the threat emanating from Russia and China's growing space capabilities poses increasing challenges when it comes to maintaining free access to or use of space. This may become problematic for the Netherlands, because both military and commercial satellites form a crucial part of terrestrial infrastructure. Key functions in our society depend on satellites. Whether accidental or intentional, the loss or interruption of satellite signals would immediately have a disruptive effect on society.[8] In addition, space is essential to defence operations: communication with deployed units, the use of satellite-guided precision weapons and intelligence analyses all depend on satellite images.

A patch bearing the logo of Bastion Lion, the biggest exercise conducted by the Royal Netherlands Army this year. During this exercise two Dutch combat battalions of 13 Light Brigade and one German battalion carried out a multi-day attack on a mock-up village in Germany. Approximately 4,000 soldiers, 1,800 vehicles and 200 drones took part in the exercise.

Military

For a number of years Russia has posed a threat to NATO countries, including the Netherlands. The military threat against NATO has remained more or less constant over the past two years. That said, the war in Ukraine has deepened the divisions between Russia and the West, thus increasing the risk of further escalation (intentional or otherwise).

This increased risk has implications for the Netherlands on account of Article 5 of the NATO Treaty,[iv] and because of the possibility of acts of sabotage being committed in the Netherlands (see chapter on sabotage). Moreover, our resilience in the face of a military threat has become more uncertain since the US has clearly indicated that it expects Europe to do more to protect its own security. Since Russia's invasion of Ukraine, Western support for the Ukrainians has become more and more extensive, but recently this support seems less certain. Europe now needs to become more self-reliant and bear responsibility for security in its own part of the world.

The changes to the world order may mean that state actors encounter less resistance and start acting more brazenly. For example, there have been various reports about Russia's use of chemical weapons in Ukraine, though this has not elicited any strong international condemnation. This could lower the threshold for using chemical weapons in other conflicts. Iran continues to develop ballistic missiles, using espionage to attempt to acquire knowledge and equipment in the Netherlands. Iran supplies these missiles not only to allies in the region, but also to Russia, for use in its war on Ukraine.

iv Article 5 of the NATO Treaty states that an attack on one member country will be considered an attack on all. This means that if one ally is attacked, the others will come to its aid.

Russia poses the biggest military threat

Relations between the West and Russia have reached an absolute nadir since the outbreak of the latter's large-scale invasion of Ukraine in February 2022. The risk of a military escalation between Russia and NATO, whether intentional or accidental, has grown. Russia is NATO's most significant military opponent and the most likely military threat to its territorial integrity. Although Europe is investing heavily in NATO's combat power, Russia has temporarily taken a military lead. Alarmingly, if the war in Ukraine were to end under the most favourable conditions for Russia, it would take only a year for the Russians to re-build their capabilities to the point that they could launch a limited military operation against NATO member states.

From Russia's perspective, Western and Russian security interests are in opposition and irreconcilable. Russia regards the confrontation between itself and the West as 'total' and existential in nature. In Russia's view, the war in Ukraine is therefore part of a broader conflict with the West. For this reason, it is difficult to imagine Russia's attitude toward Europe changing in the foreseeable future.

In the past few years Western support for Ukraine has become ever more far-reaching. This support is not only helping Ukraine to defend itself; it is also enabling the country to carry out attacks in Russia, subject to certain conditions. Continuation of this support is necessary for Ukraine to be able to defend itself against Russian military aggression. However, this support cannot necessarily be taken for granted.

Russia seeking to offset the effects of the war

In the meantime, for Russia too, the conflict has become a military and economic war of attrition. The Russian economy shows more and more signs of being a war economy, and although the economic impact of Western sanctions is substantial, Russia will not be compelled to stop the war any time soon on account of economic instability.[9] The country is trying to offset the effects of the war by forming new partnerships and looking for ways to circumvent international sanctions. Iran, North Korea and Belarus are supplying arms to Russia. Although China does not, in principle, supply Russian with arms or ammunition, Chinese companies do provide Russian companies with dual-use goods[v] and even attack drones, which can be deployed in the war in Ukraine. In the autumn of 2024 it came to light that North Korea was not only supplying arms; it was also deploying troops to fight against Ukraine. In exchange, Russia is supplying it with oil, thereby circumventing UN sanctions against North Korea. Finally, Western attempts to isolate Russia at global level have not resonated sufficiently with the rest of the world. Thus, Russia continues to trade with other parts of the world as it had before.

v A dual-use good is one where the final product has both civilian and military applications.

Systematic violation of the Chemical Weapons Convention

Shortly after Russia's invasion of Ukraine, reports started emerging that Russia had used tear gas in occupied Ukrainian territory. The use of chemical weapons, including tear gas, as part of a military campaign is strictly prohibited under the Chemical Weapons Convention, of which Russia is a signatory. Since February 2022 the Ukrainian Ministry of Defence has registered over 6,000 incidents in which Russia has used chemical weapons against the Ukrainian armed forces. An independent investigation by the Organisation for the Prohibition of Chemical Weapons (OPCW) confirmed that tear gas has been used.[10]

Since March 2024 there have been many media reports about the use of chloropicrin, a choking agent. For this reason the US and the UK imposed sanctions on Russia on 1 May and 8 October 2024, respectively. On 4 July 2025 the AIVD and MIVD, together with the German Foreign Intelligence Service (BND), also publicly confirmed that Russia was systematically using chemical weapons, including chloropicrin. This joint publication also contained a warning that Russia was seeking to step up its use of chemical weapons in Ukraine. The absence of a strong international response may lower the threshold for state actors to use chemical weapons, not only in Ukraine but in other conflict zones as well.

Nuclear rhetoric by Russia and Iran

In November 2024 Russia revised its nuclear doctrine, formally lowering the threshold for the use of nuclear weapons. This move should not be equated to an increased willingness to use nuclear weapons. It is possible that Russia took this step mainly for the deterrent effect it would have on the West.

Nuclear rhetoric is not limited to Russia. Before the Israeli and US attacks in June, it seemed that Iran would have enough highly enriched uranium for the production of several nuclear weapons in the very near future.[11] However, there were no indications that Iran was engaged in the other activities needed to develop a nuclear explosive. The growing unrest in the Middle East has prompted hardliners to call for a revision of a 2003 fatwa against nuclear weapons. Furthermore Iran has threatened to withdraw from the Non-Proliferation Treaty if sanctions suspended under the nuclear deal were to be reinstated.[12] In addition, the International Atomic Energy Agency has stated that Iran is not allowing the IAEA to verify that its nuclear programme is intended for purely civil applications.[13] These developments have increased concerns about Iran's nuclear programme.

Ongoing concerns about Iran's weapons programme

Iran continues to further develop ballistic missiles. International sanctions mean that Iran has limited access to Western knowledge and technology. For that reason it is seeking to acquire this knowledge and equipment though espionage in countries like the Netherlands, via covert recruiting networks, knowledge institutions, students and researchers, and by other means. Iran is also actively pursuing collaboration with Russia in order to acquire more technologically advanced military capabilities. Despite the sanctions Iran is making progress in developing ballistic missiles. For example, in 2024 it deployed self-produced ballistic missiles for the first time against Israel, as part of the direct escalation of the conflict between the two countries. The threat is not limited to Iran, however: that same year, Iranian allies like Lebanese Hezbollah and the Yemeni Houthis also used missiles developed by Iran. Iranian weapons can be used against Dutch military personnel in Iraq and are currently being used in the Red Sea, where the Dutch Navy was active in 2024. Iran has also supplied Russia with short-range ballistic missiles and attack drones for its war on Ukraine. In this way, Iran's ballistic missile programme directly affects the Netherlands' security interests in Europe.

Attacks by Iran-backed groups entail extra costs and risks to international shipping

The instability in the Middle East poses major risks to international shipping, especially around the Arabian Peninsula.[vi] *These waters are vital for the efficient transport of large quantities of goods worldwide. The Netherlands is heavily dependent on oil and gas which is transported from the Persian Gulf via the Strait of Hormuz. Every part of this sea passage is a potential bottleneck that could disrupt transportation along the entire route. The same goes for the Panama Canal, the Bosporus, and the straits of Gibraltar, Taiwan and Malacca. The more these Sea Lines of Communication (SLOC) become unusable, the greater the possible unforeseen effects.*

Since November 2023 Houthis have been carrying out attacks in the Red Sea on both civilian and military vessels and against Israel. Shortly after the outbreak of the war in Gaza, their focus was mainly on attacking ships linked to Israel, but other ships have also been the target of attacks. Since then, more and more shipping companies have avoided the southern part of the Red Sea. In 2014 the Houthis took control of Sana'a, the capital of Yemen, and they have since become the de facto authority in the north of Yemen. They maintain friendly relations with Iran, characterised by arms deliveries, financial flows and personnel support from the Iranian Revolutionary Guard. Analysts agree that while the Houthis do cooperate with Iran, they are not directly controlled by Iran.

The obstruction of local shipping traffic does not have a direct impact on the Netherlands. Long-distance shipping is another matter, however. Dutch-flagged vessels and vessels under another flag that deliver goods of economic importance to Europe are now often adjusting their route between Europe and Africa and Asia, so as to avoid the waters around the Arabian Peninsula as much as possible. This leads to longer voyage times and higher transport costs. So the Houthi attacks not only pose a physical threat but also have an economic impact, mainly on countries in the region.

vi This encompasses the whole area of the Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Gulf of Aden, Bab el-Mandeb and Red Sea.

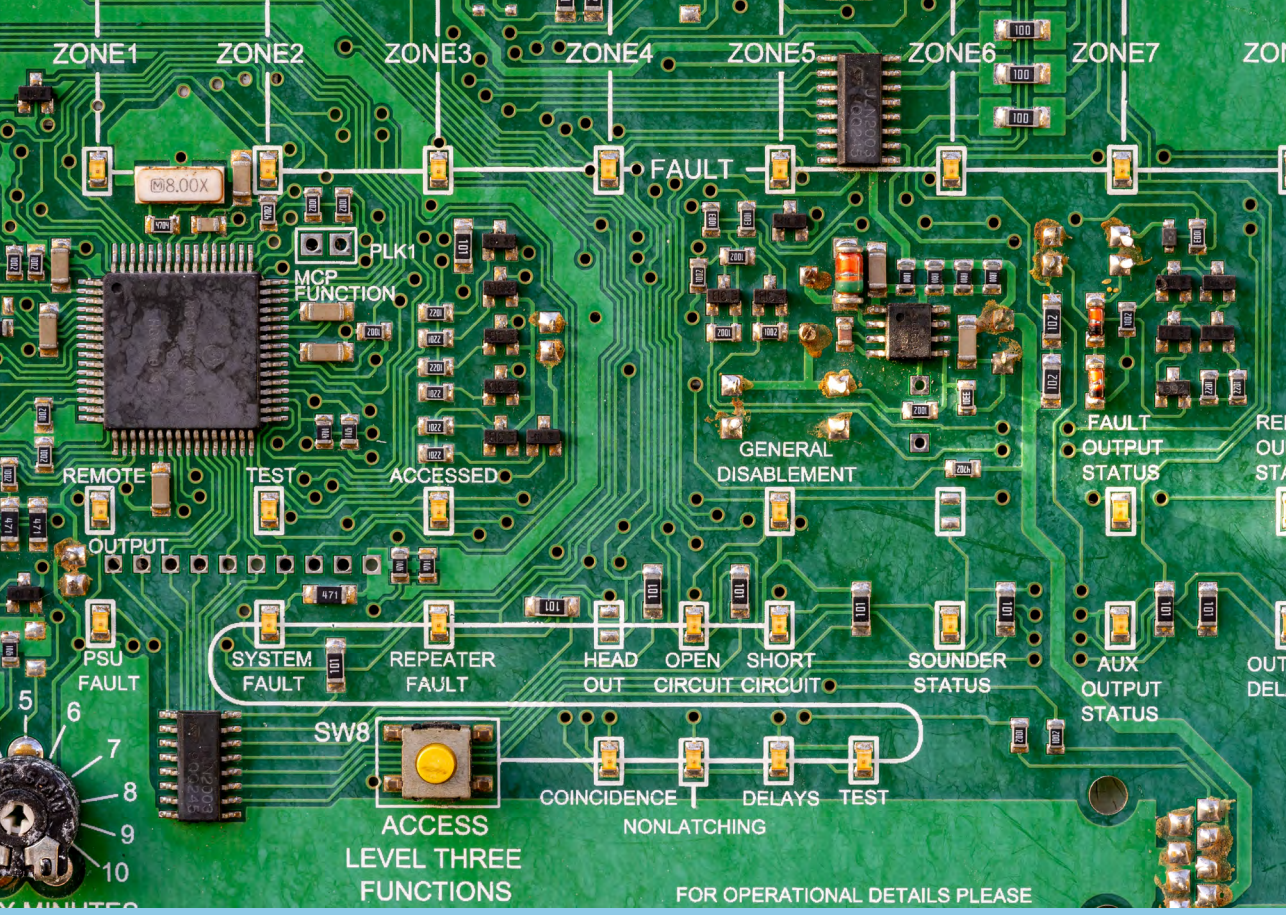
Threat to the Caribbean part of the Kingdom

The Caribbean part of the Kingdom of the Netherlands, specifically the ABC islands (Aruba, Bonaire and Curaçao), continue to feel the direct impact of the political, economic and humanitarian situation in Venezuela. The relationship between the Netherlands and Venezuela is tense, partly because the Netherlands does not recognise Maduro's claim that he won the presidential elections in 2024. It is unlikely that Venezuela has any intention of entering into a military conflict with the Netherlands, though there is a chance of inadvertent escalation, due to the relatively low level of military professionalism in Venezuela.

In addition, increasing instability within Venezuela could have repercussions for Aruba, Bonaire and Curaçao, for example in the form of migration from Venezuela to the islands, and cross-border crime. Current migration from Venezuela is already putting pressure on the islands, but a large-scale influx of migrants could potentially have a major impact on social stability and the economy. For example, the islands' medical facilities and legal system are small in scale and therefore vulnerable.

Significance to the Netherlands

- *If an attack were to occur on NATO territory, the Netherlands would be directly involved in the ensuing conflict on account of Article 5 of the NATO Treaty. The war in Ukraine has deepened the divisions between Russia and the West, thus increasing the risk of further escalation, whether intentional or accidental. That risk is determined in part by Russia's ongoing investment in its own military, the degree to which NATO is able to use its own military capabilities as an effective deterrent, the degree of Western cohesion and Russia's perception of it, and the way in which the build-up of NATO's military capabilities influences Russia's threat perception.*
- *Increasingly, Europe needs to fend for itself when it comes to providing for its own security. Any military escalation would place heavy demands on the Netherlands, not only its armed forces but on society as a whole. For example, the Netherlands is a transit country for NATO materiel, and it could be involved in the reception of war refugees and the injured.*
- *Unrest elsewhere in the world impacts the Netherlands, and it can have consequences for travel and international trade, and can also be a catalyst for threats to the Netherlands, for example in the form of terrorism or in the economic realm.*



Close-up of a green motherboard with chips and other components. Chips process data by following certain instructions such as computers, smartphones, tablets, and washing machines. They are used in various devices and appliances. All the connected components communicate via the motherboard.

Espionage

Espionage is a method of gathering information and knowledge for economic, political/governmental and military objectives, but it can also be used to monitor diaspora communities and dissidents. Espionage can be carried out both digitally and via human sources, for example through the diaspora, people in strategic positions, or intelligence officers at embassies.

The threat of espionage posed by countries such as China, Russia and Iran has remained at the same high level since 2022. Furthermore, it appears that more and more countries are seeking to spy on the Netherlands, especially by digital means, with the help of offensive cyber programmes. Such forms of espionage are easy to carry out, which makes them relatively common. The increase may be attributable to shifts in the established world order, but it may also be due to the fact that intelligence and security services now have a better grasp of state threats.

Traditional espionage via human sources remains a threat

Countries including China, Russia and Iran engage in espionage in the Netherlands. Foreign governments and intelligence services make use of networks of human sources, including members of diaspora communities. Here, too, in the Netherlands, various countries are attempting to recruit civilians and organisations for the purpose of intelligence gathering. This includes people who work in strategic positions or in critical sectors or who have access to relevant data (including personal data). Countries can also station intelligence officers at embassies.

Since Russia's invasion of Ukraine, a number of Western countries have expelled hundreds of Russian intelligence officers. This makes it more difficult for Russian intelligence and security services to recruit human sources in Western countries under diplomatic cover and to maintain contact with existing human sources. This issue can potentially be addressed in part by digital means. In addition, the Russian services have extensive opportunities to use forms of non-diplomatic cover to gather intelligence in the European Union, including the Netherlands. This could include deploying undercover operatives in the business world or academia.

Russia gathers not only political intelligence, on subjects like the European Union and foreign ministries, but also military intelligence, for example about NATO and defence ministries. When it comes to the Netherlands, Russia's focus is on the many international organisations headquartered here (see the chapter 'Diplomatic and political measures').

Man arrested on suspicion of violating state secrets
In October 2023 a man was arrested on suspicion of possessing and revealing state-secret information. The court has not yet given judgment in this case. According to the Public Prosecution Service, the man, a Dutch national of Moroccan origin, was on his way to Morocco, and at the time of his arrest he was in possession of a large number of digital documents (including state secrets). One of these was an AIVD analysis of Moroccan intelligence activities in the Netherlands. The man, who worked at the NCTV and consequently had access to this kind of information, is suspected of violating state secrets, either on his own initiative or at the behest of a foreign power.[14]

Digital espionage is becoming more extensive

More and more countries, including Russia, China, Iran and North Korea, have offensive cyber programmes that can be employed for espionage purposes.[15] In addition, the number of countries developing greater offensive capabilities in this area is on the rise. Such programmes, which are often part of large-scale international campaigns, can also be deployed against the Netherlands and our interests.

Every country has its own reasons for spying. For example, Russian cyber activities targeting Europe are focused on political espionage, covert influencing activities and digital sabotage (see following chapter). Since the Russian invasion of Ukraine in 2022, the AIVD and MIVD have noted an increase in the number of actors within the Russian government and of parties supported or directed by the Russian government that are involved in digital espionage. Their operations affect the Netherlands directly or indirectly, for example by compromising systems belonging to our allies.

For a long time China concentrated on economic espionage, but it has since broadened its focus and set up a large, advanced and professional digital espionage programme. Chinese attack groups are active around the world, targeting companies, governments and organisations. China's need for information is unprecedented, embracing almost every subject that could be relevant to the country: the diplomatic sphere, parliamentary affairs, military matters, the economy, technology, science, the armed forces, geography, finance, dissidents, health, sport, personal data, travel information, bulk data and telecommunications. Given this great and wide-ranging need for information, any country in the world could potentially be hit by a Chinese cyberattack, and Chinese state actors are also focusing systematically on countries in Europe, including the Netherlands. In addition, virtually all Chinese state cyber actors can opportunistically target Dutch interests if they happen to encounter vulnerabilities there. These digital activities are now so advanced and extensive that it is likely that only a fraction of Chinese cyber operations against Dutch interests could be detected in time and then mitigated. This too presents a major challenge to the Netherlands' resilience.

Iran mainly uses its digital espionage programme in the Middle East and against the United States. Specifically, the country engages in political espionage in the region, targeting its main opponents. In addition Iran gathers information about Iranian dissidents, organisations or opponents of the regime regardless of where they live, including those based in the Netherlands, and it collects bulk personal data in the aviation sector.[16] These sorts of espionage activities can engender a sense of insecurity or anxiety, both in diaspora communities and in society more broadly.

North Korea mainly uses digital attacks for financial gain. North Korean actors also seek to steal cryptocurrency in the Netherlands, using such attacks and stolen funds as a way of circumventing the sanctions imposed on North Korea. The country uses freelance North Korean IT specialists for this purpose. With the help of false identities, they manage to get hired by companies abroad in order to earn money for the regime, for example by stealing data or cryptocurrency. It is conceivable that the proceeds of these activities are being used to finance weapons programmes. For all these reasons, the European Union has imposed sanctions on the head of the RGB, the North Korean intelligence service.[17] The country also uses espionage, for example in the form of information theft from educational and research institutions. There are currently no indications that other countries are helping North Korea with its cyberattacks, or that it is purchasing advanced commercial spyware.

Significance to the Netherlands

- *Traditional espionage using human sources generally targets specific individuals, organisations or institutions. This can stir up feelings of insecurity and fear within diaspora communities and in society more broadly. This threat has remained unchanged in recent years.*
- *In addition, more countries are now engaging in digital espionage, with the help of offensive cyber programmes. Such forms of espionage are easy to carry out and do not necessarily have a specific target. State actors gather bulk data relating to people living in the Netherlands, which they can later use to further their own interests. It is possible that more digital espionage is now being observed because intelligence and security services have a better grasp of state threats.*
- *Countries like Russia and China have large-scale espionage programmes, which enable them to gather information, including in the Netherlands, that can be used at a later time. Such information can be used, for example, to carry out simple acts of digital sabotage and disruption attacks (see following chapter).*

The Coastguard monitors and enforces security in the North Sea.

Sabotage

In the grey zone between war and peace, acts of sabotage (or attempted sabotage) are taking place throughout Europe. Russia and pro-Russian or Russia-allied individuals are carrying out more acts of sabotage than before, and taking greater risks in the process.

Russia has the unwavering aim of fomenting unrest in Europe, regardless of the course of the war in Ukraine. Because acts of sabotage fall below the threshold of Article 5 of the NATO Treaty, it is expected that the number of operations will continue to increase. With these acts of sabotage, Russia is seeking to further its objectives without sparking a full-scale war with NATO.

While there are no known examples of physical acts of sabotage by state actors, the AIVD and MIVD have uncovered preparatory activities on the part of Russia. Moreover, events elsewhere in Europe can have an influence on the Netherlands. The Netherlands is an attractive target, due in part to its critical maritime infrastructure in the North Sea and its role as a transit country. In contrast to physical sabotage, small-scale acts of digital sabotage and disruption have been observed in the Netherlands, as well as preparatory activities to that end. Of all cyber threats, digital sabotage could potentially have the greatest impact on Dutch society. It can lead to social upheaval, the failure of critical infrastructure, disruption to military operations (or preparations) and economic damage.[18]

Physical sabotage in the Netherlands conceivable

The intensity of acts of physical sabotage by Russia in the European Union has increased since Russia's invasion of Ukraine, especially in countries that border on Russia. Russia and pro-Russian or Russia-allied individuals are exhibiting a greater appetite for risk than a few years ago, and they are carrying out aggressive, provocative or even violent acts. Russia is also recruiting civilians, including criminals, for these activities, and these individuals may not be aware of the true nature of the jobs they are being asked to do. The targets of acts of sabotage include organisations that are involved in some way in the war in Ukraine or in supporting Ukraine, as well as, increasingly, military and logistical locations in Europe.

These acts have various aims. On the one hand they seek to delay the delivery of Western supplies to Ukraine. On the other hand, they are a way of sowing division within the West and of undermining Ukraine by means of intimidation. In addition, Russia can use sabotage operations as a way of testing where the West's red lines are when it comes to Russian aggression on their territory. In this regard Russia seems to be in search of a model whereby it can disrupt Western support for Ukraine to the greatest possible extent without provoking the West into a military escalation.

The Netherlands as a possible target

The Netherlands is an attractive target for state actors because of its position as a transit country in the event of a large-scale military conflict, and the presence of critical maritime infrastructure in the North Sea. The North Sea contains key internet cables, gas pipelines and wind farms that are crucial for the functioning of the Netherlands and neighbouring countries. The task of protecting and monitoring this vast and freely accessible territory poses a challenge to the Netherlands. The sabotage of critical processes, whether physical or digital in nature, can threaten our national security. It is conceivable that Russia is capable of carrying out physical acts of sabotage in the Netherlands, although no such operation is known to have occurred as yet. In all likelihood Russia is mapping out critical infrastructure and engaging in activities that suggest espionage and preparatory acts for physical disruption and sabotage.[19]

The likely purpose of these sabotage activities is to enhance Russia's options for action, especially prior to a conflict situation. It is consistent with Russia's strategic military thinking that, at the outset of a conflict, efforts should be made as soon as possible to disrupt or destroy the opponent's critical processes, such as communications, the power supply and logistical capacity.

If the Netherlands' critical infrastructure is sabotaged on a large scale, the consequence could be societal disruption. The Netherlands could also experience the effects of sabotage on critical infrastructure elsewhere in Europe.[20] Given the interconnectedness of the European electricity grid, a disruption in Germany could lead to a power cut in the Netherlands, for example. The failure of critical infrastructure is a possibility that has already become reality on a number of occasions in the European Union.

Simple digital sabotage and disruption attacks in the Netherlands

Attempts at – and preparations for – digital sabotage have been observed in the Netherlands. Countries such as Russia, Iran and China use offensive cyber programmes to disrupt or sabotage critical physical and digital infrastructure, either now or in the future. Sabotage attempts and preparations by various parties, including Russia, have been observed in the Netherlands.

The Netherlands has been the target of simple digital disruption attacks, such as DDoS (distributed denial of service) attacks. Besides being easy to carry out, such attacks often have only a limited impact. A digital sabotage attack can, however, have a lasting impact on the availability of digital services, processes or systems. Some digital disruption attacks have been linked to Russia.[21] For example, various political parties reported that in June 2024, on the day of the European elections in the Netherlands, their websites were not fully accessible due to DDoS attacks. Responsibility for these DDoS attacks was claimed by pro-Russian hacktivists. Previously, in June and August 2023, access to the websites of Dutch seaports and airports was

disrupted, and in some cases completely cut off, on account of DDoS attacks. Responsibility for these attacks was also claimed by pro-Russian hacktivist groups with suspected ties to the Russian government. The AIVD and MIVD determined that in 2024 a state-backed hackers' group was responsible for a cyber sabotage attack on the operating system of a public facility in the Netherlands.

Other European countries that openly support Ukraine were subjected to attacks in 2024 by Russian advanced persistent threats.[vii] This happened, for example, to political parties in Germany and government institutions in Poland and the Czech Republic. Previously, there were similar attacks in Lithuania, Slovakia, Sweden and elsewhere.[22] In September 2024 the MIVD warned about the possibility of cyber operations by Unit 29155 of the Russian military secret service. These hackers' focus is on identifying and disrupting Western assistance to Ukraine. Their operations mainly target Western governments and critical infrastructure.

The Netherlands is not the primary target of Iranian digital sabotage. However, recent Iranian sabotage activities against Western allies are a cause for concern. In 2023 the systems of various US drinking water and water purification plants were compromised by state-backed Iranian hackers operating under the collective name of CyberAv3ngers. According to the US, this group is affiliated with the Iranian Revolutionary Guard, Iran's elite military corps. Access to drinking water is an aspect of critical infrastructure; misuse of the associated systems can have a major impact on the health of the local population.[23]

vii This term refers to the actor's use of advanced means to operate unobserved for a longer period of time.

Significance to the Netherlands

- *Physical and digital sabotage in the Netherlands can lead to societal disruption. An act of sabotage targeting a critical sector could result in the temporary unavailability of electricity, the internet, payment systems or clean drinking water. This could have far-reaching consequences. For example, a power cut can affect telecom systems, the internet, rail traffic or hospitals.*
- *Russia uses sabotage to sow fear and unrest in Europe, in the expectation that this will reduce the political and societal will to engage in conflict with that country. The number of sabotage operations is expected to increase further.*

In Haarlem, in June 2024, an attempted assassination was made on an Iranian national residing in the Netherlands. The police arrested two suspects. One of them is also suspected of the failed assassination of a Spanish politician and critic of Iran.

State-sponsored interference

State actors are seeking to influence Dutch society and political decision-making. In addition to the aforementioned espionage objectives, they also try to intimidate members of the diaspora or engage in subversive influencing via disinformation or hack-and-leak operations.

For example, countries such as Iran, Pakistan, Morocco and Türkiye collect intelligence about – or from – their diaspora communities in the Netherlands. Other countries, such as China, Eritrea and Syria, are also presumed to be doing so, because they are known to gather intelligence in other European countries about or with the help of their own diasporas.[24] These countries continue to see Dutch nationals as their own citizens because they or their parents or grandparents were born there. In October 2024 the AIVD and NCTV published 'Crossing Borders', an analysis of such state-sponsored interference in diaspora communities. 'Subversive influencing' refers to efforts by state actors to improve their reputation, enlarge their influence abroad and bend public opinion and political decision-making to their will.

State-sponsored interference by known countries has been as prevalent as ever since 2022, and the number of countries using such methods seems to be on the rise. As with espionage, this increase in state-sponsored interference could be the result of a changing world order, in which more countries stand to benefit from such forms of interference. At the same time, it is also possible that the Netherlands' enhanced efforts to recognise state threats have made it easier to identify them.

Transnational repression of diasporas

State-sponsored interference can entail deep infiltration of diaspora communities. Foreign governments have various reasons for such interference, such as protecting internal stability, expanding their influence or countering criticism and threats. They can silence political opponents, for example by threatening their families,[25] and persuade (or coerce) members of the diaspora to gather intelligence.[26] In exceptional cases people run the risk of falling victim to physical violence, abduction or even murder. Such threats of violence by foreign governments are referred to as 'transnational repression'.

Transnational repression is generally carried out by, or at the behest of, foreign intelligence services. To this end countries also use bodies and individuals with which they do not have a direct relationship. These proxies can be organisations or companies, nationalist individuals or groups, hackers' collectives or local criminal groups. They have relevant capabilities that governments can use for their own goals, plus the advantage of plausible deniability.

Iran linked to assassinations

Iran in particular has a long tradition of carrying out attacks on dissidents abroad.[27] In Haarlem, in June 2024, an attempted assassination was carried out on an Iranian national residing in the Netherlands. The police arrested two suspects. One of them is also suspected of the failed assassination of a Spanish politician and critic of Iran. Intelligence suggests that it is likely that Iran is responsible for the two attempted assassinations. Previously, criminals from Amsterdam murdered a Dutch person of Iranian origin in Almere in 2015, and in 2017 criminals may have been involved in the assassination of another Iranian Dutch person, from The Hague.[28] The AIVD has strong indications that Iran was involved in both killings. Similar incidents are thought to have occurred in Belgium, France, Germany, Sweden and the UK.[29] Iran also sometimes uses extremist individuals or groups (like Hezbollah) to carry out attacks. These are typically Shi'ites who are nationals of a country other than Iran or Lebanon.[30]

Iran focuses on Jewish and Israeli targets in Europe with the help of criminals

In addition to targeting diaspora communities, Iran focuses on Jewish and Israeli individuals, companies, organisations and diplomatic representations.[31] Since the outbreak of the war in Gaza on 7 October 2023 this threat has increased. Since early 2024 various attacks have been carried out on Israeli targets in Sweden and Denmark.[32] In Sweden the perpetrators are thought to be criminal youths, whose gang leaders are believed to have been recruited by Iran.[33] Iran has also allegedly sent two undercover agents to Sweden to murder Jews.[34] It is believed to be engaged in similar activities in Germany and France.[35]

It is probable that Iran is seeking to hit Israeli or Jewish targets in response to the war in Gaza and Israeli attacks on Lebanon, Syria and Iran. The choice of Scandinavia may be related to the Quran-burning protests in Sweden and Denmark. According to the Swedish security service (Säpo), the Iranian Revolutionary Guard hacked a text messaging service and disseminated inflammatory messages.[36] This is not the first time Iranian digital actors have taken action in response to certain events, such as the Quran burnings. It is therefore conceivable that developments that are politically sensitive in Iran could be disrupted or influenced by Iranian cyber actors. Iran's activities in Scandinavia may possibly be determined by its existing ties to criminal gangs. The gang leaders are thought to be in Iran, and they are used by the regime to transmit orders to young gang members in Scandinavia. In exchange for financial gain, possibly combined with criminal pressure or coercion, criminal youths are believed to be induced to carry out attacks.[37]

In the Netherlands, it does not appear that criminal youths are being controlled from Iran, though the country does have links with more experienced criminal networks that could engage in activities in the Netherlands. In theory, these networks could also be deployed against Israeli objects.

Subversive influencing aimed at changing public opinion

Subversive influencing' refers to efforts by state actors to improve their reputation, enlarge their influence abroad and bend public opinion and political decision-making to their will. This is happening at local and national level, and within the European Union. In Europe various incidents of covert political interference

(or suspected interference) have been exposed by the media. For example, in December 2024 an influential Chinese businessman was expelled from the UK on suspicion of engaging in espionage for China. It transpired that he had ties to the United Front Work Department (UFWD), a wing of the Chinese Communist Party involved with interference in other countries.[38] Earlier that year a Chinese-German staff member of an MEP for the Alternative für Deutschland (AfD) party was arrested on suspicion of leaking parliamentary documents from the European Parliament to China.[39] The bribery of MEPs by Qatar and Morocco in 2022 and the Russian influencing operation involving the Voice of Europe digital platform[viii] further underscore the fact that leading figures within the domestic and international political sphere are being used by state actors.[40]

Such examples of subversive influencing have received more publicity in recent years, but this has not led to a decrease in such actions. It is therefore expected that state actors are carrying out covert forms of interference in Europe. The Netherlands does not generally seem to be a primary target because foreign governments prefer to focus on countries with more international influence. Known attempts at covert influencing targeting the Netherlands and its actual effects have proved to be relatively minor. However, state actors are opportunistic: when opportunities present themselves within Dutch institutions, they will be seized upon.[41] Successful influencing operations could potentially have a significant impact on the way the Netherlands' democratic system functions. Countries also spread disinformation to foster fear and division and undermine democratic institutions. When such campaigns target other countries, the effect can also be felt in the Netherlands.

Disinformation is aimed at influencing the diaspora, Dutch society as a whole, and political decision-making. The party most responsible for spreading disinformation is Russia, though China too is increasingly active in this regard. In 2024, for example, a pro-Chinese online network belonging to a Chinese PR company was found to be spreading disinformation via fake news sites, including a number of Dutch sites. Mainstream news alternated with fake articles containing pro-Chinese narratives, conspiracy theories about the West and negative stories about critics of the Chinese regime. The websites gained virtually no traction.[42]

Russian attempts at subversive influencing

Russia's covert influencing campaigns mainly target countries it deems to be susceptible to such techniques, or countries in which it feels it has a certain strategic or historical interest. Russia is also capable of recognising opportunities and exploiting them in smaller states. By means of covert influencing operations, Russia aims to influence Western political decision-making regarding Russia to its own advantage, and to undermine general political and military support for Ukraine. At the same time, Russia is also seeking to undermine political and societal cohesion in the West and weaken its political opponents. Finally, Russia uses covert influencing techniques with respect to the West in order to promote its own internal stability.

Russia uses these techniques in both the physical and digital domains, so as to influence public debate and political and governmental decision-making processes. For example, since the start of the war in Ukraine,

viii Using the Voice of Europe digital portal, Russia conducted a systematic, international campaign involving the manipulation of the media and distortion of facts in order to destabilise Ukraine, the European Union and its members, and to win the support of European politicians.

Russia has secretly organised 'peace demonstrations' in the Netherlands, which served to give the Russian domestic audience the impression that Europe's support for Ukraine was on the wane. Russian disinformation (e.g. alternative explanations about the origins of the war in Ukraine) has resonated with anti-institutional and right-wing extremist movements in the Netherlands. Russia suggests that the war was provoked by Ukraine or that it was consequence of Western expansion, whereas in reality it is the result of Russia's illegal invasion of a sovereign country.

Russia digitally recruiting local residents in Germany to sow division

In 2024 Russia recruited a number of people online to carry out simple acts of sabotage with a political message. A total of 270 cars were stickered and had their exhaust pipes blocked with expanding foam. Initially, environmental activists were blamed, but an investigation by Der Spiegel revealed that the true perpetrators were three men, from Germany, Serbia and Bosnia and Herzegovina, who had been paid by the Russian secret service. The men had been sent instructions on the messaging app Viber on how to carry out the mission and plant 'evidence' pointing to environmentalists. According to the investigation by Der Spiegel, the primary aim was to turn people against the Green party (i.e. Bündnis 90/Die Grünen).[43] This is not the first time Russia has hired 'amateurs' in Europe to carry out these sorts of activities for relatively little financial compensation: last year, the Belgian state security service (the VSSE) reported seeing an increase in 'freelance agents' working for Russia.[44]
No activities involving such agents have yet been observed in the Netherlands, but given the incidents of this nature that have taken place in Belgium, Germany and other European countries, it is conceivable.

Turkish diaspora policy

According to research by the Clingendael Institute for International Relations, Türkiye is pursuing an ideologically driven diaspora policy, with mixed results.[45] In the Netherlands, Türkiye seeks to promote good citizenship, strengthen cultural and religious ties with the motherland and gain votes for the AKP, the biggest Turkish political party.[46] Much of this policy is lawful, and does not involve intimidation or monitoring of the diaspora. According to previous studies by the Clingendael Institute, a quarter of Dutch nationals of Turkish origin feel unsafe due to Turkish influence.[47] This sentiment is mainly found among non-voters and people who support opposition parties. Such feelings of insecurity can lead to self-censorship, thus limiting freedom of expression. By contrast, almost 50% of Dutch people of Turkish origin think that Turkish engagement has a positive effect on the community's safety.

Israeli attempt to influence Dutch politics and society

Israel is also seeking to influence political and public opinion in other countries, including the Netherlands. This is illustrated by the dissemination of a report by the Israeli Ministry for Diaspora Affairs and Combating Antisemitism, in response to the public disturbances surrounding the football match between Ajax and Maccabi Tel Aviv in November 2024. The report was not shared with the Dutch government through official channels; instead it was sent directly to specific politicians and journalists.[48] The Dutch Minister of Justice and Security and the Minister of Foreign Affairs described this decision as unusual and, given the possible negative consequences for people in the Netherlands, undesirable.[49] The individuals mentioned in the report could be subjected to intimidation or threats, or in the worst-case scenario, physical violence.[50]

Iran using cyber programme for subversive influencing

Iran has an offensive cyber programme for various ends, including subversive influencing. This programme is mainly used in the Middle East and against the United States, but the Netherlands has been a target as

well. Besides using the programme for political ends, Iran uses it for economic or financial reasons, albeit less frequently.[51] Iran employs this programme to gather knowledge about Iranian dissidents, organisations and opponents, engage in political espionage and collect bulk personal data from the aviation sector.[52] Online entities allied with Iran are also attempting to amplify certain messages or force changes to policy by means of hack-and-leak operations.

In a traditional hack-and-leak operation, a hack grants an entity access to sensitive data (whether personal or organisational in nature), which is then shared with the news media or on social media, or with certain individuals or institutions. Sensitive information is immediately published or, depending on the goal, first manipulated. In this way, intimidating cyber operations can be carried out by a state actor, a state-backed hackers' collective or by an independent group, such as a hacktivist group. Online entities allied to Iran have used these sorts of operations to influence public opinion about the war in Gaza. For example, Iran has attempted to cast Israel in a negative light while portraying its own actions positively. This is not the first time that Iran has made use of these online entities. During a large-scale cyber operation in Albania in 2022, it is highly probable that Iran used online entities to publish (allegedly) stolen data and to convey the message that the People's Mojahedin, an Iranian resistance movement, was no longer welcome in the country. The US Department of Justice has also accused three members of the Iranian Revolutionary Guard of interference, claiming that they carried out a hack-and-leak operation to steal documents belonging to a presidential candidate's campaign staff, which they intended to share with the media.[53]

In addition Iran is probably spreading disinformation to further its objectives. According to OpenAI, Iran has used fake news sites and artificial intelligence to generate content in order to spread disinformation.[54] During US elections in 2020, 2022 and 2024 Iran spread disinformation in order to influence the public debate.

Significance to the Netherlands

- *The impact of transnational repression aimed at a particular diaspora community or individual parties in the Netherlands is substantial. Some members of diaspora communities are afraid to speak out due to feelings of insecurity prompted by threats or even attacks. Transnational repression can also lead to tensions and feelings of insecurity among various groups in the Netherlands. The Netherlands attaches a great deal of importance to constitutional freedoms, including the freedom of expression. These sorts of actions have a negative effect on the constitutional freedoms of people living in this country, thus undermining societal and political stability.*
- *For most foreign governments the Netherlands is not an important target for subversive influencing, and our democratic institutions are sufficiently resilient that attempts at influencing are by no means always successful. However, state actors are opportunistic, and they will seize any chance to gain influence in Dutch society and political decision-making.*
- *The threat of state-sponsored interference on the part of known parties like Russia and Iran has remained more or less the same since 2022. The number of countries that use such methods seems to be on the rise, however. In addition to the changing world order, this could also be due to improved monitoring of state threats.*

The RWG container terminal at the Port of Rotterdam's Maasvlakte 2.

Economic measures

State actors employ both legitimate and covert economic instruments to achieve their geopolitical and other goals. While the primary goal is to promote the country's own economic position, instruments such as acquisitions and investments can also be used to achieve other strategic goals. In addition, the economy is also strongly connected to geopolitics. In this way strategic dependencies are used as a form of political or economic leverage. Moreover, an increasing number of countries are pursuing a protectionist economic policy, with trade barriers and restrictions on the trade in technological knowledge and goods. Many countries are using economic instruments, with China as the most notable example. Since President Trump took office for his second term, there has been an increased use of economic instruments by the United States.

The undesirable transfer or acquisition of knowledge and technology is another technique that can be used to further economic, as well as military, goals. This threat has long been high, but state actors facing sanctions are now seeking alternative ways of acquiring technological knowledge. Amid such sanctions, state actors are more likely to use covert means to acquire knowledge. Both economic instruments and technological knowledge are ways of expanding a country's political and military power.

Strategic dependencies being exploited as a form of leverage

Many countries are pursuing a strategically autonomous economy. Being dependent on a product or service from another country can entail major risks, especially if the dependencies are strategic in nature. This is the case when the product, service or technology is crucial for safeguarding public interests, such as the economy and society, or when the dependency poses a risk to the continuity of critical processes or affords third parties access to sensitive information. The risk of disruption to supplies depends on a variety of factors, including the level of market concentration and the scope for substitution, the nature of our relations with the country in question, and the degree of mutual dependence.[55]

Countries exploit these dependencies and use them as leverage. An example of this is Russia, which openly and covertly assesses how it can protect its interests in the changing energy market and delay the energy transition. In this way it seeks to continue exploiting countries' dependence on fossil energy for as long as possible. Shortly before and after the outbreak of the war in Ukraine, the supply of gas from Russia to EU member states was scaled back or halted entirely, in order to exert political, economic and social pressure. This had a financial impact on many Dutch people too, on account of higher energy bills and associated inflation. The EU has now largely phased out its energy dependence on Russia.

Western dependence on China

China is also developing its own industry and supply chains to reduce its dependence on global value chains. At the same time, other countries are becoming more dependent on China because increasingly it is setting technological standards, pricing competitors out of the market by scaling up production, and making large-scale investment in key technologies. This gives China economic advantages and boosts its ability to exert influence on other countries. When standards set by China lead to a 'lock-in effect', other countries have no choice but to elaborate on these standards, thereby reinforcing the state actor's dominant position. Lock-in effects could lead to high-risk strategic dependencies, for example if the Netherlands were to become dependent on Chinese technologies and suppliers for critical infrastructure, such as energy supplies, telecom networks, water supplies and transport infrastructure.

The West's dependence on China is particularly evident with respect to sustainability, such as green technology, and raw materials. The country has become an essential player in the worldwide energy transition, acquiring a dominant position in green technology supply chains. For example, the EU and the US are largely dependent, for the short and medium term, on Chinese solar panels, wind turbines and batteries, and the associated technologies and raw materials. In addition, China has a monopoly when it comes to mining and processing a large number of raw materials. This includes raw materials that play a major role in the digital and aerospace domains. China can use this dependence to exert pressure on other powers.

Trade conflicts forcing the Netherlands and the EU to act

More and more countries are pursuing a protectionist economic policy. They are doing so in various ways, including by supporting their own companies with financial advantages or by erecting trade barriers against foreign companies or governments. Trade in technological knowledge and goods is obstructed in order to protect the country's own security and economic and technological development (and thus its position of geopolitical power), to reduce that of another country, or to punish another country for certain activities. For example, the Netherlands has imposed export restrictions on the semiconductor industry on the grounds of national security. For its part, China has announced export restrictions of its own for certain raw materials on which the West depends for the production of semiconductors.

The United States is also deploying economic instruments. A trade conflict between the US and the EU has become more likely since President Trump took office. In addition, economic tensions between the US and China have increased further in recent months, due in part to the broad use of economic instruments such as import tariffs. Countries like the Netherlands risk being drawn into this conflict as well; the US will increasingly urge its partners to follow its lead, especially in the realm of technology. The Netherlands will continue to make its own national security decisions, in collaboration with its European partners. In both cases, trade conflicts illustrate the vulnerability of European supply chains: many European governments and companies are dependent on Chinese and US suppliers. This could put the EU in a difficult position if one of those countries wishes to disengage from the other and expects the Union to do the same. In addition, a trade conflict can be harnessed to exert diplomatic pressure, leading to trade disruptions, price increases and a loss of markets; this will have an impact on the Netherlands' competitiveness and business model and thus its prosperity.

Acquisition of technology is crucial to the power struggle

Technology and technological advances are central elements of the power struggle between state actors. Parties that control key technologies, such as biotechnology, quantum technology, artificial intelligence and semiconductor technology, can dictate the geopolitical agenda and create a strong foundation for their future earning model. Several countries, particularly the US and China, are therefore locked in a global 'tech race'. Countries looking to take the lead in the development of technologies are investing on a large scale. The Netherlands and the EU are falling behind in more and more technological areas, and this entails risks to our security and economy. It creates concentrations of economic power among countries that develop successful technologies, and this could harm the Netherlands' earning capacity. It also creates high-risk strategic dependencies. Knowledge and technology from the West can also be deployed for the development of weapon systems and espionage capabilities, or for surveillance equipment which can be used to suppress human rights.

When countries lack the knowledge and technology needed to achieve their geopolitical ambitions, they actively seek it out abroad. Various countries are attempting to acquire European and Dutch knowledge and technology, in both the academic and private sectors. This may occur openly, for example, in the form of corporate acquisitions, joint publications, talent recruitment, scholarships or grants, and international forums. It can also occur illegally, via espionage (including digital espionage), non-transparent investments that conceal state-sponsored interference, or the circumvention of export restrictions.

A well-known method used by state actors to acquire knowledge and technology is to enlist the help of insiders, people who are already working for a knowledge institution or company. The term 'insider threat' refers to the possibility that these individuals could leak knowledge or technology to state actors, either legally or illegally. For example, state actors could require students to return to their homeland after their studies, as a condition of a scholarship. This increases the chance that the knowledge they acquired in the Netherlands will be transferred to their government or to allied organisations. In some cases the knowledge or technology might be sensitive in nature, such as dual-use technology with both civil and military applications. Moreover, foreign intelligence officers in the Netherlands can also illegally assemble their own network of human sources to acquire knowledge and technology. Such a network could consist of both Dutch nationals and foreign nationals.[56]

The covert acquisition of our knowledge and technology threatens the knowledge security of Dutch educational and research institutions, companies' innovation and earning capacity, and the striking power of the armed forces. It can also make the Netherlands more dependent in strategic areas, such as critical infrastructure. Given the increased focus on knowledge and technology as geopolitical assets and the global tech race, this threat will persist in the years ahead and may even grow, as long as the Netherlands retains its leading position in certain technological domains. What is more, knowledge institutions may lose their leading strategic position in the medium term.

There are also concerns about the way in which state actors and state-allied companies collect personal data from individuals. This is done through apps (which are often free), products (often cheap) and services, or by simply buying the data. This personal data can be used for technological development, but it can also be exploited when state actors use it and related data on a large scale to conduct analyses of population groups.

China greatest threat to Dutch economic and knowledge security

For years, China has posed the greatest threat to Dutch companies and knowledge institutions in terms of economic security and knowledge security. Chinese president Xi Jinping firmly believes that knowledge and innovation serve China's national security. The Chinese government seeks to be one of the world's leading nations, and its economic and technological goals are closely bound up with its military and other security goals. For example, President Xi wants China to eventually be self-sufficient and technologically independent. The development of high-value technologies such as semiconductors, artificial intelligence and quantum technology is essential to this.

This means there is significant overlap between China's technological needs and fields in which Dutch knowledge institutions and companies conduct research. Individuals and institutions with ties to the Chinese military-industrial complex continue to approach Dutch knowledge institutions to collaborate on research into dual-use technologies, such as artificial intelligence. In practice, this remains a question of finding the right balance: the exchange of technological knowledge is important for economic and other reasons, but it also entails risks. The Chinese government continues to invest enormous amounts of money in talent recruitment programmes in order to bring people with high-value knowledge and know-how to China or to put that knowledge in service of Chinese interests in some other way.

Chinese researchers making overtures to Dutch knowledge institutions
Between 2012 and 2022 over 90 Chinese researchers (including members of the military) acquired knowledge at Dutch knowledge institutions. In 2021 a Chinese researcher received a doctorate from a Dutch university of technology, where he conducted research on hypersonic aircraft. This person studied in China at the Air Force Engineering University (AFEU), an educational institution that falls under the People's Liberation Army, offering courses in technological fields and air combat training. After obtaining his doctorate in the Netherlands, he was given a permanent contract at the AFEU. His research has both civil and military applications. This knowledge can be applied in research on aerospace engineering and on the development of hypersonic weapons.[57]

The Netherlands is the target of technology acquisition activities by Russia, Iran and North Korea

Russia, Iran and North Korea are also trying to acquire technological knowledge in the Netherlands in order to expand their power. Russia, for example, focuses on the development of military applications of various technologies, an ambition that has only grown as a result of the war in Ukraine. International sanctions impede access to sensitive technology and equipment. Russia is therefore seeking to acquire this technology by covert means, for example by using front companies to circumvent export restrictions. There have been recent cases in the Netherlands in which individuals and companies have evaded the sanctions regime against Russia and have supplied dual-use goods to Russian companies. This happens both directly and indirectly, via countries such as Armenia, Kazakhstan, Türkiye and Turkmenistan in order to circumvent sanctions.[58] These goods include computer components, drones and chips.

Russian engineer suspected of industrial espionage
Since 2024 there has been a case pending against a Russian engineer who is suspected of committing industrial espionage against ASML. Among other things, he is alleged to have stolen design manuals for microchips and then shared them via email, chat and online files. He also allegedly paid brief visits to Russia, where he may have handed over even more information in person. This transfer of information may have led to advances in Russia's chip technology.[59]

Iran, too, wishes to acquire knowledge and technology in the Netherlands and other Western countries, including via covert networks, knowledge institutions, students and researchers. This mainly concerns knowledge and technology for the development and maintenance of ballistic missiles. North Korea gathers information about scientific research and international political positions. Information relating to high-grade military and other technology has also been stolen from organisations, including ones in the Netherlands.

Tensions surrounding Taiwan could affect Dutch economy

On the other side of the world, there are mounting tensions over Taiwan. China still seeks to reunite Taiwan with the mainland, and to gain control over the vast majority of the South China Sea. Although China has not yet crossed the line of engaging in armed conflict with Taiwan, in recent years the number and scale of Chinese military and paramilitary exercises, patrols and reconnaissance missions has increased. A crisis in that part of the world would have a major, direct impact on the Netherlands. For the Netherlands as a trading nation and for the global economy in general, the maritime trade routes in the South China Sea and the Taiwan Strait are of vital importance. In addition, Taiwanese companies are essential to the production of semiconductors. This makes the island a critical link in the production chains for both civil and military electronics. The economic impact of a conflict is difficult to predict, but would very likely be significant.

Significance to the Netherlands

- *The use of economic instruments by state actors could have major consequences for the Netherlands. In the short term, life could become more expensive due to higher energy prices and trade conflicts. Trade barriers could also lead to a situation where Dutch companies are less productive and where there is a structural decline in their competitiveness. Trade conflicts and export restrictions on certain raw materials or products (including semi-finished products) could have negative effects on both the Dutch economy and our leading position in certain technical domains. This could make the Netherlands more dependent on other countries.*

- *The use of economic instruments by countries such as China remains a frequent and serious problem. The risk of trade conflicts has been on the rise since President Trump took office. The imposition of sanctions against the trade in technological knowledge and goods is one of the factors leading state actors to engage in covert acquisition activities. Because of its leading position in a number of sectors, the Netherlands will remain an attractive target for state actors.*

- *Technology is increasingly important in geopolitical power relations. This is leading to a global tech race in which countries around the world are investing heavily in key technologies. The Netherlands and the European Union are increasingly lagging behind when it comes to emerging technologies. This will result in strategic dependencies, which could undermine our security and prosperity.*

- *The use of economic instruments also impacts our effectiveness and the sustainment capability of our armed forces. The availability of crucial technologies from Taiwan could be threatened by, for example, emerging territorial and trade conflicts. Technological acquisition can also have far-reaching consequences. When other countries have access to the same technological knowledge, they can become stronger, and the effectiveness of our armed forces may decline.*

UN Headquarters in New York,
where the Security Council meets.

Diplomatic and political measures

Countries are increasingly willing to actively use their power to defend their interests within international institutions and partnerships. Although this is nothing new, the changes in the world order seem to be having an even greater effect. For example, countries are taking advantage of opportunities to gain power and pursue their interests more effectively. This could lead to a decline in the Netherlands' influence on the international stage.

State actors see international institutions and partnerships as a means of gaining influence, for example by undermining those bodies' effectiveness and credibility, or by altering prevailing frameworks and norms. Such forums can also be a target for state actors: this can undermine the continuity and independence of international judicial institutions and thus threaten the international legal order. Lastly, in order to boost their influence, non-Western countries are setting up alternative institutions or partnerships, over which the West has little or no influence.

Influencing existing institutions

Various countries are dissatisfied with the existing world order, which is based on Western rules, and wish to bring it more in line with their own interests. Thus, various state actors are striving to reduce or replace US hegemony and to replace the current model of the international legal order. The United States itself is also assuming a different position vis-à-vis the international legal order than in previous decades. For its part, the Netherlands, as a relatively small player with an open economy and limited military resources, actually benefits from an international order that functions on the basis of justice rather than power.

Countries are attempting to increase their clout by influencing existing institutions from the inside and the outside. For example, various states are using their veto in the UN Security Council to block resolutions that are line with UN objectives. In this way they are undermining the UN's effectiveness and credibility. In 2024, for example, Russia blocked oversight measures regarding international sanctions against North Korea. The supply of North Korean arms and troops to Russia for the war in Ukraine is a plausible explanation for the Russian veto.[60] Since the outbreak of the war in Gaza in 2023, the US has used its veto to block multiple resolutions in the Security Council about a ceasefire in Gaza. This is nothing new: the five permanent members of the Security Council regularly use their veto to serve their own geopolitical interests; three-quarters of all vetoes since 1989 have come from Russia and the US.[61]

One consequence of evolving power relations is that more countries are attempting to influence the frameworks and norms of international forums and institutions from the inside by taking up positions within these bodies. For example, China is seeking to secure the placement of Chinese nationals in key UN positions, starting at director level. In this way it hopes to better integrate Chinese interests and views into the UN, in order to adapt the international legal order to a model more favourable to China.

Institutions now a target for state actors

The function and role of international institutions and partnerships, and the national interests associated with them, can make them a target for state actors. The purpose may be to frustrate that role or to acquire valuable information. Examples of this include Russia's attempted hack of the OPCW in 2018 and the attempt by a Russian intelligence officer – foiled by the AIVD in 2022 – to obtain a position as an intern at the International Criminal Court.[62] Although the Netherlands was not the primary target of these operations, such activities by state actors do have an impact on democracy and the rule of law, of which these institutions are a part.

Known targets of state-sponsored interference include international institutions that are based in this country, such as the International Criminal Court and the International Court of Justice.[63] The US and Israel have publicly threatened the ICC, and the US has imposed sanctions on it.[64] This could undermine or even halt the work of the Court, in part because its access to financial services may be restricted or blocked entirely. At present, sanctions have been imposed only on the ICC prosecutor, because of the ICC arrest warrant against the Israeli prime minister and former minister of defence. The sanctions list could be expanded, however. Over time, the US sanctions could have far-reaching consequences for the functioning of the Court, and thus for the prosecution and trial of individuals suspected of international crimes, such as genocide, crimes against humanity or war crimes.[65] For a number of countries, the courts are also an attractive target for espionage and subversive influencing because their nationals might be tried there.

Such actions could undermine the continuity and independence of international judicial institutions, and they consequently pose a direct threat to the international legal order. In addition they have an impact on the Netherlands, due to our collaborative relationship with those institutions and because, as host country, we are responsible for the courts' security. When the Netherlands shares information with these institutions and it ends up in the hands of state actors, this also affects national security.

Parallel institutions serve as a counterweight

Existing international institutions and multilateral partnerships can also be influenced or undermined by the establishment of new and alternative institutions and partnerships. By setting up new partnerships in which the West has little to no influence, countries seek to expand their geopolitical influence. This way, they can also challenge existing political spheres of influence, such as the US or the EU, and thus restructure the world order, or at least make it more diverse. Through such actions China portrays itself as the leader of the 'Global South'. By playing a leading role in these institutions and launching global initiatives in areas like infrastructure, development and security, China has created a 'diplomatic order' that exists in parallel to Western consultative bodies like the G7. Every country has the right to initiate alternative partnerships and thereby broaden its influence, but over the long term this can erode or undermine existing international institutions through which the Netherlands pursues its own interests. This can reduce the Netherlands' international influence unless it is able to ensure its inclusion on certain fronts or in particular initiatives.

When it comes to the establishment of alternative partnerships, mid-sized states and emerging actors play a key role. These countries are aware of their increased strategic interest and are making use of the rivalry and conflict between the major powers.[66] This could be observed, for example, in 2023 when over 40 countries expressed an interest in joining BRICS, an economic partnership that seeks to serve as a counterweight to Western hegemony over the world economy. This alliance, which has since welcomed five new members, has only gained strategic importance in recent years. BRICS countries carry more and more economic weight; over 50% of the world's population lives in one of these countries. Moreover, some countries are increasingly bonding over anti-Western sentiment, despite their political, geographic or cultural differences. At the same time, there are substantial conflicting interests and hostility between various BRICS countries, and a lack of unity on the position they should take vis-à-vis the West.[67] Some countries are seeking to overhaul a major part of the international legal order, while others are attempting to reform certain aspects of the existing world order.

Seeking cooperation

Finally, countries within both existing and new partnerships are seeking to persuade other actors to join them in pursuit of their own goals, and this could change the global or regional balance of power. Depending on the situation, countries receive economic, political or military advantages in exchange for support. For example, Russia, China, Iran and North Korea are working together more and more on military and diplomatic matters, thus further undermining the current international legal order. It should be noted that these collaborations are neither straightforward nor without hindrances. Various countries, including China and Russia, are strengthening their ties with African countries. Whereas China's presence is focused mainly on economic investment, including infrastructure projects, Russia is looking for partners in the security domain. In exchange for its security cooperation, Russia regularly receives support from various African countries in international forums like the United Nations, for example in relation to the war in Ukraine.

Russia increasingly active in Africa

Over the past few years Russia has gradually expanded its military and paramilitary presence in Africa, and it intends to become even more active on the continent. When a ceasefire is eventually reached in Ukraine, it is likely that Russia will reserve materiel and personnel for deployment in Africa. Russia's military and paramilitary presence in Africa is part of the hybrid geopolitical conflict it is waging, as a systemic rival of the West. Africa forms the southern flank of the European part of the NATO area. Russia's presence could thus pose a threat to units of NATO countries and the critical infrastructure and supply lines they depend on. In Africa, Russia is also undermining the West in military terms: French and US troops are being forced to withdraw by pro-Russian regimes. In addition, Russia is pursuing its economic interests by obtaining access to critical raw materials or by preventing the West from accessing them. Finally, Russia's military and paramilitary presence in other countries has an influence on the security situation there, for example in the way jihadism is combated.

Significance to the Netherlands

- *As host country of the International Criminal Court and the International Court of Justice, the Netherlands has a special responsibility. The presence of these courts also makes the Netherlands a specific target for espionage and subversive influencing. What is more, foreign threats and sanctions on international courts could have a knock-on effect with respect to the host country. For example, countries may decide to impose sanctions that also affect Dutch nationals, or they may reject visa applications from Dutch nationals.*
- *The influencing of existing institutions and the establishment of parallel institutions are consequences of evolving power relations. Countries like China are taking advantage of opportunities to gain more power and pursue its interests more effectively. Such developments may serve to reduce the Netherlands' influence on the international stage.*

End notes

1 AIVD, MIVD and NCTV, Threat Assessment on State Actors no. 2, November 2022, p. 7; National Network of Safety and Security Analysts (ANV), Government-Wide National Security Risk Analysis, 2022, p. 36.

2 Scientific Council for Government Policy (WRR), 'The Netherlands in a Fragmenting World Order', 2024.

3 ANV, 'Leidraad risicobeoordeling Rijksbrede Risicoanalyse Nationale Veiligheid' (Risk Assessment Guide: Government-Wide National Security Risk Assessment), 2022; NCTV, 'Veiligheidsstrategie voor het Koninkrijk der Nederlanden 2023-2029' (Security Strategy for the Kingdom of the Netherlands, 2023-2029), 2023, p. 11-12.

4 WRR, 'The Netherlands in a Fragmenting World Order'.

5 The Arctic Institute – Center for Circumpolar Security Studies, 'China's Polar Silk Road: Long Game or Failed Strategy?', 14 November 2023.

6 Ministry of Economic Affairs, Letter to parliament containing the government's response regarding the long-term space agenda, 21 February 2025.

7 Ministry of Foreign Affairs, Letter to parliament introducing space security policy, 5 March 2021

8 Ministry of Defence, Defence Space Agenda, November 2022.

9 Alexandra Prokopenko, 'Russia's Economic Gamble: The Hidden Costs of War-Driven Growth', Carnegie Politika, 20 December 2024.

10 Organisation for the Prohibition of Chemical Weapons (OPCW), 'Report of the OPCW Technical Assistance Visit on the Activities Carried Out in Support of a Request by Ukraine', 14 February 2025; OPCW, 'Report of the OPCW Technical Assistance Visit on the Activities Carried Out in Support of a Request by Ukraine', 18 November 2024.

11 Office of the Director of National Intelligence, 'Iran's Nuclear Weapons Capability and Terrorism Monitoring Act of 2022', July 2024.

12 Jamie Kwong and Nicole Grajewski, 'Will Iran withdraw from the Nuclear Non-Proliferation Treaty?', War on the Rocks, 1 November 2024; 'The nuclear fatwa that wasn't – How Iran sold the world a false narrative', Atlantic Council, 9 May 2024; Michael Eisenstadt and Mehdi Khalaji, 'Iran's flexible fatwa: how "expediency" shapes nuclear decision making', Washington Institute for Near East Policy, 4 February 2021.

13 International Atomic Energy Agency (IAEA), 'Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)', 27 May 2024.

14 'OM: Topmedewerker van Nationaal Coördinator Terrorismebestrijding spioneerde voor Marokko' (Prosecutors say senior NCTV staff member was spying for Morocco), De Volkskrant, 7 February 2024; 'Medewerkers NCTV en politie aangehouden' (NCTV and police staff arrested), Public Prosecution Service, 1 November 2023.

15 AIVD, 'Offensief cyberprogramma: een ideaal businessmodel voor staten' (Offensive cyber programme: an ideal business model for states), June 2019.

16 AIVD and NCTV, 'Crossing Borders: State-sponsored Interference in Diaspora Communities in the Netherlands', October 2024.

17 Council of the European Union, 'Council Implementing Regulation (EU) 2025/389 implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine', 24 February 2025.

18 MIVD and AIVD, 'Dreigingsbeeld militaire en hybride dreigingen' (Assessment of Military and Hybrid Threats), December 2024.

19 Ministry of Infrastructure and Water Management, Letter to parliament detailing progress on the strategy to protect North Sea infrastructure, 10 June 2024; MIVD, 2023 Annual Report, April 2024; MIVD and AIVD, '24/2 – De Russische aanval op Oekraïne: een keerpunt in de geschiedenis' (24/2 – Russia's attack on Ukraine: a turning point in history), February 2023.

20 MIVD and AIVD, 'Dreigingsbeeld militaire en hybride dreigingen' (Assessment of Military and Hybrid Threats).

21 NCTV, 2024 Cybersecurity Assessment for the Netherlands, October 2024.

22 Council of the European Union, 'Cyber: Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation', 3 May 2024.

23 Joint Cybersecurity Advisory, 'IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities', 18 December 2024; 'VS looft 10 miljoen dollar uit voor informatie over aanvallers waterbedrijven' (US offers $10 million reward for information on perpetrators of attack on water companies), security.nl, 8 August 2024; 'VS meldt aanval op industrieel controlesysteem Amerikaans waterschap' (US reports attack on industrial control system of American water authority), security.nl, 29 November 2023.

24 AIVD and NCTV, 'Crossing Borders'.

25 Dana Moss, Marcus Michaelsen and Gillian Kennedy, 'Going after the family: transnational repression and the proxy punishment of Middle Eastern diasporas', Global Networks (22), 2022, p. 735-751.

26 AIVD and NCTV, 'Crossing Borders'.

27 Matthew Levitt, Magnus Ranstorp and Norman Roule, 'Mapping Iranian external actions worldwide', Washington Institute for Near East Policy, 9 August 2024; Matthew Levitt, 'Trends in Iranian External Assassination, Surveillance, and Abduction Plots', CTC Sentinel, February 2022, p. 1-11.

28 AIVD and NCTV, 'Crossing Borders'; '23 jaar en 6 maanden celstraf voor moord op een Iraanse man in Almere in 2015' (23 years and six months for murder of Iranian man in Almere in 2015), Leeuwarden and Arnhem Court of Appeal, Rechtspraak.nl, 24 November 2022; 'Liquidatie Iraanse activist Ahmad Mola Nissi (52)' (Assassination of Iranian activist Ahmad Mola Nissi (52)), Opsporing Verzocht, 30 June 2019; 'Rotterdamse criminelen achter moord op Iraanse activist' (Rotterdam criminals behind murder of Iranian activist), RTV Rijnmond, 3 July 2018.

29 Matthew Levitt and Sarah Boches, 'Iranian External Operations in Europe: The Criminal Connection', ICCT, 16 October 2024; Levitt, Ranstorp and Roule, 'Mapping Iranian external actions'; 'Iran is using criminal networks in Sweden', Säkerhetspolisen, 30 May 2024; 'Iran may be behind attacks on Israeli embassies, Sweden says', BBC News, 2 October 2024.

30 Levitt and Boches, 'Iranian external operations in Europe'; Ioan Pop and Mitchell D. Silber, 'Iran and Hezbollah's pre-operational modus operandi in the West', Studies in Conflict & Terrorism 44 (2), 2021, p. 156-179; 'Norwegian Police Security Service: Person accused of terrorism in Copenhagen has unclear connection to Norway', Norwegian News Agency (NTB), 8 October 2024.

31 Levitt, 'Trends in Iranian External Assassination', p. 2.

32 'Schietpartij bij defensiebedrijf in Göteborg; laatste in serie anti-Israëlische aanslagen' (Shooting at defence firm in Gothenburg; latest in series of anti-Israeli attacks), De Volkskrant, 10 October 2024. 'Two Swedish teens arrested in Copenhagen in connection with Israeli embassy blasts', Euronews, 3 October 2024; 'Israëlische ambassades in toenemende mate doelwit van geweld' (Israeli embassies increasingly targets of violence), Trouw, 3 October 2024; 'Iran may be behind attacks on Israeli embassies, Sweden says', BBC News, 2 October 2024; Levitt, Ranstorp and Roule, 'Mapping Iranian external actions'.

33 Levitt and Boches, 'Iranian external operations in Europe'; 'Sweden wants EU to classify Revolutionary Guards as terrorist organization', VOA, 13 October 2024; 'Swedish gangs as intermediaries for Iran – this is what has happened', Swedish Herald, update 4 October 2024; Levitt and Boches, 'Iranian external operations in Europe'; Levitt, Ranstorp and Roule, 'Mapping Iranian external actions'.

34 'Swedish FM confronts Iran over murder plot against Jews', AFP, 15 February 2024.

35 'Iran jaagt in Europa op Israëlische doelwitten en tegenstanders: "Ik wist dat ze iemand gingen sturen", zegt de dissident uit Haarlem' (Iran hunts for Israeli targets and opponents in Europe: '"I knew they would send someone," says Haarlem dissident'), NRC Handelsblad, 5 September 2024.

36 'Sweden blames Iran for cyber-attack after Quran burning', BBC News, 24 September 2024; Levitt, Ranstorp and Roule, 'Mapping Iranian external actions'.

37 Levitt and Boches, 'Iranian external operations in Europe'.

38 'Chinese vertrouweling prins Andrew als spion VK uit gezet' (Chinese confidant of Prince Andrew expelled from UK as spy), NOS, 13 December 2024.

39 'Politie doorzoekt kantoor van Europarlementariër Krah in spionagezaak' (Police raid office of MEP Maximilian Krah in espionage case), NOS, 7 May 2024; 'AfD-lijsttrekker in Brussel blijft aan en zegt aangehouden medewerker te ontslaan' (AfD party leader in Brussels will stay on, and says arrested staff member has been dismissed), NOS, 24 April 2024.

40 AIVD and NCTV, 'Crossing Borders'.

41 Ibid.

42 'Paperwall: Chinese Websites Posing as Local News Outlets Target Global Audiences with Pro-Beijing Content', Citizen Lab, 7 February 2024.

43 'Niet de "groene activisten", maar de Russen zaten achter Duitse uitlaten vol schuim' (The Russians, not 'green activists', were behind the foam-filled German exhaust pipes), NRC Handelsblad, 5 February 2025; 'Deutschlandweite Sabotage-serie offenbar von Russland gesteuert' (Germany-wide acts of sabotage apparently the work of Russia), Der Spiegel, 5 February 2025.

44 'Rusland schakelt "freelance-agenten" in voor hybride oorlogsvoering, "zoals bij Uber"' (Russia deploys 'freelance agents' for hybrid warfare, 'Uber style'), Het Nieuwsblad, 17 January 2025.

45 Christopher Houtkamp, Nienke van Heukelingen, Teun van der Laan, 'Patriottisme ontmoet pragmatisme: het Turkse diasporabeleid in Nederland' (Patriotism meets pragmatism: Turkish diaspora policy in the Netherlands), Clingendael Institute, 2024, p. 11.

46 Ibid, p. 12.

47 Christopher Houtkamp, Nienke van Heukelingen, Teun van der Laan, Erwin van Veen, 'Het Turkse diasporabeleid in Nederland: Onderzoek naar het perspectief van de Turks-Nederlandse gemeenschap en het Turkse diasporabeleid' (Turkish diaspora policy in the Netherlands: a study of the perspective of the Turkish-Dutch community and Turkish diaspora policy), Clingendael, 2023, p. 2.

48 Ministry of Justice and Security, Letter to parliament on the report by the Israeli Ministry for Diaspora Affairs and Combating Antisemitism, 29 November 2024.

49 Parliamentary Paper, House of Representatives, 2024, 36 651-34; 'Diplomatieke tik op de Israëlische vingers voor rapport vol beschuldigingen' (Diplomatic rap on Israel's knuckles for report full of accusations), NRC Handelsblad, 29 November 2024

50 'Israël noemt vredesactivist Thomas van Gool spil in aan Hamas gelieerd netwerk, nu wordt hij bedreigd' (Israel calls peace activist Thomas van Gool a key figure in a network allied to Hamas; now he is being threatened), Het Parool, 24 November 2024.

51 AIVD, 'Offensief cyberprogramma' (Offensive cyber programme); NCTV, 2024 'Cybersecurity Assessment for the Netherlands', p. 44.

52 AIVD and NCTV, 'Crossing Borders'.

53 'Three IRGC Cyber Actors Indicted for "Hack-and-Leak" Operation Designed to Influence the 2024 U.S. Presidential Election', US Department of Justice, 27 September 2024.

54 Microsoft, 'Microsoft threat intelligence report: Iran steps into US election 2024 with cyber-enabled influence operations', 9 August 2024, p. 1-4; Steven Lee Myers, Tiffany Hsu and Farnaz Fassihi, 'Iran Emerges as a Top Disinformation Threat in U.S. Presidential Race', New York Times, 4 September 2024; 'OpenAI blokkeert Iraanse beïnvloedingsoperatie die ChatGPT misbruikte' (OpenAI blocks Iranian influencing operation that misused ChatGPT), Dutch IT Channel, 21 August 2024.

55 Ministry of Economic Affairs and Climate Policy, 'Kabinetsaanpak Strategische Afhankelijkheden' (The government's approach to strategic dependencies), 12 May 2023.

56 AIVD and NCTV, 'Crossing borders'; AIVD, MIVD and NCTV, Threat Assessment on State-Sponsored Actors 2, p. 34.

57 'China stuurt gericht tientallen militaire onderzoekers naar Nederland om gevoelige kennis te vergaren' (China sends dozens of military researchers to the Netherlands to gather sensitive knowledge), Follow the Money, 20 May 2022.

58 'Nederlandse bedrijven lijken sancties Rusland te omzeilen, veel handel met "uitwijklanden"' (Dutch companies are apparently circumventing Russia sanctions, lots of trade with 'evasion countries'), De Volkskrant, 10 December 2024.

59 'AIVD: Opgepakte ASML-medewerker stond in contact met Russische inlichtingendienst' (AIVD: Arrested ASML employee was in contact with Russian intelligence service), Trouw, 6 February 2025; 'Russische oud-medewerker ASML verdacht van diefstal bedrijfsgeheimen' (Russian former ASML employee suspected of stealing trade secrets), NOS, 6 December 2024.

60 'Rusland houdt controle op VN-sancties Noord-Korea tegen' (Russia blocks monitoring of UN sanctions on North Korea), NOS, 28 March 2024.

61 Oxfam Policy & Practice, 'Vetoing Humanity: How a few powerful nations hijacked global peace and why reform is needed at the UN Security Council', 19 September 2024.

62 'MIVD: we hebben Russische hack van OPCW in Den Haag voorkomen' (MIVD: We prevented a Russian hack of the OPCW in The Hague), NOS, 4 October 2018; 'AIVD: infiltratie Russische spion bij Strafhof voorkomen' (AIVD: infiltration of ICC by Russian spy prevented), NOS, 16 June 2024.

63 AIVD and NCTV, 'Crossing Borders'.

64 'Internationaal Strafhof veroordeelt sancties van VS tegen medewerkers' (ICC condemns US sanctions against its staff), NOS, 7 February 2025; '"VS dreigt met wraak tegen Strafhof Den Haag"' (US threatens revenge against ICC) in The Hague), BNR, 30 April 2024.

65 '79 landen veroordelen Amerikaanse sancties tegen Internationaal Strafhof' (79 countries condemn US sanctions against ICC), NOS, 7 February 2025.

66 ANV, Hoofdrapport Trendanalyse Nationale Veiligheid (National Security Trend Analysis), 2024.

67 Ibid.

July 2025
This publication is a joint release of:

General Intelligence and Security Service
(AIVD)
english.aivd.nl

Military Intelligence and Security Service
(MIVD)
english.defensie.nl

National Coordinator for Counterterrorism
and Security (NCTV)
english.nctv.nl