Threat Assessment State Actors 2025

Persistent threats in times of growing uncertainty

Cover photo:*More than two months before the start of the NATO summit, the street where the meeting will be held at the end of June is no longer open to traffic.*

Persistent threats in times of growing uncertainty

The State Actors Threat Assessment (DBSA) 2025 is being published in a turbulent time when international relations are becoming more unpredictable. Over the past two years, state threats to the Netherlands and our interests have remained undiminished in many areas, and the threat of sabotage has increased. None of the threats described in the DBSA have diminished. However, resilience to state threats is increasingly accompanied by uncertainty about the near future.

Changes in global relations

The global power balance is shifting, and the question is what the future global order will look like. The era of liberal-Western values seems to be over. Countries in the "Global South" are becoming less interested in the West and are establishing new institutions and partnerships to counterbalance existing spheres of political influence. Changes in the global order appear to be having an increasingly powerful impact, for example, because countries are increasingly willing to actively use their power to defend their interests within international institutions and partnerships. These changes could have significant consequences for the Netherlands and our national security; the openness of Dutch society, democracy, and economy makes our country vulnerable.

The threat of state actors remains undiminished

Within these changes in global relations, state actors threaten Dutch national security in various ways.[i] A direct military attack by Russia on NATO territory is unlikely, but as the tensions between Russia and the West deepen, the risk of (unintended) further escalation has increased. Russia is increasingly carrying out sabotage actions to stoke fear and unrest in Europe, anticipating that political and societal willingness to engage in conflict with the country will then decline. Such actions are expected to continue to increase because sabotage actions fall below the threshold of a military conflict and thus fall under Article 5 of the NATO Treaty. Russia can continue to pursue its objectives through sabotage actions without actually engaging in war with NATO. Physical and digital sabotage can lead to social disruption, the disruption of vital infrastructure, the disruption of military operations or preparations for them, and economic damage. Of all cyber threats, digital sabotage potentially has the greatest impact on Dutch society.

i The six national security interests are: territorial, physical, economic and ecological security, social and political stability, and international rule of law and stability.

Many other threats remain as strong as ever. The threat of espionage by countries like China, Russia, and Iran remains high. Moreover, a growing number of countries appear to be attempting to influence Dutch society and political decision-making through low-threshold digital espionage, intimidation, or the dissemination of disinformation. It is possible that more countries are deploying such means as a result of the changing world order. The increased Dutch focus on identifying state threats may also have contributed to better signaling of such threats. Espionage, low-threshold disruptive attacks, transnational repression, and subversive influence can fuel feelings of unrest and insecurity within diaspora communities or society more broadly. Such actions undermine social and political stability.

The economy is closely linked to geopolitics. Strategic dependencies are used as a means of political or economic leverage. More and more countries are pursuing protectionist economic policies with trade barriers and restrictions on the trade of technological knowledge and goods. The use of economic instruments by state actors can have major consequences for the Netherlands. In the short term, life can become more expensive due to trade conflicts, export restrictions, or
increased energy prices.

Moreover, the threat of unwanted knowledge and technology transfer remains high. Due to sanctions, state actors are seeking alternative ways to acquire technological knowledge, for which they are more likely to resort to covert acquisition. If other countries acquire the same technological knowledge as the Netherlands through (covert) acquisition, our leading position in certain technological domains could decline in the long term, or the competitiveness of Dutch companies could structurally decline. Moreover, it could strengthen other countries militarily, thus reducing the effectiveness of our armed forces.

Increasing uncertainty about resilience

The threat from state actors remains undiminished, but resilience to it has become more uncertain. The Netherlands and other European countries remain highly dependent on the United States, including in the areas of security, defense, economy, raw materials, and technology. These security dependencies have become more vulnerable because European countries' threat perception and appreciation of the current international legal order have increasingly diverged from those of non-European countries. The choices made by state actors impact the Netherlands, even when these choices are not directly aimed at the Netherlands. This entails significant uncertainties and risks to national security. The changes in the global order and our resilience could contribute to state actors becoming less resilient and acting more boldly. Europe is increasingly self-reliant and will primarily have to ensure the security of its own part of the world.

Table of contents

A Finnish pilot is in an F-18. Leeuwarden Air Base is hosting the international Ramstein Flag exercise. This NATO exercise replaces the annual Royal Netherlands Air Force exercise, normally called Frisian Flag.

Introduction

This is the 2025 Threat Assessment for State Actors (DBSA), prepared by the General Intelligence and Security Service (AIVD), the Military Intelligence and Security Service (MIVD), and the National Coordinator for Counterterrorism and Security (NCTV). The 2025 DBSA reflects the most important developments in state threats to national security since the publication of the previous DBSA in November 2022. The goal is to raise awareness of the nature and severity of these threats. The threat assessment thus provides the analytical basis for policy follow-up.

State actors strive to advance their interests as effectively as possible. Some states unintentionally or unintentionally harm others, while others deliberately harm the interests of others. Whether consciously or unconsciously, intentionally or unintentionally, our national security can be affected in all cases. The DBSA focuses specifically on this threat posed by state actors. The DBSA uses the following definition of state threats:

> *Coercive, subversive, misleading, or covert activities by or on behalf of state actors, below the threshold of armed conflict, which may harm the national security interests of the Netherlands through a combination of the objectives pursued, the means used, and the resulting effects.*[1]

This DBSA comes at a time of turbulence, with international relations becoming increasingly unpredictable. The most striking developments are the wars in Ukraine and Gaza, tensions around Taiwan and the Red Sea, and the strained transatlantic relationship.[2]All these events also affect the Netherlands and our national security interests. In some cases, they affect the Netherlands directly, while in others, they pose an indirect or latent threat that our country must guard against.

Compared to the previous DBSA from 2022, the threat remains as strong as ever in many areas, and the threat of sabotage has increased. None of the threats have diminished. Furthermore, resilience against state threats is increasingly accompanied by uncertainty about the near future, partly due to geopolitical developments. Therefore, it remains crucial to recognize state threats and then implement the most effective countermeasures.

Methods and targets of state actors

National security is threatened by state actors in various ways, as outlined in the previous DBSAs from 2021 and 2022. Actors threaten national security using a variety of methods, which are not always strictly separate and may be interrelated. These methods include:

- Military: including the development and conspicuous manifestations of conventional and nuclear weapons, the deployment of military units or operations – whether or not by *proxies*.[ii]
- Espionage: the collection of intelligence by physical or digital means for economic, political, administrative and military purposes, or to maintain visibility on the diaspora and dissidents.
- Sabotage: the deliberate damage to military and civilian targets to, for example, delay war deliveries, sow fear and division, or test when opponents will react.

- State interference: in addition to forms of espionage, this also concerns threats of violence or influencing the diaspora and undermining influence, for example by spreading disinformation or *hack-and-leak* -operations.[iii]
- Economy: Instruments within the economic domain, such as corporate acquisitions and investments, can be used legitimately and covertly to achieve geopolitical and military objectives through civilian companies. Unwanted transfer of knowledge and technology (acquisition) can also occur.

- Diplomacy and politics: this involves influencing or countering existing institutions, establishing parallel institutions and forming alliances in order to increase one's own influence.

These methods can be deployed against targets across the entire spectrum of Dutch society. For example, against democratic processes, policymakers, people or organizations involved in political decision-making, and (inter)national bodies such as NATO, but also against educational and knowledge institutions or international institutions on Dutch soil. Businesses and top sectors can become victims of espionage, for example, and specific diaspora and religious communities can be used by state actors to sow discord.
In short, both the methods that state actors can employ and their targets are diverse.

ii Proxies are third parties, such as corporations, hacker groups, or local criminal groups, employed by foreign governments for their capabilities and ability to conceal their own involvement.

iii Hack-and-leak operations involve gaining access to sensitive personal or organizational information through a hacking attack, and then sharing this information, whether manipulated or not, via (social) media or to specific individuals and organizations.

National security interests

If state actors threaten one or more national security interests to such an extent that societal disruption occurs, national security is at stake. Threats to national security are undesirable, regardless of their impact. Protecting national security must ensure that individuals, organizations, and communities can function unhindered. DBSA 2025 describes the most important geopolitical developments, state threats against the Netherlands, and the impact of these developments and threats on our national security. The impact is considered in the context of the six national security interests.[3]

These are:

- Territorial security (including digital security);
- Physical security;
- Economic security;
- Ecological safety;
- Social and political stability, and
- International rule of law and stability.

Reading guide

This DBSA begins with a contextual chapter on the changing world order, specifically addressing shifts in the geopolitical power balance and the emergence of new theaters of conflict. Six chapters follow, categorized by the methods employed by state actors: military, espionage, sabotage, state interference, economics, and diplomacy and politics.

The Hera spacecraft in a cleanroom at the European Space Research and Technology Centre (ESTEC). ESA's spacecraft will study asteroid deflection as part of a planetary defense mission called Hera.

12

Netherlands in a changing world order

The era of liberal-Western values dominating, often driven by American dominance, seems to be over. The global power balance is shifting, and the future of the global order remains to be seen. It is clear, however, that these changes could have significant consequences for the Netherlands and our national security. The openness of Dutch society, democracy, and economy makes our country vulnerable. Our country's security is therefore closely linked to the security of the rest of the world.

Shifts in the balance of power

The changing world order is accompanied by fragmentation; this is a common thread running through the Threat Assessment of State Actors 2025. The WRR report *The Netherlands in a fragmenting world order* describes the fragmentation along three tracks: poles of power, scenes and worldviews.[4]

First, the unipolar world order is transforming into a multipolar one. In such a different world order, the dominance of the United States and the entire West will decline in favor of countries like China, Russia, India, Iran, Saudi Arabia, Turkey, and Indonesia. The global center of gravity—demographic, economic, and otherwise—is shifting east and south. Countries are becoming less attached to the West and are establishing new institutions and partnerships to counterbalance existing spheres of political influence. Each power is pursuing its own interests, which often conflict with those of others. Thus, the partnership between China and Russia has deepened even though they do not share common goals. For now, the emergence of such a multipolar world order seems inevitable.

Secondly, countries are active in more arenas and are framing these arenas from a security perspective. Economic activities are undertaken not only for economic reasons, but also as a prerequisite for their own security. An example is the global computer chip market, where countries take measures to prevent the most advanced equipment from falling into the hands of systemic rivals. This also applies to the social and digital arena, where state actors influence diaspora communities based on their own security interests. These arenas have, of course, existed for a longer period, but have gained importance in recent years.

Third, there is the fragmentation of worldviews. Countries like Russia and Iran can be seen as systemic rivals of the West, and China, which remains a major trading partner with which the Netherlands shares significant economic interests, must sometimes be considered a systemic rival. China considers a change in the international legal order necessary to gain greater influence on the world stage or to maintain domestic political power. Moreover, countries attempt to influence existing institutions and partnerships to their advantage and create their own alliances to advance their own interests. It is unlikely that the attitude of these systemic rivals towards the Netherlands and our interests will change in the near future.

The United States' changing posture has implications for our national security
For years, the focus of American security policy has been shifting away from Europe and more toward the power competition with China. This has accelerated with the inauguration of President Trump, who has also clearly indicated that more is expected of Europe for its own security. The changing, more transactional stance of the United States creates uncertainty for Dutch national security, partly due to the United States' significant dependencies in areas such as security. The United States is a key ally, but it is clear that Europe is increasingly self-reliant and will primarily have to ensure the security of its own part of the world.

From the North Pole to space

Physical locations have always been important battlegrounds, and this has become evident once again in recent years. For example, US President Trump has explicitly put Greenland and the Panama Canal on the map, and the interest of various countries in the Arctic and space has increased significantly in recent years. This interest in the Arctic stems from its existing gas and metal reserves, as well as its potential for maritime navigation.[5]Russia, in cooperation with China, is building numerous ports along its northern coast to control shipping routes that are becoming increasingly accessible due to climate change. Russia is also strengthening its military installations in the region and is engaging in limited but increasing military cooperation with China around the Arctic. The rising tensions surrounding the Arctic could lead to power shifts there and potential regional instability.

Space as a contested domain

Space has also become increasingly strategically important. What is geopolitically contested on Earth now finds its way into space. The "space race" of about half a century ago is once again in full swing, stimulating a wide range of innovations. The number of players in space is rapidly increasing, and space powers are expanding their capabilities and (military) ambitions. After all, the space domain is crucial for defense, security, economics, science, research, and innovation: people around the world use satellites and satellite services extensively every day for communication, financial transactions, navigation, weather forecasting, and internet access, for example.[6]

At the same time, space is becoming an increasingly contested domain, with a growing number of countries developing capabilities to restrict or deny other users access to or use of space assets, ranging from disruption and degradation to the physical destruction of satellites.[7]The threat from Russia and growing Chinese space capabilities, in particular, are increasingly posing challenges to maintaining unfettered access to or use of space. This could become problematic for the Netherlands, as both military and commercial satellites are a crucial part of Earth's infrastructure. Key societal functions depend on satellites. Loss or disruption of satellite signals, whether intentional or not, has a direct, disruptive effect on society.[8]In addition, the space domain is essential for Defense operations: communication with deployed units, the use of satellite-guided precision weapons, and intelligence analysis are all based on satellite images.

A patch with the logo for Bastion Lion, the largest exercise of the Royal Netherlands Army this year. During this exercise, two Dutch combat battalions from the 13th Light Brigade and one German combat battalion will carry out a multi-day assault on a training village in Germany. Approximately 4,000 soldiers, 1,800 vehicles, and 200 drones will participate in the exercise.

16

Military

For several years now, there has been a Russian threat against NATO countries, including the Netherlands. The military threat against NATO has remained more or less constant over the past two years. However, the war in Ukraine has deepened the tensions between Russia and the West, increasing the risk of (unintended) further escalation.

This increased risk affects the Netherlands because of Article 5 of the NATO Treaty[iv] and because of the possibility of sabotage being carried out in the Netherlands (see the chapter on Sabotage). Furthermore, resilience against a military threat has become more uncertain since the United States has clearly indicated that more is expected of Europe for its own security. Since the Russian invasion of Ukraine, Western support for that country has grown increasingly substantial, but recently this seems less and less self-evident. Europe is increasingly self-reliant and will primarily have to ensure the security of its own part of the world.

The shifts in the global order could contribute to state actors becoming less resistant and more audacious. For example, there have been various reports about Russia's use of banned chemical weapons in Ukraine, without this leading to strong international condemnation. This could result in lowering the threshold for deploying chemical weapons in other theaters of conflict. Iran continues to develop ballistic missiles, for which it is attempting, among other things, to acquire knowledge and equipment in the Netherlands through espionage. Besides supplying these missiles to allies in the region, Iran is supplying them to Russia for use in its war against Ukraine.

iv Article 5 of the NATO Treaty states that an attack on one member is considered an attack on all. Allies therefore assist each other when one of their countries is attacked.

Biggest military threat comes from Russia

Relations between the West and Russia have plummeted since the large-scale Russian war against Ukraine in February 2022. The risk of (unintended) military escalation between Russia and NATO has increased. Russia is the largest military adversary and the most likely military threat to the territorial integrity of the NATO alliance. Although Europe is investing heavily in NATO combat power, Russia has temporarily gained a military advantage. Worryingly, after the potential end of the war in Ukraine, and under the most favorable conditions for Russia, Russia would need only a year to build up sufficient capabilities for a limited military operation against NATO member states, if desired.

For Russia, Western and Russian security interests are conflicting and incompatible. The confrontation between Russia and the West has a "total" and existential character for Russia. In Russia's view, the war in Ukraine is therefore part of a broader conflict with the West. A change of course in Russia's attitude toward Europe in the foreseeable future is therefore difficult to imagine.

In recent years, Western support for Ukraine has grown increasingly substantial. This not only helps Ukraine with its national defense but also enables it, under certain conditions, to launch attacks in Russia. Continued support is essential for Ukraine to defend itself against Russian military aggression. However, this support is not always self-evident.

Russian attempts to compensate for the consequences of the war

Meanwhile, the war is also a war of military and economic attrition for Russia. The Russian economy is increasingly showing signs of a war economy, and although the effects of Western sanctions on the Russian economy are significant, Russia is not yet forced to stop the war in the short term due to economic instability.[9] The country is trying to compensate for the consequences of the war by establishing new partnerships and seeking ways to avoid international sanctions. Iran, North Korea, and Belarus supply weapons to Russia. Although China does not, in principle, supply weapons and ammunition to Russia, Chinese companies do *dual use* goods[v] and even attack drones to Russian companies that could be deployed in the war in Ukraine. In the fall of 2024, North Korea was revealed to be supplying not only weapons but also military personnel that were actually deployed against Ukraine.

In return, Russia supplies oil, among other things, which circumvents United Nations sanctions against North Korea. Finally, Western attempts to isolate Russia globally are not sufficiently resonating with the rest of the world. Thus, Russian trade with other parts of the world continues unabated.

v With dual-use goods, the end product has both civil and military applications.

Systematic violation of the Chemical Weapons Convention

Shortly after the Russian invasion of Ukraine, the first reports emerged that Russia had used tear gas on occupied Ukrainian territory. The use of chemical weapons as part of a military campaign, including tear gas, is prohibited under the Chemical Weapons Convention, a treaty to which Russia is also a signatory. Since February 2022, the Ukrainian Ministry of Defense has recorded more than 6,000 incidents in which Russia has used chemicals against Ukrainian forces. The Organisation for the Prohibition of Chemical Weapons (OPCW) has confirmed, through independent investigations, that tear gas was used.[10]

Since March 2024, the media has frequently reported on the use of chloropicrin, a suffocating chemical weapon. The United States and the United Kingdom imposed sanctions on Russia for this reason on May 1 and October 8, 2024, respectively. On July 4, 2025, the AIVD (General Intelligence and Security Service) and MIVD (Military Intelligence and Security Service), together with the German foreign intelligence service BND, also publicly confirmed that Russia is systematically using chemical weapons, including chloropicrin. Moreover, this joint publication contains a warning about an intensification of Russian chemical weapons use in Ukraine. The lack of a strong international response to this could contribute to lowering the threshold for state actors to deploy chemical weapons, not only in Ukraine but also in other conflict zones.

Nuclear rhetoric by Russia and Iran

In November 2024, Russia revised its nuclear doctrine, formally lowering the threshold for using nuclear weapons. This lowering does not equate to an increased willingness to deploy nuclear weapons. Russia may be primarily concerned with the deterrent effect of this policy on the West.

Nuclear rhetoric isn't limited to Russia. Before the Israeli and American attacks in June 2025, Iran could have acquired enough highly enriched uranium to produce several nuclear weapons within a very short time.[11] However, there were no indications that Iran was engaged in the other necessary activities to develop a nuclear explosive. However, the growing unrest in the Middle East did lead to political calls among *hardliners* to a *fatwa* to revise the 2003 nuclear weapons ban. Furthermore, Iran threatened to withdraw from the Non-Proliferation Treaty if sanctions suspended under the nuclear deal were reimposed.[12] The International Atomic Energy Agency further stated that Iran had failed to verify that its nuclear program served exclusively civilian purposes.[13] These developments increased concerns about Iran's nuclear program.

Continuing concerns about Iranian weapons development

Iran continues to pursue the further development of ballistic missiles. Due to internationally imposed sanctions, the Iranian regime has limited access to Western knowledge and technology. Therefore, Iran attempts to acquire this knowledge and equipment through espionage in countries like the Netherlands. This is done through covert acquisition networks, knowledge institutions, students, and researchers. Iran also explicitly seeks cooperation with Russia to acquire more technologically advanced military capabilities. Despite the sanctions, Iran is also making progress in ballistic missile development. For example, in 2024, it used its own developed ballistic missiles against Israel for the first time during the direct escalation between the two countries. However, the threat is not limited to Iran itself: Iranian allies such as the Lebanese Hezbollah and the Yemeni Houthis also used Iranian-developed missiles that same year. Iranian weapons could be used against Dutch troops in Iraq and in the Red Sea, where the Dutch navy was active in 2024. Furthermore, Iran has supplied Russia with short-range ballistic missiles and attack drones for the war against Ukraine. This means that Iran's ballistic missile program also directly affects Dutch security interests in Europe.

Attacks by Iran-backed groups pose costs and risks to international maritime shipping *The instability in the Middle East poses significant risks to international maritime transport, particularly around the Arabian Peninsula.*[we] *These waters are crucial for the efficient transport of large quantities of goods worldwide. The Netherlands is particularly dependent on oil and gas transported from the Persian Gulf via the Strait of Hormuz. Every link along this route is a potential bottleneck that can disrupt transport for the entire remainder of the journey. This also applies, for example, to the Panama Canal, the Bosphorus, and the Straits of Gibraltar, Taiwan, or Malacca. The more of these so-called Sea Lines of Communication (SLOC) become unusable, the greater the potential unforeseen consequences.*

Since November 2023, the Houthis have been carrying out attacks on (civilian) shipping in the Red Sea and on ships headed towards Israel. Shortly after the outbreak of the war in Gaza, the focus was primarily on attacking ships with Israeli links, but other vessels have also been targeted. Since then, the southern Red Sea has been avoided by an increasing number of shipping companies. In 2014, the Houthis seized power in Sana'a, the capital of Yemen, and have since become the de facto authority in northern Yemen. They maintain close ties with Iran, among others, through arms shipments, financial flows, and personnel support for the Iranian Revolutionary Guard. Analysts agree that the Houthis cooperate with Iran, but are not directly controlled by it.

The impact of the disruption of destination traffic is not directly a concern for the Netherlands. This is different for through shipping. Dutch-flagged ships and ships under other flags, for example, delivering goods of economic importance to Europe, are now often rerouting their routes between Europe and Africa and Asia to avoid the waters around the Arabian Peninsula as much as possible. This leads to longer sailing times and higher transport costs. Therefore, the Houthi attacks pose not only a physical threat but also have an economic impact, primarily on countries in the region.

we This concerns the entire area of the Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Gulf of Aden, Bab el-Mandeb, Red Sea.

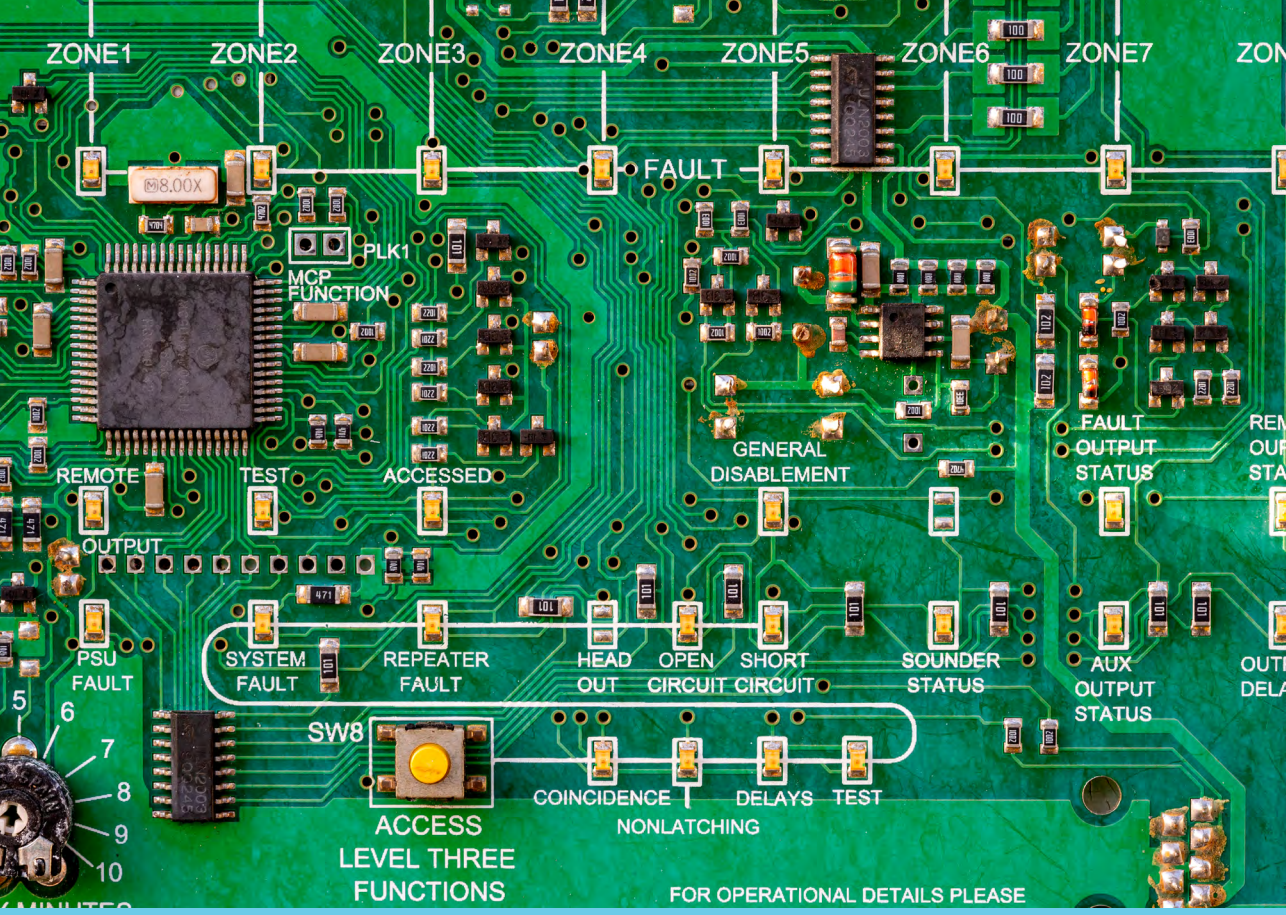
Threat against the Caribbean part of the Kingdom

The Caribbean part of the Kingdom of the Netherlands, specifically the ABC islands of Aruba, Curaçao, and Bonaire, continues to be directly affected by the political, economic, and humanitarian situation in Venezuela. Relations between the Netherlands and Venezuela are tense, partly because the Kingdom does not recognize Maduro's claimed victory in the 2024 presidential elections. It is unlikely that Venezuela intends to engage in a military conflict with the Kingdom, but the risk of unintended escalation exists due to Venezuela's relatively low level of military professionalism.

In addition, increasing instability within Venezuela could impact Aruba, Bonaire, and Curaçao, for example, through migration from Venezuela to the islands and cross-border crime. While current Venezuelan migration is putting pressure on the islands, a large-scale migration flow could potentially severely strain social stability and the economy. Services, such as medical facilities and the judicial system, are small-scale on the islands and therefore vulnerable.

Meaning for the Netherlands

- *If an attack were to take place on NATO territory, this would mean direct involvement of the Netherlands under Article 5 of the NATO Treaty. The war in Ukraine has deepened the tensions between Russia and the West, increasing the risk of (unintended) further escalation. This risk is partly determined by the ongoing Russia's investments in its own military apparatus, the extent to which NATO is able to counter this with military capacity for deterrence, Western cohesion and Russian perception thereof, and the way in which the build-up of NATO countries' military capabilities influences Russian threat perception.*
- *Europe is increasingly dependent on itself for its security. A possible military escalation would demand a lot from our country, both from the armed forces and from society as a whole. The Netherlands, for example, is a transit country for NATO equipment and can be involved in the care of wounded and war refugees.*
- *Unrest in the world affects the Netherlands and can have consequences for travel or international trade, but can also be a catalyst for threats against the Netherlands in the areas of terrorism or the economy, for example.*



A close-up of a green motherboard with chips and other components. Chips process data according to specific instructions. They are used in various types of devices, such as computers, smartphones, tablets, washing machines, etc. All interconnected components communicate via the motherboard.

22

Espionage

Espionage is a method of obtaining information and knowledge for economic, political, administrative, and military purposes, but can also be used to maintain visibility on the diaspora and dissidents. Espionage occurs digitally and through human sources, for example, through the diaspora, people in strategic positions, or through intelligence officers at embassies.

The threat of espionage by countries like China, Russia, and Iran has remained high since 2022. However, there appear to be a growing number of countries seeking to spy on the Netherlands, particularly digitally through offensive cyber programs. Such forms of espionage are easily accessible, making them relatively common. The increase may be due to shifts in the established world order, but it may also be related to improved intelligence and security services' understanding of state threats.

Ongoing classical espionage through human sources

Countries such as China, Russia, and Iran, among others, conduct espionage activities in the Netherlands. Foreign governments and intelligence agencies utilize networks of human sources. These can also include members of diaspora communities. In the Netherlands, too, several countries attempt to recruit citizens and organizations to gather intelligence. This includes individuals working in strategic positions, vital sectors, or who have access to relevant (personal) data. Countries can also station intelligence officers at embassies.

Since the Russian invasion of Ukraine, several Western countries have expelled hundreds of Russian intelligence officers. This makes it more difficult for Russian services to recruit human sources in Western countries under diplomatic cover and to maintain contact with existing human sources. This gap may be partially bridged using digital means. Moreover, Russian services still have ample opportunities to

To use non-diplomatic cover to gather intelligence within the European Union, including the Netherlands. This includes using business or academic pretexts.

Russia collects political intelligence, such as on the European Union and foreign ministries, and military intelligence, such as on NATO and defense ministries. Regarding the Netherlands, Russia also focuses on the many international organizations based here.
(see chapter Diplomatics and politics).

Arrest on suspicion of violating state secrets

In October 2023, a man was arrested on suspicion of possessing and disclosing state secrets. The judge has not yet issued a verdict in this case. According to the Public Prosecution Service, the man, a Dutch national of Moroccan descent, was on his way to Morocco and, at the time of his arrest, had a large number of digital (state secret) documents with him, including an analysis by the AIVD (General Intelligence and Security Service) on Moroccan intelligence activities in the Netherlands. The man, who had access to this type of information through his position at the NCTV (National Coordinator for Security and Counterterrorism), is suspected of violating state secrets, whether or not on behalf of a foreign power.[14]

Digital espionage on the rise

More and more countries, including Russia, China, Iran and North Korea, have offensive cyber programs that can be used for espionage.[15]In addition, the number of countries developing larger offensive capabilities in this direction is increasing. Such programs are often part of (large-scale) international campaigns and can also be deployed against the Netherlands and its interests.

Every country engages in espionage for its own reasons. For example, Russian cyber activities against Europe are aimed at political espionage, covert influencing activities, and digital sabotage (see next chapter). Since the Russian invasion of Ukraine in 2022, the AIVD (General Intelligence and Security Service) and the MIVD (Military Intelligence and Security Service) have recognized an increase in the number of actors within the Russian government, or those supported or directed by the Russian government, engaged in digital espionage. Their operations affect the Netherlands directly or indirectly, for example, through the compromise of systems of Dutch allies.

For a long time, China focused primarily on economic espionage, but this limited focus is no longer the case. The country has established a large, sophisticated, and professional digital espionage program. Chinese attack groups operate worldwide, targeting companies, governments, and organizations. China's information needs are unprecedented and encompass virtually every topic potentially relevant to the country: diplomacy, parliamentary affairs, military, economics, technology, science, armed forces, geography, finance, dissidents, health, sports, personal data, travel information, bulk data, and telecommunications. Given this large and diverse information need, cyberattacks can target any country in the world, and Chinese state actors also systematically target countries in Europe, including the Netherlands. Moreover, virtually all Chinese state cyber actors can opportunistically target Dutch interests if they find vulnerabilities there. These digital activities have now become so sophisticated and extensive that likely only a portion of Chinese cyber operations against Dutch interests are detected and subsequently mitigated in a timely manner. This also poses a major challenge to Dutch resilience.

Iran uses its digital espionage program primarily in the Middle East and against the United States. Specifically, the country focuses on political espionage in the region and against primary adversaries. In addition, Iran gathers intelligence on Iranian dissidents, organizations, or opponents of the regime, regardless of their location, including in the Netherlands, and collects bulk personal data from the aviation sector.[16]
This kind of espionage activities can lead to feelings of insecurity or fear for both diaspora communities and society more broadly.

North Korea uses digital attacks largely for financial gain. North Korean actors also attempt to steal cryptocurrencies in the Netherlands, using their attacks and the resulting profits to circumvent sanctions against North Korea. The country also uses North Korean freelance IT professionals, who are hired abroad under false identities by companies to earn money for the regime, including by stealing data or cryptocurrencies. It is conceivable that the proceeds from these actions are also used to finance weapons programs. For example, the European Union has imposed sanctions on the head of North Korea's intelligence agency, RGB.[17]
In addition, the country focuses on espionage, for example, by stealing information from educational and research institutions. There are currently no indications that North Korea receives assistance from other countries in its digital attacks or purchases sophisticated commercial spyware.

Meaning for the Netherlands

- *Classic human source espionage typically targets specific individuals, organizations, or Institutions. This can fuel feelings of insecurity and fear within diaspora communities or more broadly in society. This threat has remained constant in recent years.*
- *In addition, a growing number of countries are engaging in digital espionage through offensive cyber programs. Such forms of espionage are easily accessible and untargeted. State actors are collecting massive amounts of digital data from Dutch citizens, which they can later use to further their own interests. It is possible that more digital espionage is being observed because the intelligence and security services' understanding of state threats is improving.*
- *Countries like Russia and China use large-scale espionage programs, which they can use to gather information in the Netherlands for later use. Such information can be used, for example, in low-threshold digital sabotage and disruption attacks (see the next chapter).*

The Coast Guard monitors and maintains safety on the North Sea.

26

Sabotage

In the gray area between war and peace, sabotage actions or attempted sabotage are taking place across Europe. Russia and those allied with Russia or pro-Russian groups are carrying out more sabotage actions than before, taking greater and greater risks.

Russia has the continuing intention to foment unrest in Europe through sabotage, regardless of the outcome of the war in Ukraine. Because sabotage actions remain below the threshold of Article 5 of the NATO Treaty, the number of actions is expected to continue to increase. Russia is attempting to achieve its objectives with these actions without engaging in an actual war with NATO.

While there are no known examples of physical sabotage by state actors in the Netherlands, the AIVD (General Intelligence and Security Service) and MIVD (Military Intelligence and Security Service) have discovered preparatory actions from Russia. Moreover, events elsewhere in Europe could impact the Netherlands. The Netherlands is a potential target, partly due to its vital maritime infrastructure in the North Sea and its status as a transit country. Small-scale digital sabotage and disruption actions, as well as preparatory actions for such operations, do occur in the Netherlands. Of all digital threats, sabotage potentially has the greatest impact on Dutch society. Sabotage can lead to social disruption, the disruption of vital infrastructure, the disruption of military operations or preparations for them, and economic damage.[18]

Physical sabotage is also conceivable in the Netherlands

The intensity of physical Russian sabotage actions in the European Union has increased since the Russian invasion of Ukraine, particularly in countries bordering Russia. Russia and those affiliated with or pro-Russian groups are demonstrating a greater appetite for risk than a few years ago and are engaging in aggressive, provocative, or even violent activities. Russia is also recruiting (criminal) citizens for these kinds of actions, who may not realize their purpose. Sabotage actions are targeting organizations involved in various ways in or supporting the war in Ukraine, and increasingly targeting military and logistical locations in Europe.

The sabotage activities have multiple objectives. On the one hand, they are aimed at delaying Western supplies to Ukraine. On the other hand, they are intended to sow division in the West and undermine support for Ukraine by instilling fear. Moreover, by deploying sabotage activities, Russia can test where the West draws red lines regarding Russian aggression on its own territory. Russia appears to be seeking a model in which it can maximally disrupt Western support for Ukraine without provoking a military escalation by the West.

The Netherlands as a possible target

The Netherlands is an attractive target for state actors due to its position as a transit country in the event of a large-scale military conflict and the presence of vital maritime infrastructure in the North Sea. The North Sea contains important internet cables, gas pipelines, and wind farms that are crucial to the functioning of the Netherlands and its neighboring countries. Protecting and monitoring this vast and freely accessible area poses a challenge for the Netherlands. Sabotage of vital processes can threaten our national security, whether it occurs physically or digitally. It is conceivable that Russia is capable of carrying out physical sabotage in the Netherlands, although this has not yet happened as far as we know. For example, the country is likely mapping vital infrastructure and undertaking activities that indicate espionage and preparatory actions for physical disruption and sabotage.[19]

The purpose of these sabotage activities is likely to provide Russia with additional options for action, particularly prior to a conflict. It is consistent with Russian military-strategic thinking to disrupt or damage an opponent's vital processes, such as communications, energy supplies, and logistical capabilities, as quickly as possible in the event of an emerging conflict.

Large-scale sabotage of Dutch vital infrastructure could lead to societal disruption. The Netherlands could also suffer the consequences of sabotage of vital infrastructure elsewhere in Europe.[20]Due to the interconnectedness of the European electricity grid, a disruption in Germany, for example, could also lead to outages in the Netherlands. The potential for critical infrastructure failure has already been concretely addressed several times in the European Union.

Low-threshold digital sabotage and disruption attacks in the Netherlands

In the Netherlands, digital sabotage attempts, as well as preparatory actions, have been observed. Countries such as Russia, Iran, and China use offensive cyber programs to disrupt or sabotage (in the future) vital physical and digital infrastructure. Sabotage attempts, including by Russia, as well as preparatory actions, have been observed in the Netherlands.

In the Netherlands, low-threshold digital disruption attacks occur. DDoS attacks are a prime example. They are low-threshold and often have limited impact. A digital sabotage attack, on the other hand, can permanently affect the availability of digital services, processes, or systems. Some digital disruption attacks have been linked to Russia.[21]For example, several political parties reported that their websites were difficult to access due to DDoS attacks in June 2024, the day of the European elections in the Netherlands. The DDoS attacks were claimed by pro-Russian hacktivists. Previously, in June and August 2023, websites of Dutch ports and airports were also affected.

temporarily impaired or unavailable due to DDoS attacks. These attacks were also claimed by pro-Russian hacktivist groups, suspected of affiliation with the Russian government. The AIVD (General Intelligence and Security Service) and the MIVD (Military Intelligence and Security Service) determined that in 2024, a state-sponsored hacker group was responsible for a cyber sabotage attack against the digital operating system of a public facility in the Netherlands.

In other European countries that explicitly support Ukraine, attacks by Russian terrorists took place in 2024 *advanced persistent threats*.[vii] This happened, among other places, against political parties in Germany and government institutions in Poland and the Czech Republic. Similar attacks previously took place in Lithuania, Slovakia, and Sweden, among other places.[22] Furthermore, in September 2024, the MIVD (Military Intelligence and Security Service) warned of cyber operations by unit 29155 of the Russian military intelligence service. These hackers' focus is, among other things, on monitoring and disrupting Western aid to Ukraine. Their operations are primarily aimed at Western governments and critical infrastructure.

The Netherlands is not a primary target of Iranian digital sabotage. Recent Iranian sabotage activities against Western allies are a cause for concern. In 2023, the systems of several American drinking water and water purification companies were compromised by state-sponsored Iranian hackers operating under the group name CyberAv3ngers. According to the United States, this group is affiliated with the Iranian Revolutionary Guard Corps, Iran's elite military force. Access to drinking water is part of vital infrastructure; misuse of associated systems can have a significant impact on the health of the local population.[23]

vii An advanced persistent threat involves an actor using advanced means to operate undetected for extended periods of time.

Meaning for the Netherlands

- *Physical and digital sabotage actions in the Netherlands can lead to social disruption. A Sabotage targeting one of the vital sectors can lead to temporary unavailability of electricity, internet, payment transactions, or clean drinking water. This can have far-reaching consequences. For example, a power outage can impact telecom services, internet access, train traffic, or the functioning of hospitals.*

Russia is using sabotage to stoke fear and unrest in Europe, expecting it to diminish political and societal willingness to engage in conflict with the country. The number of sabotage attacks is therefore expected to continue to rise.

In June 2024, an assassination attempt was made in Haarlem on an Iranian living in the Netherlands. Police arrested two suspects. One of them is also suspected of the failed assassination attempt on a Spanish politician and Iran critic.

30

State interference

State actors attempt to influence Dutch society and political decision-making. Besides the aforementioned espionage purposes, they also attempt to intimidate diasporas, or engage in subversive influence through disinformation or hack-and-leak operations.

For example, countries like Iran, Pakistan, Morocco, and Turkey gather intelligence on or through their diaspora communities in the Netherlands. Other countries, such as China, Eritrea, and Syria, are also likely to do so, as they are known to gather intelligence on or through their diasporas in other European countries.[24] These authorities continue to view Dutch citizens as subjects because they or their (grand)parents were born there. In October 2024, the AIVD and NCTV published their analysis "Over de grens" (Across the Border), about such state interference in diaspora communities. Subversive influence involves efforts by state actors to enhance their reputation, increase their influence abroad, and manipulate public opinion and political decision-making to their advantage.
to put.

State interference by known countries has remained high since 2022, and the number of countries using such methods also appears to be increasing. As with espionage, this increase may be due to a shifting global order, allowing more countries to benefit from such forms of interference. At the same time, the Netherlands' increased focus on identifying state threats may have contributed to better signaling them.

Transnational repression against diaspora

State intervention can have a profound impact on diaspora communities. Foreign governments have various reasons for doing so, such as protecting their internal stability, increasing influence, or countering criticism and threats. They can silence political opponents, for example, by threatening family members.[25]and persuade members of diaspora communities to gather intelligence, either through coercion or otherwise.[26]In exceptional cases, people run the risk of becoming victims of physical violence, kidnapping, or even murder. Such threats of violence by foreign governments are also called transnational repression.

Transnational repression is usually carried out by, or at the initiative of, foreign intelligence services. Countries also use organizations and individuals with whom they have no direct relationship, known as proxies. These include organizations or companies, nationalist individuals or groups, hacker groups, and local criminal groups. Proxies possess relevant capabilities that governments can use for their own purposes, and they also have the advantage of *plausible deniability*: the ability to deny direct involvement.

Iran linked to assassinations

Iran in particular has a long tradition of attacking dissidents abroad.[27] In June 2024, an attempted assassination of an Iranian resident of the Netherlands was made in Haarlem. Police arrested two suspects. One of them is also suspected of the failed assassination attempt on a Spanish politician and Iran critic. Intelligence suggests that Iran is likely responsible for the two assassination attempts. Previously, criminals from Amsterdam murdered an Iranian-Dutch citizen in Almere in 2015, and criminals may have been involved in the assassination of an Iranian-Dutch citizen from The Hague in 2017.[28] The AIVD has strong indications that Iran was involved in both assassinations. Similar incidents likely occurred in Belgium, Germany, France, the United Kingdom, and Sweden.[29] In addition, Iran sometimes uses extremist groups such as Hezbollah or individuals to carry out attacks, and frequently uses Shiites with a nationality other than Iranian or Lebanese.[30]

Iran is targeting Jewish and Israeli targets in Europe using criminals

Besides diaspora communities, Jewish and Israeli individuals, companies, organizations, and diplomatic representations have also been targeted by Iran.[31] This threat has increased since the outbreak of the Gaza war on October 7, 2023. Since the beginning of 2024, several attacks have been carried out on Israeli targets in Sweden and Denmark.[32]
In Sweden, the attacks are said to have been carried out by young criminals, whose gang leaders were allegedly recruited by Iran.[33]
Iran is also said to have sent two people undercover to Sweden to murder Jews.[34] The country is said to be carrying out similar activities in Germany and France.[35]

Iran is likely attempting to strike Israeli or Jewish targets in response to the Gaza war and Israeli attacks on Lebanon, Syria, and Iran. The choice of Scandinavia may be related to the Koran burnings in Sweden and Denmark. According to the Swedish security service Säpo, the Iranian Revolutionary Guard hacked a text messaging service and distributed inflammatory messages.[36] Iranian digital actors have often acted in response to specific events, such as the Quran burnings. It is therefore conceivable that developments that are politically sensitive in Iran are disrupted or influenced by Iranian cyber actors. Iran's activities in Scandinavia may be determined by existing ties to criminal gangs. Presumably, the gang leaders are located in Iran and are used by the regime to give orders to young gang members in Scandinavia. In exchange for financial gain, possibly combined with criminal pressure or coercion, young criminals are allegedly incited to carry out attacks.[37]

In the Netherlands, no juvenile criminals appear to be similarly controlled from Iran. However, the country does have criminal connections that could carry out activities in the Netherlands. These are more experienced criminal networks. In theory, these could also be deployed against Israeli targets.

Undermining influence to change image

Subversive influence involves efforts by foreign governments to enhance their reputation by suppressing criticism, increasing their influence, and manipulating public opinion and political decision-making. This occurs at both local and national levels, as well as within the European Union. In Europe, several incidents of (alleged) covert political interference have been reported by the media. For example, in December 2024, an influential Chinese businessman was expelled from the UK on suspicion of spying for China. He was found to have ties to the *United Front Work Department (UFWD)*, a wing of the Chinese Communist Party concerned with interference in other countries.[38]Earlier that year, a Chinese-German staff member of a Member of the European Parliament*Alternative for Germany*arrested on suspicion of passing on parliamentary documents from the European Parliament to China.[39]The bribery of MEPs by Qatar and Morocco in 2022 and the Russian influence operation surrounding the digital platform 'Voice of Europe'[viii]also agree that leading figures in (inter)national politics are used by state actors.[40]

Such examples of subversive influence have received more publicity in recent years than before, but this has not led to a decrease in such actions. State actors are therefore expected to continue conducting covert interference activities in Europe. The Netherlands generally does not appear to be a primary target, as foreign governments tend to focus their activities on countries with greater international influence. The known attempts at covert influence targeting the Netherlands and their actual effects have proven relatively small. However, state actors are opportunistic; they will seize opportunities to gain influence within Dutch institutions.[41]
Successful influence campaigns can potentially have a significant impact on the functioning of the Dutch democratic system. Moreover, countries spread disinformation to stoke fear and division and undermine democratic institutions. When this is aimed at other countries, it can also reverberate in the Netherlands.

Disinformation is aimed at influencing the diaspora, Dutch society, and political decision-making. Disinformation is primarily spread by Russia, but China is also playing an increasingly active role. In 2024, for example, a pro-Chinese online network, operated by a Chinese PR firm, was identified, spreading disinformation through fake news websites, including several Dutch ones. Regular news reports were interspersed with fake articles containing pro-Chinese narratives, conspiracy theories about the West, and negative messages about critics of the Chinese regime. The websites had virtually no reach.[42]

viii Through the digital portal "Voice of Europe," Russia waged a systematic, international campaign of media manipulation and fact-finding to destabilize Ukraine, the European Union, and its member states, and to woo European politicians.

Russian attempts at subversive influence

Russia focuses its covert influence primarily on countries it deems susceptible or to which it attaches particular strategic or historical importance. Russia is also capable of opportunistically identifying and exploiting opportunities in smaller states. Through covert influence, Russia attempts to influence Western political decision-making regarding Russia to its own advantage and to undermine overall political and military support for Ukraine. Russia also seeks to undermine Western political and social cohesion and weaken Russia's political opponents. Finally, Russia uses covert influence on the West to promote Russian domestic stability.

Russia deploys covert influence tactics in both the physical and digital domains, aimed at influencing public debate and the political and administrative decision-making process. For example, since the beginning of the war in Ukraine, Russia has secretly organized several so-called "peace demonstrations" in the Netherlands, which served to give the Russian population the impression that Europe is opposed to support for Ukraine. Russian disinformation resonates in the Netherlands with anti-institutional and right-wing extremist movements. Alternative explanations for the outbreak of the war in Ukraine are circulating: it is alleged to have been provoked by the country itself or to be a consequence of Western expansion, while in reality it is an illegal Russian invasion of a sovereign neighbor.

Russia is digitally recruiting local residents in Germany to sow division

In 2024, Russia recruited several people online to carry out low-level sabotage operations with a political message in Germany. For example, more than 270 cars were covered in foam and stickers. Initially, the actions were attributed to environmental activists, but an investigation by Der Spiegel revealed that at least three men from Germany, Serbia, and Bosnia-Herzegovina were involved, paid by Russian intelligence. The men received instructions for the actions and the provision of evidence via the messaging app Viber. According to Der Spiegel's investigation, the primary goal was to incite hatred against the political party The Greens (Bündnis 90/Die Grünen).[43] *This isn't the first time Russia has hired "amateurs" in Europe to carry out such activities for relatively low fees; the Belgian State Security Service also reported an increase in so-called "freelance agents" working for Russia last year.*[44] *No activities involving such agents have yet been observed in the Netherlands, but this is conceivable given the events in Belgium, Germany and other European countries.*

Turkish diaspora policy

According to research by Clingendael, Turkey is pursuing an ideologically driven diaspora policy with mixed effects.[45]In the Netherlands, this involves promoting good citizenship, strengthening cultural and religious ties with the mother country, and gaining votes for the largest Turkish political party, the AKP.[46]Much of this policy does not involve intimidation or monitoring of diasporas and is legally permissible. Previous research by Clingendael found that a quarter of Dutch people of Turkish descent feel unsafe because of Turkish influence.[47]According to the report, these feelings of insecurity are particularly prevalent among non-voters and supporters of opposition parties. Feelings of insecurity can lead to self-censorship and thus restrict freedom of expression. In contrast, almost fifty percent of Turkish Dutch citizens believe that Turkish involvement has a positive effect on the safety of the community.

Israeli attempt to influence Dutch politics and society

Israel also attempts to influence political and public opinion abroad, including in the Netherlands. This was illustrated by the distribution of a report from the Israeli Ministry of Diaspora and Countering Antisemitism, following the unrest surrounding the Ajax-Maccabi Tel Aviv football match in November 2024. The report was not shared with the Dutch government through official channels, but was sent directly to specific politicians and journalists.[48]The method of distribution was described as unusual and undesirable by the Dutch Ministers of Justice and Security and Foreign Affairs because of the possible negative consequences for Dutch residents.[49]In this way, the persons mentioned can be intimidated or threatened, or in the most serious cases, attacked.[50]

Iran uses cyber program for subversive influence

Iran uses an offensive cyber program for purposes including subversive influence. This program is primarily deployed in the Middle East and against the United States, but also against the Netherlands. Besides political objectives, Iran uses it, to a lesser extent, for economic or financial purposes.[51]Iran uses this program to gather knowledge about Iranian dissidents, organizations, and opponents, conduct political espionage, and collect bulk personal data within the aviation sector.[52]Iran-linked online personas also attempt to amplify messages or force policy changes through hack-and-leak operations.

In a classic hack-and-leak operation, someone gains access to sensitive personal or organizational information through a hacking attack, and then shares this information via (social) media or with specific individuals and organizations. Sensitive information is published directly or, depending on the objective, first manipulated. In this way, intimidating cyber operations can be carried out by a state actor, a state-sponsored hacking group, or an independent group, such as a hacktivist group. Online personas affiliated with Iran used such operations to target the public perception of the Gaza war. In this way, Iran attempted to portray Israel in a negative light while portraying its own actions positively. These online personas have been used by Iran before. During a large-scale cyber operation in Albania in 2022, Iran very likely used online personas to publish (allegedly) stolen data and convey the message that the People's Mujahideen of Iran resistance movement should no longer be welcome in the country.

The U.S. Justice Department also charged three members of Iran's Revolutionary Guard Corps with interference, alleging they sought to share documents stolen from a presidential candidate's campaign staff with the media through a hack-and-leak operation.[53]

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

Meaning for the Netherlands

- *The impact of transnational repression on diaspora or individual stakeholders in the Netherlands is Significant. Some people belonging to diaspora communities are afraid to speak out due to feelings of insecurity, fueled by threats or even attacks. Transnational repression can also lead to tensions and feelings of insecurity between different groups in the Netherlands. The Netherlands attaches great importance to constitutional freedoms, including freedom of expression. These kinds of actions undermine the constitutional freedoms of Dutch citizens and thus undermine social and political stability.*

- *The Netherlands is not a major target for subversive influence for most foreign governments, and its democratic institutions are so resilient that influence attempts are not always successful. However, state actors are opportunistic and will seize opportunities to gain influence in Dutch society and political decision-making.*

The threat of state interference from well-known countries like Russia and Iran has remained more or less stable since 2022. The number of countries using such methods does appear to be increasing, which could be due not only to the changing world order but also to an improved understanding of state threats.

The RWG container terminal on Rotterdam's Second Maasvlakte.

Economy

State actors employ legitimate and covert economic instruments to achieve their (geopolitical) goals. When the primary objective is to advance their own economic position, instruments such as acquisitions and investments can also be used to achieve other strategic objectives. Moreover, the economy is closely linked to geopolitics. Strategic dependencies are used as a means of political or economic leverage.

More and more countries are also pursuing protectionist economic policies with trade barriers and restrictions on the trade of technological knowledge and goods. Many countries are deploying economic instruments, with China as the most prominent example. Since the inauguration of US President Trump, the United States has increasingly used economic instruments.

Unwanted knowledge and technology transfer, or acquisition, can also be used for economic as well as military purposes. This threat was already high, but due to sanctions against countries, state actors are seeking alternative ways to acquire technological knowledge. Because of the imposed sanctions, state actors are more likely to resort to covert acquisition. Both economic instruments and technological knowledge are means to increase political and military power.

Strategic dependencies used as leverage

Many countries strive for a strategically autonomous economy. Dependence on a product or service from another country can entail significant risks, especially if it involves high-risk strategic dependencies. This is the case when the product, service, or technology in question is crucial to the functioning of public interests, such as the economy and society, or the dependency poses a risk to the continuity of vital processes or access to sensitive information by third parties. The risk of supply interruptions depends, among other things, on the degree of

market concentration and the possibility of substitution, the nature of relations with the country and the degree of mutual dependence.[55]

Countries are using dependency relationships as strategic leverage. One example is Russia, which is openly and secretly assessing how it can protect its interests in the changing energy market and delay the energy transition. This way, it aims to maintain its dependence on fossil fuels for as long as possible. Shortly before and after the outbreak of the Ukrainian war, gas supplies from Russia to European member states were scaled back or stopped altogether to exert political, economic, and social pressure. This also affected many Dutch citizens financially through higher energy bills and the associated inflation. The European Union has now largely reduced its energy dependence on Russia.

Western dependence on China

China is also developing its own industrial and supply chains to reduce its dependence on global value chains. At the same time, other countries are becoming more dependent on China by increasingly setting technological standards, driving competitors out of the market by scaling up production, and investing heavily in key technologies. This offers China economic advantages and the opportunity to exert influence on other countries. When a so-called *lock-in effect*Based on the standards set by China, other countries must build on these standards, allowing the state actor to assume an increasingly dominant position. Lock-in effects can lead to risky strategic dependencies, for example, if the Netherlands becomes dependent on Chinese technologies and suppliers for vital infrastructure, such as energy supplies, telecom networks, water supplies, and transport infrastructure.

The West's dependence on China is undeniable, particularly in the areas of sustainability, such as green technology, and raw materials. The country has emerged as a vital player in the global energy transition and has acquired a dominant position in green technology supply chains. For example, the European Union and the United States are largely dependent on Chinese solar panels, wind turbines, and batteries, as well as the related technologies and raw materials required for these, for the short and medium term. Furthermore, China holds a monopoly on the mining and processing of a large number of raw materials. This includes raw materials that play a significant role in, among other things, the digital and space domains. China can leverage this dependence to exert pressure on
other powers.

Trade conflicts force the Netherlands and the European Union to act

More and more countries are pursuing protectionist economic policies. They do this, for example, by supporting their own companies with financial incentives or by erecting trade barriers against foreign companies or governments. Trade in technological knowledge and goods is hampered to protect their own security and economic and technological development—and thus their geopolitical power—to diminish that of another country, or to punish another country for certain activities. For example, the Netherlands has implemented export restrictions for national security reasons.

imposed on the semiconductor industry. In turn, China has imposed export restrictions on certain raw materials that the West depends on for semiconductor production.

The United States is also deploying economic instruments. With the inauguration of President Trump, a trade conflict between the United States and the European Union has become more likely. Moreover, economic tensions between the United States and China have escalated recently, partly due to the widespread use of economic instruments such as the imposition of import tariffs. Countries like the Netherlands also run the risk of being dragged into this situation; the United States will increasingly force partners to comply, especially on technology issues. The Netherlands will continue to pursue its own national security considerations in cooperation with its European partners. In both cases, trade conflicts highlight the vulnerability of European supply chains: many European governments and companies are dependent on Chinese and American suppliers within their supply chains. This could place the European Union in a difficult position if one of these countries wants to decouple itself from the other and demands the European Union do the same. Furthermore, a trade conflict can be used to exert diplomatic pressure and lead to trade disruptions, price increases, and a loss of markets. This affects the competitiveness and earning capacity and therefore the prosperity of the Netherlands.

Technology acquisition is crucial for power struggles

Technology and technological developments are central to the power struggle between state actors. Whoever controls key technologies, such as biotechnology, quantum technology, artificial intelligence, and semiconductor technology, also has a geopolitical influence and creates a strong starting position for their future earning power. There is therefore a so-called global*tech race*The current situation is particularly pronounced between the United States and China. Countries seeking to lead the way in technological development are investing heavily. The Netherlands and the European Union are falling behind in an increasing number of technological areas, posing risks to our security and economy. This creates concentrations of economic power among countries that successfully develop technologies, which can be detrimental to Dutch earning capacity. Risky strategic dependencies are also emerging. Furthermore, knowledge and technology from the West can be used to develop weapons systems and espionage capabilities, or for surveillance equipment that jeopardizes human rights.

When countries lack the knowledge and technology needed for their geopolitical ambitions, they actively seek it abroad. Several countries are attempting to acquire European and Dutch knowledge and technology, both in the academic and private sectors. This can happen openly, for example, through acquisitions, joint publications, talent recruitment, grants, and international forums. However, it can also occur illegally, through (digital) espionage, opaque investments that conceal state intervention, or the circumvention of export restrictions.

A well-known way for state actors to acquire knowledge and technology is by using individuals already employed at a knowledge institution or company. These are also known as insiders.*insider threat*The threat posed by these insiders is the ability to leak knowledge and technology to state actors through legal or illegal means. State actors can, for example, require students to return to their home country after graduation as a condition for receiving a scholarship. This increases the likelihood that the knowledge acquired in the Netherlands will be transferred to the government or affiliated organizations. In some cases, this may involve sensitive knowledge and technology, such as dual-use technology for both civilian and military applications. Moreover, foreign intelligence officers in the Netherlands can also illegally build their own network of human resources to acquire knowledge and technology. This network can consist of both Dutch and foreign individuals.[56]

The covert acquisition of our knowledge and technology threatens the knowledge security of Dutch educational and research institutions, the ability of companies to innovate and generate revenue, and the effectiveness of the armed forces. It can also contribute to the Netherlands' increasing strategic dependence, including in the area of vital infrastructure. Given the increased focus on knowledge and technology as a means of geopolitical power and the global tech race, this threat will persist in the coming years and may even increase as long as the Netherlands maintains leading positions in certain technological domains. Knowledge institutions may also lose their strategic leadership position in the medium term.

There are also concerns about the ways in which state actors and affiliated companies collect (personal) data from citizens. This happens, for example, through (free) apps, (cheap) products and services, or the purchase of personal data. This personal data can be useful for technological developments, but can also be misused when state actors use the personal data and related data on a large scale to conduct analyses on population groups.

China is the biggest threat to Dutch economic security and knowledge security

For years, China has posed the greatest threat to Dutch companies and knowledge institutions in terms of economic and knowledge security. Chinese President Xi Jinping explicitly considers knowledge and innovation to be at the service of China's national security. The Chinese government strives to become a leading nation in the world, intertwining economic and technological goals with military and other security objectives. President Xi wants the country to eventually be self-sufficient and technologically independent of foreign countries. The development of advanced technologies such as semiconductors, artificial intelligence, and quantum technology is essential for this.

There is a strong overlap between China's technological needs and topics also being researched by Dutch knowledge institutions and the private sector. Individuals and institutions with ties to the Chinese military-industrial complex continue to reach out to Dutch knowledge institutions to conduct joint research on dual-use technologies, such as artificial intelligence. In practice, the search for the right balance continues: the exchange of technological knowledge is (economically) important, but therefore also carries risks. The Chinese government continues to invest enormous sums of money in bringing people with high-quality knowledge and skills to China or otherwise making their knowledge available to Chinese interests through so-called talent recruitment programs.

Chinese scientists seek rapprochement with Dutch knowledge institutions
Between 2012 and 2022, more than ninety Chinese (military) scientists gained knowledge at Dutch knowledge institutions. In 2021, a Chinese scientist obtained his doctorate from a Dutch technical university, where he conducted research on hypersonic aircraft. The scientist studied in China at the Air Force Engineering University (AFEU), a branch of the People's Liberation Army that provides technical training and air combat training. After receiving his doctorate in the Netherlands, the scientist was given a permanent position at the AFEU. His research has both civilian and military applications. The knowledge can be applied in space research, but also in the development of hypersonic weapons.[57]

The Netherlands is the target of technological acquisition activities by Russia, Iran and North Korea. Russia, Iran, and North Korea are also attempting to acquire technological expertise in the Netherlands to expand their dominant position. Russia, for example, focuses on developing military applications for various technologies—an ambition intensified by the war in Ukraine. International sanctions hinder access to sensitive technology and equipment. Therefore, Russia attempts to acquire this technology covertly, for example, by deploying front companies to circumvent export restrictions. There have been recent examples in the Netherlands where individuals and companies have evaded the sanctions regime against Russia and supplied dual-use goods to Russian companies. This is happening both directly and indirectly, via "conduit countries" such as Armenia, Kazakhstan, Turkey, and Turkmenistan.[58]This includes computer components, drones and chips.

Russian engineer suspected of industrial espionage
A Russian engineer has been facing legal action since 2024 on suspicion of industrial espionage at ASML. He is alleged to have stolen microchip manuals and then shared them via email, chats, and online files. He also allegedly made brief visits to Russia where he may have physically handed over more information. This knowledge transfer may have advanced Russian chip technology.[59]

Iran also seeks to acquire knowledge and technology in the Netherlands and other Western countries, including through covert acquisition networks, knowledge institutions, and students and researchers. This primarily concerns knowledge and technology for the development and maintenance of ballistic missiles. North Korea gathers information about scientific research and international political positions. Information has also been stolen from organizations focused on high-end (military) technology, including organizations in the Netherlands.

Tensions surrounding Taiwan could hit the Dutch economy

On the other side of the world, tensions are rising around Taiwan. China remains committed to uniting Taiwan with the mainland and gaining control over the vast majority of the South China Sea. Although China has not yet crossed the threshold of an armed conflict with Taiwan, the number and scale of Chinese military and paramilitary exercises, patrols, and reconnaissance have been increasing in recent years. A crisis there would have a direct and significant impact on the Netherlands. The maritime trade routes through the South China Sea and the Taiwan Strait are crucial for the Netherlands as a trading nation and the global economy in general. Furthermore, Taiwanese companies are essential in the production of semiconductors. This makes the island a critical link in the production chains for civilian and military electronics. The economic impact of a conflict is difficult to predict, but would likely be significant.

Meaning for the Netherlands

- *The use of economic instruments by state actors can have major consequences for the Netherlands. In the short term, life can become more expensive due to increased energy prices and trade conflicts. In addition, trade barriers contribute to Dutch companies becoming less productive and to a structural decline in competitiveness (possibly). Trade conflicts and*

  Export restrictions on certain raw materials or (semi-)finished products can have negative consequences for both the Dutch economy and our leading position in certain technological domains. This can lead to the Netherlands becoming more dependent on other countries.

- *The use of economic instruments by countries like China remains high and serious. The risk of trade conflicts has increased since US President Trump took office. The imposition of sanctions against the trade in technological knowledge and goods contributes to state actors feeling more compelled to resort to covert acquisition. The Netherlands, due to its leading position in several sectors, will remain an attractive target for state actors.*

Technology is increasingly central to geopolitical power dynamics. This is leading to a global tech race, with significant investments in key technologies worldwide. The Netherlands and the European Union are increasingly falling behind in emerging technology areas. This creates strategic dependencies and could undermine our security and prosperity.

- *The deployment of economic resources also affects the effectiveness and sustainability of our armed forces. Access to crucial technologies from Taiwan, for example, could be threatened by escalating territorial and trade conflicts.*

  Technological acquisition can also have far-reaching consequences. When other countries gain access to the same technological knowledge, they can become stronger, while the effectiveness of our armed forces can decline.

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

Diplomatic and political

Countries are increasingly willing to actively use their power to defend their interests within international institutions and partnerships. While this is nothing new, the changes in the global order appear to be having an increasingly powerful impact. Countries are using these opportunities to gain power and better represent their interests. This could contribute to the decline of Dutch influence on the international stage.

State actors view international institutions and alliances as a means to gain influence, for example, by undermining their effectiveness and credibility or by changing the prevailing frameworks and norms. Such bodies can also be targeted by state actors, which can undermine the continuity and independence of international legal institutions and thus directly threaten the international legal order. Finally, to increase their influence, non-Western countries establish alternative institutions and partnerships over which the West has limited or no influence.

Influencing existing institutions

Several countries are dissatisfied with the existing global order, based on Western rules, and want to align it more closely with their own interests. For example, various state actors are seeking to reduce or replace American hegemony and to replace the current model of the international legal order. The United States also takes a different stance on the international legal order than in recent decades. As a relatively small player with an open economy and limited military resources, the Netherlands actually benefits from an international order based on law rather than power.

Countries attempt to gain influence by influencing existing institutions from within and without. For example, several states use their veto power in the United Nations Security Council to block resolutions that align with UN objectives. In doing so, they undermine the effectiveness and credibility of the United Nations. For example, in 2024, Russia blocked oversight measures regarding international sanctions against North Korea. The North Korean supply of weapons and manpower to Russia for the war in Ukraine is a plausible explanation for this.

the Russian veto.[60]Since the outbreak of the Gaza War in 2023, the United States has vetoed several Security Council resolutions concerning a ceasefire in Gaza. This is not new; the five permanent members of the Security Council often use their veto power to serve their own geopolitical interests; three-quarters of all vetoes issued since 1989 have come from Russia and the United States.[61]

One consequence of the shifting power dynamics is that more countries are attempting to influence the frameworks and norms of international bodies and institutions from within by taking positions within these bodies. For example, China is attempting to appoint Chinese nationals to key positions within the United Nations, starting from the director level. In this way, it hopes to increasingly integrate Chinese interests and views within the UN, thereby adapting the international legal order to a model favorable to China.

Institutions as targets of state actors

International institutions and partnerships can be targets for state actors due to their function, role, and the interests countries have in them. This can involve thwarting that role or acquiring valuable information. Examples include the Russian hacking attempt on the OPCW in 2018 and the disruption by the AIVD (General Intelligence and Security Service) in 2022 of a Russian intelligence officer who was seeking an internship at the International Criminal Court in The Hague.[62]Although the Netherlands was not the primary target, such activities by state actors affect the Dutch democratic constitutional state, of which these institutions are part.

Well-known targets of state interference are international institutions present in the Netherlands, such as the International Criminal Court and the International Court of Justice.[63]The United States and Israel publicly threatened the court, and the United States imposed sanctions.[64]This could damage or even halt the court's work, partly because the court may have limited or no access to financial services. Currently, sanctions have only been imposed against a chief prosecutor due to the court's arrest warrants for the Israeli prime minister and former defense minister. However, further expansion of the sanctions list is realistic in the long term. The US sanctions could have far-reaching consequences for the court's functioning in the long term, and thus for the prosecution and trial of individuals suspected of committing international crimes such as genocide, crimes against humanity, or war crimes.[65]The courts are also an interesting target for espionage and subversive influence for a large number of countries, because their subjects can be tried there.

These kinds of activities can undermine the continuity and independence of international legal institutions; they thus pose a direct threat to the international legal order. Moreover, they impact the Netherlands, due to the cooperative relationship and because the host country is responsible for the security of the courts. When the Netherlands provides information to such institutions and it reaches state actors through clandestine channels, this also affects national security.

Parallel institutions 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 establishing new partnerships in which the West has limited or no influence, countries attempt to expand their geopolitical influence. Moreover, they can counterbalance existing political spheres of influence, such as the United States or the European Union, and thus restructure or at least diversify the global order. China presents itself as the leader of the "Global South." Through its pioneering role within these institutions and by launching global initiatives in infrastructure, development, and security, China has created a "diplomatic order" that parallels Western consultative bodies like the G7. Every country has the right to initiate alternative partnerships and thus become more influential, but this can ultimately undermine or undermine existing international institutions—in which the Netherlands represents its interests. Consequently, the Netherlands' international influence may decline unless it joins forces on certain fronts or initiatives.

Mid-sized states and emerging players play a key role in establishing alternative partnerships. These countries are aware of their increased strategic importance and are exploiting the rivalry and conflict between the major powers.[66]This was evident, among other things, in 2023, when more than forty countries expressed their interest in joining BRICS, an economic alliance aimed at countering Western hegemony over the global economy. The alliance, now expanded to five countries, has gained further strategic importance in recent years. BRICS countries are increasingly wielding economic power; more than fifty percent of the world's population lives in these countries. Moreover, some countries are increasingly united by anti-Western sentiment, despite their political, geographical, and cultural differences. At the same time, the divergences of interest and hostility between various BRICS countries remain significant, and there is no consensus on their stance toward the West.[67]Some countries are trying to overhaul much of the international legal order, while others are trying to reform certain aspects of the existing global order.

Looking for collaboration

Finally, within existing and new partnerships, countries attempt to win over other actors to pursue their own goals, potentially shifting global or regional power dynamics. Countries occasionally receive economic, political, or military benefits in exchange for support. For example, Russia, China, Iran, and North Korea are increasingly collaborating militarily and diplomatically, further undermining the current international legal order. These partnerships, however, are neither self-evident nor smooth. Several countries, including China and Russia, are strengthening their ties with African countries. While the Chinese presence is primarily focused on economic investments, including infrastructure projects, Russia seeks cooperation within the security domain. In return, Russia regularly receives support from various African countries in international forums such as the United Nations, for example, in relation to the war in Ukraine.

Russia increasingly active in Africa

Russia has steadily expanded its (para)military presence in Africa in recent years and intends to become even more active on the continent. If a ceasefire is reached in Ukraine, it is likely that Russia will free up military equipment and personnel for deployment in Africa. The Russian (para)military presence in Africa is part of Russia's (hybrid) geopolitical struggle as a systemic rival to the West. Africa forms the southern flank of the European portion of NATO territory.

The Russian (para)military presence there could potentially pose a threat to NATO units and the critical infrastructure and supply lines on which they depend. Russia also undermines the West militarily in Africa: French and American troops have been forced to withdraw by pro-Russian regimes. Furthermore, Russia pursues economic interests by gaining access to vital raw materials or attempting to deny them to the West. Finally, the Russian (para)military presence in countries influences the security situation there, for example, in the fight against jihadism.

Meaning for 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 prime target for espionage and subversive influence. Moreover, foreign threats and sanctions against international courts can also have an impact on the Netherlands. For example, countries can decide to impose sanctions that also*

  Dutch citizens may be affected or visa applications from Dutch citizens may be rejected.

- *The influence of existing institutions and the establishment of parallel institutions are consequences of the changing power relations. Countries like China use these opportunities to gain power and better serve their interests. Such developments can contribute to the Dutch influence on the international*

  scene decreases.

Endnotes

1 AIVD, MIVD, and NCTV, 'Threat Assessment State Actors 2', November 2022, p. 7; National Security Analysts Network (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, 'Risk Assessment Guide for the National Security Risk Analysis for the Government', 2022; NCTV, 'Security Strategy for the Kingdom of the Netherlands 2023-2029', 2023, pp. 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', November 14, 2023.

6 Ministry of Economic Affairs, 'Letter to Parliament with the Cabinet's response to the long-term space agenda', February 21, 2025.

7 Ministry of Foreign Affairs, 'Letter to Parliament regarding the introduction of space security policy', March 5, 2021.

8 Ministry of Defense, 'Defense Spatial Agenda', November 2022.

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

10 Organization 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', February 14, 2025; OPCW, 'Report of the OPCW Technical Assistance Visit on the Activities Carried Out in Support of a Request by Ukraine', November 18, 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, November 1, 2024; 'The nuclear fatwa that wasn't: How Iran sold the world a false narrative', The Atlantic Council, May 9, 2024; Michael Eisenstadt and Mehdi Khalaji, 'Iran's flexible fatwa: How "expediency" shapes nuclear decision making', The Washington Institute for Near East Policy, February 4, 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)', May 27, 2024.

14 "OM: Top employee of the National Coordinator for Counterterrorism spied for Morocco," De Volkskrant, February 7, 2024; "NCTV and police employees arrested," Public Prosecution Service, November 1, 2023.

15 AIVD, 'Offensive Cyber Program: An Ideal Business Model for States', June 2019.

16 AIVD and NCTV, 'Across the Border: State Interference in Diaspora Communities in the Netherlands', October 2024.

17 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 AIVD and MIVD, 'Threat assessment: military and hybrid threats', December 2024.

19 Ministry of Infrastructure and Water Management, "Parliamentary Letter on the Progress of the North Sea Infrastructure Protection Strategy," June 10, 2024; MIVD, "Annual Report 2023," April 2024; MIVD and AIVD, "24/2 - The Russian Attack on Ukraine: A Turning Point in History," February 2023.

20 AIVD and MIVD, 'Threat Assessment: Military and Hybrid Threats'.

21 NCTV, 'Cybersecurity Assessment Netherlands 2024', October 2024.

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

23 America's Cyber Defense Agency, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities," December 18, 2024; "US Offers $10 Million for Information on Water Company Attackers," security.nl, August 8, 2024; "US Reports Attack on US Water Board's Industrial Control System," security.nl, November 29, 2023.

24 AIVD and NCTV, 'Across the Border'.

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, 'Across the Border'.

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

28 AIVD and NCTV, 'Over de grens' (Across the border); '23 years and 6 months in prison for murder of Iranian man in Almere in 2015', Court of Appeal of Leeuwarden and Arnhem, Rechtspraak.nl, November 24, 2022; 'Liquidation of Iranian activist Ahmad Mola Nissi (52)', Opsporing Verzocht, June 30, 2019; 'Rotterdam criminals behind murder of Iranian activist', RTV Rijnmond, July 3, 2018.

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

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

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

32 'Shooting at defense company in Gothenburg; latest in series of anti-Israeli attacks', De Volkskrant, October 10, 2024. 'Two Swedish teens arrested in Copenhagen in connection with Israeli embassy blasts', Euronews, October 3, 2024; 'Israeli embassies increasingly targeted by violence', Trouw, October 3, 2024; 'Iran may be behind attacks on Israeli embassies, Sweden says', BBC News, October 2, 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, October 13, 2024; 'Swedish gangs as intermediaries for Iran – this is what has happened', Swedish Herald, update October 4, 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, February 15, 2024.

35 Iran is hunting Israeli targets and opponents in Europe: "I knew they were going to send someone," says the dissident from Haarlem, NRC Handelsblad, September 5, 2024.

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

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

38 'Chinese confidant Prince Andrew expelled from UK as spy', NOS, December 13, 2024.

39 "Police search MEP Krah's office in espionage case," NOS, May 7, 2024; "AfD list leader in Brussels stays on and says he will fire arrested employee," NOS, April 24, 2024.

40 AIVD and NCTV, 'Across the Border'.

41 Idem.

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

43 "Not the 'green activists,' but the Russians were behind German exhausts full of foam," NRC Handelsblad, February 5, 2025; "Germany's Sabotage Series Offenbar von Russland Gesteuert," Der Spiegel, February 5, 2025.

44 Russia Uses 'Freelance Agents' for Hybrid Warfare, 'Like Uber', Het Nieuwsblad, January 17, 2025.

45 Christopher Houtkamp, Nienke van Heukelingen, Teun van der Laan, 'Patriotism Meets Pragmatism: Turkish Diaspora Policy in the Netherlands', Clingendael, 2024, p. 11.

46 Ditto, p.12.

47 Christopher Houtkamp, Nienke van Heukelingen, Teun van der Laan , Erwin van Veen, 'The Turkish diaspora policy in the Netherlands: Research into the perspective of the Turkish-Dutch communities and the diaspora policy of Turkey', Clingendael, 2023, p.2.

48 Ministry of Justice and Security, 'Letter to Parliament: Report of the Israeli Ministry of Justice and Security', November 29, 2024

49 Parliamentary Papers II, Session Year 2024, 36651-34; 'Diplomatic slap on the wrist for Israeli report full of accusations', NRC Handelsblad, November 29, 2024

50 Israel calls peace activist Thomas van Gool a key figure in Hamas-affiliated network, now he's being threatened, Het Parool, November 24, 2024.

51 AIVD, 'Offensive Cyber Program'; NCTV, 'Cyber Security Assessment Netherlands 2024', p. 44. AIVD

52 and NCTV, 'Across the Border'.

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

54 Microsoft, 'Microsoft threat intelligence report: Iran steps towards US election 2024 with cyber-enabled influence operations', August 9, 2024, p.1-4; Steven Lee Myers, Tiffany Hsu, and Farnaz Fassihi, “Iran Emerges as a Top Disinformation Threat in US Presidential Race,” New York Times, September 4, 2024; 'OpenAI blocks Iranian influence operation that abused ChatGPT', Dutch IT Channel, August 21, 2024.

55 Ministry of Economic Affairs and Climate Policy, 'Cabinet Approach to Strategic Dependencies', May 12, 2023. AIVD and

56 NCTV, 'Across the Border'; AIVD, MIVD, and NCTV, Threat Assessment of State Actors 2, p. 34.

57 China is sending dozens of targeted military researchers to the Netherlands to gather sensitive knowledge, Follow the Money, May 20, 2022.

58 Dutch companies appear to be circumventing Russian sanctions, with extensive trade with "escape countries," De Volkskrant, December 10, 2024.

59 AIVD: Arrested ASML employee was in contact with Russian intelligence service, Trouw, February 6, 2025; Russian former ASML employee suspected of stealing trade secrets, Nieuwsuur, December 6, 2024.

60 "Russia blocks UN sanctions on North Korea," NOS, March 28, 2024.

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

62 "MIVD: We prevented Russian hack of OPCW in The Hague," NOS, October 4, 2018; "AIVD: Infiltration of Russian spy at ICC prevented," NOS, June 16, 2024.

63 AIVD and NCTV, 'Across the Border'.

64 "International Criminal Court condemns US sanctions against employees," NOS, February 7, 2025; "US threatens revenge against The Hague Criminal Court," BNR, April 30, 2024.

65 NOS, "79 countries condemn US sanctions against International Criminal Court," February 7, 2025.

66 ANV, "Main report Trend Analysis National Security," 2024.

67 Idem.

July 2025
This publication is a joint publication of:

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

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

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