Threat Assessment State-sponsored Actors 2

November 2022

AIVD, MIVD and NCTV

Contents

Executive Summary

This Threat Assessment State-sponsored Actors (TASA) is a joint analysis of the the General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst – AIVD*), the Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst – MIVD*) and the National Coordinator for Counterterrorism and Security (*Nationaal Coördinator Terrorismebestrijding en Veiligheid – NCTV*). It offers an insight into which national security interests are or could be harmed by state and state-sponsored actors and the form that this could take (from now on the term state actor will be used). The aim of the threat assessment is to increase awareness of the nature and scope of the threat from state actors. The purpose of this document is to steer (policy) efforts to counter these threats.

State actors are increasingly threatening national security interests in various ways. This is partly being driven by key geopolitical developments. The most notable and concerning development is the war in Ukraine, which is affecting various national security interests. The Netherlands is increasingly also facing threats to its economic security. This threat has existed for some time, but it has come into ever sharper focus during the past few years.

This TASA addresses four key messages:

1. The territorial security of the EU, NATO and the Netherlands is under further pressure

The war between Russia and Ukraine and its consequences are a major cause of the increased threat in respect of the territorial security of the EU, NATO and therefore the Netherlands. The war has placed significant strain on relations between Russia and the West. Although Russia probably has no intention of engaging in a military conflict with NATO countries, its rhetoric threatening nuclear warfare is increasing the risk. In addition, the threat to Dutch digital integrity is still as high as ever as the Netherlands is still the target of offensive cyber programmes from state actors.

2. The social and political stability of the Netherlands is still being impacted by state-sponsored interference

The Netherlands and its allies are still the target of intelligence activities and (covert) influencing activities by state actors. Digital and physical espionage is a major problem. Government authorities in the Netherlands, the EU and NATO are the target of such activity. Furthermore, state influencing activities, deliberate or otherwise, are putting a strain on cohesion within Dutch society. In addition, diaspora communities and opponents of authoritarian regimes are the target of various open and covert forms of influencing and interference from their countries of origin.

Threat Assessment State-sponsored Actors 2

3. The Netherlands is increasingly facing open and covert threats against its economic security

The threat to economic security has become more pronounced than ever over the past few years. The threat to economic security is three-fold. Firstly, critical processes continue to be vulnerable to sabotage and, due to investments and takeovers, to the unwanted influence of state actors. Secondly, there has been an increase in the abuse of risky strategic dependencies. European dependency on Russian gas has shown this all too clearly recently. Finally, Dutch companies, knowledge institutes and researchers are being widely targeted by (digital) activities that are attempting to capture high-end technology, for example through cyber espionage or by circumventing export restrictions. The theft and leaking of knowledge pose a risk of unfair competition and undesirable end use, for example for military purposes. China represents the greatest threat to Dutch knowledge security.

4. The international rule of law is increasingly coming under pressure

The international rule of law is coming under increasing pressure. It is being questioned by various state actors and portrayed as a Western construct, and is therefore systematically compromised. International norms such as non-intervention, non-proliferation and peaceful settlement of disputes are also being violated and international institutions are increasingly being used as a platform on which state actors are attempting to undermine the international rule of law.

There is a close link between the threats described in this threat assessment. This means that the activities of state actors are impacting, or may impact, multiple national security interests. The interwoven threats described below, combined with current geopolitical developments, mean that an integrated approach to increasing resilience is more important than ever.

Introduction

The Threat Assessment State-sponsored Actors (herein referred to as TASA1) produced by the General Intelligence and Security Service (AIVD), the Military Intelligence and Security Service (MIVD) and the National Coordinator for Security and Counterterrorism (NCTV) was published in January 2021.[1] A new version of this threat assessment is now available. This assessment details the main developments since January 2021. The Threat Assessment State-sponsored Actors 2022 (hereinafter referred to as TASA2) reflects the joint vision of AIVD, MIVD and NCTV with regard to state actors to national security interests. The aim of the TASA2 is to increase awareness of the nature and scope of the threat from state actors. The purpose of the TASA2 is thus to steer (policy) efforts to counter these threats.

As with the TASA1, the focus in this threat assessment is on national security interests. To this end, the TASA2 explores a number of national security interests: territorial security, social and political stability, economic security and the international rule of law.[2] This methodology allows various threats to be clustered in themes, thus revealing general trends.

Since the publication of the previous threat assessment, a few important international developments have occurred that impact national security interests. The most notable and concerning development is the war in Ukraine. This armed conflict between two nation states is affecting various national security interests and is therefore mentioned in several places in this threat assessment. As the threat to economic security has increased, this subject features prominently in the TASA2. The threat in relation to economic security has existed for some time, but it has come into ever sharper focus during the past few years. This threat is affecting large parts of Dutch society. In many cases, it is a latent threat that is not immediately recognised as as such by everyone, or only takes a longer period of time to have a visible impact. Countering this threat requires a broad societal effort by parties concerned that goes beyond the traditional security sector. To bring this threat to the attention of a wider audience, the TASA2 goes into economic security in more depth.

1 Threat Assessment State-sponsored Actors, AIVD, MIVD and NCTV, February 2021.

2 Ecological security has not been included in this threat assessment. Threats to physical security interests have been included under the national security interests of territorial security, social and political stability and economic security.

Threats from state actors

Coercive, undermining, misleading, or covert activities by or on behalf of state-sponsored actors, below the threshold of armed conflict, which could harm the national security interests of the Netherlands through a combination of pursued goals, used means, and associated effects.

Reading guide

The following chapters will set out the main developments in the threats from state actors for four areas of national security interests since the TASA1. The chapter on economic security goes into more depth and sets out why economic security is becoming ever more important, why specifically the intentions of a few state actors represent a threat to economic security and how these state actors are using their weapons of power to threaten security.

Threats from state actors and the interests they threaten must be considered in their related context in order to be able to understand them. This relationship between the various threats and national security interests will be examined in the final chapter of this threat assessment.

It is important to state that national security interests are being threatened in a number of ways and by multiple state actors. However, in order to describe the threat in concise terms, the TASA2 is focusing on the main threats and the analysis is therefore not exhaustive. Readers will therefore notice that there is a strong focus on Russia and China in this threat assessment. These state actors currently pose the greatest threat to national security interests, be this in a number of different ways.

Territorial security of the EU, NATO and the Netherlands under further pressure

The war between Russia and Ukraine and its consequences are a major cause of the increased threat in respect of the physical integrity of NATO and EU territory. In addition, the threat against Dutch digital integrity remains as high as ever. For these reasons, territorial security of the European Union (EU), NATO and the Netherlands has come under further pressure since the TASA1.

Increased pressure on the integrity of EU and NATO territory

The Russian invasion of Ukraine and the ensuing war has placed significant strain on relations between Russia and the West. Russia probably has no intention of instigating open warfare with NATO countries. Russian rhetoric threatening the use of nuclear weapons and the modernisation of its weapons systems does increase the risk, contributing to instability. However volatile Venezuela's politics may still be, it is unlikely that this country will harm the territorial integrity of the Kingdom of the Netherlands.

Territorial security interests

'The unimpeded functioning of the Netherlands and its EU and NATO allies as independent states in the broader sense, or territorial security in the narrower sense.'

Territorial security concerns not only the integrity of our national territory and that of our allies, but also the integrity of the digital domain: the availability, confidentiality and integrity of essential information services and infrastructure and processes that depend on this.

Relations between Russia and the West under strain as a result of Ukraine war

The war in Ukraine represents the first major armed conflict between two countries on European soil since 1945, pushing relations between Russia, the EU and NATO to a new low. Although it is difficult to predict how the war in Ukraine will play out, it is possible that there will be a long-term armed conflict in Europe with features of a hybrid conflict. This is about more than an armed conflict between Russia and Ukraine: it is a conflict over spheres of influence, with Russia trying to impose its will, or annex parts of its former sphere of influence by economic and military means. Russia purports to be defending itself against the increasing expansion of the West as represented by NATO. However, Russia probably has no intention at this point of instigating open warfare with NATO countries.

In the same way that the West's perception of the threat from Russia has increased as result of Russia's invasion of Ukraine, the West's response to this invasion has increased the threat Russia feels from the West. The war in Ukraine has resulted in a desire on the part of the EU to strengthen its common security and defence policy. This will boost the 'European' arm of NATO, although Europe remains heavily dependent on the United States (US) militarily. From Russia's perspective, the military assistance the West is giving Ukraine will contribute to the further militarisation of Russia's foreign and security policy. The forthcoming accession of Finland and Sweden to NATO will further increase Russia's perception of being encircled by NATO. This perception will in the long term be decisive in shaping relations between the Netherlands and Russia. Even after the war in Ukraine has ended (however that is brought about), Russia will continue to regard NATO as an existential threat.

Role of nuclear weapons in Russia's security thinking has increased risk

Despite the increased rhetoric from the Russian leadership threatening nuclear warfare, there is no indication to date that Russia actually wants to deploy nuclear weapons in Ukraine. Nuclear deterrence has always played a central role in Russian security thinking, whereas it has taken something of a back seat in the West. The role played by tactical and strategic nuclear weapons in Russian military attitudes towards coercion and deterrence makes the war in Ukraine particularly concerning, as it increases the risk of escalation.[3] Russia sees this war as a regional armed conflict, and from its perspective this then legitimises the use of tactical nuclear weapons.[4] In addition, Russia has been modernising its nuclear weapons systems since the beginning of this century. Some of these systems can have an extremely destabilising effect in crisis situations. Due to the short flight times and the uncertainty surrounding the loader, these systems are putting pressure on decision-making processes.

Development of weapons and modernisation of Russian armed forces contributing to instability

Russia is investing in new weapons systems that can have the effect of increasing instability. Russian capability to engage in electronic warfare has improved significantly in recent years, enabling Russia to locally and temporarily disrupt communications, navigation and radar systems in a coordinated manner. This and other capabilities, such as anti-satellite weapons enable the military information position and therefore strength of the NATO alliance to be undermined and societies to be disrupted. In addition, Russia is investing in replacing its existing missile systems with new, more advanced systems. Specific hypersonic missile systems are an increasing priority for Russia.

Although the modernisation of Russian warfare is concerning, Russia is fighting against labour shortages, obsolete production equipment, corruption and cash shortages. The Russian invasion of Ukraine and the ensuing packages of sanctions imposed by the West are having a significant negative impact on the increasing modernisation and development of Russian warfare.

3 Strategic nuclear weapons are designed to destroy the economic and military potential and political will of opponents and have an intercontinental range. Tactical and therefore non-strategic nuclear weapons are particularly intended to achieve a (localised) military effect during a military operation.

4 Russia categorises armed conflicts on the basis of objectives, scope and intensity. A local conflict is regarded by Russia as a war with limited military and political objectives, conducted within the borders of the country concerned. The threat of using tactical nuclear weapons fits such a conflict, within the Russian perspective of conflict and deterrence. Since the beginning of the 21st century, actual deployment of tactical nuclear weapons has been linked by Russia to a regional conflict, involving a war with significant military and political objectives, between multiple countries within a region, with the involvement of a (regional) superpower or alliance. In the case of a major armed conflict, a war between alliances or global superpowers in which the warring parties are pursuing absolute military and political objectives, the use of strategical nuclear weapons is an option for Russia.

Development of hypersonic missiles is a cause for concern

Hypersonic missiles are a new class of weapons that are set to blur the hitherto standard distinction between existing ballistic and cruise missiles. Hypersonic missiles can be fitted with either a nuclear or conventional loader. Interception is harder for hypersonic missiles than for other types of missiles due to the combination of their high speed, range, altitude, low visibility to missile defence systems and agility. As a result, opponents are forced to develop other sensors and countermeasures for missile defence to facilitate the requisite shorter response times. Hypersonic missiles are therefore a challenge for (Western) missile defence systems.

Venezuela still volatile

Venezuela, the Kingdom's largest neighbouring country, still represents a threat to the political, economic and social stability of the region, including the Caribbean parts of the Kingdom. The country has been in the midst of an economic and political crisis since 2017 and the ensuing insecurity and instability still persist today. The geopolitical interests of superpowers such as the US, Russia and China are still playing a role here, among other factors. In addition, the interconnectedness of organised crime and the Venezuelan armed forces in illegal drug, gold and arms trafficking in Venezuela is also having a destabilising effect on the region. It is still unlikely that this country will harm the territorial integrity of the Kingdom of the Netherlands. As it happens it is unlikely that the country will want to risk an armed conflict with the Kingdom of the Netherlands. There is still a chance of an unintentional escalation of a conflict through possible misinterpretations and incidents as a result of a decline in the professionalism of the military within Venezuela.

Threat to digital integrity of the Netherlands still high

As a result of the activities of state actors engaged in an offensive programme of cyber attacks aimed at harming the security interests of the Netherlands and the EU and NATO alliances, the digital integrity continues to be under pressure. Examples of countries with such a cyber programme include Russia, China, Iran and North Korea. In addition to this, cyber attacks on supply chains (supply chain attacks) and the exploitation of vulnerabilities in commonly used software products by state actors are keeping the threat to digital integrity at a continued high level.

The Netherlands still the target of cyber attacks from state actors

As the Cyber Security Assessment Netherlands 2022 states, cyber attacks by state actors have become the new normal.[5] Cyber capabilities are relatively cheap, scalable, difficult to attribute and produce a significant, often long-term result. State actors use these capabilities against a wide range of possible targets to reach political, military, economic and/or ideological targets. The Netherlands is facing significant threats in the digital domain that have the ability to do considerable damage. The greatest threat comes from China, Russia and, to a lesser extent, Iran and North Korea. For instance, China is deploying its cyber capabilities to obtain high-end technology, Russia is focusing on prepositioning for sabotage against critical infrastructure, while Iran, for instance, is engaging in digital espionage activities against universities and North Korea is known to be betting on digital currency theft to finance its state coffers. Depending on the capabilities of individual cyber actors and the intelligence services of these countries, they are capable of carrying out espionage or sabotage. This can represent a direct or indirect threat to the digital integrity of the Netherlands and its allies.

Cyber activities against supply chains threaten digital integrity

State actors are targeting their digital espionage activities on targets in the public and private sectors both within the Netherlands and abroad. As part of this, attacks have been launched on the digital parts of supply chains. An attack on supply chains targets one or more critical points in the chain. The actor can reach a large number of organisations through these crucial points. Such cyber attacks therefore not only have an impact on direct victims, but also on chains of suppliers, customers and citizens using the services provided by the affected organisations. Despite this broad scope, such attacks often have a limited number of targets. Although a few attacks targeting Dutch organisations have been identified, most of the organisations targeted have been outside of the Netherlands. However, these attacks have featured abuse of vulnerabilities in commonly used software products that are also used on an extremely large scale in the Netherlands within both the public and private sector. As a result, cyber attacks on supply chains result in a significant risk of the integrity of the digital infrastructure of Dutch organisations, and thus Dutch digital integrity, being breached.

5 Cyber Security Assessment Netherlands, NCTV, July 2022.

Vulnerabilities in software

Digital activities of state actors are targeted at, for example, ensuring rapid operationalisation of vulnerabilities in commonly used software products (referred to as zero-day or one-day vulnerabilities). A zero-day vulnerability is a vulnerability for which no patch is available yet, but which has been discovered by hackers and can be exploited. As soon as a zero-day has been publicised, it is called a one-day vulnerability. The software producers affected often do not have a security patch immediately available, which means that (state) actors can exploit these vulnerabilities in the meantime.

Ultimately, the Netherlands remains a key hub in global digital networks and infrastructure. It is attractive for many state actors, including emerging cyber actors such as Turkey, for example, to exploit Dutch ICT infrastructure, as this is of a high quality and it is relatively simple to hire ICT capacity. For instance, Dutch servers have been used in a number of international cyber attacks. In such cases, the Netherlands is serving as a springboard for state-sponsored attacks that could harm third-party countries, possibly including allies.

The social and political stability of the Netherlands is still being impacted by state-sponsored interference

State actors continue to engage in intelligence activities and (covert) influencing activities, targeted at the Netherlands and its allies. Furthermore, diaspora communities and opponents of authoritarian regimes are still the target of influencing and interference from state actors. For these reasons, state-sponsored interference impacting the social and political stability of the Netherlands is still an issue.

The Netherlands and its allies continue to be a target of intelligence and (covert) influencing activities

The intelligence and influencing activities of various state actors in the Netherlands constitute a persistent threat to social and political stability. As stated in the previous threat assessment, it is not possible to give an absolute indication of whether intelligence and influencing activities have increased or decreased. There have certainly been developments since then that have contributed to this threat.

Social and political stability interests

'Social and political stability concerns the unimpeded continued existence of a social climate in which individuals can function undisturbed and in which groups of people cohabit within the achievements of the Dutch democratic state and its shared values.'

Social and political stability consists of two main components: the democratic and lawful state and democratic society. The democratic and lawful state includes, for example, political and administrative integrity, the functioning of government and the free exercise of vertical basic rights such as freedom of worship and freedom of speech.

Democratic society includes, for example, (acceptance of) the legitimacy of the government, solidarity in society, free exercise of horizontal basic rights aimed at fostering mutual relations between citizens and free and independent media and academia. Whenever social and political stability is at risk, this means disruptions to the daily lives of the population, an attack on democratic institutions and norms and values and a disruption to the social and societal climate of Dutch society, such as polarisation and the emergence of enemy stereotypes.

The Netherlands is a target of political espionage

Digital and physical political espionage in which state actors seek to gather political intelligence represents a major problem for the Netherlands. Government authorities in the Netherlands are the target of (digital) espionage activities of state actors. Organisations of which the Netherlands is a member, such as the EU and NATO, are also major targets of state actors. These state actors use the Netherlands as a springboard to gather political intelligence about the EU and NATO.

The war in Ukraine has been a tipping point in the already poor relations between Russia and the Netherlands and its allies. Regardless of how the situation in Ukraine pans out, Russia's desire to gather intelligence is very unlikely to diminish. In response to the Russian invasion of Ukraine in early 2022, European countries declared more than 350 intelligence officers under diplomatic cover as persona non grata. 17 Russian intelligence officers were expelled from the Netherlands. These expulsions represented a serious setback for the Russian intelligence services. Russia will very likely attempt to rebuild its intelligence presence within diplomatic representations.

Influencing activities aimed at weakening the cohesion of Dutch society

The covert (political) influencing activities of various state actors in the West, including in the Netherlands, are wittingly and unwittingly placing a strain on the cohesion within Dutch society, the EU and NATO. Russia in particular is heavily engaged in covert influencing targeted against the West.

Russian efforts are focused, for example, on creating a picture pleasing to Russia: both in terms of public debate and in the political and administrative system. In addition, Russian efforts are focussed on undermining political unity in the West, for example by increasing existing divides. In doing so, Russia is not confining itself to a specific political movement in Europe, but instead opportunistically looks for opportunities for covert political influencing in the West. For instance, Russia sees an opportunity to use the economic uncertainties in Europe as a result of the war in Ukraine: it is attempting to covertly push the narrative that these uncertainties are the result of anti-Russian decisions of Western policy makers. Russia is able to deploy a wide range of means to do this and thus further polarise debate in society.

Although the main focus of Russia's activities in this field is currently in other countries, it is also focusing its efforts on the Netherlands. For example, attempts are being made in the Netherlands to cast doubt on both the facts of the downing of flight MH17 and the MH17 criminal trial.

The EU (member states), including the Netherlands, may come under political and social pressure from various neighbouring countries within the EU, as they are wilfully abusing, or triggering, migrant flows towards the EU. Belarus, for instance, has allowed migrants to travel to its own country only to deliberately let them through to (and across) the border with the EU. Belarus is therefore increasingly using migrants as a political weapon, including to put pressure on decision-making processes.

Large-scale harvesting of personal data by state actors concerning

State actors, including China, are gathering personal data on a large scale, both from open sources (for example, from social media profiles) and closed sources (for example, by hacking hotel chains, telecommunications companies or medical institutions). Personal data can be of use to state actors in a number of ways. The data is gathered primarily with a view to monitoring and identifying relevant persons and population groups for, among other purposes, recruitment and/or influencing purposes. China uses personal data obtained to discredit opponents with influencing operations through social media channels or to spread Chinese views. Although there has been extensive gathering of personal data in the Netherlands by China, there are as yet no indications of targeted Chinese influencing activities aimed at Dutch targets.

Such extensive gathering of personal data is concerning, including in the long term. In addition to usage for influencing purposes, large quantities of personal data can also be used to further develop technologies which can be used, for example, to increase military strength and espionage capabilities. .

Diaspora communities and opponents of foreign governments remain target of influencing and interference

Foreign forms of influencing and interference often focus on diaspora communities and opponents (for example, critics or political dissidents) of foreign governments. A state actor engages in influencing and interference activities to influence its target such that the target declares solidarity with the political objectives of the state actor – or by enforcing solidarity behaviour. As TASA1 outlined, influencing and interference activities can take various different open and covert forms, from influencing through (dis) information campaigns to intimidation or threats and even to the use of violence and assassination.

Diaspora communities in the Netherlands still targeted by countries of origin

Iran, China and Russia are engaging in diverse intelligence and influencing activities, targeted at, among others, the diaspora in the Netherlands. This is unchanged from the situation described in the TASA1. Within these communities there is often a need to maintain an ability to enter the country of origin as they still have family living there and they still hold assets there. There is also a tie to the country of origin due to cultural and religious beliefs. State actors can use and abuse this and implicitly or explicitly place pressure on the community to conform. This conformism can take different forms: from self-censorship in political debate to active involvement in intelligence services. In addition, state actors can mobilise members of diaspora communities to promote the interests of the country of origin, for instance by having them openly express certain views.

In addition to the three countries mentioned above, there are also various other state actors, including countries with a relatively large diaspora in the Netherlands, such as Morocco and Turkey, who are focussing intelligence and influencing activities on their diaspora. The extent of undesirable interference in diaspora communities may increase, for example when conflicts emerge in their country of origin or around the time of elections in that country. For instance, Turkish parliamentary and presidential elections in 2023, partly due to the Turkish diaspora policy, will have an impact in other countries, including possibly the Netherlands.

Intelligence and influencing activities impact the sense of safety felt within diaspora communities and can, particularly where large communities are involved, affect the mutual cohesion within these communities. In addition, such activities can cast doubt on the loyalty of certain groups and lead to mistrust within Dutch society.

Opponents of authoritarian regimes are at increased risk

Opponents of authoritarian regimes, for example (political) dissidents and critics, are at increased risk of being intimidated, threatened, arrested or persecuted, particularly if they are located themselves in the authoritarian countries concerned. This particularly applies to people who may or may not have dual nationality and originally come from the country concerned. In addition, Dutch citizens are at risk of being picked up in certain countries for diplomatic purposes (hostage diplomacy). The assessment of this threat has not changed since TASA1.

Some state actors are also prepared to kidnap opponents abroad or to use violence against them, or in extreme cases even carry out assassinations. Last year, for example, a Pakistani Briton in the United Kingdom was found guilty of plotting the murder of a Pakistani dissident living in the Netherlands. Iran has also kidnapped dissidents abroad during the past few years to put them on trial in their own country, possibly resulting in a death sentence.

Salman Rushdie's attacker possibly inspired by Iran's fatwa

State actors can indirectly push a form of influence that goes against democratic values such as freedom of speech. This itself can lead to threats of violence against opponents, dissidents or critics. An example of this was the attack this year on the British-Indian writer Salman Rushdie. Rushdie has been under threat since the publication of his book The Satanic Verses (1988), which is regarded as blasphemous by some in the Islamic community. The publication of the book led to violent protests worldwide at the time. In 1989 the Iranian ayatollah Khomeini, then the highest leader of Iran, issued a fatwa (a religious decree) encouraging Muslims worldwide to kill Rushdie and others who were involved in the book.

The current Supreme Leader Ali Khamenei said in 2019 that the fatwa is 'permanent and irrevocable'. The Iranian regime denies any form of involvement in the assassination attempt but does consider that it is Rushdie's own fault that he was stabbed. It is said that he roused the wrath of the Islamic community with his 'insults'.

The Netherlands is increasingly facing threats to its economic security

The economic security of the Netherlands is increasingly facing open and covert threats from state actors. The Netherlands has to deal with the chain reactions of the sabotaging of critical processes in other countries and has risky strategic dependencies on other state actors. Dutch companies, knowledge institutes and researchers are being widely targeted by various state-sponsored activities attempting to seize high-end technology.

Critical processes vulnerable to state-sponsored activities

Although no actual sabotaging of critical infrastructures has taken place in the Netherlands, the Netherlands has had to deal with the consequences of sabotage elsewhere in Europe recently. In addition, investments by foreign parties are also making Dutch critical infrastructure vulnerable.

In the TASA1, it was already reported that preparations to disrupt and sabotage critical infrastructures had been identified. It cited the threat against submarine infrastructure, such as submarine cables and pipelines. Russian entities are mapping this infrastructure and engaging in activities indicative of espionage and preparations for disruption and sabotage. This threat is still very present. The as yet

unattributed undersea explosions in September 2022 involving the Nord Stream gas pipelines have added to this. These incidents have exposed the vulnerability of European critical processes to sabotage activities. The Netherlands can also be affected by the consequences of sabotage elsewhere in Europe. For instance, the damage to the Nord Stream gas pipelines affected gas prices. Another example of sabotage of critical infrastructure is the disruption of civil satellite communication systems in Europe. These were recently disrupted by a malicious software update that was likely aimed at crippling Ukrainian satellite communications.

Economic security interests

'The unimpeded functioning of the Netherlands as an effective and efficient economy.'

Three elements are essential to the economic security of the Netherlands: the continuity of critical processes, the mitigation of risky strategic dependencies and the prevention of the undesired transfer of knowledge and technology.

The continuity of critical processes forms the basis for all Dutch economic and societal activities. These are processes, such as the supply of power, that are so critical to the functioning of Dutch society that a failure of or disruption to these processes will result in serious social disruption and economic harm. To guarantee the continuity of these processes, it is important that the requisite infrastructure continues to function and that the providers of these processes can take charge independently without being under undesirable foreign pressure.

The second element relates to the mitigation of risky strategic dependencies which state actors may be able to exploit for geopolitical purposes. The Netherlands is an open economy focused on international trade, attracting foreign investment and securing global access to knowledge and technology. As such, the Dutch economy is closely tied to global production chains. These global ties are helping to generate economic growth. The Netherlands is benefiting from these ties. However, it does result in (mutual) dependency on other countries. Dependency can bring risks, for example when we are dependent on a small number of other countries for rare earth metals or (fossil) fuels, technology, products or services where an alternative supplier cannot quickly be found. In addition, high-risk strategic dependencies can occur when state actors exert unwanted influence on Dutch public interests. In this case, dependency can be used as a strategic tool for applying pressure for geopolitical purposes.

Ultimately it is important for economic security that undesirable transfer of knowledge is prevented. Sensitive knowledge and technology that is leaked can be used by a state actor in a way that affects national security interests, economic interests or innovative strength, or that is at odds with what we consider ethical in the Netherlands. The transfer of high-quality knowledge or technology can lead to undesirable end use by another state actor, for example in surveillance applications, military equipment or to enhance digital attacks. In addition, Dutch economic interests can be harmed if valuable and exclusive knowledge and technology are leaked abroad.

Threat Assessment State-sponsored Actors 2

State actors invest in parts of Dutch critical processes. Chinese companies are active, for example, in the Dutch logistics and transport sector, the telecommunications sector and the energy sector, or Chinese technology is used in sensitive areas within these sectors. Chinese investments in these sectors seem for the time being to be motivated by economic reasons, but this can nevertheless create a high-risk strategic dependency. This dependency increases Chinese capabilities to use (digital) espionage, sabotage and political pressure. This can pose a threat to the continuity of these processes and therefore to national security.

Increased risk of misuse of strategic dependencies

International trade boosts Dutch wealth and creates mutual dependencies. It has become all too apparent with time that there are also risks attached to some of these dependencies. In the context of the war in Ukraine, Russia is using European energy dependency, for example, to exert political pressure. In addition, there is the issue of high-risk strategic dependency on critical raw materials and states are attempting to assume crucial positions in the production chains of high-end technologies.

The Netherlands is heavily dependent on other countries for its energy supply. It became clear last year that this poses major risks. Russia is using European dependency on Russian oil and gas to exert pressure on EU member countries and to undermine European cohesion. This is impacting oil and gas prices and supply security. It is leading, for example, to high inflation, curbing economic growth and may spark social unrest.

In addition, the Netherlands is dependent on other countries for critical raw materials, such as rare earth metals. These raw materials are increasingly necessary for the (digitalising) industry, but also to facilitate the transition to sustainable energy. A certain number of countries are world leaders in the mining, refinement and supply of these raw materials. For example, many raw materials from Africa, Australia or South America first have to go via China for refinement before they arrive in Europe. China is also taking up strategic positions in the mining of foreign mines (in Africa and Latin America for example) to thus strengthen its grip on raw material chains. The dependence on raw material chains can be abused by state actors to exert pressure. In 2010, China used Japanese dependence on raw materials as a geopolitical tool when it blocked the export of rare earth materials to Japan due to a conflict about a group of islands in the East China Sea. State actors could in the same way use the Dutch strategic dependency on critical raw materials for geopolitical purposes.

Dutch knowledge economy attractive target for state actors

The Netherlands is among the world leaders in terms of the most dynamic and competitive knowledge economies in the world and is a global frontrunner in the development and application of high-quality knowledge in some sectors. This makes the Dutch knowledge economy an attractive target for countries that wish to acquire knowledge and technology.

Ultimately, high-risk strategic dependencies develop because states try to determine international (ICT) production standards.[6] As a result of economic and technological growth, some countries are increasingly able to determine or influence technical standards. China is a particularly important player in this respect by virtue of its active role on various international standards committees. In addition, setting standards can be problematic when standards are determined by companies where state actors are (covertly) exerting influence in the background. Setting standards can provide an advantage for the state actors' own industry and therefore secure substantial economic benefits. State actors can also abuse their position as a definer of standards to promote their own standards and values that often do not align with Western standards and values.

6 International technical standards are intended to improve the quality, security and compatibility of products and services. They form the basic specifications for technologies on which companies can build as they develop these technologies further. Set standards can play a guiding role in the global development of new technologies, both technologies with a civil purpose that contribute to economic and social prosperity and technologies with a military purpose.

Leaking and theft of knowledge and technology as concerning as ever

States engage in large-scale activities to acquire knowledge and technology in the Netherlands. They use a wide scale of legal and illegal methods to do this (see the chapter Economic security in depth). There is a strong overlap between the intelligence needs of various state actors and the knowledge and technology sectors in which the Netherlands is one of the global frontrunners. In acquiring this knowledge and technology, there is a risk of undesirable end use for military purposes, for example, and Dutch companies would face unfair competition, which affects their earnings model. This means that the undesirable transfer of knowledge and technology is as concerning as ever.

China is in many areas an important and valued partner to the Netherlands, Dutch businesses and Dutch knowledge institutes. At the same time, China represents the greatest threat to Dutch knowledge security. The country has been striving for strong economic and technological growth for a long time now. To achieve this growth, Chinese parties are actively looking for technologies that are central to Chinese policy objectives. Both legal and illegal collection methods are used to get hold of these technologies. Dutch companies, knowledge institutes and researchers are being widely targeted by various (digital) attacks attempting to seize high-end technology. In addition, knowledge and technology are acquired through academic collaboration and through investments and takeovers.

Russia and Iran are also using various collection methods to acquire foreign technology. Russia has a strong need for Western technology and equipment as it attempts to bridge its technological gap in various areas. This shortfall, combined with the international sanctions imposed on the country following the annexation of the Crimea in 2014 and the war in Ukraine, have resulted in certain Russian production and development projects falling behind. Russian intelligence services are actively looking for technology in the Netherlands. Iran in turn is carrying out a variety of covert and open activities to acquire high-end technology and sensitive knowledge and goods in respect of proliferation in the Netherlands. For example, it is using covert networks to acquire goods subject to export restrictions from Dutch manufacturers and intermediaries. In addition, Iran has a keen interest in the high-quality knowledge of Dutch (technical) universities.

Economic security in depth

Why economic security is becoming increasingly more important

There is an increasing degree of (geo)politicisation of the (global) economy, with economic instruments being used as a lever of power. Countries are prioritising mitigating high-risk strategic dependencies. There is also a *tech race* between countries to lead the development of emerging and disruptive key technologies. Greater importance is being attached to economic security interests as a result of these developments.

Geopolitics increasingly dominating the global economy

Increasing competition and power struggles between countries show how interwoven politics and economics really are. This is resulting in, for example, further (geo)politicisation of the (global) economy, in which the Netherlands, just like other countries, must find its place. On the one hand, economic and the associated technological developments are forming the basis for political and military power. On the other hand, economic instruments are being used by countries, particularly the superpowers, as a lever of power to achieve geopolitical objectives. The most recent and striking example of this is the way in which Russia and the West deploy various economic instruments back and forth as a power tool against each other.

Strategic autonomy a priority for state actors

Countries are increasingly prioritising achieving a certain degree of strategic autonomy. State actors want to prevent or diminish high-risk strategic dependencies as much as possible by reducing dependencies on other countries or by being self-sufficient. They can do this by diversifying risk, for example. This will make them less susceptible to economic pressure tactics of other countries. For their technology policy, they are investing, for example, in identifying and, where possible, removing bottlenecks in international production processes that could lead to strategic dependencies. In the most extreme cases, this can result in

Taiwan case demonstrates the interconnectedness of economic security and geopolitics

The tensions surrounding Taiwan are affecting economic security. A large part of the global production of computer chips takes place in Taiwan. The supply security of computer chips has been under pressure worldwide for some time now. Escalation in the Taiwan Strait would likely have seriously disruptive effects on global production chains. The Chinese People's Liberation Army has recently carried out military exercises around Taiwan that were unprecedented in terms of their intensity and scope. It has increased the risk of possible accidents and miscalculations. Escalation may have major implications for the stability of the region and international shipping, to name but two issues. Both are vitally important to the Netherlands. Due to this strategic dependency, escalation in the Taiwan Strait will also have far-reaching consequences for the economic security of the Netherlands. Global production chains may be affected, possibly triggering huge negative effects.

existing production processes being disconnected in order to exclude certain countries, thereby creating or reducing opportunities for economic pressure. These production processes are often extremely complex and interconnected internationally. This means that disconnecting processes without a loss of quality or cost efficiency is very difficult in the first instance.

Tech race crucial for geopolitical power

Key technologies[7] such as, for example, quantum technology and artificial intelligence will, over the coming years, increasingly influence the global balance of power. The development of such technologies is very labour-, knowledge- and capital-intensive, resulting in a disproportionate concentration of economic power in those countries that are successful in developing these technologies. In addition, these technologies can also significantly increase the military strength and espionage capabilities of countries. Whoever becomes decisive in the area of these key technologies will therefore play a defining role geopolitically. There is therefore what is known as a tech race going on between countries (particularly the US and China) who want to be forerunners in the development of such technologies.

7 Key technologies can change society in a systematic way due to the huge influence that the technology has on the earning capacity and/or military capabilities of a country. This often involves dual-use technology, the end product having both a civil and military use. A number of terms are used for these technologies, such as key technologies, sensitive technologies, system technologies and emerging & disruptive technologies. The term key technologies is used in this document due to the key role that these technologies play in the geopolitical technology race and their huge economic and social value. Examples of these technologies include artificial intelligence, photonics and quantum technologies.

Why China, Russia and Iran are carrying out activities that threaten economic security

Various state actors represent a threat to the economic security of the Netherlands. This more in-depth analysis will focus on countries posing the greatest threat, namely China and Russia. In addition, we will also look at Iran, due to the specific threat with regard to sensitive knowledge and instruments in respect of proliferation. These three countries need Western knowledge and technology for their economic and military development.

China striving for Western technology for economic and military development

China has set itself a number of closely related economic and military objectives. To achieve economic modernisation and independence from foreign technology, China is investing in strategic multi-year plans and policy initiatives. Examples of this include *Made in China 2025*, the *Belt and Road Initiative* and the *Military-Civil Fusion*. The emphasis is on self-sufficiency and technological and scientific independence from other countries in strategic sectors, particularly in respect of Western technology. By having the necessary technology at their own disposal, China can thus minimise the risks of dependency, for example if the US uses its economic position as leverage.

In addition, China seeks to have a 'world-class' military that can measure up to that of any other country by no later than 2049. To achieve this, the Chinese People's Liberation Army is working on a transformation to a military with high-end technology. The Chinese People's Liberation Army is working firstly on a technological catch-up to acquire modern hardware and secondly on using new key technologies, such as artificial intelligence and quantum technology.

Chinese intentions are therefore closely tied in with the global *tech race*. To realise its economic and military objectives, China needs to improve its innovative capability and competitive position and acquire high-quality scientific and technological knowledge. As Western countries still have a leading position in terms of their knowledge, this is resulting in significant Chinese interest in advanced Western knowledge and technology. Internationally, the Netherlands has a good reputation in respect of technologies that are important for the global tech race. There is therefore a strong overlap between the Chinese need for high-end technology and certain technologies in which the Netherlands is a front runner. Chinese interest in these technologies and the activities the Chinese government uses to undertake these pose a threat to the economic security of the Netherlands.

Russia's intentions focused on the energy sector and Western knowledge and technology

Due to its enormous reserves of fossil fuels, including gas and oil, Russia holds a crucial position on the energy market. Russia wants to maintain this position and has shown that it is prepared to use European dependence on Russian energy suppliers as a tool for applying pressure in response to Western sanctions following the war in Ukraine.

The phasing out of (Russian) fossil fuels by European countries represents a direct threat to the Russian economy. Russia is heavily dependent on income from oil and gas for its state revenue. This phasing out of Russian energy, combined with the wider global energy transition, is threatening Russia's prosperity level and the country's internal stability and international position of power. Russia is therefore assessing both openly and covertly how it can protect its interests in the changing energy economy and how it can slow down the transition. With the time saved, Russia hopes to generate income from fossil reserves for as long as possible and find alternative sales markets.

In addition, Russia needs Western knowledge and technology. Russia has also recognised the importance of key technologies such as quantum technology and artificial intelligence and has ambitions to develop military uses for these technologies. Russia will probably also want to learn lessons from the war in Ukraine and solve problems with the weapons systems used by refining weapons systems. However, Russia has allowed itself to lag behind technologically compared to the West and China and has also been cut off from access to sensitive technology as a result of international sanctions. It will therefore try to gather this technology covertly and to invest in independent technology projects, for example by using front companies to circumvent export restrictions, as recently evidenced by the MIVD. Attention needs to be paid here to possible Russian interest in maritime, communication, chemical and laser technology.

Iran wants to acquire sensitive knowledge and instruments in respect of proliferation

Iran is seeking to develop and maintain ballistic missiles and has a nuclear programme. Due to international sanctions, the Iranian regime has only limited access to the Western knowledge and technology that it needs for this. Iran is particularly lacking high-end equipment and practical knowledge of how to use this sensitive equipment in respect of proliferation. The West has the edge in this. For this reason, Iran wants to acquire this knowledge and equipment in Western countries, including the Netherlands, via, for example, covert procurement networks, knowledge institutions and students and researchers.

Threat Assessment State-sponsored Actors 2

How state actors are threatening economic security

State actors use both legitimate and illegitimate activities to achieve their aims. In many instances this involves legal economic activities that nevertheless pose a threat, such as takeovers and investments, purchasing certain technology and establishing international partnerships. In other cases, state actors use covert methods more, such as digital espionage and the use of insiders to acquire knowledge. The various legal and illegal means are used by states both individually and in combination with each other. The combined, hybrid use of tools increases the chances of successfully obtaining or reproducing a product or technology.

Cyber attacks

The use of cyber means is an important way in which state actors threaten economic security. This involves cyber attacks aimed at Dutch companies and knowledge institutions in order to steal technology. In addition, they include preparations to steal knowledge or to commit digital sabotage and actual digital sabotage. Dutch organisations are, for example, widely targeted by various digital attacks by states in order to seize high-quality technology and knowledge. Such attacks are undertaken against (defence) companies and knowledge institutions, for instance. In addition, cyber attacks can be used to sabotage critical infrastructure. Preparations to sabotage critical infrastructure have been reported in Europe.

Investments

Investments represent another means with which state actors seek to achieve their economic and, in some cases, geopolitical aims. This includes investing in sectors and investments in, or full takeovers of Dutch companies by foreign parties. In some cases, there is a state actor directly behind the investments. In most cases, however, investments and takeovers are performed by private companies, where these parties go to some lengths to hide the fact that there is a state actor behind the company. A number of strategic takeovers of Dutch companies by state actors have taken place in the Netherlands during the past few years. High-quality knowledge can be leaked and strategic dependencies can be created as a result of such investments. Investments elsewhere in the EU or in allied countries can provide scope for political and diplomatic pressure, with possible effects for the Netherlands as a result.

Insider threats

State actors can also use what are known as insiders. An *insider threat* refers to the threat ensuing from people (formerly) employed in Dutch companies and knowledge institutions. Insider threats can occur through legal and illegal means.

A legal form of (undesirable) transfer of knowledge via an insider threat is the knowledge that is leaked through foreign students and researchers who are studying or carrying out research at Dutch knowledge institutions. State actors often create return obligations for the students concerned, for example by linking conditions to scholarships. Collaboration between Dutch knowledge institutions and foreign knowledge institutions can result in an undesirable transfer of knowledge. Some foreign institutions are affiliated to the military of a state actor, bringing a risk of undesirable end use (for military purposes).

Insider threats also include illegal forms of undesirable transfer of knowledge. It has been established, for example, that foreign intelligence officers are attempting to build a network of sources in order to acquire knowledge and technology. These intelligence officers maintain covert contacts with (foreign) employees within Dutch companies or knowledge institutions. Intelligence officers are also regularly found at conferences and contact is made online, for example through LinkedIn, most likely with a view to finding and recruiting sources.

(Illegal) export

Circumventing export restrictions and exporting non-controlled (but high-end) technology can pose a threat to economic security. State actors use complex ownership structures and trade channels to circumvent such restrictions, for example, in order to conceal the true end user. This is done using various methods, including deceiving exporters and using front companies and intermediaries. When using front companies, state actors use a company registered in the Netherlands that on paper complies with all the necessary regulations but in reality does not carry out any significant profit-driven business activities. Instead, such a company is primarily occupied with purchasing the technology in which the country concerned is interested. The export of non-controlled high-end technology can also represent a threat. For example, if the export of technology may contribute to undesirable military programmes or human rights abuses, will create an undesirable dependency (now or in the future) or could undermine the long-term innovativeness of the Netherlands.

Procurement and tendering processes

Procurement and tendering processes in the Netherlands are attractive to state actors. Lots of information is often divulged during a procurement or tendering process, including through public tendering documents. The documents often clearly show the type of expertise companies have, and through this potential targets are identified. In addition, procurement and tendering processes can provide state actors with access to sensitive systems or information or enable state actors to get their hands on part of the market. Over time, this market share can deliver high-risk strategic dependencies. Furthermore, goods and services delivered provide state actors with opportunities for sabotage and espionage. During the past few years, a risk of espionage has been reported in tendering processes for the Dutch Ministry of Defence, the police and other Dutch government authorities.

Threat Assessment State-sponsored Actors 2

Legislation and regulations

Using national legislation, countries can exercise influence on economic relations with other countries. For example, they can adapt protectionist measures for certain economic sectors or award these sectors extensive forms of state aid. This can favour the country's own industry and upset the level-playing field. In the longer term, an uneven playing field can lead to high-risk strategic dependencies. In addition, state actors can enshrine extensive access to business information in legislation and regulations, for example on the grounds of national security interests. Companies and individuals are then legally obliged to cooperate with the government within the framework of national security. The development of high-end technologies, for example in the aerospace industry, can thus be categorised as a national security interest. In this way, foreign entities in the Netherlands are obliged to transfer the knowledge and goods that they acquire as a result of collaboration with Dutch companies or knowledge institutions to the country of origin. Legislation could also require Dutch companies abroad to transfer knowledge and technology.

International rule of law increasingly coming under pressure

The international rule of law is coming under increasing pressure. This trend has continued further since the TASA1. The international rule of law is being questioned by various state actors and portrayed as a Western construct, and is therefore systematically compromised. International norms such as non-intervention, non-proliferation and peaceful settlement of disputes are also being violated and international institutions are increasingly being used as a platform on which state actors are attempting to undermine the international rule of law.

International rule of law is being systematically attacked

Some countries have been questioning the international rule of law and how it is functioning for a long time now. These countries regard the current international rule of law as a Western construct, designed to further Western interests. Russia and China in particular are currently attacking the existing international order. Russia is undermining the international rule of law and often seems to act as a disruptor in multilateral contexts. China believes in international stability and a functioning multilateral system, but wants to remould the system to align with its own vision in the long term. The countries find common ground in their opposition to what they see as the Western-oriented international rule of law, their anti-US stance and geostrategic competition with the West. Against this backdrop, both countries seek to drive the US and Europe apart and to undermine the credibility of the West in the eyes of other countries. President Putin of

International rule of law and stability

'A well functioning international system of standards and agreements, aimed at promoting international peace and security, including human rights, and effective multilateral institutions and regimes, as well as the sound functioning of countries bordering the Kingdom of the Netherlands and in the immediate neighbourhood of the EU.'

The Netherlands as a relatively small country has a major interest in enforcing the existing international rule of law. National security is indeed dependent on the functioning of the international system of standards, agreements and institutions that protects the sovereignty of all countries and ensures that major state actors cannot use violence to impose their will on smaller countries. The Netherlands as an open economy also has a major interest in enforcing existing agreements on matters such as free shipping and world trade.

Russia and his Chinese counterpart Xi Jinping issued a joint declaration on the eve of the Olympic Games outlining their alternative version of the world order and the multilateral system. At the same time, there are also major differences of opinion between Russia and China and signs of mutual distrust. It is by no means clear how relations between China and Russia will pan out.

Norms of state sovereignty and non-intervention under pressure

The consequences of the war in Ukraine for the Netherlands and its allies have been addressed at length in several places in this threat assessment. However, Russia's aggression towards Ukraine is also having a huge impact on the international rule of law. The war demonstrates yet again the vulnerability of the international norms of state sovereignty and peaceful coexistence. The attack on Ukraine shows that Russia is prepared to seriously violate the sovereignty of another country to preserve its sphere of influence against unwanted Western influence. Russia thinks in terms of its 'own' spheres of influence, as part of which it believes that it has the right to perform militarily operations in countries that belong to it. This way of thinking is at odds with the principles of state sovereignty and non-intervention on which the international rule of law is based.

Non-proliferation norms are being eroded

The international rule of law is also being threatened because non-proliferation agreements are increasingly under pressure. Iran, for example, is actively working on developing ballistic missiles and it has a nuclear programme. The development of Iran's nuclear programme in particular has become more concerning since the last threat assessment. Since the withdrawal of the US from the Iran nuclear deal,

Iran believes that it is no longer bound by these agreements and is forging ahead with its enrichment of uranium.[8] If Iran did produce nuclear weapons, this would have major consequences for the stability of the region. It is possible that this will lead to a nuclear arms race in the Middle East, with other countries in the region also developing nuclear weapons.

In addition, the norm shunning the use of chemical weapons is also under pressure following the use of chemical weapons by Russia, Syria and North Korea in recent years.[9] The erosion of this norm may lower the threshold for the use of chemical weapons in the future.

Increasing assertiveness affecting peaceful resolution of disputes

The norm of peaceful resolution of disputes is under pressure due to the increasing assertiveness of various state actors. A good example are the increasing tensions in the South China Sea. Several countries around the South China Sea are laying overlapping maritime claims to the area. The majority of these countries are concerned about the way in which China is using a military presence to enforce its military claims. China has de facto authority over various islands (artificial or otherwise) in the area and has set up military bases on at least three of these islands. All three of these bases are in disputed maritime territory. China has for a number of years also been ignoring a binding ruling by the Permanent Court of Arbitration's arbitral tribunal on the Philippines' maritime claims regarding the South China Sea. In doing so, China has demonstrated that it is prepared to compromise the norm of peaceful resolution of disputes.

Increasing assertiveness on the part of China cannot be separated from the build-up of China's military. The country has been working on building up a world-class military for a long time now. To this end, China is investing heavily in its navy, air force, space capabilities and new military technologies. China now has a modern navy with the largest number of ships in the world. These fleet is able to cover large distances, allowing China to exercise more influence within the region and ultimately around the world. Although China is not a direct military threat to the Netherlands, the extensive modernisation of its armed forces and the lack of transparency regarding China's strategy and intentions represent a challenge to international security.[10]

8 The *Joint Comprehensive Plan of Action* (JCPOA).

9 Russia's incursions of this norm relate to the assassinations of Skripal and Navalny using chemical weapons, in North-Korea chemical weapons were involved in the assassination of the brother of Kim Jong-un and Syria used chemical weapons against its own population during its civil war.

10 In order to have world-class armed forces by 2049, China is investing in the modernisation and expansion of its land forces, navy and air force. Over the past few years, China has also built up a large arsenal of dual capable cruise weapons and ballistic missiles which enable them to attack targets from a long distance. Furthermore, China is investing in space applications and anti-satellite weapons, allowing them to achieve information dominance in a conflict and deny opponents access to the space domain. Finally, China is investing heavily in new technologies such as artificial intelligence, quantum technology and hypersonic weapons in order to close the gap with the West more quickly. For example, the country is working on swarm technology. This will enable large numbers of unmanned systems to carry out commands as a coordinated swarm using artificial intelligence, possibly resulting in air defence systems being overwhelmed.

Disruption 'illegal' at the International Criminal Court of The Hague

Russia is attempting to influence or frustrate the functioning of international institutions. In June 2022, the AIVD disrupted the operations of a Russian intelligence officer with a Brazilian alias identity who was due to be undertaking an internship at the International Criminal Court in The Hague. By assuming another identity, such illegals are often difficult to uncover. The intelligence officer would potentially have been able to cause considerable harm during his internship by gathering intelligence about investigations within the International Criminal Court, for example, infiltrating computer systems, influencing investigations or identifying sources. The fact that the International Criminal Court is investigating possible war crimes by Russia in Ukraine makes it a target of particular interest for Russia. In addition to the damage that Russia would thus have been able to cause to the functioning of the International Criminal Court, it could have discredited the position of the Netherlands as a host country. Such activities not only jeopardise the upholding of the international rule of law, but also compromise social and political stability.

International institutions increasingly being used as a platform to undermine the international rule of law

State actors are increasingly exerting their influence in international institutions to undermine important international rules and norms. For example, in February 2022, shortly after its invasion of Ukraine, Russia blocked a resolution of the UN Security Council condemning Russia's aggression and endorsing Ukrainian sovereignty. In May 2022, in the same UN Security Council, China and Russia both vetoed a resolution of the US to impose new sanctions on North Korea following various tests of ballistic missiles. In addition, over the past few years China has set up a number of parallel international institutions through which it can hollow out existing international institutions and increase its international influence.

The fact that state actors are succeeding more now than they did in the past in undermining or influencing the international rule of law through decision-making in international institutions is also due to the diminishing influence of liberal democracies on the world stage. The number of liberal democracies vis-à-vis the number of authoritarian states has decreased over the past few years. This has emboldened authoritarian regimes to spread their authoritarian world view beyond their own borders. China, for example, is attempting to promote its own version of 'democracy' internationally. China is presenting an alternative version of democracy compared to the Western definition, in which local circumstances are decisive and in which the concept of democracy can be interpreted differently on a case-by-case basis.

In conclusion

National security interests are being threatened by state actors in a number of ways. The threat has increased compared to the TASA1. State actors are increasingly prepared to actively use their power to defend or further their interests. Territorial security has come under further pressure primarily as a result of the war in Ukraine. The social and political stability of the Netherlands is also still being impacted by state-sponsored interference. In addition, the Netherlands is facing more and more frequent threats against its economic security and the international rule of law is increasingly coming under pressure.

There is a close link between the threats described in this threat assessment. This means that the activities of state actors are impacting, or may impact, multiple national security interests. A clear example of this is the way in which Russia is using European energy dependency to attack other countries economically and create social unrest. In doing this it is seeking to undermine European cohesion. Russia's activities therefore represent a threat not only to economic security but also to social and political stability. This demonstrates not only the mutual interconnectedness of national security interests, but also the fact that threats from state actors should not be considered separately for each security interest, but should always be considered in mutual coherence.

The various national security interests are vulnerable and are being substantially threatened and attacked by state actors, but not always to the same extent. The vulnerability of national security interests is not only dependent on the threat from state actors, but also on the resilience of the Netherlands itself. Counter-measures are required to reduce vulnerability and thus increase the resilience of the Netherlands against threats from state actors.

The interconnectedness of threats, combined with current geopolitical developments, mean that an integrated approach to increasing resilience is more important than ever. This applies on three different levels. Firstly, the extent and intensity of threats from state actors mean that it is crucial for the Netherlands to work with other countries facing the same sort of threat. The Russian attack on Ukraine has shown that the Netherlands is dependent on international cooperation in order to counter the threats resulting from this attack. Secondly, a coordinated approach within the Dutch government and between the government and society is important. For example, to come up with a response to the legal and illegal way in which an undesirable transfer of knowledge to China is taking place. Targets of state actors span the entire breadth of society. Finally, it is therefore imperative that there is broad public awareness of the nature and scope of the threats emanating from state actors.

November 2022
This publication is a joint release of:

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

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

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