Between peace and war

The war in Ukraine and the Russian threat in Europe

Summary

The AIVD and MIVD observe that Russia considers itself to be entangled in a broader and existential conflict with the West. This conflict takes place in the military, economic, and ideological field. To Russia, the war in Ukraine is only part of this. As a result of the war in Ukraine, the relationship between Russia and the West has reached a new low. Existing contrasts have been sharpened and deepened by the war. As a result, a military conflict between Russia and the West is no longer inconceivable. Russia has not only shown itself capable of handling the substantial losses in Ukraine, but even of expanding and reforming the armed forces. The Russian armed forces are preparing for the possibility of a conflict with NATO and carry out various activities to test the West's willingness to escalate.

Russia is preparing for a lengthy confrontation with the West, also in the military domain. It is estimated that in the worst-case scenario after the end of the war in Ukraine, Russia will need less than a year to build enough capacity for a military operation with limited geographical goals. This military operation would likely not aim for the military defeat of NATO but at breaking up the alliance and forcing concessions on the European security architecture. This does not mean that at this moment, Russia actually has the intention to progress to action.

In addition to this military threat, since autumn 2023 the Russian threat has increasingly manifested in hybrid activities[1] which Russia develops in various places in Europe. This threat is anything but new, but it has increased. By carrying out cyberattacks, influencing activities, and (digital) sabotage actions, Russia attempts to play Western countries off against each other and undermine Western political and social support for Ukraine. Over the course of 2024 Russia appeared to show an increased willingness to take risks. These activities increasingly showed a physical component of violence. In the Netherlands too, various Russian hybrid activities have been observed, including preparations for sabotage.

The AIVD and MIVD expect that Russia will continue to carry out such hybrid activities. Even after a potential ceasefire in Ukraine. The AIVD and MIVD expect this hybrid threat to come and go in waves, with moments of escalation and de-escalation. Europe, and the Netherlands, will have to take into account Russia's increased willingness to take risks that it has come to show over the course of 2024.

In order to be prepared for possible further military escalation and at the same time ward off the Russian hybrid threat, the Netherlands must increase its own resilience. Government organisations, knowledge institutions, and the commercial sector must also remain alert. Because if such vital sectors were to shut down, it could cause serious disruption to society.

[1] In this publication hybrid activities refer to: influencing activities in both the physical and digital domain, including cyberattacks, covert influencing activities, and sabotage actions.

Contents

Introduction

With this publication the General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst - AIVD) and Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst - MIVD) of the Netherlands offer an insight into the Russian threat which has become more visible in Europe over the past couple of years. In the wake of the war in Ukraine, a military escalation between Russia and the West has become conceivable. The AIVD and MIVD are furthermore concerned about the increased threat posed by Russian hybrid activities in the grey zone between peace and war.

On 24 February 2022, Russia started a large-scale military invasion in Ukraine. Now the war in Ukraine has become the largest and most deadly conflict in Europe since the Second World War. The Russian invasion in Ukraine, which at the time of the invasion was called a *Zeitenwende* by German Chancellor Scholz, does mark an actual turning point in history. Russia still suffers great losses, without achieving its operational goals: the 'denazification' and demilitarisation of Ukraine.

As a consequence of the war, the relationship between Russia and the West has reached a new low. Russia is looking for rapprochement to alternative partners and markets in part as a result of Western sanctions and other initiatives to isolate Russia. Russia is also seeking to join international cooperations which could counterbalance the international order which Russia believes is dominated by the United States.

Russia's perception
In order to assess the Russian threat, it is crucial to understand Russia's perception. It should be noted that a perception is by definition subjective. It is not an isolated fact or the truth. In this publication, we refer to the Russian perception, with which we mean the way in which Russia sees the world.

In Russia's perception, the war in Ukraine is only one part of a larger and existential conflict between Russia and the West. Russia's goal is to rearrange the European security architecture. Moreover, Russia is preparing for a long-term confrontation with the West, also in the military field. This does not automatically mean that Russia intends to initiate a military conflict.

In the context of this broader confrontation, the Russian threat has increasingly manifested in Europe since autumn 2023. This threat is not only of a military nature. The Russian threat has increasingly manifested in Europe through hybrid activities.

Over the years, Russia has carried out a multitude of hybrid activities, also in Europe. Russia does so in both times of peace as well as during crises and war. These activities can take place both in the physical as well as in the digital domain. Think, for example, of covert influencing, cyberattacks, spreading disinformation, economic destabilisation, or concrete attacks on vital infrastructure. In this publication, we will further discuss cyberattacks, covert influencing activities, and (digital) espionage actions.

The goal of these hybrid activities is a complex one. Russia attempts to influence or frustrate political decision-making, incite social discord, and undermine the trust in our democratic system. Moreover, with these activities Russia attempts to undermine the unity in the West and the public support for Ukraine. It also uses these activities to disrupt the military materiel support which is delivered to Ukraine.

Characteristic is that with these hybrid activities Russia attempts to realise the aforementioned while by taking a minimal risk of military escalation which would result in an open armed conflict with the West. The use of hybrid means could be an alternative for an armed conflict.

The number of reports on (suspected) Russian cyberattacks, influencing activities, and (digital) sabotage actions in Europe has strongly increased since autumn 2023. These activities can vary from demonstrations, vandalism, and arson to disruption of international air traffic by drones, damaging (submarine) cables, and sending explosive packages via air transport. The AIVD and MIVD establish that the hybrid threat posed by Russia has increased. However, this does not mean that Russia's suspected involvement can be established in every case.

Now the war in Ukraine has become the largest and most deadly conflict in Europe since the Second World War.

In order to be prepared for a possible military escalation with Russia and to protect against the increased hybrid threat Russia poses, the Netherlands must strengthen its resilience. Government organisations, knowledge institutions, and the commercial sector must also remain alert. Because if such vital processes and sectors are shut down it could cause serious disruption to society.

The AIVD and MIVD carry out a joint investigation into the different types of Russian activities which pose a threat to the democratic legal order, allied interests, and other national security interests. With this joint publication, the AIVD and MIVD want to increase the awareness of the Russian threat and, with that, increase the resilience of Dutch society. This publication builds on the picture painted in February 2023 in the publication *24/2 The Russian attack on Ukraine: a turning point in history.*

This publication will first discuss Russia's perception of the West. Then, we deal with the course of the war in Ukraine and the possibility for a further escalation to an open military conflict between Russia and NATO. A picture is also painted of the so-called hybrid threat Russia poses, which has increasingly manifested since autumn 2023 in various places in Europe. Here we will go into more detail on Russian covert influencing activities, (cyber)sabotage activities, and (suspected) sabotage activities in the maritime domain and disruptions of the air traffic by drones. Lastly, we will briefly discuss the broader impact of the war in Ukraine on Dutch society.

1.
Russia in conflict with the West

In Russia's perception the war in Ukraine is not just a war with a neighbouring country. Russia believes that the war in Ukraine is expressly part of broader and existential conflict with the West. This broader conflict takes place in the military, economic, and ideological field. The Kremlin realises that the military conflict – the war in Ukraine – is finite and will eventually be resolved at the negotiating table.

Since their large-scale military invasion in Ukraine, Russia has been looking for new markets and (trade) partners in the economic field because of Western sanctions. Even though according to the Kremlin the economic conflict with the West will continue for a long time, Russia still appears convinced it can bear the consequences. Even though it is increasingly the question whether this is and will remain the case. However, to Russia the most fundamental part of the broader conflict with the West is the ideology. It is a conflict between conflicting and incompatible world views which are based on contrary norms and values systems: the perverse and decadent West versus the unique Russian civilisation.

From the Russian perspective this unique Russian civilisation should be protected from the aggressive and expansionist West. Putin is willing to pay a high price, as shown by Russia's large personnel and materiel losses in Ukraine. Russia's perception is connected to zero-sum thinking in which only one party can win, which also means there will always be a loser. This narrative is likely also motivated by a less reason: the regime wants to remain in power.

As yet, the Russian regime is stable, even though this is increasingly enforced through repression and various initiatives which are intended to enable Russian authorities to exercise more control over the digital information domain. In a certain way, these initiatives are aimed at further isolating Russia from Western influences, which may pose a threat to the stability of the regime.

'Surrounded by a hostile West'

In this fundamental battle, the Kremlin believes that the West aims at strategically defeating Russia and destabilising the country. Furthermore, Moscow believes that the West infringes on Russia's right to a sphere of influence. According to Russia, the West is attempting to detach countries such as Ukraine from Russia, to include them in Western institutions such as NATO and the EU, and in this way the West advances to the Russian borders. This perception plays a central part and Russia invariably deems it one of the 'root causes' for the war in Ukraine. As a consequence of the war, the image of Russia surrounded by a hostile West is not only being perpetuated, but also strengthened. Europe currently invests in preparations for a possible military escalation with Russia. The Kremlin sees these investments as a confirmation of Europe's offensive hostile ambitions and explicitly calls Europe part of the 'problem' with increasingly sharper phrasing.

Russian Armata T-14 tanks during a military parade in Moscow, Russia

1.1 The Russian narrative

Narrative within Russia
Since the invasion, the Kremlin has made every effort to legitimise the war for itself and the society. It goes back to means which, in the eyes of Putin and his allies, have proven their worth during the Soviet era but stem from tsarist Russia: far-reaching indoctrination with one indisputable and 'typically Russian' system of values and norms imposed from above. In this indoctrination, Russia is presented as an independent civilisation with a messianic mission. The Kremlin perceives and propagates isolation from the West as regained sovereignty. Here, Moscow primarily focuses on young people, especially via education. In a short time, almost the entire Russian educational system has become interspersed with ideological courses and activities. A 'correct' view on national history plays a leading role in this.

In this 'correct' view on Russia's national history the current war against Ukraine is connected to the Second World War when the Soviet Union defeated Nazism.

In order to garner domestic support for the war in Ukraine and morally justify the war, Putin appeals to Russia's role in the victory over Nazi Germany in the Second World War. Putin claims fascism has resurfaced in Ukraine. According to Putin, it again falls to Russia to defeat this 'fascist monster'.

Narrative towards other countries
In an international context, Russia wants to show that the Western attempts to isolate the country only have a limited effect. In this, Russia focuses on international cooperations such as BRICS or the Shanghai Cooperation Organisation (SCO). It wants to counterbalance the international order which Russia believes is dominated by the United States. According to Russia, the strategic partnerships Moscow has formed are crucial to continue Russia's war efforts in Ukraine. Moscow presents a number of these strategic partnerships, such as the relationship with Beijing, as successful and equal. In reality however it seems more like a marriage of convenience which was established in an unequal way.

1.2 Support Russian society

There still appears to be a lot of support for the war among the Russian population, even though this is also partially enforced through increasingly repressive means. Any form of criticism of the Russian 'special military operation' in Ukraine is suppressed, as well as public criticism of the Russian leadership. Until now the Kremlin has been able to deal with the challenges the war brings. The question is how long Russia can carry on like this. In the meantime, the Kremlin appears to acknowledge that a possible ceasefire or post-conflict scenario will bring along political, economic, and social challenges. It struggles with how to deal with this. Think, for example, of the reintegration of the large number of soldiers in Russian society. Some of them are injured and traumatised. There are also criminals returning to Russian society who literally fought for their freedom. Moreover, former private military contractors, former mobilised persons, and persons working in the defence industry will experience a decrease in income. The Kremlin is also apprehensive of possible dissatisfaction about Russian 'concessions' during the negotiations; this dissatisfaction could lead to domestic unrest.

1.3 Negotiations

Despite the mentioned domestic challenges Russia is confronted with as a result of the war in Ukraine, President Putin brings a maximalist attitude to the negotiating table. He tries to reach an agreement on Russia's terms. Even though Moscow realises that wars generally end through negotiation, these negotiations look very different from a Russian perspective to the Western perspective.

Here, Russia wants to address the 'root causes' of the conflict and indicates only wanting to speak with the United States, and then expressly about rearranging the European security architecture. Russia's goal is to influence and weaken developments it perceives to be threatening, such as NATO's presence which has moved closer to the Russian borders[2] since 1997. No matter the time frame, NATO membership for Ukraine is out of the question for Russia. Moreover, Russia views Western peace initiatives with suspicion and tries to prevent its most important partners from participating in such initiatives.

As yet, the course of the peace negotiations underlines the complexity of reaching an agreement. Russia's willingness to negotiate mainly says something about the willingness to end the war in a diplomatic way, not that Russia is actually willing to make concessions. Russia uses the negotiations mainly as a vehicle for establishing certain results or forcing concessions which are beneficial to Russia, partially on the basis of the situation on the Ukrainian battlefield.

[2] We refer to 1997 because in this year an agreement was made between NATO and Russia with, among other things, the pledge that the then NATO members would not station a substantial number of military personnel and materiel in other European countries.

2.
Course of the war in Ukraine

On the eve of Russia's large-scale military invasion in Ukraine, the Kremlin seemed convinced that Russia would be able to obtain its goals for this 'special military operation' in only a couple of days. By now, the war in Ukraine has become a real battle of attrition. Russia still suffers great losses without achieving its operational goals: the 'denazification' and demilitarisation of Ukraine. In part as a result of continued support from China, Iran, and North Korea, Russia does have numerical advantage both as regards personnel and materiel. This gives Russia a strategic advantage.

Destroyed Russian tank in Sviatohirsk, Ukraine. 12 February 2023.

2.1 Ukraine

Despite the West's continued support, the Ukrainian armed forces face structural shortages. Without large-scale mobilisation and intensified military support from other countries, Ukraine would be unable to solve these shortages.

Ukraine's temporary tactical success after conquering Russian territory in Kursk did not lead to a strategic advantage. In March 2025 the Ukrainian armed forces retreated in an organised way under increased Russian pressure. By now, Russia has reconquered the majority of this territory.

The Ukrainian armed forces carry out successful attacks on places in Russia far behind the front lines, so-called deep strikes. They do this more often with more advanced, self-produced long-distance drones which target the Russian petrochemical sector, the defence industry, military supply lines, and air defence. Nevertheless, as yet these deep strikes have not led to a strategic turning point in the conflict.

Ukrainian attacks with increasingly advanced *Unmanned Surface Vessels* (USVs) on the Russian fleet in the Black Sea area have not led to a turning point either. The intensity of these attacks strongly decreased in 2024. This is in part due to Russia deciding to position the fleet in a more eastern direction.

2.2. Russia

Despite the large personnel and materiel losses, limited territorial gains on the Russian side, and Western sanctions - which have consequences for the Russian production capacities of advanced weapons - until now Russia has been able to handle the losses. Even though it remains to be seen whether Russia will be able to continue this economically in the long term, until now Russia has shown itself able to produce, revise, and modernise sufficient military materiel with its defence industry. For example, various branches of Russia's armed forces have made considerable investments into the integration of unmanned systems. They use the lessons learned from the war in Ukraine to increase the effectiveness of these unmanned systems. Furthermore, Russia is supported by China, Iran, and North Korea, among others, in which Pyongyang also supplied troops which were deployed by Russia to the front line in Kursk. In part as a result of the material support Russia receives from these countries, it can use a limited part of its own production to add to its strategic reserves.

Russia shows an undiminished willingness to target the borders of NATO's air space when attacking Ukraine, in which Russia accepts the risks of border incidents with physical victims.

Ahead of a possible ceasefire and a post-conflict scenario in Ukraine, Russia is developing ambitious plans to reform and expand its armed forces. Central to this is the preparation for a possible military conflict with NATO.

In this context, in 2024 Russia revised its public nuclear doctrine. The 'nuclear threshold' has been *de facto* lowered. The goal here is to increase the deterring effect of nuclear weapons, without losing credibility and freedom of action. Revising the public nuclear doctrine can be seen as a step of escalation in the war in Ukraine, but mainly plays a role in the broader relations between Russia and the West.

2.3 Conceivability military escalation

As previously mentioned, Russia believes that the war in Ukraine is part of a larger and existential conflict with the West. One of the main questions is how big the risk is that the war in Ukraine will result in an open military conflict between Russia and the West (NATO).

A scenario in which Russia will carry out a military operation against NATO that is limited as regards time and geography, is as yet deemed unlikely. However, according to the AIVD and MIVD, Europe will have to make preparations for such a scenario.

The AIVD and MIVD estimate that in the worst case scenario, after ending the war in Ukraine Russia will need less than a year to develop enough capacity for a military operation with limited geographical goals. Such a military operation will not aim for the military defeat of NATO but for breaking up the alliance and forcing concessions as regards to the European security architecture. This expressly does not mean that Russia currently has the intention to proceed with a military escalation of the broader conflict with the West. For the time being, Russia has other, less risky options to weaken the NATO alliance.

The fast development of military capacity gives Russia the opportunity to exert pressure on Europe. Moreover, Russia is increasing the pressure on Europe by developing activities in the hybrid domain. Their approach is to remain under the escalation limit of an open military conflict. However, Russia does not have complete control over the effects of these hybrid activities, as a result of which these activities do increase the risk of (unintentional) military escalation. Even without an open military conflict the increased Russian hybrid activities have a considerable impact on the national security of the Netherlands and other European countries. This is further elaborated upon in the next chapter.

3. The threat of Russian hybrid activities in Europe

Since late 2023, Europe has increasingly been confronted with hybrid activities by Russia in various places, both in the physical and digital domain. Hybrid activities are a combination of influencing activities such as covert influencing, cyberattacks, spreading disinformation, economic destabilisation, or concrete attacks on e.g. vital infrastructure. Furthermore, Russia continues to develop classic espionage activities to obtain intelligence on the intentions, capabilities, and activities of the West in relation to Russia or issues important to Russia. Information on this is crucial to Russia, also for developing the above-mentioned hybrid activities.

3.1 Why does Russia carry out hybrid activities?

Hybrid activities are not a new phenomenon in the least. For a very long time such activities have been a concrete part of the Russian political-strategic and military thinking. The goal of hybrid activities is complex.

In a general sense, these activities are aimed at undermining a society. Think, for example, of influencing the public debate, influencing and frustrating political decision-making, and undermining trust in the Western political-administrative system. Through these activities, the resilience of a society can come under pressure.

In the context of the war in Ukraine and the broader conflict Russia believes it is entangled with the West. Russia attempts to undermine the public, political, and military support for Ukraine with these activities. Russia does this by playing into feelings of fear for a further escalation of a military conflict with Russia. Furthermore, Russia uses these activities to weaken the political cohesion and drive apart Western alliances such as NATO and the European Union. Russia also tries to use the hybrid activities to gauge the West's response to their actions: it attempts to gain an insight into the West's 'red lines' and any possible countermeasures and reprisals.

Fire in Diehl Metal factory after suspected Russian sabotage in Berlin, Germany. 3 May 2024.

3.2 Plausible deniability: obfuscating (Russia's) involvement

Even though the services establish that the threat posed by Russian hybrid activities has increased, the suspected Russian involvement behind various hybrid incidents cannot always be confirmed. This is due in part to these hybrid activities being based on the principle of plausible deniability and therefore by definition are difficult to trace back. In many cases Russia's involvement is purposefully camouflaged. The Russian activities in the hybrid domain are aimed at causing the biggest effect while taking the smallest risk at causing a (large-scale) military escalation.

This does not mean that this principle of plausible deniability is true in all cases. In some cases, Russia chooses to implicitly or even explicitly show its involvement. This way, Russia wants to show it is capable of developing activities anywhere and anytime.

3.3. Increased willingness to take risks

Since 2024 Russia has been taking more risks when carrying out hybrid activities. With this increased willingness to take risks, Russia has developed influencing activities with a violent component to an increasing extent, in which they put up with the fact that these activities may result in material damage and even physical damage. Russia also has acted more openly and assertively than before 2024. Russia may have experienced it as convenient and positive that its involvement has regularly been suspected or discovered.

On the next pages, we will discuss a number of concrete forms of Russian hybrid activities.

Since 2024 Russia has been taking more risks when carrying out hybrid activities.

4.
(Covert) influencing by Russia

Russian influencing can take place overtly as well as covertly. This chapter focuses on the influencing activities Russia develops covertly. Covert influencing is one of Russia's classic hybrid means. Driving forces behind the Russian covert influencing activities are, among others, the Russian intelligence and security services and the Russian Presidential Administration (PA). The involved Russian state bodies can appeal to almost all parts of Russian society and use a so-called whole of society approach. Russia appeals to like-minded persons, networks, and organisations which are used to support and carry out Russian influencing campaigns, wittingly or unwittingly.

4.1 Opportunism and pragmatism leading

In covert influencing activities, the Kremlin primarily focuses on a number of countries which are politically leading in Europe, such as Germany and France. Moreover, it focuses on countries where Russia assesses there to be a fertile breeding ground or susceptibility for narratives that favour the Kremlin or disinformation spread by Russia.

This does not mean in the least that the Netherlands is completely out of Russia's sights. Russia mainly acts on the basis of opportunism and pragmatism. That is why smaller countries that are less powerful politically are also on Russia's radar as a target of covert influencing campaigns. For example, as a result of political statements or decisions in relation to the war in Ukraine, the Netherlands could become a more prominent target of Russian covert influencing activities.

Furthermore, the Netherlands is a host country for various international organisations Russia sees as targets, such as the Organisation for the Prohibition of Chemical Weapons (OPCW) and the International Court of Justice.

4.2 Disinformation campaigns

For many years, Russia has also used disinformation campaigns within the digital information domain. After the start of the large-scale military invasion in Ukraine in 2022, Russia continued to spread disinformation, fake news, and narratives that favour the Kremlin through various channels. In this, Russia uses both Russian and foreign (social) media and plays into existing social polarisation in the West in an opportunistic way. It also uses formal and informal proxy networks of influencing agents. Moscow can appeal to a broad and international network of journalists and content creators who knowingly or unknowingly contribute to making and spreading disinformation and narratives that favour the Kremlin.

Sanctions have somewhat limited the spread of Russian fake news and narratives that favour the Kremlin, but Moscow is still always able to influence the public debate in the West through the digital information domain and physical networks.

Chairs in Dutch Parliament's House of Representatives, The Hague.

Disinformation campaign: Doppelgänger

Doppelgänger is a Russian disinformation campaign that has been widely reported on. In this campaign Russia copied over seven hundred websites of e.g. European media. The long-term campaign was launched in spring 2022 with the goal of supplying mainly Western readers with information that favours the Kremlin. As a result of the identical layout readers were supposed to believe that the information stemmed from familiar and trustworthy European news companies. The Russian Social Design Agency carried out the campaign by order of the Kremlin.

4.3 Covert impact via demonstrations

In the physical domain, Russia focuses on the covert organisation of demonstrations or tries to piggyback on demonstrations with mainly a pacifist or anti-NATO nature. For example, in May 2023 Russia seized upon a demonstration of Extinction Rebellion in The Hague in order to spread expressions that favour the Kremlin. Extinction Rebellion does not appear to have been aware of this at any moment. Russia attempts to utilise such activities primarily for publicity to convince the Russian population that there is enough criticism in the West of the political and military support to Ukraine. For example, every now and then Russian state media reports on demonstrations in the Netherlands in which participants carry out a message that favours the Kremlin. An example of this are the peace demonstrations on the Dam Square in Amsterdam, where messages that favour the Kremlin are propagated. One of the Dutch participants in this demonstration, who supports anti-institutional extremism, recently received a decoration from an organisation related to Russia in the Netherlands for his contribution to the 'keeping of the peace'.

4.4 Covert influencing European Parliament

Russia also focuses on European politicians, including members of the European Parliament, who have a certain sympathy for the Kremlin or ideas that favour the Kremlin. Russia attempts to forge bonds with these politicians by for example funding international trips and providing payment. One of the more remarkable examples in this context is the so-called Voice of Europe case. Members of parliament and employees were paid to spread Russian propaganda in the European Parliament and through a journalistic medium.

The Kremlin attempts to undermine the political cohesion in the West by for example focussing on European politicians and tempting them through misleading 'jokes' to make sensitive or confidential statements.

Other ways in which Russia increasingly carries out covert influencing campaigns in the physical domain vary from placing caskets near the Eiffel Tower, accompanied by the text 'French soldiers of Ukraine', to defacing or destroying government buildings, office buildings, media companies, and other symbolic locations in European cities.

Misleading and eliciting: the Russian duo Vovan and Lexus

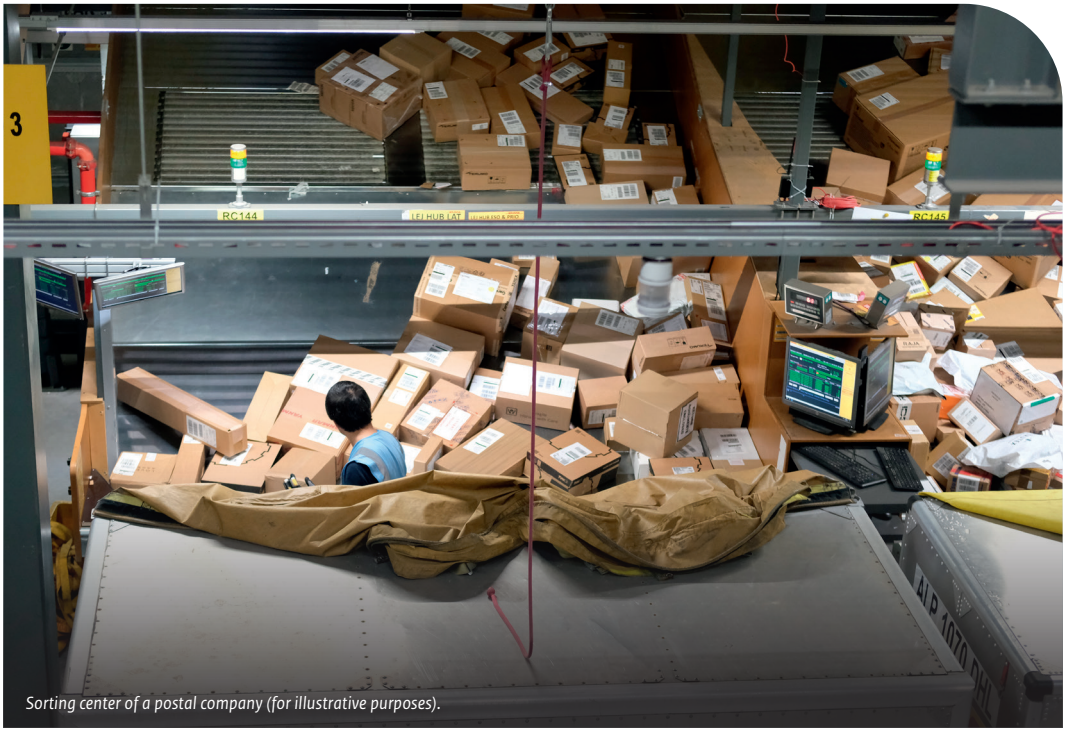
The Russian comedy duo Vovan and Lexus regularly carries out misleading 'jokes'. These jokes target European politicians and dignitaries of the European Central Bank and the International Olympic Committee. The duo elicits statements from them that could get Russia unique information which could be used at a later time to discredit the persons or the countries they represent. These activities are increasingly in line with the Kremlin's narrative.

5.
Sabotage activities

Since spring 2024, Russia's hybrid activities in various places in Europe have become more brazen and aggressive. This shows from an increase in the number of sabotage activities. These activities are illustrative of Russia's aforementioned increased willingness to take risks.

The AIVD and MIVD use the following definition for sabotage: wilfully damaging military and civil targets, for example to delay war shipments, to sow fear and discord, or to test when and how opponents respond. The Russian sabotage activities are not new. During the Cold War, Russian intelligence and security services intensively worked on sabotage plans against the West.

By means of sabotage activities on European territory, Russia broadly tries to reach the same goals as they do with the other hybrid activities described in this publication. In the case of sabotage activities in the physical domain, Russia is especially focussed on the following two goals: undermining society's support for Ukraine, and the actual disruption of military materiel support of Europe to Ukraine.



Sorting center of a postal company (for illustrative purposes).

5.1 Increased willingness to take risks

The increased willingness to take risks mainly manifests in Russia's acceptance that sabotage activities could lead to fatalities or to material damage. Retaliation also appears to play a part in Russia's increased willingness to take risks, specifically for Ukrainian attacks with *deep strikes* on targets far behind the front lines on Russian territory. The Kremlin states that these attacks cannot take place without Western support and expressly holds the West responsible.

5.2 Reports on sabotage

Since spring 2024, various media have described an increase in sabotage activities in Europe. Sometimes, this reporting is done on the basis of suspicions of Russian involvement, without there being concrete indications for it. The reports do not always distinguish between actual sabotage and plans for sabotage. Even though the AIVD and MIVD also state that there is an increase in sabotage activities, not all incidents can be attributed to Russia on the basis of intelligence.

Reports in which suspected Russian sabotage activities are presented as fact may lead to a distorted picture of the extent of Russian sabotage activities in Europe. As a result, they may unintentionally contribute to Russia's goals. The impression may arise that Russia is able to attack Europe anywhere and anytime. Out of opportunism, Russia will allow this idea to endure or even attempt to strengthen it. This does not only cause social unrest and fear for further escalation, but also feeds into the feeling that Europe is unable to protect its citizens.

5.3 Escalation and de-escalation of sabotage activities

Sabotage activities which can be attributed to the Russian intelligence and security services came to a head (for now) in the summer of 2024. After this the number of sabotage activities decreased. As yet, it is unclear why Russia scaled down its sabotage activities in Europe at the time. A cautious increase in sabotage activities can be observed since the summer of 2025. This suggests that Russia keeps open its options for escalation and de-escalation with regard to sabotage activities.

Attributing sabotage activities can be difficult for many reasons and can require a lengthy investigation. An example of this is an explosion in 2014 near a Czech ammunition depot, which was only publicly attributed to the Russian military intelligence service (GRU) in 2021. The explosion took place during the Russian illegal annexation of Crimea and was possibly related to Czech weapon deliveries to support Ukraine.

So far, these sabotage activities have been mainly focused on countries at Europe's eastern flank, including the Baltics and Poland. Furthermore, Russian sabotage activities focus on countries which Russia believes play a prominent role in supporting Ukraine, for example the United Kingdom and Germany. The AIVD and MIVD have identified various cyberoperations and preparations for sabotage in the Netherlands.

5.4 Sabotage in Europe

The media reported various sabotage actions which were attributed to Russia. For example, on 12 March 2025 Poland brought charges against a Belarusian resident for committing arson at a home improvement store in Warsaw. The arson attack took place in spring 2024. The suspect allegedly acted by order of the Russian intelligence and security services.

In Estonia, seven persons were arrested for destroying the cars of the Estonian Minister of the Interior and a journalist. The suspects played different roles by order of the Russian intelligence and security services. This included gathering information and carrying out attacks.

In February 2025, a Ukrainian was sentenced to eight years in prison by a court in Poland for carrying out arson attacks and sabotage in Poland encouraged by Russia. According to the public prosecutor the suspect was recruited via Telegram and was allegedly paid to commit an arson attack on a paint factory in Wroclaw.

In November 2024 a railway in the east of Poland on the route from Warsaw to Lublin was damaged. This train line connects Warsaw with the Ukrainian border and is important for the supply of (military) aid. According to the Polish authorities, which carried out multiple arrests in relation to this, these were sabotage activities directed by Russia.

Sabotage activities with parcel post

One of the most advanced and riskiest sabotage activities to date of which involvement of the Russian intelligence and security services was established are the parcels which were sent to addresses in Europe and North America in the summer of 2024. Some of these parcels were test parcels, but in some cases they contain *improvised incendiary devices* (IIDs). A number of these parcels combusted in sorting centres of commercial post companies in Europe.

The AIVD and MIVD established that test parcels were also sent from the Netherlands. These parcels did not contain incendiary materials. The services estimate that this likely did not concern a sabotage activity which targeted the Netherlands, but a reconnaissance during which the logistical routes and the timing of the shipping of the parcels were identified. The sender was recruited online and he was highly likely unwitting; unaware of the underlying goals of the shipment nor of the fact that they acted by order of Russia.

In a few cases Russia made plans for sabotage activities aimed at human lives. One remarkable example of this is the thwarted plans to assassinate the director of the German weapons manufacturer Rheinmetall[3]. These plans were aimed at disrupting the Western military support to Ukraine and discouraging other European weapons manufacturers.

5.5 Adjusted modus operandi

The Russian intelligence and security services have started to use a different modus operandi in carrying out sabotage activities. In part due to the large-scale extradition of Russian intelligence officers under diplomatic cover by a large number of European countries, which followed the Russian invasion in Ukraine in 2022, it has become more difficult for the Russian intelligence and security services to develop activities in Europe. In order to remedy this, the Russian services started to use different tactics. They applied themselves to using layered networks. These networks consist of coordinators, facilitators, and so-called *low-level* agents who carry out the sabotage actions.

These *low-level* agents are approached via messaging apps such as Telegram or via personal contacts. They are asked to gather information, spread fake news or disinformation, or carry out cyberattacks. Moreover, they are often asked to map potential targets for sabotage activities, carry out reconnaissance, or actually carry out sabotage activities. Before they receive payment, the low-level agent is often asked to prove that the assignment has been executed, often by providing video footage.

A clear profile for these *low-level* agents cannot be given. It does often concern persons who see sabotage activities as a way to easily and quickly make money. These, sometimes underage, *low-level* agents often do not seem aware that they carry out activities by order of Russia. They operate *unwittingly* and as so-called *useful idiots*. They often do not appear to have an ideological drive or sympathy for Russia. However, various identified *low-level* agents had a criminal past and a criminal record. As opposed to intelligence officers, these *low-level* agents have received little to no training. Even though the use of these agents is in line with the principle of plausible deniability, the risk of identified or failed operations increases as a result of the lack of training, but also a lack of motivation.

[3] Rheinmetall plays a prominent role in the supply of materiel support to Ukraine.

6.
(Suspected) sabotage at sea and in the air

From the second half of 2024 the number of suspected sabotage incidents at sea has strongly increased. These incidents concern cable failures and damage (to varying degrees) of submarine communications cables. The media also expressly pays attention to these incidents. Intelligence investigation shows that as yet, for the majority of these suspected sabotage incidents it cannot be established that sabotage actually took place. On the basis of our own intelligence picture these incidents cannot be directly attributed to Russia. This does not mean that it is inconceivable that Russia is developing these kinds of activities.

Ship of the Finish coastguard nearby the taken shadow fleet Eagle S, Finland. 30 December 2024.

Complexity attribution
There are various reasons as a result of which it is difficult to attribute these maritime incidents to Russia. Think, for example, of the aforementioned principle of plausible deniability. But also for incidents where a Russian link has been established, this does not automatically mean that sabotage took place. Even though various submarine incidents, for example in the Baltic Sea, are linked to Russia, these links can be explained in the regional context and are not necessarily suspicious.

For example, it is normal for some of the ships in the Baltic Sea to sail under the Russian flag and call at Russian ports; this simply fits the profile of the shipping there. Furthermore, cable failures are a regular global occurrence. For most of these 'regular' incidents, there is a combination of factors at play: a lot of maritime activity in the area, relatively shallow water, and a high density of submarine infrastructure. These three circumstances are also in place for the Baltic Sea.

Most cable failures are caused by fishing or ship anchors (that have broken away). Moreover, in many cases bad weather and 'bad seamanship' play a part.

Examples of suspected sabotage incidents in the maritime domain

On 17 and 18 November 2024 two submarine cables were damaged in the Baltic Sea. This highly likely occurred when one of the anchors of the merchant ship *Yi Peng 3* dragged along the seabed. The ship, which sailed under Chinese flag, left from a Russian port. At least part of the ship's crew allegedly had the Russian nationality. Besides the suspicion and this link to Russia, it has not been established that this actually was sabotage.

Early January 2025, the media reported on the ship *Eagle S*, which belongs to the Russian 'shadow fleet'. This ship highly likely caused a failure of the *Estlink 2* in the Gulf of Finland. As yet, it has not been established whether this was actual sabotage.

On 26 January 2025, a submarine communications cable between Sweden and Latvia was damaged. This time, it was the anchor of the ship *Vezhen* which dragged along the seabed. The Swedish authorities, which had levied an attachment on the ship, came to the conclusion on the basis of a multidisciplinary investigation that no sabotage activities had taken place.

More recently, on 31 December 2025, the Finnish authorities boarded the cargo ship the *Fitburg* after a telecommunications cable in the Gulf of Finland was damaged. Here, too, the anchor of the ship, which was travelling from Saint Petersburg to Haifa (Israel), was allegedly responsible for damaging the cable. The incident is under investigation by the authorities, which allowed the ship to continue its course on 12 January 2026. As yet, it is too early to establish whether actual sabotage was carried out.

Impact as yet limited
Telecommunications cables have a high level of redundancy; if a cable breaks down, another cable can often 'take over'. Additionally, the infrastructure is generally quickly repaired. This considerably limits the effects of these incidents as regards time and extent.

Espionage at sea
As yet in the Netherlands there are no examples of maritime sabotage of e.g. submarine cables. However, it has been established that Russia maps the infrastructure of the North Sea, Baltic Sea, Atlantic Ocean, and other waters and develops (submarine) activities which indicate espionage. This causes concern because the acquired knowledge can be used for sabotage purposes at a later date.
The number of reports on launches of (suspected) Russian drones from cargo ships which are located in Russian waters has also strongly increased.

For example, in May 2025 the cargo ship *HAV Dolphin* was inspected after reports that drones were allegedly launched above the North Sea and Baltic Sea from that ship. The whole crew of the ship which sailed under the flag of Antigua and Barbuda was Russian. The inspection did not yield any evidence. A similar case took place with relation to the Russian cargo ship Lauga. Close to the German island of Borkum seven drones were seen in the vicinity of the ship. This ship also had a fully Russian crew, and inspection of the ship also yielded no evidence or additional indications for suspicion of espionage.

Drone observations
In addition to increased media attention for observations of drones (unmanned systems) that can (possibly) be attributed to Russia, the AIVD and MIVD have in the past two years also received an increasing number of reports on observations of drones near vital infrastructure, airports, and for example military facilities in the Netherlands. For these kinds of reports, it is also the case that establishing suspected Russian involvement is complicated. More than that, in various incidents it appears difficult to even establish whether what was observed were actually drones or not. There where these were observed, it could not be established who operated the drone nor whether an activity had taken place that could be attributed to Russia. Similar to the incidents in which submarine cables were damaged, it does not mean that it is inconceivable that Russia would use drones to (seriously) disrupt air traffic.

For these kinds of reports, it is also the case that establishing suspected Russian involvement is complicated.

7. Digital attacks and cybersabotage

Also in the digital domain, Russia now develops a large variety of influencing activities: from cyberespionage to cybersabotage. Since 2023 AIVD and MIVD have observed an increase in the number of cyberactors on the Russian side in the cyberdomain. Also in the cyberdomain Russia increasingly uses a whole-of-society approach: with a cooperation of various private and government entities Russia shapes its offensive cyberprogrammes. The goals of the activities in the cyberdomain connect to the aforementioned goals to sow fear and discord, undermine support to Ukraine, and test the West on its willingness to escalate.

We can distinguish between two types of cyberactors: state(-sponsored) attack groups and state-backed hacker groups. State(-sponsored) attack groups (*advanced persistent threats* or *APTs*) are often part of the Russian intelligence and security services. These attack groups often carry out lengthy and targeted cyberoperations, which are aimed at government bodies and vital infrastructure in Western countries. State-backed hacker groups pretend to be independent hacktivists, but are often supported or even directed by the Russian state.

Both before and after the large-scale invasion of Russia in Ukraine, Russia carried out cyberactivities in the cyberdomain at a large scale, for example DDoS attacks, hack-and-leak attacks, and so-called defacements[4].

Russia still does this. Furthermore, in the weeks following the large-scale invasion, Russia deployed wipers[5]. Along the way, in the cyberdomain Russia has been focussing more on obtaining military and diplomatic information on Ukraine as well as NATO allies. While the war continued, Russia's cyberactivities became more complex, in part because of the West's continued support to Ukraine. With these cyberactivities Russia has started focusing more expressly on the (vital) infrastructure - not just in Ukraine, but also in the West.

With a cooperation of various private and government entities Russia shapes its offensive cyberprogrammes.

[4] DDoS: digital attack on the capacity of online services or the supporting servers of network equipment, as a result of which they could become overloaded and go offline. Hack-and-leak: stolen data is leaked to create a political or social effect or to sell them to other parties. Defacement: the undesired adaptation of a web page by hackers, in which the original page is often replaced by political messages.

[5] Wipers: digital attacks in which data is deleted, causing work stations and servers to become unserviceable.

AIVD and MIVD news articles warning for the Russian cyberactor Laundry Bear.

7.1 Russian cyberattacks in the Netherlands

In the Netherlands too, Russian activities have been observed in the cyberdomain. These activities vary from low-effort to more refined attacks which are often motivated by opportunism and pragmatism. In an attempt to hamper Dutch voters during voting in the European elections of 2024, Russian state-backed hacker groups carried out DDoS attacks, before and during the elections. These attacks were aimed at e.g. websites of political parties and companies in the Dutch public transport sector.

The Netherlands can also become an indirect victim of cyberattacks, for example through activities targeting Dutch allies. Russian cyberactors have already obtained sensitive information in this way, such as personal data of Dutch government employees and Dutch companies.

Furthermore, the AIVD and MIVD have observed more digital attacks targeting mobile devices such as phones. Because messaging applications are used a lot around the world and can be abused in various ways by malicious actors, messaging apps are a vulnerable means of communication and with that a preferred target of Russian cyberactors. Over the past year, the services have established that a Russian cyberactor obtained access to the messaging accounts of multiple Dutch government employees. In this they did not only gain access to the compromised accounts, but these accounts were even taken over so that contact persons assumed they were in contact with the victim. Russian cyberactors also still target numerous victims by sending malicious emails or chat messages.

Cyberattacks in the Netherlands
In November 2024 Russian state-sponsored hackers, linked to the Russian hacker collective Z-Pentest, gained access through a hack to the operating system of a fountain in the centre of a Dutch city. They attempted to change the composition of the water.

The Dutch National Police was also targeted by a digital espionage attack in which work-related contact details of police employees were obtained by a cyberactor which, at that time, was not known to the public. This cyberactor is highly likely supported by the Russian state and was given the name LAUNDRY BEAR by the services. It has been carrying out cyberattacks on Western governments, companies, and other organisations since at least 2024. The attacks of this cyberactor are often directed at targets which are relevant for Russia's war efforts in Ukraine, such as the Ministries of Defence of NATO countries, branches of the armed forces, and defence suppliers. The Dutch police appears to have been a target for opportunistic reasons.

Furthermore, in April 2025 many websites of Dutch cities and provinces were unreachable after DDoS attacks by Russian state-backed hacker groups. In the run-up to and during the NATO summit of 2025 in The Hague, mainly low-effort cyberattacks from Russian cyberactors were observed. This concerned, among other things, preparations for a phishing campaign by the aforementioned actor LAUNDRY BEAR.

7.2 From hacking systems to sabotage

The aforementioned increased willingness to take risks on the Russian side also shows in the cyberdomain. The AIVD and MIVD establish that not only the technical knowledge and capabilities of different state-backed hacker groups have increased, but also the willingness to actually carry out (cyber)sabotage after hacking and compromising systems.

The cyberattacks target allies of the European Union and NATO, as well as targets in the Netherlands. In addition to the framework above, an unsuccessful cyberoperation was carried out in the Netherlands which targeted a company in the Dutch vital infrastructure.

Russia possibly carried out this operation to get into position for cybersabotage. The arrest of two minors on suspicion of espionage in September 2025 illustrates that this threat also manifests itself in the Netherlands.

Moreover, the past year Russian state(-sponsored) attack groups and state-backed hacker groups have carried out more cyberoperations in which sensitive information was obtained. Russia can then use this information to carry out activities in the physical domain, for example in Russian acts of war in Ukraine. Most notable is that the hacker groups work very opportunistically and 'take what they can get'. In this, they compromise various operating systems, often with insufficient security. This broad range of targets makes it difficult to anticipate such attacks

8.
Impact on Dutch society

The war in Ukraine and what Russia believes to be an existential conflict with the West have a broader impact on Dutch society. As described, Russia attempts to play into existing social polarisation and to increase this. This does not always mean that there is a structural and coordinated intention which is directed by the Kremlin or other actors linked to the Russian state. The narrative which favours the Kremlin does resonate with the anti-institutional extremist movement and matches parts of the anti-institutional narrative.

Hofvijver nearby Binnenhof, The Hague.

The anti-institutional narrative includes the idea of an evil elite which controls all influential institutions and uses its power to suppress 'regular citizens'. To legitimise this repressive policy, the elite allegedly devises different crises such as the COVID-19 pandemic, the nitrogen pollution crisis, and also the continued conflict in Ukraine.

The anti-institutional extremist movement in the Netherlands is still mostly pro-Russian. The movement sees president Putin as a 'saviour' who dares take on the evil elite in the West and dares question the international order dominated by this evil elite.

To a certain extent this is similar for radical right-wing and right-wing extremist movements. Even though as yet, this pro-Russian attitude only contributes to a very limited extent to the further spread of narratives which favour the Kremlin, this pro-Russian attitude does possibly make the extremist movement susceptible to Russian (covert) influencing.

However, radical and extremist movements may see it as an opportunity to approach Russia as an 'ally' which strives for partially comparable goals. This does not mean that Russia will automatically accept the requests of these radical and extremist movements.

But the support which may stem from possible interaction could contribute to the spread, normalisation, and legitimisation of its own extremist ideology. Furthermore, interactions between actors linked to the Russian state and radical and extremist movements may increase the extremist and terrorist threat of these movements. This can also be seen in various attacks in a number of European countries[6]. To this day, Russia has hardly directly contributed to the extremist and terrorist threat in the Netherlands.

In addition, the steps which Europe is currently taking to prepare for a possible open military conflict with Russia may cause a counterreaction among anti-military and pacifist movements. Russia can play into these possible counterreactions and use them to spread statements that favour the Kremlin.

8.1. No indications for travel by groups of Dutch extremists

There are still no indications that large groups of Dutch citizens with an extremist ideology travelled to Ukraine to fight on the Ukrainian or Russian side in the war. Even though some extremist movements in the Netherlands have sympathy for certain fighters or militias, the war in Ukraine plays an extremely limited role in their propaganda.

Effects of the war on the jihadist threat

The possible effects of the war in Ukraine as described in the previous publication from 2023[7] have been partially confirmed.

It is likely that the decrease in Russian activities in Syria contributed to Bashar al-Assad, who was backed by Russia, having to step down in 2024. This resulted in ISIS in Syria experiencing a minor resurgence in 2025. A number of ISIS members who previously resided in Ukraine, especially in 2022, came to Europe. They were linked to Islamic State Khorasan Province (ISKP), originally the Afghan branch of ISIS. They are members of the external ISIS attack network which is located in Syria. Some of them have been involved in concrete attack planning. In Western Europe, a number of these attack plans were disrupted in 2022, 2023, and 2024. In the Netherlands, two persons were also arrested: a man from Tajikistan and a woman from Kyrgyzstan.

[6] See theme chapter: increasing Russia state threat contributes to the extremist and terrorist threat to a limited degree, Threat assessment Terrorism the Netherlands, dated 17 June 2025.

[7] 24/2 The Russian attack on Ukraine: a turning point in history.

9.
Conclusion

The AIVD and MIVD observe that Russia considers itself to be entangled in a broader and existential conflict with (in Russia's perception) the perverse and decadent West. This conflict takes place in the military, economic, and ideological field, of which the last is the most fundamental. In Russia's eyes this existential conflict is a conflict not only between conflicting, but even incompatible world views based on contrary norms and value systems. Russia presents itself as a unique civilisation. In this light Russia prepares for a long-term confrontation with the West.

EU flags in Brussels, Belgium.

Military course in Ukraine
Russia still suffers great losses without obtaining its operational goals: the 'denazification' and demilitarisation of Ukraine. Despite the considerable losses, the high economic price, and the limited territorial gains, the war in Ukraine is progressing in Russia's favour. Even though Moscow realises that in the end the war will be resolved at the negotiating table, Moscow appears almost entirely unwilling to make any actual concessions.

Russia's goal is to rearrange the European security architecture in which it wants a veto on developments the country perceives to be a threat. To this day and with the help of countries such as China, Iran, and North Korea, Russia has shown itself capable of handling and compensating the suffered personnel and materiel losses in Ukraine. At the same time, Russia is able to carry out some limited developments its ambitious expansion plans for the armed forces. Ahead of a possible ceasefire and post-conflict scenario, Russia expressly prepares for a possible military conflict with NATO.

Military escalation no longer inconceivable
As yet a direct military conflict between Russia and NATO is unlikely, but since the war in Ukraine it has become conceivable.

The AIVD and MIVD estimate that in the worst case scenario, after ending the war in Ukraine Russia will need less than a year to develop enough capacity for a military operation with limited geographical goals. Such a military operation will not aim for the military defeat of NATO but at breaking up the alliance and forcing concessions as regards the European security architecture. This does not mean that at this moment, Russia actually intends to take action. According to the AIVD and MIVD, Europe will, however, have to prepare for such a scenario.

Increased hybrid threat
The AIVD and MIVD also assess that the hybrid threat posed by Russia has increased. In part as a result of the war in Ukraine, since autumn 2023 this hybrid threat has manifested more expressly in Europe. In the Netherlands too various Russian hybrid activities have been observed, including preparations for sabotage. The Netherlands is and remains an interesting target country for Russia in part because of the support to Ukraine and the fact that the Netherlands is a host country to various international organisations Russia sees as a target.

The AIVD and MIVD expect that the threat of hybrid Russian activities will continue. Even after a possible ceasefire in Ukraine. Driven by pragmatism and opportunism, Russia will continue to use the possibilities our open society offers. A new modus operandi Russia deploys here is the use of so-called *low-level* agents: persons who received little to no training contribute to sabotage activities, in which they often are not aware that the directions come from Russia.

The AIVD and MIVD expect this hybrid threat to come and go in waves, with moments of escalation and de-escalation.

In the coming years, the AIVD and MIVD expect this hybrid threat to come and go in waves, with moments of escalation and de-escalation. Europe, but also the Netherlands, will have to take into account Russia's increased willingness to take risks shown over the course of 2024.

Because of the experience Russia is gaining as regards hybrid activities and the technical capabilities it is developing here, the AIVD and MIVD also deem it likely that in the future Russia will carry out more impactful hybrid activities.

Threat in the long and short term

Because of developments in the war and the continuous support of the West to Ukraine, Russia believes that Europe has more expressly become a 'part of the problem'. This, in addition to Western sanctions and other attempts at isolating Russia, causes Russia to approach alternative partners and forums on the international stage. The goal is to counterbalance the international order which in Russia's perception has been dominated by the United States since the Second World War. Russia has proven relatively successful in this, even though Russia is less dominant in various of these relationships–that are crucial to Moscow–than it would like to be. As described in this publication the Russian perception of the West is directly connected to the threat Russia projects onto the West. Regardless of the outcome of the war in Ukraine, Russia will likely continue to pose a threat to the Netherlands, Dutch interests elsewhere, and our allies.

Importance of cooperation

The battle Russia is fighting as autocratic regime against Western democracies is asymmetrical. Where the Dutch services are democratically embedded with an accompanying supervisory system, the Russian services act on the basis of different rules. To counter the Russian threat, (public-private) cooperation is crucial in both the national and international context.

The AIVD and MIVD have their own, unique tasks in this. In addition to investigating threats, the services support the increase in resilience of government organisations, knowledge institutions, and companies of vital sectors. The AIVD and MIVD help these institutions to expand their knowledge on the dangers of espionage, sabotage, and knowledge theft. This is done on the basis of e.g. (technical) publications on threats and sharing concrete perspectives for action. Together with the National Coordinator for Security and Counterterrorism (Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCTV) and the National Cyber Security Centre (Nationaal Cyber Security Centrum, NCSC), the services provide advice to organisations on their (digital) resilience.

The cooperation with domestic and foreign partners and the joint support to Ukraine continue to be important. The services take action to counter threats together with their partners. As a result, the services actively play into relevant technologies and continuously build on an innovation network for the government, knowledge institutions, and private partners. For the security of Europe and the rest of the world.

General Intelligence and Security Service
P.O. Box 20010 | 2500 EA The Hague
aivd.nl

Military Intelligence and Security Service
P.O Box 20701 | 2500 ES The Hague

February 2026