Tussen vrede en oorlog

De oorlog in Oekraïne en de Russische dreiging in Europa

Samenvatting

De AIVD en MIVD nemen waar dat Rusland zich verwikkeld ziet in een breder en existentieel conflict met het Westen. Dit conflict speelt zich af op militair, economisch en ideologisch vlak. De oorlog in Oekraïne is daar voor Rusland slechts een onderdeel van. De relatie tussen Rusland en het Westen heeft als gevolg van de oorlog in Oekraïne een nieuw dieptepunt bereikt. Bestaande tegenstellingen zijn door de oorlog verder verscherpt en verdiept. Als gevolg hiervan is een militair conflict tussen Rusland en het Westen niet langer ondenkbaar. Rusland is niet alleen in staat gebleken de substantiële verliezen in Oekraïne op te vangen, maar zelfs de krijgsmacht uit te breiden en te hervormen. Daarbij bereidt de Russische krijgsmacht zich voor op de mogelijkheid van een conflict met de NAVO en voert deze verschillende activiteiten uit om de escalatiebereidheid van het Westen te testen.

Rusland bereidt zich voor op een langdurige confrontatie met het Westen - ook op militair gebied. De inschatting is dat Rusland na het beëindigen van de oorlog in Oekraïne in het meest ongunstige scenario mogelijk minder dan een jaar nodig heeft om voldoende capaciteiten op te bouwen voor een militaire operatie met beperkte geografische doelstellingen. Deze militaire operatie zal dan waarschijnlijk niet gericht zijn op het militair verslaan van de NAVO, maar op het uiteenspelen van het bondgenootschap en het afdwingen van concessies ten aanzien van de Europese veiligheidsarchitectuur. Dit betekent niet dat Rusland momenteel ook daadwerkelijk de intentie heeft om hiertoe over te gaan.

Naast deze militaire dreiging, komt de Russische dreiging sinds het najaar van 2023 steeds nadrukkelijker tot uiting via hybride activiteiten[1] die Rusland op verschillende plekken in Europa ontplooit. Deze dreiging is allesbehalve nieuw, maar is wel toegenomen. Rusland probeert aan de hand van cyberaanvallen, beïnvloedingsactiviteiten en (digitale)sabotageacties westerse landen uit elkaar te spelen en de westerse politieke en maatschappelijke steun voor Oekraïne te ondergraven. In de loop van 2024 is Rusland hierbij een grotere risicobereidheid gaan tonen. Deze activiteiten kregen in toenemende mate een geweldscomponent in het fysieke domein. Ook in Nederland zijn verschillende Russische hybride activiteiten waargenomen, waaronder voorbereidingen voor sabotage.

De AIVD en MIVD verwachten dat Rusland dergelijke hybride activiteiten blijft inzetten. Ook na een eventueel staakt-het-vuren in Oekraïne. Deze hybride dreiging zal naar verwachting van de AIVD en MIVD blijven bestaan in een golfbeweging, met momenten van escalatie en de-escalatie. Daarbij zal Europa, en ook Nederland, rekening moeten houden met de grotere risicobereidheid die Rusland in de loop van 2024 is gaan tonen.

Om voorbereid te zijn op een mogelijke verdere militaire escalatie en tegelijkertijd de Russische hybride dreiging te pareren, moet Nederland de eigen weerbaarheid vergroten. Daarbij is alertheid noodzakelijk van overheidsorganisaties, kennisinstellingen en het bedrijfsleven. Want als vitale sectoren uitvallen, kan dat de samenleving ernstig ontregelen.

[1] In deze publicatie wordt onder hybride activiteiten verstaan: beïnvloedingsactiviteiten in zowel het fysieke als digitale domein, waaronder cyberaanvallen, heimelijke beïnvloedingsactiviteiten en sabotageacties.

Inhoudsopgave

Inleiding

Met deze publicatie bieden de AIVD en MIVD inzicht in de Russische dreiging die de afgelopen paar jaar steeds zichtbaarder is in Europa. In het kielzog van de oorlog in Oekraïne is een militaire escalatie tussen Rusland en het Westen voorstelbaar geworden. Daarnaast maken de AIVD en MIVD zich zorgen over de toegenomen dreiging van Russische hybride activiteiten in de *grey zone*: het schemergebied tussen vrede en oorlog.

Op 24 februari 2022 begon Rusland een grootschalige militaire invasie in Oekraïne. Inmiddels is de oorlog in Oekraïne het grootste en meest dodelijke conflict in Europa sinds de Tweede Wereldoorlog. De Russische inval in Oekraïne die destijds door bondskanselier Scholz een *Zeitenwende* werd genoemd, markeert daadwerkelijk een keerpunt in de geschiedenis. Rusland lijdt nog altijd grote verliezen, zonder zijn operationele doelstellingen ('denazificatie' en demilitarisatie van Oekraïne) te behalen.

De relatie tussen Rusland en het Westen heeft in navolging van deze oorlog een nieuw dieptepunt bereikt. Rusland zoekt, mede als gevolg van westerse sancties en andere initiatieven om Rusland te isoleren, toenadering tot alternatieve partners en afzetmarkten. Ook zoekt het aansluiting bij internationale samenwerkingsverbanden die een tegenwicht kunnen bieden aan de internationale orde die in de Russische perceptie wordt gedomineerd door de Verenigde Staten.

Russische perceptie
Voor het duiden van de Russische dreiging is begrip van de Russische perceptie cruciaal. Daarbij dient te worden opgemerkt dat een perceptie per definitie subjectief is. Het is geen op zichzelf staand feit of waarheid. In deze publicatie wordt gerefereerd aan de Russische perceptie, oftewel de wijze waarop Rusland naar de wereld kijkt.

De oorlog in Oekraïne is in de Russische perceptie slechts een onderdeel van een breder en existentieel conflict tussen Rusland en het Westen. Het doel van Rusland is om de Europese veiligheidsarchitectuur te herzien. Daarbij bereidt Rusland zich voor op een langdurige confrontatie met het Westen, ook militair. Dat betekent overigens niet automatisch dat Rusland de intentie heeft om een militair conflict te initiëren.

In de context van deze bredere confrontatie komt de Russische dreiging sinds het najaar van 2023 steeds nadrukkelijker tot uiting in Europa. Deze dreiging heeft niet alleen een militair karakter. De Russische dreiging uit zich in toenemende mate in Europa via hybride activiteiten.

Rusland zet al jaren een veelheid aan hybride activiteiten in, ook in Europa. Dit doet Rusland zowel in vredestijd als in crises en oorlogstijd. Deze activiteiten kunnen zowel in het fysieke als in het digitale domein plaatsvinden. Te denken valt aan heimelijke beïnvloeding, cyberaanvallen, de verspreiding van desinformatie, economische destabilisatie of concrete aanvallen op de vitale infrastructuur. In deze publicatie wordt verder ingegaan op cyberaanvallen, heimelijke beïnvloedingsactiviteiten en (digitale) sabotageacties.

Het doel van deze hybride activiteiten is meerledig. Zo probeert Rusland politieke besluitvorming te beïnvloeden of te frustreren, maatschappelijke verdeeldheid aan te wakkeren en het vertrouwen in ons democratisch bestel te ondermijnen. Daarnaast probeert Rusland met deze activiteiten de onderlinge eenheid in het Westen en het publieke draagvlak voor de steun aan Oekraïne te ondermijnen. Ook gebruikt het deze activiteiten om de militair-materiële steun te verstoren die aan Oekraïne wordt geleverd.

Kenmerkend hierbij is dat Rusland met deze hybride activiteiten de hierboven genoemde doelstellingen probeert te realiseren met zo min mogelijk risico op een militaire escalatie die uitmondt in een openlijk gewapend conflict met het Westen. De inzet van hybride middelen kan daarmee dus een alternatief zijn voor een gewapend conflict.

Het aantal meldingen over (vermeende) Russische cyberaanvallen, beïnvloedingsactiviteiten en (digitale) sabotageacties in Europa is sinds het najaar van 2023 sterk toegenomen. Deze activiteiten variëren van demonstraties, vandalisme en brandstichting tot verstoringen van internationaal vliegverkeer door drones, de beschadiging van (onderzeese) kabels en de verzending van brandstichtende pakketten via luchttransport. De AIVD en MIVD constateren dat de hybride dreiging van Rusland is toegenomen. Toch betekent dit niet dat de vermeende Russische hand in alle gevallen kan worden vastgesteld.

Inmiddels is de oorlog in Oekraïne het grootste en meest dodelijke conflict in Europa sinds de Tweede Wereldoorlog.

Om voorbereid te zijn op een eventuele militaire escalatie met Rusland en om ons beter te kunnen weren tegen de toegenomen hybride dreiging van Rusland, moet Nederland de eigen weerbaarheid vergroten. Daarbij is alertheid noodzakelijk van overheidsorganisaties, kennisinstellingen en het bedrijfsleven. Want als vitale processen en sectoren uitvallen, kan dat de samenleving ernstig ontregelen.

De AIVD en MIVD doen gezamenlijk onderzoek naar de verschillende soorten Russische activiteiten die een dreiging vormen voor de democratische rechtsorde, bondgenootschappelijke belangen en andere nationale veiligheidsbelangen. Met deze gezamenlijke publicatie willen de AIVD en MIVD het bewustzijn over de Russische dreiging vergroten en daarmee de weerbaarheid van de Nederlandse samenleving versterken. De publicatie borduurt voort op het beeld dat is geschetst in februari 2023, in de publicatie *24/2 De Russische aanval op Oekraïne: een keerpunt in de geschiedenis*.

In deze publicatie wordt allereerst ingegaan op de Russische perceptie van het Westen. Vervolgens wordt ingegaan op het verloop van de oorlog in Oekraïne en de mogelijkheid van een verdere escalatie tot een openlijk militair conflict tussen Rusland en de NAVO. Ook wordt een beeld geschetst van de zogeheten hybride dreiging van Rusland, die zich sinds het najaar van 2023 steeds nadrukkelijker op verschillende plekken in Europa manifesteert. Hierbij wordt afzonderlijk ingegaan op Russische heimelijke beïnvloedingsactiviteiten, (cyber)sabotageactiviteiten en (vermeende) sabotageactiviteiten in het maritieme domein en verstoringen van het luchtverkeer door drones. Tot slot wordt beknopt ingegaan op de bredere impact van de oorlog in Oekraïne op de Nederlandse samenleving.

1.
Rusland in conflict met het Westen

De oorlog in Oekraïne is vanuit de Russische perceptie niet zomaar een oorlog met een buurland. De oorlog in Oekraïne is in Russische ogen nadrukkelijk onderdeel van een breder en existentieel conflict met het Westen. Dit bredere conflict speelt zich af op militair, economisch en ideologisch vlak. Daarbij beseft het Kremlin dat het militaire conflict – de oorlog in Oekraïne – eindig is en uiteindelijk aan de onderhandelingstafel zal worden beëindigd.

Op economisch vlak is Rusland sinds de grootschalige militaire inval in Oekraïne vanwege westerse sancties op zoek naar nieuwe afzetmarkten en (handels)partners. Hoewel het economische conflict met het Westen volgens het Kremlin nog langere tijd zal voortduren, lijkt Rusland er nog altijd van overtuigd de gevolgen hiervan te kunnen dragen. Al is het steeds nadrukkelijker de vraag of dat daadwerkelijk zo is en of dat zo blijft. Het meest fundamentele onderdeel van het bredere conflict met het Westen ligt vanuit het Russische perspectief echter op ideologisch vlak. Het is een conflict tussen botsende en onverenigbare wereldbeelden die zijn gebaseerd op strijdige waarden- en normensystemen: het perverse en decadente Westen versus de unieke Russische beschaving.

Vanuit Russisch perspectief dient deze unieke Russische beschaving beschermd te worden tegen het agressieve en expansionistische Westen. Hierbij is Putin – getuige ook de grote personele en materiële verliezen die Rusland lijdt in de oorlog in Oekraïne – bereid een hoge prijs te betalen. De Russische perceptie is gekoppeld aan een *zero-sum*-denken, waarbij er altijd slechts één partij winnaar kan zijn en er dus altijd ook een verliezer is. Waarschijnlijk ligt aan dit narratief ook een minder hoogdravende reden ten grondslag, namelijk regimebehoud.

Vooralsnog is het Russische regime stabiel, al wordt dat afgedwongen met steeds meer repressie en verschillende initiatieven die ertoe moeten leiden dat de Russische autoriteiten meer controle kunnen uitoefenen op het digitale informatiedomein. Deze initiatieven zijn er in zekere zin op gericht om Rusland verder te isoleren van westerse invloeden, die een bedreiging kunnen vormen voor de stabiliteit van het regime.

'Omsingeld door een vijandig Westen'

In deze fundamentele strijd is het Westen er volgens het Kremlin op gericht om Rusland een strategische nederlaag toe te brengen en te destabiliseren. Daarnaast meent Moskou dat het Westen inbreuk pleegt op het Russische recht op een invloedssfeer. Volgens Rusland probeert het Westen landen als Oekraïne los te weken van Rusland, op te nemen in westerse instituties als de NAVO en de EU en rukt het Westen op die manier op naar de Russische grenzen. Deze perceptie speelt een centrale rol en wordt door Rusland steevast als een van de 'grondoorzaken' van de oorlog in Oekraïne genoemd. Het beeld van een Rusland dat is omsingeld door een vijandig Westen is als gevolg van de oorlog niet alleen bestendigd, maar ook verdiept. Europa investeert momenteel om voorbereid te zijn op een eventuele militaire escalatie met Rusland. Het Kremlin ziet deze investeringen als een bevestiging van de offensieve vijandige ambities van Europa en benoemt Europa expliciet en in steeds scherpere bewoordingen als onderdeel van het 'probleem'.

Russische Armata T-14 tanks tijdens een m litaire parade in Moskou, Rusland.

1.1 Het Russische narratief

Narratief binnen Rusland
Sinds de inval stelt het Kremlin alles in het werk om de oorlog voor zichzelf en de bevolking te legitimeren. Het grijpt daarbij terug op middelen die in de ogen van Putin en zijn medestanders hun nut hebben bewezen in de Sovjettijd maar hun wortels hebben in tsaristisch Rusland: vergaande indoctrinatie met één, van bovenaf opgelegd, onbetwistbaar en 'typisch Russisch' normen- en waardenstelsel. Rusland wordt hierbij gepresenteerd als een afzonderlijke beschaving met een messianistische missie. Het Kremlin ziet en propageert isolatie van het Westen als herwonnen soevereiniteit. Moskou richt zich daarbij primair op de jeugd, en doet dat met name via het onderwijs. Zo is in korte tijd vrijwel het gehele Russische onderwijstraject doorspekt met ideologische vakken en activiteiten. Een 'juiste' kijk op de nationale geschiedenis speelt daarin een hoofdrol.

Vanuit deze 'juiste' kijk op de nationale geschiedenis moet de huidige oorlog tegen Oekraïne worden verbonden aan de Tweede Wereldoorlog, toen de Sovjet-Unie het nazisme overwon.

Om binnenlandse steun voor de oorlog in Oekraïne te verwerven en de oorlog moreel te rechtvaardigen, appelleert Putin aan de rol die Rusland heeft gespeeld in de overwinning op Nazi-Duitsland in de Tweede Wereldoorlog. Het fascisme heeft volgens Putin de kop opgestoken in Oekraïne. Volgens Putin is het dan ook opnieuw aan Rusland om dit 'fascistische monster' te verslaan.

Narratief naar het buitenland
In internationaal verband wil Rusland laten zien dat de westerse pogingen om het land te isoleren slechts beperkt effect hebben. Daarbij richt Rusland zich onder meer op internationale samenwerkingsverbanden zoals BRICS of de Shanghai Cooperation Organisation (SCO). Het wil hiermee een tegenwicht bieden aan de internationale orde die in de Russische perceptie wordt gedomineerd door de Verenigde Staten. Volgens Rusland zijn de strategische partnerschappen die Moskou heeft gesloten cruciaal om de Russische oorlogsinspanningen in Oekraïne voort te zetten. Een aantal van deze strategische partnerschappen, zoals de relatie met Beijing, wordt door Moskou gepresenteerd als succesvol en gelijkwaardig. In de praktijk is echter eerder sprake van een verstandshuwelijk dat op ongelijke voet tot stand is gekomen.

1.2 Draagvlak Russische bevolking

Er lijkt nog altijd veel draagvlak voor de oorlog bij de Russische bevolking, al wordt dit deels ook afgedwongen met steeds repressievere middelen. Iedere vorm van kritiek op de Russische 'speciale militaire operatie' in Oekraïne wordt de kop ingedrukt, net als openlijke kritiek op het Russische leiderschap. Tot op heden weet het Kremlin het hoofd te bieden aan de uitdagingen die de oorlog met zich meebrengt. De vraag is hoe lang Rusland dat vol kan houden. Ondertussen lijkt het Kremlin voor zichzelf te erkennen dat een eventueel staakt-het-vuren of post-conflictscenario politieke, economische en sociale uitdagingen met zich zal meebrengen. Het worstelt met de vraag hoe hiermee om te gaan. Denk bijvoorbeeld aan de re-integratie van grote aantallen militairen in de Russische samenleving. Een deel van hen is gewond en getraumatiseerd. Ook keren criminelen terug in de Russische samenleving, die zich letterlijk hebben vrijgevochten. Daarnaast zullen voormalig contractmilitairen, ex-gemobiliseerden en personen werkzaam in de defensie-industrie een inkomensval ervaren. Verder is het Kremlin beducht op mogelijke ontevredenheid over Russische 'concessies' bij de onderhandelingen; deze ontevredenheid kan leiden tot binnenlandse onrust.

1.3 Onderhandelingen

Ondanks de hierboven genoemde binnenlandse uitdagingen waarmee Rusland wordt geconfronteerd als gevolg van de oorlog in Oekraïne, stelt president Putin zich maximalistisch op aan de onderhandelingstafel. Hij probeert tot een overeenkomst op Russische voorwaarden te komen. Hoewel Moskou zich realiseert dat oorlogen doorgaans via onderhandelingen eindigen, zien deze onderhandelingen er vanuit Russisch perspectief wezenlijk anders uit dan vanuit westers perspectief.

Daarbij wil Rusland de 'grondoorzaken' van het conflict adresseren en geeft het aan uitsluitend met de Verenigde Staten te willen spreken - en dan nadrukkelijk over het herschikken van de Europese veiligheidsarchitectuur. Het Russische doel hierbij is het beïnvloeden en afzwakken van ontwikkelingen die het als bedreigend ervaart, zoals de NAVO-presentie die sinds 1997 verder is opgeschoven richting de Russische grenzen[2]. Zo is NAVO-lidmaatschap voor Oekraïne – ongeacht op welke termijn – onbespreekbaar voor Rusland. Daarbij blijft Rusland westerse vredesinitiatieven met argwaan tegemoet treden en probeert het partners die voor Rusland belangrijk zijn te weerhouden om deel te nemen aan dit soort initiatieven.

Het verloop van de vredesonderhandelingen onderstreept vooralsnog de complexiteit om tot een akkoord te komen. De Russische onderhandelingsbereidheid zegt vooral iets over de bereidheid om de oorlog op een diplomatieke wijze op te lossen, maar niet dat Rusland bereid is om wezenlijke concessies te doen. Rusland gebruikt de onderhandelingen vooral als vehikel om behaalde resultaten te bestendigen of concessies af te dwingen die gunstig zijn voor Rusland, mede op basis van de situatie op het Oekraïense slagveld.

[2] Er wordt verwezen naar 1997 omdat in dat jaar een basisakkoord is gesloten tussen de NAVO en Rusland met onder meer de toezegging dat de toenmalige NAVO-leden geen substantiële hoeveelheid militairen en materieel zouden stationeren in andere Europese landen.

2.
Verloop van de oorlog in Oekraïne

Aan de vooravond van de grootschalige militaire inval van Rusland in Oekraïne leek het Kremlin ervan overtuigd dat de Russische doelstellingen van deze 'speciale militaire operatie' in slechts een paar dagen zouden worden behaald. Inmiddels is de oorlog in Oekraïne een ware slijtageslag geworden. Rusland lijdt nog altijd grote verliezen, zonder zijn operationele doelstellingen (de 'denazificatie' en demilitarisatie van Oekraïne) te behalen. Wel beschikt het, mede als gevolg van aanhoudende steun van onder meer China, Iran en Noord-Korea, zowel qua personeel als materieel over een numeriek overwicht. Dit levert Rusland een strategisch voordeel op.

Verwoeste Russische tank in Sviatohirsk, Oekraïne. 12 februari 2023.

2.1 Oekraïne

De Oekraïense strijdkrachten kampen ondanks de aanhoudende steun van het Westen met structurele tekorten. Zonder grootschalige mobilisatie en geïntensiveerde militaire steun uit het buitenland, zijn die tekorten niet op te lossen.

Het tijdelijke tactische succes aan Oekraïense kant met de inname van Russisch grondgebied in Koersk, heeft Oekraïne geen strategisch voordeel opgeleverd. In maart 2025 hebben de Oekraïense strijdkrachten zich onder toenemende Russische druk georganiseerd teruggetrokken. Rusland heeft inmiddels het grootste deel van dit grondgebied heroverd.

De Oekraïense strijdkrachten voeren succesvolle aanvallen uit op plekken in Rusland die ver van de frontlinies liggen - zogeheten *deep strikes*. Dit doen zij steeds vaker met meer geavanceerde, zelfgeproduceerde langeafstandsdrones, die zich onder meer richten op de Russische petrochemische sector, de defensie-industrie, militaire toevoerlijnen en de luchtverdediging. Desondanks hebben deze *deep strikes* tot op heden niet geleid tot een strategische kanteling in het conflict.

Wat ook nog niet tot een strategische kanteling heeft geleid, zijn de Oekraïense aanvallen met steeds geavanceerdere *Unmanned Surface Vessels* (USV's) op de Russische vloot in het Zwarte Zeegebied. De intensiteit van deze aanvallen is in 2024 sterk afgenomen. Dit komt mede omdat Rusland vervolgens besloot om de vloot meer in oostelijke richting te positioneren.

2.2. Rusland

Ondanks de grote personele en materiële verliezen, beperkte terreinwinst aan Russische zijde en westerse sancties – die gevolgen hebben voor de Russische productiecapaciteiten van geavanceerde wapens – heeft Rusland de verliezen tot op heden weten op te vangen. Alhoewel het de vraag is of Rusland ook op de lange termijn economisch in staat is om dit te blijven doen, is het tot op heden in staat gebleken om met zijn defensie-industrie voldoende militair materieel te produceren, te reviseren en te moderniseren. Zo hebben de verschillende Russische krijgsmachtonderdelen aanzienlijk geïnvesteerd in de integratie van onbemande systemen. Ze gebruiken daarbij de geleerde lessen uit de oorlog in Oekraïne om de effectiviteit van de inzet van deze onbemande systemen te vergroten. Bovendien wordt Rusland gesteund door onder meer China, Iran en Noord-Korea, waarbij Pyongyang ook troepen heeft geleverd die door Rusland zijn ingezet aan de frontlinie in Koersk. Mede door de materiële steun die Rusland ontvangt van deze landen, kan het een beperkt deel van de eigen productie gebruiken om de strategische reserves aan te vullen.

Rusland toont een onverminderde bereidheid om bij luchtaanvallen op Oekraïne de randen van het NAVO-luchtruim op te zoeken, waarbij Rusland het risico op grensincidenten met fysieke slachtoffers accepteert.

Vooruitlopend op een eventueel staakt-het-vuren en een post-conflictscenario in Oekraïne, geeft Rusland invulling aan ambitieuze plannen om de Russische krijgsmacht te hervormen en uit te breiden. De voorbereiding op de mogelijkheid van een militair conflict met de NAVO staat hierbij centraal.

In deze context heeft Rusland in 2024 zijn openbare nucleaire doctrine herzien. Hierin is de 'nucleaire drempel' de facto naar beneden bijgesteld. Doel hiervan is het afschrikwekkende effect van nucleaire wapens te vergroten, zonder daarbij in te boeten aan geloofwaardigheid en handelingsvrijheid. Het herzien van de openbare nucleaire doctrine kan worden gezien als een escalatiestap in de oorlog in Oekraïne, maar speelt vooral een rol in de bredere betrekkingen tussen Rusland en het Westen.

2.3 Voorstelbaarheid militaire escalatie

Zoals genoemd is de oorlog in Oekraïne in de Russische perceptie slechts een onderdeel van een breder en existentieel conflict met het Westen. Eén van de centrale vragen in dit verband is dan ook hoe groot het risico is dat de oorlog in Oekraïne uitmondt in een openlijk militair conflict tussen Rusland en het Westen (de NAVO).

Een scenario waarin Rusland een in tijd en geografie beperkte militaire operatie tegen de NAVO zal uitvoeren, wordt vooralsnog als onwaarschijnlijk ingeschat. Europa zal zich volgens de AIVD en MIVD echter wel moeten voorbereiden op een dergelijk scenario.

De AIVD en MIVD schatten in dat Rusland na het beëindigen van de oorlog in Oekraïne in het minst gunstige scenario mogelijk minder dan een jaar nodig heeft om voldoende capaciteiten op te bouwen voor een militaire operatie met beperkte geografische doelstellingen. Een dergelijke militaire operatie zal niet gericht zijn op het militair verslaan van de NAVO, maar op het uiteenspelen van het bondgenootschap en het afdwingen van concessies ten aanzien van de Europese veiligheidsarchitectuur. Dit betekent nadrukkelijk niet dat Rusland momenteel daadwerkelijk de intentie heeft om over te gaan tot een militaire escalatie van het bredere conflict met het Westen. Vooralsnog heeft Rusland andere, minder risicovolle opties om het NAVO-bondgenootschap te verzwakken.

De snelle opbouw van militaire capaciteiten biedt Rusland de mogelijkheid om druk uit te oefenen op Europa. Bovendien voert Rusland de druk op Europa op door activiteiten te ontplooien in het hybride domein. Het is hierbij de insteek om onder de escalatiegrens van een openlijk militair conflict te blijven. Echter, Rusland heeft niet volledig grip op de effecten van deze hybride activiteiten, waardoor deze activiteiten wel het risico verhogen op (onbedoelde) militaire escalatie. En ook zonder een openlijk militair conflict, hebben de toegenomen Russische hybride activiteiten een aanzienlijke impact op de nationale veiligheid van Nederland en andere Europese landen. Dit wordt in het volgende hoofdstuk verder toegelicht.

3.
De dreiging van Russische hybride activiteiten in Europa

Europa wordt sinds eind 2023 op verschillende plekken en in toenemende mate geconfronteerd met hybride activiteiten van Rusland, zowel in het fysieke als in het digitale domein. Hybride activiteiten zijn een combinatie van beïnvloedings-activiteiten, zoals heimelijke beïnvloeding, cyberaanvallen, de verspreiding van desinformatie, economische destabilisatie of concrete aanvallen op bijvoorbeeld de vitale infrastructuur. Daarnaast blijft Rusland klassieke spionageactiviteiten ontplooien om inlichtingen te vergaren over onder meer de intenties, capaciteiten en activiteiten van het Westen in relatie tot Rusland of vraagstukken die voor Rusland belangrijk zijn. Informatie hierover is cruciaal voor Rusland, ook voor het ontplooien van de hierboven genoemde hybride activiteiten.

3.1 Waarom zet Rusland hybride activiteiten in?

Hybride activiteiten zijn allerminst een nieuw fenomeen. Dergelijke activiteiten zijn al zeer lange tijd een concreet onderdeel van het Russische politiek-strategische en militaire denken. Het doel van hybride activiteiten is meerledig.

In algemene zin is de inzet van deze activiteiten erop gericht een samenleving te ondermijnen. Denk aan beïnvloeding van het publieke debat, het beïnvloeden en frustreren van politieke besluitvorming en het ondermijnen van het vertrouwen in het westerse politiek-bestuurlijke bestel. Door deze activiteiten kunnen de veerkracht en weerbaarheid van een samenleving onder druk komen te staan.

In de context van de oorlog in Oekraïne en het bredere conflict met het Westen waarin Rusland zich verwikkeld ziet, probeert Rusland met deze activiteiten om zowel de publieke als de politieke en militaire steun aan Oekraïne te ondermijnen. Dit doet Rusland door in te spelen op gevoelens van angst voor een verdere escalatie van een militair conflict met Rusland. Daarnaast zet Rusland deze activiteiten in om de politieke cohesie te verzwakken en westerse bondgenootschappen zoals de NAVO en de Europese Unie uiteen te spelen. Ook probeert Rusland via deze hybride activiteiten te zien hoe het Westen daarop reageert: het probeert de ‘rode lijnen’ van het Westen inzichtelijk te maken en een beeld te krijgen van eventuele tegenmaatregelen en represailles.

Brand in fabriek van Diehl Metal na vermoedelijke Russische sabotage in Berlijn, Duitsland. 3 mei 2024.

3.2 Plausibele ontkenning: het verhullen van (Russische) betrokkenheid

Hoewel de diensten constateren dat de dreiging van Russische hybride activiteiten is toegenomen, kan de vermeende Russische hand achter verschillende hybride incidenten lang niet altijd worden vastgesteld. Dat komt mede doordat deze hybride activiteiten doorgaans gebaseerd zijn op het principe van plausibele ontkenning en dus per definitie niet makkelijk te herleiden zijn. Betrokkenheid van Rusland wordt in veel gevallen bewust gemaskeerd. De Russische activiteiten in het hybride domein zijn erop gericht om maximaal effect te sorteren, met een zo klein mogelijk risico op een (grootschalige) militaire escalatie.

Dat betekent niet dat dit principe van plausibele ontkenning in alle gevallen opgaat. In sommige gevallen kiest Rusland ervoor om de Russische hand juist impliciet of zelfs expliciet te laten zien. Op die manier wil Rusland laten zien dat het in staat is om waar ook ter wereld en wanneer het maar wil activiteiten te ontplooien.

3.3. Toegenomen risicobereidheid

Vanaf 2024 is Rusland meer risico's gaan nemen bij de inzet van hybride activiteiten. Met deze grotere risicobereidheid heeft het in toenemende mate beïnvloedings-activiteiten ontplooid met een geweldscomponent, waarbij voor lief wordt genomen dat deze activiteiten materiële schade en zelfs fysiek letsel tot gevolg kunnen hebben. Daarbij ging Rusland ook veel openlijker en assertiever te werk dan voor 2024. Dat regelmatig de Russische betrokkenheid is ontdekt of verondersteld, heeft Rusland mogelijk als handig en positief ervaren.

Op de volgende pagina's wordt ingegaan op een aantal concrete verschijningsvormen van Russische hybride activiteiten.

Vanaf 2024 is Rusland meer risico's gaan nemen bij de inzet van hybride activiteiten.

4.
(Heimelijke) beïnvloeding door Rusland

Beïnvloeding door Rusland kan zowel openlijk als heimelijk plaatsvinden. In dit hoofdstuk ligt de nadruk op beïnvloedingsactiviteiten die Rusland heimelijk ontplooit. Heimelijke beïnvloeding behoort tot één van de klassieke hybride middelen van Rusland. Drijvende krachten achter de Russische heimelijke beïnvloedingsactiviteiten zijn onder meer de Russische inlichtingen- en veiligheidsdiensten en de Russische Presidentiële Administratie (PA). De betrokken Russische staatsorganen kunnen een beroep doen op nagenoeg alle onderdelen van de Russische samenleving en hanteren hierbij een zogeheten *whole of society*-benadering. Hierbij doet Rusland een beroep op gelijkgestemde personen, netwerken en organisaties in het buitenland die al dan niet bewust worden ingezet voor het ondersteunen en uitvoeren van Russische heimelijke beïnvloedingsactiviteiten.

4.1 Opportunisme en pragmatisme leidend

Het Kremlin richt zich bij heimelijke beïnvloedingsactiviteiten primair op een aantal landen dat een politieke voortrekkersrol heeft in Europa, zoals Duitsland en Frankrijk. Daarnaast richt het zich op landen waarvan Rusland oordeelt dat er een grotere voedingsbodem of ontvankelijkheid bestaat voor Kremlin-gezinde narratieven of door Rusland verspreide desinformatie.

Dat betekent allerminst dat Nederland volledig buiten schot blijft. Rusland handelt in grote mate op basis van opportunisme en pragmatisme. Daardoor kunnen ook kleinere en politiek minder gewichtige landen in het vizier komen als doelwit van heimelijke beïnvloedingscampagnes. Zo kan ook Nederland – bijvoorbeeld als gevolg van politieke uitspraken of beslissingen in relatie tot de oorlog in Oekraïne – een meer prominent doelwit worden van Russische heimelijke beïnvloedingsactiviteiten.

Daarnaast is Nederland een gastland voor verschillende internationale organisaties die Rusland als doelwit ziet, zoals de Organisation for the Prohibition of Chemical Weapons (OPCW) en het Internationaal Gerechtshof.

4.2 Desinformatiecampagnes

Ook in het digitale informatiedomein zet Rusland sinds jaar en dag desinformatie-campagnes in. Rusland bleef ook na de start van de grootschalige militaire invasie in Oekraïne in 2022 via verschillende kanalen desinformatie, nepnieuws en Kremlin-gezinde narratieven verspreiden. Hierbij maakt Rusland gebruik van zowel Russische als buitenlandse (sociale) media en speelt het op opportunistische wijze in op bestaande maatschappelijke tegenstellingen in het Westen. Tevens gebruikt het formele en informele proxy-netwerken van beïnvloedingsagenten. Moskou kan zich hierbij beroepen op een breed en internationaal netwerk van journalisten en contentmakers die zowel bewust als onbewust meewerken aan het maken en verspreiden van Kremlin-gezinde narratieven en desinformatie.

Stoelen in de Tweede Kamer, Den Haag.

Desinformatiecampagne: Doppelganger
In één van de breedst uitgemeten Russische desinformatiecampagnes – Doppelganger – heeft Rusland meer dan zevenhonderd websites nagemaakt van onder meer Europese media. De meerjarige campagne werd gelanceerd in de lente van 2022 met als doel om met name westerse lezers te voeden met Kremlin-gezinde informatie. Door de identieke opmaak zouden lezers moeten veronderstellen dat deze informatie afkomstig was van bekende en door een breed publiek vertrouwde Europese nieuwsbedrijven. De Russische Social Design Agency heeft de campagne in opdracht van het Kremlin uitgevoerd.

Sancties hebben de verspreiding van Russisch nepnieuws en Kremlin-gezinde narratieven enigszins ingeperkt, maar Moskou slaagt er nog altijd in om het publieke debat in het Westen te beïnvloeden via het digitale informatiedomein en fysieke netwerken.

4.3 Heimelijke impact via demonstraties

In het fysieke domein zet Rusland onder meer in op de heimelijke organisatie van demonstraties of probeert het mee te liften op demonstraties met veelal een pacifistisch of anti-NAVO-karakter. Zo greep Rusland in mei 2023 een demonstratie aan van Extinction Rebellion in Den Haag om Kremlin-gezinde uitlatingen te verspreiden. Extinction Rebellion lijkt hiervan op geen enkel moment op de hoogte te zijn geweest. Rusland probeert dergelijke activiteiten primair publicitair te benutten om de Russische bevolking ervan te overtuigen dat er in het Westen de nodige kritiek is op de politieke en militaire steun aan Oekraïne. Zo wordt er in Russische staatsmedia zo nu en dan aandacht besteed aan demonstraties in Nederland waarbij deelnemers een Kremlin-gezinde boodschap uitdragen. Een voorbeeld daarvan zijn vredesdemonstraties op de Dam in Amsterdam, waarbij Kremlin-gezinde boodschappen worden gepropageerd. Eén van de Nederlandse deelnemers aan deze demonstraties, een aanhanger van het anti-institutioneel extremisme, heeft onlangs een onderscheiding gekregen van een aan Rusland gelieerde organisatie in Nederland voor zijn bijdrage aan ‘het behoud van vrede’.

4.4 Heimelijke beïnvloeding Europees Parlement

Rusland richt zich ook op Europese politici – onder wie Europarlementariërs – met een zekere sympathie voor het Kremlin of Kremlin-gezinde denkbeelden. Het probeert deze politici aan zich te binden via bijvoorbeeld door Rusland vergoede internationale reizen en betalingen. Een van de meer in het oog springende voorbeelden in dit verband is de zogeheten Voice of Europe-casus. Hierbij kregen parlementariërs en medewerkers betaald voor de verspreiding van Russische propaganda in het Europees Parlement en via een journalistiek medium.

Het Kremlin probeert de politieke cohesie in het Westen ook te ondermijnen door zich bijvoorbeeld te richten op Europese politici en hen bijvoorbeeld via misleidende 'grappen' te verleiden tot het doen van gevoelige of vertrouwelijke uitlatingen.

Andere manieren waarop Rusland in het fysieke domein in toenemende mate heimelijke beïnvloedingsactiviteiten inzet, lopen uiteen van het plaatsen van doodskisten nabij de Eiffeltoren, vergezeld van de tekst 'Franse soldaten uit Oekraïne' tot het bekladden of vernielen van overheidsgebouwen, bedrijfspanden, mediabedrijven en andere symbolische locaties in Europese steden.

Misleiding en ontlokking: het Russische duo Vovan en Lexus

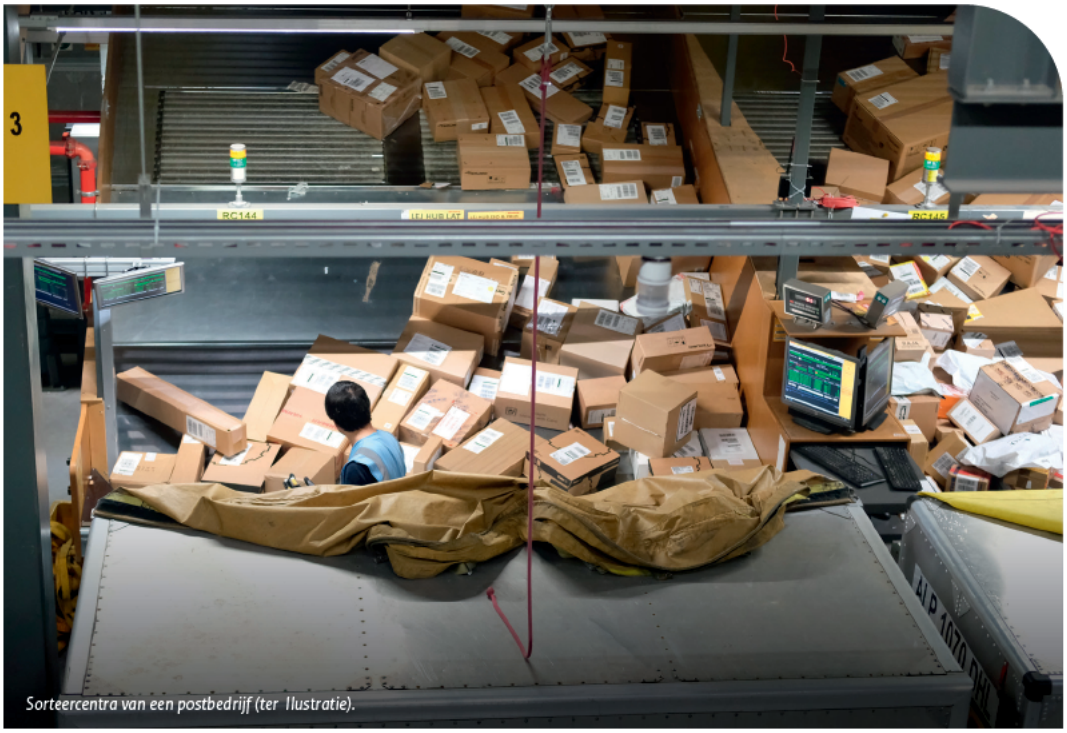
Het Russische komische duo Vovan en Lexus voert geregeld misleidende 'grappen' uit. Deze grappen zijn gericht op onder meer Europese politici en hoogwaardigheids-bekleders van bijvoorbeeld de Europese Centrale Bank en het Internationaal Olympisch Comité. Het duo ontlokt hen uitspraken die Rusland unieke informatie kunnen opleveren of op een later moment kunnen worden benut om personen of de landen die zij vertegen-woordigen in diskrediet te brengen. Deze activiteiten sluiten steeds meer aan bij het narratief van het Kremlin.

5. Sabotageactiviteiten

Sinds het voorjaar van 2024 zijn de hybride activiteiten van Rusland op meerdere plekken in Europa brutaler en agressiever. Dit is ook terug te zien in een toename van het aantal sabotageactiviteiten. Deze activiteiten zijn illustratief voor de reeds genoemde toegenomen risicobereidheid van Rusland.

De AIVD en MIVD gebruiken de volgende definitie voor sabotage: het moedwillig beschadigen van militaire en civiele doelwitten, bijvoorbeeld om oorlogsleveranties te vertragen, om angst en verdeeldheid te zaaien, of om te testen wanneer en op welke wijze tegenstanders reageren. De Russische sabotageactiviteiten zijn niet nieuw. Zo werkten de Russische inlichtingen- en veiligheidsdiensten in de Koude Oorlog intensief aan sabotageplannen tegen het Westen.

Door middel van sabotageactiviteiten op Europees grondgebied probeert Rusland in grote lijnen dezelfde doelen te bereiken als met de andere hybride activiteiten die in deze publicatie worden beschreven. In het geval van sabotageactiviteiten in het fysieke domein gaat het Rusland in het bijzonder om de volgende twee doelen: het ondermijnen van het maatschappelijke draagvlak voor steun aan Oekraïne, en het daadwerkelijk verstoren van militair-materiële steun van Europa aan Oekraïne.



Sorteercentra van een postbedrijf (ter Illustratie).

5.1 Toegenomen risicobereidheid

De toegenomen risicobereidheid uit zich met name in de Russische acceptatie dat sabotageactiviteiten in potentie slachtoffers kunnen maken of tot materiële schade kunnen leiden. Ook lijkt vergelding een rol te spelen in de toegenomen risicobereidheid aan Russische zijde - specifiek voor de Oekraïense aanvallen met *deep strikes*, op doelen ver achter de frontlinies op Russisch grondgebied. Het Kremlin stelt dat deze aanvallen niet kunnen plaatsvinden zonder westerse steun en houdt het Westen dan ook nadrukkelijk verantwoordelijk.

5.2 Berichtgeving over sabotage

Sinds het voorjaar van 2024 wordt in diverse media gesproken over een toename van sabotageactiviteiten in Europa. Soms wordt deze berichtgeving gedaan op basis van vermoedens van Russische betrokkenheid, zonder dat daar concrete aanwijzingen voor zijn. Ook wordt in berichtgeving niet altijd onderscheid gemaakt tussen daadwerkelijke sabotage en sabotageplannen. Hoewel ook de AIVD en MIVD constateren dat er een toename is van sabotageactiviteiten, kunnen lang niet alle incidenten op basis van inlichtingen worden toegeschreven aan Rusland

Berichtgeving waarin vermeende Russische sabotageactiviteiten als feiten worden gepresenteerd, kan leiden tot een vertekend beeld van de schaal van de Russische sabotageactiviteiten in Europa. Hierdoor wordt onbedoeld een bijdrage geleverd aan de Russische doelstellingen. Zo kan immers de indruk ontstaan dat Rusland waar en wanneer het maar wil kan toeslaan in Europa. Rusland zal vanuit opportunisme dat beeld laten bestaan of zelfs proberen te versterken. Dit zorgt niet alleen voor maatschappelijke onrust en angst voor een verdere escalatie, maar voedt ook het gevoel dat Europa niet in staat is zijn burgers te beschermen.

5.3 Escalatie en de-escalatie van sabotageactiviteiten

Sabotageactiviteiten die aan de Russische inlichtingen- en veiligheidsdiensten kunnen worden toegeschreven, kenden in Europa een (voorlopig) hoogtepunt in de zomer van 2024. Hierna nam het aantal sabotageactiviteiten af. Vooralsnog is onduidelijk waarom de Russische sabotageactiviteiten in Europa destijds zijn afgeschaald. Wel is sinds de zomer van 2025 weer een voorzichtige toename van sabotageactiviteiten zichtbaar. Dit suggereert dat Rusland de mogelijkheid tot escalatie en de-escalatie ten aanzien van sabotageactiviteiten openhoudt.

Het attribueren van sabotageactiviteiten kan om verschillende redenen lastig zijn en langdurig onderzoek vergen. Een voorbeeld hiervan is een explosie bij een Tsjechisch munitiedepot in 2014, waarvan pas in 2021 publiekelijk is vastgesteld dat deze kan worden toegeschreven aan de Russische militaire inlichtingendienst GRU. De explosie vond plaats ten tijde van de Russische illegale annexatie van de Krim en hield mogelijk verband met Tsjechische wapenleveranties ter ondersteuning van Oekraïne.

Deze sabotageactiviteiten zijn tot nu toe in belangrijke mate gericht op landen aan de oostflank van Europa, waaronder de Baltische staten en Polen. Bovendien richten de Russische sabotageactiviteiten zich op landen die in de Russische optiek een prominente rol spelen in de steun aan Oekraïne, bijvoorbeeld het Verenigd Koninkrijk en Duitsland. Toch hebben de AIVD en MIVD verschillende cyberoperaties en voorbereidingen voor sabotage in Nederland onderkend.

5.4 Sabotage in Europa

In de media zijn verschillende sabotageacties vermeld die worden toegeschreven aan Rusland. Zo klaagde Polen op 12 maart 2025 een Belarussische ingezetene aan voor brandstichting bij een doe-het-zelfwinkel (*home improvement store*) in Warschau. De brandstichting vond plaats in het voorjaar van 2024. De verdachte zou hebben gehandeld in opdracht van de Russische inlichtingen- en veiligheidsdiensten.

In Estland zijn zeven personen aangehouden voor het vernielen van auto's van de Estse minister van Binnenlandse Zaken en een journalist. De verdachten zouden, in opdracht van de Russische inlichtingen- en veiligheidsdiensten, verschillende rollen hebben vervuld. Zij verzamelden onder meer informatie en voerden aanvallen uit.

In februari 2025 is een Oekraïner door een rechtbank in Polen veroordeeld tot acht jaar gevangenisstraf voor brandstichting en sabotage op aanmoediging van Rusland in Polen. De veroordeelde is volgens de Poolse aanklager gerekruteerd via Telegram en zou betaald zijn om brand te stichten in een verffabriek in Wroclaw.

In november 2025 werd een spoorlijn in het oosten van Polen op het traject Warschau-Lublin beschadigd. Deze spoorlijn verbindt Warschau met de grens van Oekraïne en is belangrijk voor de aanvoer van (militaire) steun. Volgens de Poolse autoriteiten, die in dit verband meerdere aanhoudingen verrichtten, is sprake van sabotage-activiteiten die zijn aangestuurd door Rusland.

Sabotageactiviteiten met postpakketten

Een van de meest geavanceerde en meer risicovolle sabotageactiviteiten tot op heden waarvan is vastgesteld dat er sprake was van betrokkenheid van de Russische inlichtingen- en veiligheidsdiensten vormen de postpakketten die in de zomer van 2024 zijn verstuurd naar adressen in Europa en Noord-Amerika. Deze pakketten waren deels testpakketten, maar bevatten in sommige gevallen *improvised incendiary devices* (IIDs), ontbrandbaar materiaal. Een aantal van deze pakketten is tot ontbranding gekomen in sorteercentra van commerciële postbedrijven in Europa.

De AIVD en MIVD hebben vastgesteld dat ook vanuit Nederland testpakketten zijn verstuurd. Deze pakketten bevatten geen ontbrandbare materialen. Het betrof hier naar inschatting van de diensten waarschijnlijk geen sabotageactiviteit gericht op Nederland, maar een voorverkenning waarmee logistieke routes en de timing van verzending van de pakketten in kaart zijn gebracht. De verzender is online gerekruteerd en was zeer waarschijnlijk niet op de hoogte (*unwitting*) van het achterliggende doel van de verzending noch van het feit dat hij handelde in opdracht van Rusland.

In een aantal gevallen heeft Rusland plannen gemaakt voor sabotageactiviteiten gericht op mensenlevens. Een in het oog springend voorbeeld hiervan wordt gevormd door de verijdelde plannen om de directeur van de Duitse wapenproducent Rheinmetall om het leven te brengen.[3] Deze plannen waren gericht op het verstoren van de westerse militaire steun aan Oekraïne en het afschrikken van andere Europese wapenfabrikanten.

5.5 Aangepaste modus operandi

Bij het uitvoeren van sabotageactiviteiten zijn de Russische inlichtingen- en veiligheidsdiensten andere modus operandi gaan hanteren. Mede als gevolg van de grootschalige uitzetting van Russische inlichtingenofficieren onder diplomatieke dekmantel door een groot aantal Europese landen, die volgde op de Russische invasie in Oekraïne in 2022, is het voor de Russische inlichtingen- en veiligheidsdiensten moeilijker geworden om activiteiten te ontplooien in Europa. Om dit te ondervangen zijn de Russische diensten andere tactieken gaan gebruiken. Ze zijn zich onder meer gaan toeleggen op het gebruik van gelaagde netwerken. Deze netwerken bestaan uit coördinatoren, facilitators en zogeheten *low-level* agenten die de sabotageacties uitvoeren.

Deze *low-level* agenten worden benaderd via berichtenapplicaties als Telegram of via persoonlijke contacten. Aan hen wordt bijvoorbeeld gevraagd om informatie te verzamelen, nepnieuws of desinformatie te verspreiden, of cyberaanvallen uit te voeren. Daarnaast worden zij in voorkomende gevallen gevraagd om potentiële doelen voor sabotageactiviteiten in kaart te brengen, verkenningen uit te voeren of daadwerkelijk zelf sabotageactiviteiten ten uitvoer te brengen. Voordat wordt overgegaan tot betaling wordt de *low-level* agent in veel gevallen gevraagd bewijs te leveren dat de opdracht is uitgevoerd, meestal in de vorm van videomateriaal.

Een eenduidig profiel van deze *low-level* agenten is niet te geven. Wel geldt dat het in veel gevallen personen betreft die sabotageactiviteiten als manier zien om snel en gemakkelijk geld te verdienen. Deze, soms minderjarige, *low-level* agenten lijken zich veelal niet bewust dat zij activiteiten uitvoeren in opdracht van Rusland. Zij opereren daarmee *unwitting* en als zogeheten *useful idiot*. Van ideologische gedrevenheid of sympathie voor Rusland lijkt in de meeste gevallen geen sprake te zijn. Wel was er in verschillende gevallen sprake van een crimineel verleden en een strafblad. In tegenstelling tot inlichtingenofficieren zijn deze *low-level* agenten niet uitgebreid getraind of soms helemaal niet getraind. Hoewel de inzet van deze agenten in lijn is met het principe van plausibele ontkenning, neemt het risico van onderkende of mislukte operaties toe als gevolg van het gebrek aan training, maar ook door het gebrek aan motivatie.

[3] Rheinmetall vervult een prominente rol bij het leveren van militair-materiële steun aan Oekraïne.

6.
(Vermeende) sabotage ter zee en in de lucht

Vanaf de tweede helft van 2024 is ook het aantal vermeende sabotage-incidenten op zee sterk toegenomen. Deze incidenten gaan over kabelstoringen en beschadigingen (in verschillende gradaties) van onderzeekabels. Ook in de media wordt nadrukkelijk aandacht besteed aan deze incidenten. Uit inlichtingenonderzoek blijkt dat van het merendeel van deze vermeende sabotage-incidenten tot op heden niet kan worden vastgesteld dat er inderdaad sprake is geweest van sabotage. Ook kunnen deze incidenten op basis van het eigen inlichtingenbeeld niet direct toegeschreven worden aan Rusland. Dit betekent overigens niet dat het ondenkbaar is dat Rusland dit soort activiteiten ontplooit.

Schip van de Finse kustwacht bij de in beslag genomen schaduwvloottanker Eagle S, Finland. 30 december 2024

Complexiteit attributie
Er zijn verschillende redenen waarom het lastig is om deze maritieme incidenten toe te schrijven aan Rusland. Denk ook hier aan het eerder genoemde principe van plausibele ontkenning. Maar ook bij incidenten waarbij een Russische link is vastgesteld is niet automatisch sprake van sabotage. Verschillende incidenten onder water, bijvoorbeeld in de Oostzee, hebben weliswaar een Russische link, maar deze link is in de regionale context verklaarbaar en niet per se verdacht.

Zo is het normaal dat een deel van de schepen in de Oostzee onder Russische vlag vaart en Russische havens aandoet; dit past simpelweg bij het profiel van de scheepvaart daar. Bovendien vinden wereldwijd regelmatig kabelstoringen plaats. Voor de meeste van dit soort 'reguliere' incidenten geldt een combinatie van factoren: veel maritieme activiteit in het gebied, relatief ondiep water en een hoge dichtheid aan onderwaterinfrastructuur. Deze drie omstandigheden gelden ook voor de Oostzee.

De meeste kabelstoringen worden veroorzaakt door de visserij of (losgeslagen) scheepsankers. Daarnaast spelen in de meeste gevallen slechte weersomstandigheden en 'slecht zeemanschap' een rol.

Voorbeelden van vermeende sabotage-incidenten in het maritieme domein
Op 17 en 18 november 2024 raakten twee onderwaterkabels in de Oostzee beschadigd. Dit kwam zeer waarschijnlijk doordat een van de ankers van het koopvaardijschip *Yi Peng 3* over de zeebodem sleepte. Het schip, dat onder Chinese vlag voer, was vertrokken uit een Russische haven. Tenminste een deel van de bemanning van het schip zou de Russische nationaliteit hebben. Los van de verdenking en deze Russische link, is niet vastgesteld dat sprake was van sabotage.

In begin januari 2025 berichtten de media over het schip *Eagle S*, behorend tot de Russische 'schaduwvloot'. Dit schip veroorzaakte zeer waarschijnlijk een storing aan de *Estlink 2* in de Finse Golf. Tot op heden is niet vastgesteld of daadwerkelijk sprake was van sabotage.

Op 26 januari 2025 raakte een onderzeekabel tussen Zweden en Letland beschadigd. Ditmaal was het het anker van het schip *Vezhen* dat over de zeebodem sleepte. De Zweedse autoriteiten, die beslag lieten leggen op het schip, kwamen op basis van multidisciplinair onderzoek tot de conclusie dat er geen sprake was van sabotageactiviteiten.

Meer recent, op 31 december 2025, hebben de Finse autoriteiten het vrachtschip de *Fitburg* geënterd nadat een telecomkabel in de Golf van Finland beschadigd raakte. Ook hier zou het anker van het schip, dat vanuit Sint-Petersburg onderweg was naar Haifa (Israël) verantwoordelijk zijn voor de beschadiging van de kabel. Het incident wordt onderzocht door de autoriteiten, die het schip op 12 januari 2026 zijn koers lieten vervolgen. Vooralsnog is het te vroeg om vast te stellen of er daadwerkelijk sprake was van sabotage.

Impact vooralsnog beperkt
Telecommunicatiekabels hebben een hoge mate van redundantie; als een kabel kapot is, kan een andere kabel de functie vaak 'overnemen'. Ook is de infrastructuur doorgaans weer snel gerepareerd. Dit beperkt de effecten van deze incidenten dan ook aanzienlijk in tijd en omvang.

Spionage op zee
In Nederland zijn tot op heden geen voorbeelden van maritieme sabotage aan bijvoorbeeld onderzeekabels. Wel is vastgesteld dat Rusland de infrastructuur van de Noordzee, Oostzee, Atlantische Oceaan en andere wateren in kaart brengt en (onderwater)activiteiten ontplooit die duiden op spionage. Dit is zorgelijk omdat de opgedane kennis op een later moment kan worden ingezet voor sabotagedoeleinden. Ook is het aantal meldingen over lanceringen van (vermeende) Russische drones vanaf vrachtschepen die zich in Nederlandse wateren bevinden sterk toegenomen.

Zo werd in mei 2025 het vrachtschip *HAV Dolphin* geïnspecteerd na meldingen dat vanaf het schip drones zouden worden gelanceerd boven de Noord- en Oostzee. Het schip, varend onder de vlag van Antigua en Barbuda, had een volledig Russische bemanning. De inspectie leverde geen bewijsmateriaal op. Een soortgelijk voorval deed zich voor met betrekking tot het Russische vrachtschip *Lauga*. Nabij het Duitse eiland Borkum werd in de omgeving van het schip een zevental drones waargenomen. Ook dit schip had een volledig Russische bemanning en ook hier leverde inspectie van het schip geen bewijsmateriaal of aanvullende aanwijzingen op voor verdenking van spionage.

Drone-waarnemingen
In aanvulling op toenemende media-aandacht over waarnemingen van (mogelijk) aan Rusland toe te schrijven drones (onbemande systemen), hebben ook de AIVD en MIVD de afgelopen twee jaar een toenemend aantal meldingen ontvangen over waarnemingen van drones in de buurt van vitale infrastructuur, luchthavens en bijvoorbeeld militaire faciliteiten. Ook bij dit soort meldingen geldt dat het vaststellen van vermeende Russische betrokkenheid gecompliceerd is. Sterker nog, bij verschillende incidenten blijkt het zelfs lastig om überhaupt vast te stellen of daadwerkelijk drones zijn waargenomen. Daar waar dat wel het geval was, kon vervolgens niet worden vastgesteld wie de bestuurder van de drone was en daarmee evenmin of er sprake was van een aan Rusland toe te schrijven activiteit. Net als bij de incidenten waarbij onderzeekabels beschadigd zijn, betekent dit niet dat het onvoorstelbaar is dat Rusland drones zou inzetten om het luchtverkeer (ernstig) te ontregelen.

Het vaststellen van vermeende Russische betrokkenheid kan gecompliceerd zijn.

7.
Digitale aanvallen en cybersabotage

Ook in het digitale domein ontplooit Rusland inmiddels een breed scala aan beïnvloedingsactiviteiten; van cyberspionage tot cybersabotage. De AIVD en MIVD zien in het cyberdomein sinds 2023 een toename van het aantal cyberactoren aan Russische zijde. Ook in het cyberdomein gebruikt Rusland in toenemende mate een *whole of society*-benadering: met een samenspel van verschillende private en overheidsentiteiten geeft Rusland vorm aan offensieve cyberprogramma's. De doelstellingen van de activiteiten in het cyberdomein sluiten aan bij de eerder genoemde doelstellingen om angst en verdeeldheid te zaaien, steun aan Oekraïne te ondermijnen en het Westen te testen op escalatiebereidheid.

Er zijn twee typen cyberactoren te onderscheiden: statelijke aanvalsgroepen enerzijds en staatsgesteunde hackersgroeperingen anderzijds. Statelijke aanvalsgroepen (*advanced persistent threats* of APT's) behoren veelal tot de Russische inlichtingen- en veiligheidsdiensten. Deze aanvalsgroepen voeren vaak langdurige en doelgerichte cyberoperaties uit, die gericht zijn op onder meer overheidsinstanties en vitale infrastructuur in westerse landen. Staatsgesteunde hackersgroeperingen doen zich voor als onafhankelijke hacktivisten, maar worden veelal wel degelijk gesteund of zelfs aangestuurd door de Russische staat.

Zowel voorafgaand aan als na de grootschalige invasie van Rusland in Oekraïne zette Rusland in het cyberdomein op grote schaal laagdrempelige cyberactiviteiten in, zoals DDoS-aanvallen, *hack-and-leak*-aanvallen en zogeheten *defacements*[4].

Dat doet Rusland nog steeds. Daarnaast zette Rusland in de weken direct na de grootschalige invasie onder meer *wipers*[5] in. Gaandeweg is Rusland zich in het cyberdomein meer gaan toeleggen op cyberspionage om militaire en diplomatieke informatie van zowel Oekraïne als NAVO-bondgenoten te bemachtigen. Terwijl de oorlog voortduurde, werden de Russische cyberactiviteiten complexer, mogelijk mede vanwege de aanhoudende steun van het Westen aan Oekraïne. Rusland is zich met deze cyberactiviteiten nadrukkelijker gaan richten op de (vitale) infrastructuur - niet alleen in Oekraïne, maar ook in het Westen.

Met een samenspel van verschillende private en overheidsentiteiten geeft Rusland vorm aan offensieve cyberprogramma's.

[4] DDoS: digitale aanval op de capaciteit van onlinediensten of de ondersteunende servers van netwerkapparatuur, waardoor deze overbelast wordt en offline kan gaan. Hack-and-leak: gestolen data wordt gelekt om een politiek of maatschappelijk effect te creëren of om verder verhandeld te worden. Defacement: het ongewenst aanpassen van webpagina's door hackers, waarbij de originele pagina vaak wordt vervangen door politieke boodschappen.

[5] Wipers: digitale aanvallen waarbij gegevens worden gewist, zodat werkstations en servers onbruikbaar zijn.

Scherm met nieuwsart kel waarin de AIVD en de MIVD waarschuwen voor de Russische cyberactor Laundry Bear.

7.1 Russische cyberaanvallen in Nederland

Ook in Nederland zijn Russische activiteiten waargenomen in het cyberdomein. Deze activiteiten variëren van laagdrempelige tot meer geraffineerde aanvallen die vaak worden gedreven door opportunisme en pragmatisme. In een poging om het Nederlandse kiezers moeilijk te maken hun stem uit te brengen tijdens de Europese verkiezingen van 2024, voerden Russische staatsgesteunde hackersgroeperingen DDoS-aanvallen uit, voorafgaand aan en tijdens de verkiezingen. Deze aanvallen waren gericht op onder meer websites van politieke partijen en bedrijven in de Nederlandse publieke transportsector.

Nederland kan ook op indirecte wijze slachtoffer worden van cyberaanvallen, bijvoorbeeld via activiteiten gericht tegen Nederlandse bondgenoten. Op deze wijze hebben Russische cyberactoren al gevoelige informatie bemachtigd, zoals persoonsgegevens van Nederlandse overheidsmedewerkers en Nederlandse bedrijven.

Daarnaast zien de AIVD en MIVD dat er meer digitale aanvallen plaatsvinden tegen mobiele apparaten zoals telefoons. Omdat chatapplicaties wereldwijd veelvuldig worden gebruikt en op diverse manieren kunnen worden misbruikt door kwaadwillenden, zijn chatapplicaties een kwetsbaar communicatiemiddel en daarmee een gewild doelwit voor Russische cyberactoren. Afgelopen jaar hebben de diensten vastgesteld dat een Russische cyberactor toegang heeft verkregen tot de chataccounts van meerdere Nederlandse overheidsmedewerkers. Hierbij is niet alleen toegang verkregen tot de gecompromitteerde accounts, maar zijn deze accounts zelfs overgenomen, zodat contactpersonen in de veronderstelling waren dat ze contact hadden met het slachtoffer. Ook door middel van het sturen van malafide e-mails of chatberichten maken Russische cyberactoren nog steeds talloze slachtoffers.

Cyberaanvallen in Nederland
In november 2024 hebben Russische staatsgesteunde hackers, verbonden aan het Russische hackerscollectief Z-Pentest, via een hack toegang verkregen tot het besturingssysteem van een fontein in het centrum van een Nederlandse stad. Hierbij zijn pogingen ondernomen om de waardes van het water aan te passen.

Ook de Nationale Politie werd slachtoffer van een digitale spionageaanval waarbij werkgerelateerde contactgegevens van politiemedewerkers zijn buitgemaakt door een cyberactor die tot dan toe onbekend was bij het publiek. Deze zeer waarschijnlijk door de Russische staat gesteunde cyberactor, die van de diensten de naam LAUNDRY BEAR heeft gekregen, voert al sinds tenminste 2024 cyberaanvallen uit op westerse overheden, bedrijven en andere organisaties. Vaak richten de aanvallen van deze cyberactor zich op zaken die relevant zijn voor de Russische oorlogsinspanningen in Oekraïne, zoals ministeries van Defensie van NAVO-landen, krijgsmachtonderdelen en defensie(toe)leveranciers. De Nederlandse politie lijkt om opportunistische redenen doelwit te zijn geweest.

Daarnaast waren in april 2025 veel websites van Nederlandse steden en provincies onbereikbaar na DDoS-aanvallen door Russische staatsgesteunde hackersgroeperingen. In aanloop naar en tijdens de NAVO-top 2025 in Den Haag zijn vanuit Russische cyberactoren voornamelijk laagdrempelige cyberaanvallen waargenomen. Dit betrof onder meer voorbereidingen voor een phishingcampagne van de hierboven genoemde actor LAUNDRY BEAR.

7.2 Van het binnendringen van systemen tot sabotage

De eerdergenoemde toegenomen risicobereidheid aan Russische zijde laat zich ook zien in het cyberdomein. De AIVD en MIVD stellen vast dat niet alleen de technische kennis en capaciteiten van verschillende staatsgesteunde hackersgroeperingen zijn toegenomen, maar ook de bereidheid om na het binnendringen van systemen (compromittering) daadwerkelijk over te gaan tot (cyber)sabotage.

De cyberaanvallen richten zich onder meer op Europese en NAVO-bondgenootschappelijke doelwitten, maar ook op doelwitten in Nederland. In aanvulling op het kader hierboven is in Nederland een onsuccesvolle cyberoperatie uitgevoerd die gericht was op een bedrijf in de Nederlandse kritieke infrastructuur.

Rusland voerde deze operatie mogelijk uit ter voorbereiding voor cybersabotage (prepositionering). De aanhouding van twee minderjarigen op verdenking van spionage in september 2025 illustreert dat deze dreiging zich ook in Nederland manifesteert.

De afgelopen paar jaar zijn Russische statelijke aanvalsgroepen en staatsgesteunde hackers-groeperingen bovendien meer cyberoperaties gaan uitvoeren waarbij gevoelige informatie wordt bemachtigd. Deze informatie kan Rusland vervolgens gebruiken bij activiteiten in het fysieke domein, bijvoorbeeld bij Russische oorlogshandelingen in Oekraïne. Wat vooral opvalt is dat de hackers-groeperingen zeer opportunistisch te werk gaan en ‘pakken wat ze pakken kunnen’. Hierbij compromitteren ze verschillende, veelal slecht beveiligde controle- en besturingssystemen. Deze brede doelwit-selectie maakt het lastig om te anticiperen op dergelijke aanvallen.

8.
Impact op de Nederlandse samenleving

De oorlog in Oekraïne en het door Rusland gepercipieerde existentiële conflict met het Westen hebben een bredere impact op de Nederlandse samenleving. Zoals eerder beschreven, probeert Rusland in te spelen op bestaande maatschappelijke tegenstellingen en deze te vergroten. Dit betekent lang niet altijd dat sprake is van een gestructureerde en gecoördineerde inzet die wordt aangestuurd door het Kremlin of andere aan de Russische staat gelieerde actoren. Wel vindt het Kremlin-gezinde narratief zijn weerklank binnen bijvoorbeeld de anti-institutioneel-extremistische beweging en sluit het aan op onderdelen van het anti-institutionele narratief.

De Hofvijver bij het Binnenhof, Den Haag

In het anti-institutionele narratief wordt gesproken over een kwaadaardige elite die de regie voert over alle invloedrijke instituties en haar macht gebruikt om het 'gewone volk' te onderdrukken. Om dit onderdrukkende beleid te legitimeren, zou de elite verschillende crises verzinnen, zoals de coronapandemie, de stikstofcrisis, maar ook het aanhoudende conflict in Oekraïne.

De extremistische anti-institutionele beweging in Nederland is nog altijd overwegend pro-Russisch. De beweging ziet president Putin als 'verlosser' die het durft op te nemen tegen de kwaadaardige elite in het Westen en die de door deze kwaadaardige elite gedomineerde internationale orde ter discussie durft te stellen.

Datzelfde geldt in bepaalde mate voor radicaal-rechtse en rechts-extremistische bewegingen. Hoewel deze pro-Russische houding vooralsnog zeer beperkt bijdraagt aan de verdere verspreiding van Kremlin-gezinde narratieven, maakt deze pro-Russische opstelling de extremistische beweging mogelijk wel vatbaar voor Russische (heimelijke) beïnvloeding.

Omgekeerd kunnen radicale en extremistische bewegingen het als kans zien om Rusland te benaderen als 'bondgenoot' die deels vergelijkbare doelen nastreeft. Dit wil overigens niet zeggen dat Rusland automatisch ingaat op verzoeken van deze radicale en extremistische bewegingen.

Wel kan de steun die uit eventuele interactie kan voortvloeien bijdragen aan de verspreiding, normalisering en legitimering van het eigen extremistische gedachtegoed. Bovendien kunnen interacties tussen aan de Russische staat gelieerde actoren en radicale en extremistische bewegingen de extremistische en terroristische dreiging van deze bewegingen vergroten. Dit is ook te zien in verschillende aanslagen in een aantal Europese landen[6]. In Nederland heeft Rusland tot op heden echter nauwelijks direct bijgedragen aan de extremistische en terroristische dreiging.

In aanvulling hierop geldt dat de stappen die Europa momenteel onderneemt ter voorbereiding op een eventueel openlijk militair conflict met Rusland een tegenreactie kan oproepen onder anti-militaire en pacifistische bewegingen. Rusland kan op deze eventuele tegenreacties inspelen en ze gebruiken om Kremlin-gezinde uitlatingen te verspreiden.

8.1. Geen aanwijzingen voor het uitreizen van groepen Nederlandse extremisten

Nog altijd zijn er geen aanwijzingen dat grote groepen Nederlanders met een extremistische ideologie naar Oekraïne zijn gereisd om daar aan Oekraïense dan wel Russische zijde deel te nemen aan de oorlog. Hoewel er binnen een aantal extremistische stromingen in Nederland enige sympathie bestaat voor specifieke strijders of strijdgroepen, speelt de oorlog in Oekraïne een uiterst beperkte rol in hun propaganda.

Gevolgen van de oorlog voor de jihadistische dreiging

De mogelijke gevolgen van de oorlog in Oekraïne die beschreven zijn in de vorige publicatie uit 2023[7] zijn deels bewaarheid. Zo is het waarschijnlijk dat de afname van Russische activiteiten in Syrië er aan bijgedragen heeft dat de door Rusland gesteunde Bashar al-Assad in 2024 het veld moest ruimen. Dit heeft een nieuwe situatie opgeleverd waarin ISIS in Syrië sinds 2025 een bescheiden heropleving doormaakt. Ook zijn een aantal ISIS-leden die eerder in Oekraïne verbleven, met name in 2022, naar Europa gekomen. Zij waren verbonden aan de ISIS Khorasan Provincie (ISKP), de tak van ISIS die zijn oorsprong kent in Afghanistan. Zij zijn lid van het externe ISIS-aanslagnetwerk dat zich in Syrië bevindt. Een aantal van hen is betrokken geweest bij concrete aanslagplanning. In West-Europa zijn verschillende van deze aanslagplannen in zowel 2022, 2023 als 2024 verstoord. Ook in Nederland werden twee personen gearresteerd: een man uit Tadzjikistan en een vrouw uit Kirgizië.

[6] Zie themahoofdstuk: toenemende Russische statelijke dreiging draagt beperkt bij aan de extremistische en terroristische dreiging in Nederland, Dreigingsbeeld Terrorisme Nederland, d.d. 17 juni 2025

[7] 24/2 De Russische aanval op Oekraïne: een keerpunt in de geschiedenis.

9.
Conclusie

De AIVD en MIVD nemen waar dat Rusland zich verwikkeld ziet in een breder en existentieel conflict met een in Russische ogen pervers en decadent Westen. Dit conflict speelt zich af op militair, economisch en ideologisch vlak, waarbij dat laatste vlak het meest fundamentele is. Dit existentiële conflict is in Russische ogen een conflict tussen niet alleen botsende, maar onverenigbare wereldbeelden gebaseerd op strijdige waarden- en normensystemen. Rusland presenteert zich hierbij als unieke beschaving. In dit licht bereidt Rusland zich voor op een langetermijnconfrontatie met het Westen.

EU-vlaggen in Brussel, België.

Militair verloop in Oekraïne

Rusland lijdt nog altijd grote verliezen, zonder zijn operationele doelstellingen ('denazificatie' en demilitarisatie van Oekraïne) te behalen. Ondanks de zware verliezen, de hoge economische prijs en de beperkte terreinwinst verloopt de oorlog in Oekraïne relatief beter voor Rusland. Hoewel Moskou zich realiseert dat de oorlog uiteindelijk aan de onderhandelingstafel zal eindigen, lijkt Moskou niet of slechts zeer beperkt bereid tot het doen van wezenlijke concessies.

Het Russische doel is het herschikken van de Europese veiligheidsarchitectuur waarbij het een veto wil op ontwikkelingen die het land als bedreigend ervaart. Rusland slaagt er tot op heden en met hulp van landen als China, Iran en Noord-Korea in om de geleden personele en materiële verliezen in Oekraïne op te vangen en te compenseren. Tegelijkertijd is het in staat om in beperkte mate invulling te geven aan ambitieuze uitbreidingsplannen van de krijgsmacht. Vooruitlopend op een eventueel staakt-het-vuren en een post-conflict-situatie treft Rusland nadrukkelijk voorbereidingen voor een mogelijk militair conflict met de NAVO.

Militaire escalatie niet langer ondenkbaar
Een direct militair conflict tussen Rusland en de NAVO is vooralsnog onwaarschijnlijk, maar sinds de oorlog in Oekraïne is dit wel voorstelbaar geworden.

De AIVD en MIVD schatten in dat Rusland na het beëindigen van de oorlog in Oekraïne in het minst gunstige scenario mogelijk minder dan een jaar nodig heeft om voldoende capaciteiten op te bouwen voor een militaire operatie met beperkte geografische doelstellingen. Een dergelijke militaire operatie zal niet gericht zijn op het militair verslaan van de NAVO, maar op het uiteenspelen van het bondgenootschap en het afdwingen van concessies ten aanzien van de Europese veiligheidsarchitectuur. Dit betekent niet dat Rusland momenteel ook daadwerkelijk de intentie heeft om hiertoe over te gaan. Europa zal zich volgens de AIVD en MIVD echter wel op een dergelijk scenario moeten voorbereiden.

Toename hybride dreiging
Ook beoordelen de AIVD en MIVD dat de hybride dreiging van Rusland is toegenomen. Deze hybride dreiging heeft zich mede als gevolg van de oorlog in Oekraïne sinds het najaar van 2023 nadrukkelijker in Europa gemanifesteerd. Ook in Nederland zijn verschillende Russische hybride activiteiten waargenomen, waaronder voorbereidingen voor sabotage. Nederland is, en blijft, een interessant doelwitland voor Rusland vanwege onder meer de steun aan Oekraïne en het feit dat Nederland gastland is voor diverse internationale organisaties die Rusland als doelwit ziet.

De AIVD en MIVD verwachten dat de dreiging van Russische hybride activiteiten zal aanhouden. Ook na een eventueel staakt-het-vuren in Oekraïne. Rusland zal, gedreven door pragmatisme en opportunisme, gebruik blijven maken van de mogelijkheden die onze open samenleving biedt. Een nieuwe modus operandi die Rusland hierbij gebruikt is de inzet van zogenoemde '*low-level*' agenten: niet tot nauwelijks getrainde personen die meewerken aan sabotageactiviteiten, waarbij zij zich veelal niet bewust zijn van de Russische aansturing.

De AIVD en MIVD verwachten dat de dreiging van Russische hybride activiteiten zal aanhouden.

Deze hybride dreiging zal naar verwachting van de AIVD en MIVD de komende jaren blijven bestaan in een golfbeweging, met momenten van escalatie en de-escalatie. Daarbij zal Europa, maar ook Nederland rekening moeten houden met de grotere risicobereidheid die Rusland in de loop van 2024 is gaan tonen.

Door de ervaring die Rusland opdoet met de inzet van hybride activiteiten en de technische capaciteiten die het hierbij ontwikkelt, achten de AIVD en MIVD het bovendien waarschijnlijk dat Rusland in de toekomst impactvollere hybride activiteiten zal uitvoeren.

Dreiging op lange en korte termijn
Vanwege de ontwikkelingen in de oorlog en de aanhoudende steun van het Westen aan Oekraïne, is ook Europa in de Russische perceptie steeds nadrukkelijker 'onderdeel van het probleem' geworden. Dit zorgt ervoor, samen met de westerse sancties en andere pogingen om Rusland te isoleren, dat Rusland toenadering zoekt tot alternatieve partners en fora op het internationale toneel. Het doel daarbij is om een tegenwicht te bieden aan de internationale orde die in de Russische optiek sinds de Tweede Wereldoorlog wordt gedomineerd door de Verenigde Staten. Hierin is Rusland relatief succesvol gebleken, ook al is Rusland in verschillende van deze – voor Moskou cruciale – relaties minder dominant dan het graag zou willen. De Russische perceptie van het Westen heeft – zoals in deze publicatie beschreven – een direct verband met de dreiging die Rusland ook op het Westen projecteert. Ongeacht de uitkomst van de oorlog in Oekraïne, zal Rusland waarschijnlijk ook op de langere termijn een dreiging blijven vormen voor Nederland, Nederlandse belangen elders en onze bondgenoten.

Belang van samenwerking
De strijd die Rusland voert als autocratisch regime tegen de westerse democratieën is asymmetrisch. Waar de Nederlandse diensten democratisch zijn ingebed met een bijbehorend toezichtstelsel, handelen de Russische diensten op basis van andere spelregels. Om de Russische dreiging tegen te gaan is onderlinge (en publiek-private) samenwerking in zowel nationaal als internationaal verband cruciaal.

De AIVD en de MIVD hebben hierin hun eigen, unieke taken. Naast het onderzoeken van dreigingen, ondersteunen de diensten bij het verhogen van de weerbaarheid van overheidsorganisaties, kennisinstellingen en bedrijven van vitale sectoren. De AIVD en MIVD helpen deze instellingen bij het vergroten van kennis over de gevaren van spionage, sabotage en kennisdiefstal. Dit gebeurt aan de hand van onder meer (technische) publicaties over dreigingen en het delen van concrete handelings-perspectieven. Samen met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC) adviseren de diensten organisaties hiermee over (digitale) weerbaarheid

De samenwerking met partners in binnen- en buitenland en de gezamenlijke steun aan Oekraïne blijven van belang. Samen met partners treden de diensten op om dreigingen tegen te gaan. Hiervoor spelen de diensten actief in op relevante technologieën en bouwen ze doorlopend verder aan een innovatienetwerk bij de overheid, kennisinstellingen en private partners. Voor de veiligheid van Europa en de rest van de wereld.

Algemene Inlichtingen- en Veiligheidsdienst
Postbus 20010 | 2500 EA Den Haag
aivd.nl

Militaire Inlichtingen- en Veiligheidsdienst
Postbus 20701 | 2500 ES Den Haag

Februari 2026