Weerbaar in een gure wereld

Geopolitieke risico's en financiële instellingen

DeNederlandscheBank

EUROSYSTEEM

Auteurs: Maurice Doll, Frank van Dunné, Lora Steen en Thomas Vos.

Met dank aan David Keijzer voor statistische ondersteuning en de vele collega's van DNB die een bijdrage aan dit rapport hebben geleverd. Eveneens dank aan de externe experts voor de nuttige gedachtewisseling.

Inhoudsopgave

Samenvatting en hoofdboodschappen

Het geopolitieke klimaat is de afgelopen jaren aanmerkelijk guurder geworden. Multilaterale samenwerking en internationale vrijhandel, die lange tijd de motor vormden achter de groei van de wereldeconomie, hebben plaatsgemaakt voor een tijdsgewricht dat wordt gekenmerkt door een toename van protectionisme, fragmentatie en blokvorming. In deze guurdere geopolitieke omgeving krijgen conflicten tussen landen en regio's vaker een hybride karakter. Overheden zetten over-en-weer uiteenlopende middelen in om hun invloed op het wereldtoneel te behouden of vergroten, besluitvorming in andere landen te beïnvloeden of toegang te krijgen tot in het buitenland aanwezige kennis en technologie. Zo worden handelsbelemmeringen en industriepolitieke maatregelen ingezet om strategische sectoren te beschermen. Ook is sprake van een groeiend aantal financiële sancties dat westerse overheden oplegt. De toegang tot de internationale financiële infrastructuur en financiële dienstverlening wordt daarbij in toenemende mate als drukmiddel ingezet (*weaponisation of finance*).

De guurdere geopolitieke omgeving heeft via verschillende kanalen impact op financiële instellingen. Geopolitieke risico's worden doorgaans gedefinieerd als de dreiging en verwezenlijking van negatieve gebeurtenissen in verband met oorlog, terrorisme en spanningen tussen staten en politieke actoren, die een vreedzaam beloop van internationale betrekkingen beïnvloeden. Geopolitieke risico's zijn notoir met een hoge mate van onzekerheid omgeven. In een wereld met verhoogde geopolitieke onzekerheid neemt bovendien de kans op nieuwe, onverwachte schokken toe. Geopolitieke ontwikkelingen hebben via verschillende kanalen impact op financiële instellingen en de macro-economische omgeving waarin zij actief zijn. Instellingen ondervinden onder meer gevolgen via hun blootstellingen op bedrijven die gevoelig zijn voor verstoringen in mondiale toeleveringsketens en de operationele activiteiten en beleggingen die zij in potentieel kwetsbare jurisdicties hebben. Ook kunnen zij te maken krijgen met moedwillig veroorzaakte digitale of fysieke verstoringen in de eigen bedrijfsprocessen of die van kritieke toeleveranciers. Of getroffen worden door sancties. Geopolitieke spanningen vormen zo een potentiële bron van verschillende financiële en niet-financiële risico's waaraan instellingen blootstaan. Zoals inflatie-, krediet-, markt-, liquiditeits- en operationele risico's.

Integrale verankering geopolitieke risico's in het risicomanagement van instellingen

De potentiële forse impact van geopolitieke risico's onderstreept de noodzaak voor instellingen om deze risico's proactief te identificeren en integraal te beheersen. Geopolitieke risico's zijn de afgelopen jaren steeds nadrukkelijker op het netvlies van bestuurders van financiële instellingen komen te staan. Dat is goed. Het is van belang dat financiële instellingen ook de benodigde stappen zetten om de impact van geopolitieke risico's te beheersen. Dit vergt dat ze geopolitieke risico's integraal in hun risicomanagement verankeren. Dat begint bij alertheid en anticiperen op hoe geopolitieke risico's in financiële en niet-financiële risico's kunnen resulteren. Het uitvoeren van stresstesten waarmee de impact van geopolitieke risico's in beeld wordt gebracht, is hiervoor behulpzaam. Zulke stresstesten dienen gebaseerd te zijn op extreme maar plausibele scenario's, zoals bijvoorbeeld een verdere escalatie van de spanningen tussen China en Taiwan. Daarmee wordt inzichtelijk of instellingen over voldoende

buffers – in termen van zowel solvabiliteit als liquiditeit – beschikken voor het geval geopolitieke ontwikkelingen in financiële risico's manifesteren. Door dergelijke stresstesten aan te vullen met gerichte scenario-analyses wordt ook inzicht verkregen in risico's die zich niet in krediet- en marktrisicomodellen laten vatten en andersoortige beheersmaatregelen vergen. Zo kan het verkennen van een scenario waarin operationele activiteiten in een bepaalde jurisdictie noodgedwongen worden stopgezet, bijvoorbeeld als gevolg van sancties, helpen om operationele kwetsbaarheden en potentiële risico's voor de bestendigheid van het bedrijfsmodel in kaart te brengen. Het is zaak dat instellingen de opgedane inzichten uit deze vooruitblikkende analyses benutten om hun strategie en risicomanagement bij te stellen en aan te scherpen.

Toezichthouders zullen instellingen blijven uitdagen over de wijze waarop zij geopolitieke risico's in hun risicomanagement verankeren. Van financiële instellingen wordt in algemeenheid verwacht dat zij inzicht hebben in de materiële risico's waaraan ze blootstaan, deze beheersen en hierover rapporteren. Zo ook voor geopolitieke risico's. Geopolitieke risico's zullen de komende jaren een belangrijk focusgebied vormen in het toezicht. DNB zal instellingen aan de tand voelen over de wijze waarop zij de risico's die voortvloeien uit een guurdere, turbulentere geopolitieke omgeving identificeren en beheersen.[1]

Cyberweerbaarheid en naleving sanctieregelgeving vergen bijzondere aandacht

Het versterken van de cyberweerbaarheid vergt blijvende aandacht, vanwege het complexer geworden dreigingslandschap. Toezichthouders zullen toezien op adequate naleving van de nieuwe Europese regels gericht op het vergroten van de cyberweerbaarheid. Financiële instellingen staan, ook via (kritieke) toeleveranciers, bloot aan cyberrisico's. Dergelijke risico's kunnen niet alleen gevolgen voor individuele instellingen hebben, maar via vertrouwensverlies en besmetting ook voor het financieel systeem als geheel. Naast het op orde houden van de cyberbeveiliging en het met regelmaat testen daarvan, is het belangrijk dat instellingen over de benodigde veerkracht beschikken om na een cyberincident hun dienstverlening veilig en vlot te kunnen opstarten. Dit geldt niet alleen voor instellingen zelf, maar ook voor de ICT-dienstverleners waarvan zij in toenemende mate afhankelijk zijn geworden. Met de Europese *Digital Operational Resilience Act* (DORA) worden onder meer scherpere eisen aan de beheersing van ICT- en cyberrisico's in de uitbestedingsketen en de continuïteitsmaatregelen van instellingen gesteld. DNB zal, samen met de AFM, erop toezien dat instellingen de uit DORA voortvloeiende vereisten naleven.

Het toegenomen aantal opgelegde sancties door overheden stelt instellingen bloot aan verhoogde juridische en reputatierisico's. Het is van belang dat instellingen sanctieregelgeving adequaat naleven. Westerse overheden maken steeds intensiever gebruik van sancties, in het bijzonder van financiële sancties. Financiële instellingen hebben een belangrijke verantwoordelijkheid bij de naleving van deze sancties, vanwege hun sleutelrol in het betalingsverkeer, de toegang die zij tot financiële diensten verschaffen en in hun rol als belegger. Het toegenomen aantal

1 Zie ook DNB (2024) Visie op Toezicht 2025 – 2028.

sancties dat door overheden wordt opgelegd, gaat voor instellingen met verhoogde juridische en reputatierisico's gepaard. DNB ziet erop toe dat instellingen hun bedrijfsvoering zodanig inrichten dat sanctieregelgeving adequaat wordt nageleefd. Ondanks recente verbeteracties, zal een aanzienlijk aantal instellingen zich nog moeten inspannen om de naleving van sanctieregelgeving op het benodigde volwassenheidsniveau te brengen. Het detecteren van sanctieomzeiling, screenen op *dual-use* goederen - die zowel een militaire als civiele toepassing kennen – en het vaststellen van de *ultimate beneficial owners* van een onderneming, vergen daarbij in het bijzonder aandacht.

Verhogen weerbaarheid vergt ook intensieve publiek-private en Europese samenwerking

Vergroten van de weerbaarheid vergt niet alleen stappen van financiële instellingen en het bedrijfsleven, maar ook intensieve publiek-private samenwerking. Financiële instellingen zijn, net als andere bedrijven, zelf aan zet om hun risicomanagement op orde te brengen en de benodigde preventieve en mitigerende maatregelen te treffen om de continuïteit van hun dienstverlening te kunnen borgen. Verhogen van de weerbaarheid van de samenleving als geheel vergt echter ook intensieve samenwerking tussen publieke en private partijen. Zo helpt het tijdig en breed delen van cyberdreigingen tussen verschillende sectoren en met de overheid om deze dreigingen scherper in het vizier te krijgen. Publiek-private samenwerking is ook cruciaal voor het vergroten van de weerbaarheid van de vitale infrastructuur, zoals de telecomsector, de elektriciteitsvoorziening en het betalingsverkeer. Gezien de potentieel ontwrichtende effecten van digitale of fysieke verstoringen in vitale sectoren, zijn sector-overstijgende samenwerking en stevige centrale regie essentieel. In dit licht is het wenselijk dat de overheid het initiatief blijft nemen voor grootschalige (cyber)oefeningen, waarin geoefend wordt met activering van de landelijke crisisstructuur. Het is belangrijk dat de opgedane inzichten vervolgens worden benut om de weerbaarheid te verhogen.

Intensieve samenwerking in Europa is essentieel om geopolitieke risico's het hoofd te kunnen bieden. Het guurdere geopolitieke klimaat, in combinatie met het grensoverschrijdende karakter van de hieruit volgende risico's, vraagt om intensieve samenwerking in Europa. Zo is het van belang dat sanctiebeleid zoveel mogelijk Europees geharmoniseerd wordt. Dit draagt bij aan een gelijker speelveld tussen instellingen en vergemakkelijkt sanctienaleving voor instellingen die in meerdere lidstaten actief zijn. Versterken van weerbaarheid vergt ook dat beleidsmakers het belang van het verminderen van strategische afhankelijkheden zorgvuldig afwegen tegen de negatieve effecten daarvan op de economie en de verdere fragmentatie die dit in de hand kan werken. Tot slot hebben zij stappen te zetten in het vervolmaken van de interne markt – in het bijzonder de Europese kapitaalmarkt- en bankenunie. Een goed functionerende interne markt en beter werkende financieringsmarkten bieden additionele mogelijkheden tot diversificatie. Daarnaast zijn ze belangrijk voor het groeipotentieel, onder meer doordat geïntegreerde en liquide kapitaalmarkten de toegang tot financiering voor innovatieve bedrijven vergroten. Het draagt ook bij aan stabiliteit. Een goed functionerende interne markt, waarin huishoudens en bedrijven kunnen floreren, vormt immers een belangrijke bron van bescherming voor ongunstige ontwikkelingen elders.

Inleiding

Het geopolitieke klimaat is de afgelopen jaren guurder geworden. Het wereldbeeld wordt de afgelopen jaren in toenemende mate gekenmerkt door internationale rivaliteit, stagnerende multilaterale samenwerking en een beleid gericht op strategische autonomie door het afbouwen van risicovolle afhankelijkheden. De Russische inval in Oekraïne, de oplopende spanningen tussen China en Taiwan, het handelsconflict tussen de VS en China en de spiraal van geweld in het Midden-Oosten weerspiegelen deze geopolitieke spanningen.

In toenemende mate is sprake van fragmentatie van de wereldeconomie, wat tot uiting komt in een groeiend aantal handelsbeperkingen. Alleen al in 2023 zijn er, zo blijkt uit onderzoek van het IMF, wereldwijd meer dan 2.500 industriepolitieke maatregelen genomen, waarvan 70% handelsverstorend werkt.[2] Het gegroeide economisch nationalisme, waarvoor de uitslagen van recente verkiezingen in Europa en eerder ook de Brexit en het *'America First'*- beleid in de VS illustratief zijn, versterkt deze trend. Daarnaast is het moeilijker gebleken om binnen multilaterale fora, zoals de Wereldhandelsorganisatie (WTO), tot afspraken te komen. Nieuwe mondiale handelsakkoorden hebben plaatsgemaakt voor regionale en bilaterale handelsakkoorden. Deze beleidsomslag van integratie naar desintegratie, veelal ingegeven vanuit strategische overwegingen, wordt geo-economische fragmentatie genoemd.[3] Geo-economische fragmentatie heeft zijn weerslag op de wereldhandel. De groei van de wereldhandel is in een lagere versnelling gekomen en onderliggend is een verschuiving zichtbaar richting regionalisering van handelsstromen.[4]

Er is sprake van blokvorming tussen landen en regio's, waarbij overheden met uiteenlopende middelen pogen hun invloed op het wereldtoneel te bestendigen of te vergroten. De unipolaire wereldorde, met een centrale positie voor de VS, die na het uiteenvallen van de Sovjet-Unie ontstond, wordt betwist door landen en regio's die aankoersen op fundamentele veranderingen in de wereldorde.[5] Naast toegenomen spanningen tussen Rusland en het Westen als gevolg van de Russische inval in Oekraïne, springt vooral de relatie tussen de VS en China in het oog. In toenemende mate zijn zij de afgelopen decennia op geopolitiek en economisch vlak de concurrentie met elkaar aangegaan. Daarnaast hebben conflicten tussen landen vaker een hybride karakter gekregen, zoals in kader 1 wordt geschetst. Tot slot zijn ook de trans-Atlantische betrekkingen aan verandering onderhevig. Hoewel de VS voor de EU nog altijd de belangrijkste bondgenoot vormen, is de onderlinge relatie van de VS met Europa zakelijker van aard geworden.[6]

2 Evenett, S. et al. (2024) The return of Industrial Policy in data.
3 IMF (2023) Geoeconomic Fragmentation and the Future of Multilateralism.
4 ECB (2023) The EU's Open Strategic Autonomy from a central banking perspective.
5 Zie bijvoorbeeld WRR (2024) Nederland in een fragmenterende wereldorde.
6 The Economist (2024) Trump and other populists will haunt NATO's 75th birthday party.

Kader 1

Conflicten tussen landen krijgen steeds vaker een hybride karakter

Conflicten tussen landen hebben afgelopen decennia in toenemende mate een hybride karakter gekregen. Overheden zetten steeds vaker over- en-weer uiteenlopende middelen in, waarbij de lijnen van legitimiteit vervagen. Hiervoor worden middelen gebruikt zoals diplomatieke en financiële sancties, import- en exportbeperkingen, cyberaanvallen en spionage. Met het inzetten van dergelijke middelen proberen overheden hun rol op het wereldtoneel te behouden of vergroten, toegang te krijgen tot in het buitenland aanwezige kennis en technologie of besluitvorming in andere landen te beïnvloeden. Dit verschijnsel wordt hybride conflictvoering genoemd.[7] De toename van hybride conflictvoering is zowel illustratief voor de opgelopen geopolitieke spanningen, als een van de oorzaken daarvan. Technologische ontwikkeling is een andere belangrijke drijvende kracht. Het vergroot de mogelijkheden om op grotere schaal en met grotere snelheid politieke en economische activiteiten in andere landen te beïnvloeden. Ook maakt het nieuwe *modi operandi* mogelijk.[8] Gewapend conflict en openlijk militair ingrijpen worden als *last resort* beschouwd, onder andere vanwege het risico op escalatie, de hoge kosten en het beperkte draagvlak onder de bevolking.

Vanuit het westers perspectief bezien, komt de grootste dreiging vanuit Rusland en China. Rusland ziet zichzelf in een existentieel conflict met het Westen en heeft al ruimschoots voor de annexatie van de Krim in 2014 hybride conflictvoering tot officiële strategie verheven.[9] Volgens de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) vormt Nederland een belangrijk spionagedoelwit voor Rusland. Daarnaast speelt Rusland ook in Nederland in op antiwesterse sentimenten en zoekt het de confrontatie met het Westen in het cyberdomein.[10] Rusland heeft ook laten zien de afhankelijkheid van energie als drukmiddel in te zetten. China is op veel terreinen een belangrijke handelspartner van het Westen, maar tracht tegelijkertijd haar wereldwijde politieke en economische invloed te vergroten. China doet dat onder meer met strategische investeringen in de infrastructuur in Azië, Afrika, Europa en Zuid-Amerika via het *Belt and Road Initiative* en door onafhankelijk te worden van buitenlandse technologie.[11] Chinese cyberaanvallen en spionage in het Westen zijn vooral gedreven vanuit het streven naar toegang tot westerse technologie voor economische en militaire versterking. Tot slot kunnen ook middelgrote en kleinere landen een dreiging vormen voor het Westen. Zo tracht Noord-Korea via cyberaanvallen geld buit te maken om de staatskas te financieren en poogt Iran via kennisinstellingen toegang te krijgen tot westerse kennis.

7 Zie onder andere Analistennetwerk nationale veiligheid (2024), EC en Hybrid CoE (2021), NAVO (2024) en NCTV (2019).
8 Sweijs, T. (2022) Between war and peace, 'Hybrid Threats' and NATO's strategic concept.
9 De Wijk, R. et al. (2021) Russische hybride oorlogsvoering.
10 AIVD (2024) Jaarverslag 2023.
11 Zie onder andere AIVD, MIVD en NCTV (2022) en The Economist (2020).

Ook westerse overheden nemen intensiever deel aan de geopolitieke competitie. Hiervoor gebruiken ze middelen zoals exportrestricties en financiële en diplomatieke sancties (zie ook hoofdstuk 4). Voorbeelden zijn Amerikaanse importtarieven op staal en aluminium, de screening van uitgaande investeringen vanuit de VS in de richting van China en exportbeperkingen die de VS en EU-landen hebben ingevoerd op het gebied van chiptechnologie. De VS maakt hierbij strategisch gebruik van digitale en financiële afhankelijkheden, bijvoorbeeld via de centrale positie van de dollar in het internationale handels- en betalingsverkeer.[12]

De Nederlandse economie is gevoelig voor geo-economische fragmentatie. Nederland was in 2021 de zesde exporteur en achtste importeur van goederen ter wereld. Ook is Nederland een belangrijke investeerder in het buitenland en ontvanger van buitenlandse investeringen.[13] De hoge mate van openheid maakt Nederland gevoelig voor verstoringen in mondiale toeleveringsketens en handels- en kapitaalsbeperkingen. Dergelijke verstoringen en beperkingen nopen tot aanpassingen voor bedrijven. Ze kunnen tot opwaartse prijsdruk leiden en gevolgen hebben voor de economische groei en financiële stabiliteit.[14]

De (digitale) dreiging voor Nederland is onverminderd groot en verandert voortdurend. Net als in andere westerse landen vormt inmenging van andere staten in Nederland in toenemende mate een dreiging voor de sociale en economische veiligheid, zo blijkt uit publicaties van de AIVD, de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).[15] De gevolgen worden hierbij versterkt door het open karakter van Nederland, als belangrijk knooppunten voor goederen, diensten en data.[16] De grootste dreiging komt, naast Rusland, vanuit China. Met name kennisintensieve sectoren vormen een potentieel doelwit voor cyberaanvallen, spionage, sabotage en strategische overnames. Voorbeelden van deze sectoren zijn de halfgeleiderindustrie, lucht- en ruimtevaart en maritieme industrie. Daarnaast vormen vitale sectoren, zoals de energie- en de telecomsector, ook een potentieel doelwit. Dit geldt in potentie ook voor de financiële sector, vanwege de belangrijke maatschappelijke rol die financiële instellingen vervullen en de informatie en (geldelijke) activa die zij beheren.

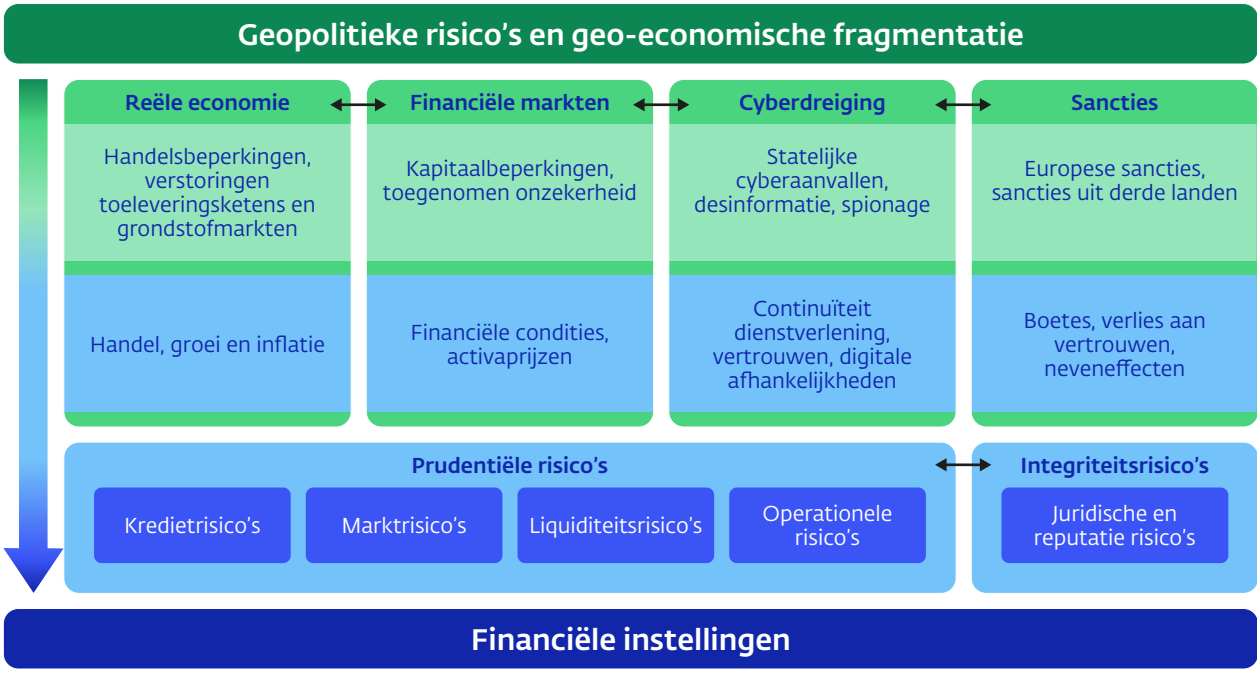
Geopolitieke ontwikkelingen kunnen via verschillende kanalen gevolgen hebben voor Nederlandse financiële instellingen. Toenemende geo-economische fragmentatie en geopolitieke risico's[17] raken financiële instellingen via verschillende financiële en niet-financiële risico's, zoals figuur 1 illustreert. De snelheid waarmee verschillende kanalen effect op financiële instellingen kunnen hebben verschilt.

12 Zie bijvoorbeeld Farrell H. en Newman A. (2024) Underground Empire - How America weaponized the world economy, Penguin Random House.
13 DNB (2024) Internationale verwevenheid scherper in beeld.
14 DNB (2023) Geo-economische fragmentatie: economische en financiële stabiliteitsgevolgen.
15 Zie onder andere NCTV (2022), AIVD (2024) en MIVD (2024).
16 ANV (2019), Geïntegreerde risicoanalyse Nationale Veiligheid, Analistennetwerk Nationale Veiligheid
17 In deze studie hanteren wij de veelgebruikte definitie van Caldara en Iacoviello (2022) voor geopolitieke risico's. Zij definiëren geopolitieke risico's als "de dreiging en verwezenlijking van negatieve gebeurtenissen in verband met oorlog, terrorisme en spanningen tussen staten en politieke actoren die een vreedzaam beloop van internationale betrekkingen beïnvloeden."

Zo kunnen cyberaanvallen op instellingen of kritieke derde partijen in potentie al op korte termijn tot forse schade leiden, terwijl het enige tijd kan duren voordat instellingen geconfronteerd worden met kredietverliezen als gevolg van opgelegde handelsbeperkingen. Bovendien kunnen verschillende kanalen elkaar versterken. Krappere financieringscondities als gevolg van toegenomen onzekerheid kunnen kredietverliezen voor banken verder doen toenemen, zeker bij bedrijven die reeds te maken hebben met verstoringen in hun toeleveringsketen. Dit kan ook met liquiditeitsrisico's gepaard gaan wanneer deze bedrijven genoodzaakt zijn een groter beroep op bestaande kredietlijnen te doen. Ook kunnen cyberaanvallen die met operationele risico's voor één instelling gepaard gaan, potentieel bredere gevolgen hebben wanneer deze het vertrouwen van spaarders in financiële instellingen aantasten.

De volgende hoofdstukken diepen de kanalen uit waarlangs geopolitieke ontwikkelingen effect hebben op financiële instellingen en gaan in op de risico's die hieruit voortvloeien. Hoofdstuk 2 gaat in op hoe geopolitieke ontwikkelingen via de reële economie en financiële markten gevolgen kunnen hebben voor instellingen en besteedt aandacht aan de blootstellingen van instellingen. Hoofdstuk 3 gaat in op de risico's die voortvloeien uit de veranderde cyberdreiging, waarbij onder andere wordt ingegaan op de rol van statelijke actoren, ketenafhankelijkheden en de noodzaak van een effectieve response- en recoveryplannen. Vervolgens gaat hoofdstuk 4 in op financiële sancties, de rol van financiële instellingen bij de uitvoering van deze sancties en de neveneffecten van sancties die tot risico's voor instellingen kunnen leiden.

Figuur 1 Geopolitieke ontwikkelingen en risico's voor financiële instellingen



Bron: DNB (2024), mede op basis van IMF (2023).

Geo-economische fragmentatie, reële economie en financiële markten

Nederlandse financiële instellingen zijn vooral gevoelig voor geo-economische fragmentatie via hun blootstellingen aan bedrijven die vatbaar zijn voor verstoringen in mondiale waardeketens. Geopolitieke ontwikkelingen kunnen daarnaast onzekerheid en volatiliteit op financiële markten teweegbrengen, wat naast marktrisico's ook tot hogere financieringskosten voor instellingen kan leiden. Het is belangrijk dat instellingen in staat zijn geopolitieke risico's tijdig te identificeren en integraal te beheersen.

2.1 Blootstellingen, krediet- en marktrisico's van financiële instellingen

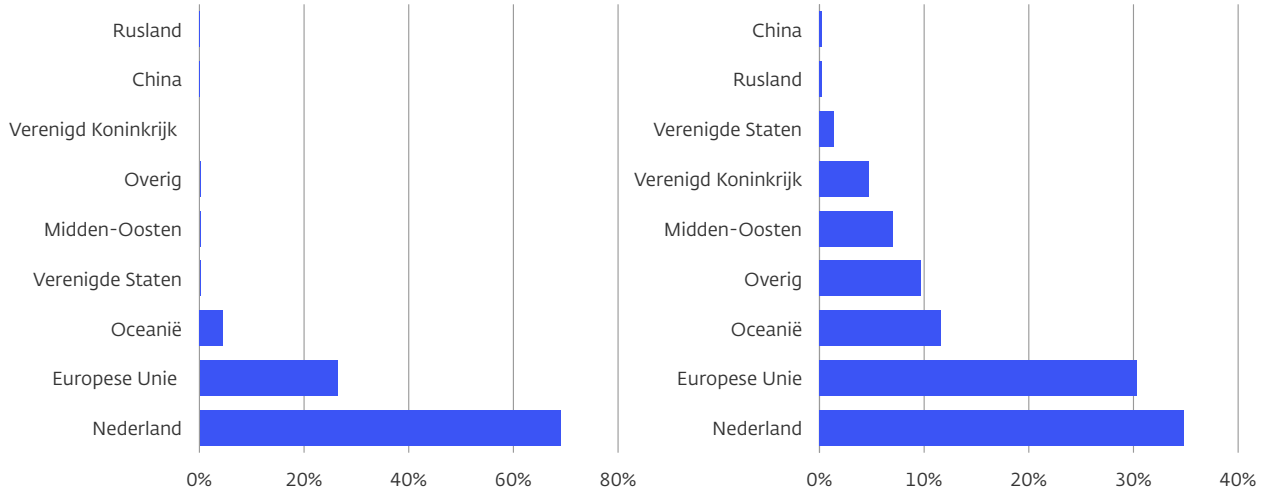
Financiële instellingen staan bloot aan geopolitieke risico's via activiteiten in landen die vanuit geopolitiek perspectief gezien op afstand van Nederland staan, bijvoorbeeld via versterkte leningen en beleggingen. Zo hebben banken, verzekeraars en pensioenfondsen af moeten schrijven op hun Russische activa na de Russische inval in Oekraïne (zie ook hoofdstuk 4). Tegelijkertijd blijkt uit eerder onderzoek van DNB dat *directe* blootstellingen van financiële instellingen op landen die op geopolitieke afstand van Nederland staan, waartoe in die analyse onder andere Rusland, Iran en China werden geschaard, bescheiden zijn en de afgelopen jaren verder afgebouwd zijn.[18] Van de totale bedrijfsleningenportefeuille van Nederlandse banken is 0,5% verstrekt aan bedrijven in deze groep landen. Nederlandse banken hebben via hun kredietportefeuille vooral een blootstelling op Nederlandse huishoudens en bedrijven uit Nederland en andere EU-landen (zie figuur 2). Ook verzekeraars en pensioenfondsen hebben via hun beleggingsportefeuille vooral een blootstelling op Nederland, andere EU-landen, de VS en het VK. Van de directe beleggingen in bedrijfsobligaties en aandelen hebben verzekeraars en pensioenfondsen minder dan 1% belegd in bedrijven die zijn gevestigd in landen die op geopolitieke afstand van Nederland staan. Verzekeraars staan overigens niet alleen via hun activa aan geopolitieke risico's bloot, maar kunnen in potentie ook via hun verplichtingen worden geraakt. Kader 2.1 gaat hier verder op in.

Financiële instellingen zijn vooral gevoelig voor geo-economische fragmentatie via de waardeketens van bedrijven. Geo-economische fragmentatie kan de beleggings- en kredietportefeuilles van financiële instellingen *indirect* raken. Doordat de bedrijven waarin zij hebben belegd, of waaraan zij krediet hebben verstrekt, te maken krijgen met verstoringen in hun toeleveringsketens, bijvoorbeeld als gevolg van handelsbeperkingen. Met name bedrijven die afhankelijk zijn van goederen en grondstoffen uit landen die op geopolitieke afstand van Nederland staan, of waarvoor deze landen een belangrijke afzetmarkt vormen, zijn kwetsbaar voor

18 Zie DNB (2024). In deze analyse is, op basis van onderzoek van Baba et al. (2023) een onderscheid gemaakt tussen gelijkgestemde, neutrale en tegenstelde landen aan de hand van het stemgedrag van landen bij een VN-resolutie over de mensenrechtensituatie in de bezette gebieden van Oekraïne. De groep 'tegengestelde' landen bestaat uit 15 landen. Deze onderliggende verdeling in groepen landen dient niet verabsoluteerd te worden, aangezien het betrekking heeft op een specifieke VN-resolutie. Bij de geografische blootstellingen van pensioenfondsen en verzekeraars zijn deelnemingen in beleggingsinstellingen buiten beschouwing gelaten.

Figuur 2 Geografische blootstelling kredietportefeuille Nederlandse banken

Leningen aan huishoudens (links, % totaal) en leningen aan bedrijven (rechts, % totaal)



Toelichting: Figuur geeft aandelen van verschillende landen en werelddelen weer in respectievelijk de totale huishoud- en bedrijfsleningenportefeuille van Nederlandse banken. De groep Oceanië omvat onder andere Australië en Nieuw-Zeeland; het Midden-Oosten omvat onder meer Turkije, Saudi-Arabië, Israël, Qatar en de Verenigde Arabische Emiraten. Data hebben betrekking op 2023.

Bron: DNB (2024).

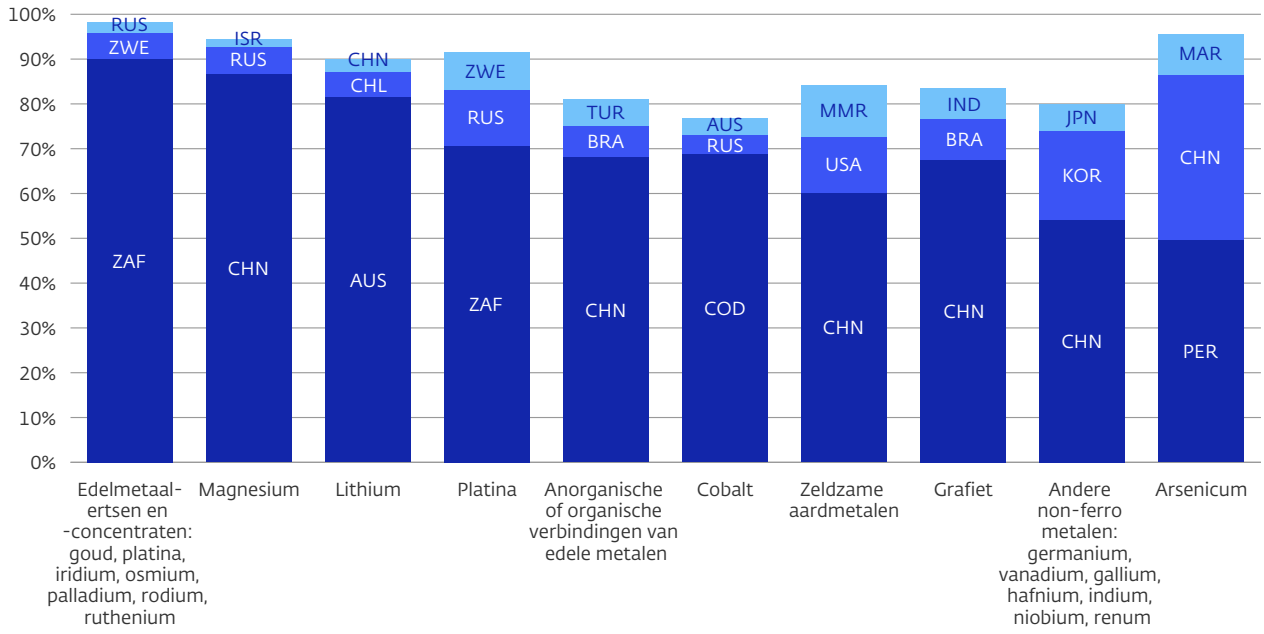
dergelijke verstoringen. Illustratief hiervoor zijn de potentiële leveringsrisico's die samenhangen met de toenemende exportbeperkingen die aan kritieke grondstoffen worden opgelegd, in combinatie met de geografisch sterk geconcentreerde winning en verwerking van deze grondstoffen (zie figuur 3).[19] Uit onderzoek van DNB blijkt dat banken met name via hun kredietverlening aan de industrie gevoelig zijn voor geo-economische fragmentatie.[20] De industrie is namelijk relatief sterk afhankelijk van importgoederen uit landen die op geopolitieke afstand van Nederland staan. Banken staan hieraan bloot doordat bedrijfsleningen aan de industrie een relatief groot aandeel in hun kredietportefeuille vormen. Hetzelfde geldt voor pensioenfondsen en verzekeraars via hun beleggingen in industriële bedrijven, wat hen blootstelt aan marktrisico's.

Ook doorwerking van geo-economische fragmentatie op de Nederlandse economie stelt financiële instellingen aan krediet-, markt- en inflatierisico's bloot. Verstoringen in mondiale waardeketens en energie- en grondstoffenmarkten kunnen negatieve effecten hebben op de wereldhandel en economische groei. Hetzelfde geldt voor industriebeleid dat erop is gericht strategische goederen lokaal te produceren en initiatieven om productie naar het eigen land terug te halen (*reshoring*). Deze ontwikkelingen kunnen op de korte- en middellangetermijn tot opwaartse prijsdruk leiden, doordat ingevoerde goederen door een duurder alternatief worden

19 Zie bijvoorbeeld OECD (2023) Raw materials critical for the green transition.
20 DNB (2024) Overzicht Financiële Stabiliteit voorjaar 2024.

Figuur 3 Sterke geografische concentratie van de winning van kritieke grondstoffen

Aandeel in de wereldwijde productie (%)



Toelichting: Figuur toont de top 3 van producerende landen voor de 10 meest productie-geconcentreerde kritieke grondstoffen. AUS = Australië, BRA = Brazilië, CHN = China, CHL = Chili, COD = Democratische republiek Congo, IND = India, ISR = Israël, JPN = Japan, KOR = Korea, MAR = Marokko, MMR = Myanmar, PER = Peru, TUR = Turkije, RUS = Rusland, ZAF = Zuid-Afrika, USA = Verenigde Staten en ZWE = Zimbabwe.

Bron: OECD (2023).

vervangen.[21] Analyses van het Centraal Planbureau (CPB) en DNB laten zien dat toenemende geo-economische fragmentatie de economische groei en reële inkomens in Nederland onder druk zet, de inflatie doet oplopen, en tot een hogere werkloosheid leidt.[22] Dit werkt door op de balans van financiële instellingen. Zo blijkt uit een stresstest die de Europese Bankenautoriteit (EBA) in 2023 op 70 Europese banken heeft uitgevoerd dat geopolitieke ontwikkelingen onder meer door een lagere groei, hogere inflatie en hogere rente een forse impact hebben op de kapitaalpositie van banken. De kapitaalratio's van banken verslechteren aanzienlijk, maar vanwege de sinds de financiële crisis verbeterde uitgangspositie zijn banken in staat deze schok op te vangen.[23] Eind dit jaar presenteert EIOPA, de Europese autoriteit voor de verzekeringssector en bedrijfspensioensector, de resultaten van een stresstest met een geopolitiek scenario voor verzekeraars.

21 ECB (2023) The EU's Open Strategic Autonomy from a central banking perspective.
22 Zie CPB (2024) en DNB (2023).
23 EBA (2023) 2023 EU-wide stress test: results.

Kader 2.1
Geopolitieke risico's en verzekeringsclaims

Verzekeraars zijn niet alleen via hun beleggingen aan geopolitieke risico's blootgesteld, maar in potentie ook via de verzekeringsverplichtingen die zij aangaan. Verzekeraars staan bloot aan zogenoemde verzekeringstechnische risico's, als gevolg van de verzekeringsdekking die zij bieden. Geopolitieke gebeurtenissen kunnen tot een onverwachte groei van claims leiden, wat in het bijzonder geldt voor schadeverzekeraars die actief zijn in specifieke segmenten, zoals lucht- en scheepvaartverzekeringen. Vaak betreft dit nicheverzekeraars. Grootzakelijke risico's worden veelal bij buitenlandse verzekeraars ondergebracht of via co-assurantie op de beurs verzekerd, waarbij risico's door meerdere verzekeraars worden gedragen. Ook indirecte gevolgen van geopolitieke risico's kunnen invloed hebben op de claims voor schadeverzekeraars. Zo kan inflatie tot hogere claims en uitkeringen leiden. Het is belangrijk dat verzekeraars alert blijven en waar nodig hun beleid aanpassen om negatieve gevolgen op hun financiële positie zoveel mogelijk te mitigeren.[24]

In het buitenland zien we dat verzekeraars dekking beperken of opheffen om risico's te beheersen, vooral in regio's die gevoelig zijn voor geopolitieke onrust. Zo hebben luchtvaartverzekeraars de dekking die zij bieden aan luchtvaartmaatschappijen met een thuisbasis in Israël en Libanon beperkt.[25] Ook het verzekeren van commerciële scheepvaart in de Rode Zee en de Straat van Hormuz staat onder druk, vanwege aanvallen door Houthi-troepen.[26] In gevallen waarin verzekeringsdekking wordt beperkt, dienen bedrijven zelf de gevolgen van schade te dragen. Voor de beheersing van verzekeringstechnische risico's is het belangrijk dat formuleringen in verzekeringspolissen, met name met betrekking tot de dekking en uitsluitingen, nauwkeurig de gewenste risicoblootstellingen van een verzekeraar weerspiegelen. Hierbij vergt ook zogenoemde 'stille dekking' de aandacht. Dit ontstaat wanneer bepaalde risico's niet expliciet zijn uitgesloten in polissen, waardoor verzekeraars geconfronteerd kunnen worden met claims waarmee bij het vaststellen van de premie geen rekening is gehouden.[27] Het is Nederlandse schadeverzekeraars overigens verboden om schades te verzekeren die worden veroorzaakt door of ontstaan zijn uit gewapend conflict, burgeroorlog, opstand, binnenlandse onlusten, oproer of muiterij die zich in Nederland voordoen.[28] Het dekken van deze risico's brengt dusdanige financiële risico's voor verzekeraars met zich mee, dat zij door materialisatie van deze risico's in financiële problemen kunnen komen.

24 Zie ook DNB (2023) Good practice beheersing inflatierisico verzekeraars.
25 Reuters (2023) Exclusive: Aviation war insurers cancel some cover for Israel, Lebanon.
26 Zie bijvoorbeeld Reuters (2024) War insurers shrug off Rubymar sinking in Red Sea, rates stable.
27 Dit is bijvoorbeeld het geval bij cyberrisico's. Zie ook DNB (2022) Verzekeraars in een veranderende wereld.
28 Dit staat bekend als het molest-verbod (artikel 3:38, Wft). Dit verbod geldt alleen voor verzekeraars die onder het toezicht van DNB vallen. Daarnaast is een uitzondering gemaakt voor zeevaart-, transport-, luchtvaart- en reisverzekeringen, mits DNB geen bezwaren heeft geuit.

Wanneer herverzekeraars de verzekeringsdekking beperken, kunnen de risico's voor de oorspronkelijke verzekeraar toenemen. Verzekeraars kunnen verzekeringstechnische risico's beperken door deze (deels) te herverzekeren. In het geval een herverzekeraar zich terugtrekt of de dekkingsvoorwaarden in negatieve zin wijzigt, kunnen verzekeraars geconfronteerd worden met een toename van de verzekeringstechnische risico's waaraan ze blootstaan. Wanneer herverzekeraars ervoor kiezen om dekking te blijven bieden worden geopolitieke risico's mogelijk weerspiegeld in een hogere premie of een hoger eigen risico.[29] Het is daarom belangrijk dat verzekeraars deze ontwikkelingen nauwlettend in de gaten houden.

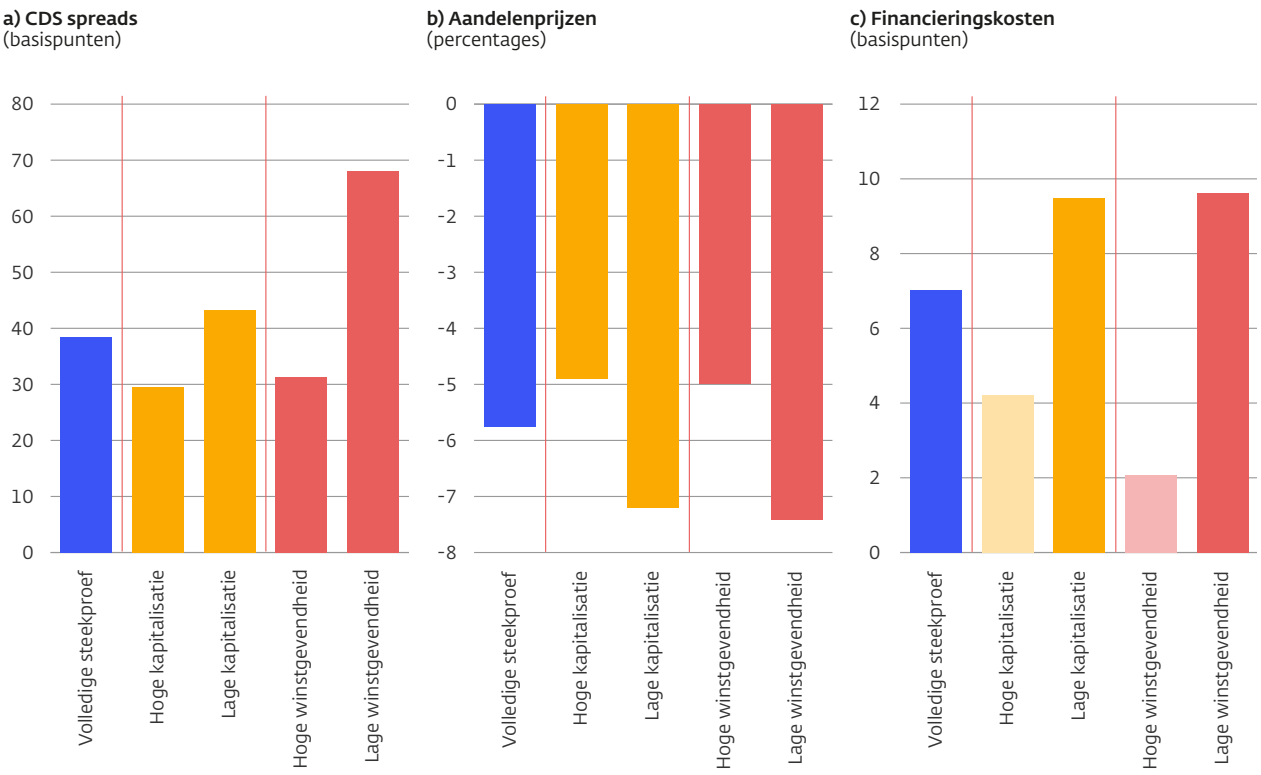
2.2 Toegenomen risico-aversie, volatiliteit en de impact op financieringskosten

Geopolitieke ontwikkelingen kunnen met volatiliteit en prijsschokken op financiële markten gepaard gaan, wat tot marktrisico's kan leiden en ook de aandelenkoersen van financiële instellingen raakt. Geopolitieke risico's en de materialisatie daarvan kunnen tot snelle verschuivingen in marktsentimenten en prijsschokken leiden. Ook kunnen verwachtingen over een gematigdere economische groei en opwaartse prijsdruk als gevolg van geopolitieke ontwikkelingen van invloed zijn op de verwachtingen die marktpartijen hebben over de winstgevendheid van bedrijven. Geopolitieke schokken gaan zodoende gepaard met lagere aandelenwaarderingen, hogere risicopremies en meer volatiliteit. Vooral waarderingen van de transport- en luchtvaartsector en delen van de industrie, waaronder de staalindustrie, blijken gevoelig voor geopolitieke schokken. Ook aandelenkoersen van banken en verzekeraars reageren sterker op geopolitieke schokken dan het gemiddelde van alle sectoren in de economie.[30] Overigens zwakt doorgaans de marktreactie enige tijd na een schok af en treedt herstel op, maar bij grotere en langdurige spanningen en toegenomen onzekerheid kunnen geopolitieke gebeurtenissen langer van invloed zijn op financiële markten.

Toegenomen onzekerheid en belemmeringen aan grensoverschrijdende kapitaalstromen leiden tot minder diversificatie. Opgelegde kapitaalrestricties beperken de mogelijkheden tot diversificatie van financiële instellingen, wat ook nadelige gevolgen kan hebben voor de schokbestendigheid van het financieel systeem als geheel. Ook toegenomen onzekerheid en risico-aversie hebben invloed op de omvang en richting van grensoverschrijdende kapitaalstromen. Zo blijkt uit onderzoek van het IMF dat toenemende spanningen tussen landen een negatief effect hebben op de omvang van grensoverschrijdende kapitaalstromen tussen deze landen.[31] Dergelijke *derisking* van financiële instellingen kan fragmentatie verder in de hand werken.

29 Insurance Insider (2023) Geopolitical risk: A growing threat to insurer profitability.
30 Zie Caldara, D. en Iacoviello, M. (2022) Measuring geopolitical risk.
31 IMF (2023) Geopolitics and financial fragmentation: implications for macro-financial stability.

Figuur 4 Sterkere marktreactie bij minder gekapitaliseerde banken



Toelichting: De coëfficiëntschattingen in deze figuur geven het effect op de CDS-spreads, aandelenprijzen en financieringskosten weer van een toename van één standaarddeviatie van de door de ECB geconstrueerde geopolitical risk index (GPR-index) op bankniveau. De GPR is een nieuws-gebaseerde maatstaf voor geopolitiek risico, waarbij een hogere waarde een grotere kans of intensiteit van ongunstig geopolitieke risico's weergeeft (zie Caldara en Iacoviello (2022)). De GPR op landniveau is door de ECB gewogen op basis van ECB-toezichtdata over de geografische blootstelling van bankactiva om een GPR-index op bankniveau te verkrijgen. De coëfficiënt-schattingen zijn gebaseerd op een panelregressie op een steekproef van 34 significante instellingen voor CDS-spreads, 31 instellingen voor aandelenkoersen en 37 instellingen voor financieringskosten, voor de periode van het eerste kwartaal van 2015 tot het derde kwartaal van 2023. Banken met een kapitaalratio boven de mediaan worden tot de categorie hoge kapitalisatie gerekend, banken met een kapitaalratio onder de mediaan tot de categorie lage kapitalisatie. Ook bij winstgevendheid is het onderscheid op basis van de mediane waarneming gemaakt. Alle coëfficiëntschattingen zijn statistisch significant op een significantieniveau van 10%, met uitzondering van de licht weergegeven schattingen. Voor een uitgebreidere toelichting zie ECB (2024).

Bron: ECB (2024).

Onzekerheid, risico-aversie en opgelegde kapitaalbeperkingen kunnen ook nadelige effecten hebben op de financieringskosten van financiële instellingen. Recent onderzoek van de ECB laat zien dat een toename van geopolitieke risico's gepaard gaat met een stijging van de *bond yields* van Europese banken, wat impliceert dat het voor banken duurder is om nieuwe marktfinanciering aan te trekken.[32] Ook stijgen de risicopremies op *credit default swaps (CDS)*

32 ECB (2024) Financial Stability Review: Turbulent times: geopolitical risk and its impact on euro area financial stability.

van Europese banken in het geval geopolitieke risico's toenemen. Bij financiële instellingen die minder goed gekapitaliseerd of minder winstgevend zijn, zijn deze effecten aanmerkelijk sterker, zoals blijkt uit figuur 4. Een toename van geopolitieke risico's kan er daarnaast toe leiden dat financiële instellingen een groter beroep op kortetermijnfinanciering moeten doen, met potentiële herfinancieringsrisico's tot gevolg. Hogere financieringskosten, toegenomen risico's en een hogere mate van onzekerheid kunnen banken vervolgens ook terughoudender maken met het verstrekken van nieuwe kredieten. Dit leidt tot krappere financieringscondities voor bedrijven en huishoudens. Uiteenlopende ontwikkelingen op financiële markten en in de reële economie kunnen elkaar zo versterken, waarbij de combinatie van hogere financieringskosten, een afgenomen kredietvraag en een verslechtering van de kredietportefeuille nadelige gevolgen kan hebben voor de winstgevendheid van banken.

2.3 Geopolitieke onzekerheden onderstrepen belang van adequaat risicomanagement

Toegenomen geopolitieke spanningen en onzekerheden onderstrepen het belang van een tijdige identificatie en adequate beheersing van risico's. DNB verwacht dat financiële instellingen inzicht hebben in alle materiële risico's en deze beheersen, wat vergt dat instellingen geopolitieke risico's verankeren in hun strategie, risicobereidheid en risicomanagementcyclus. Dit geldt zowel voor financiële risico's, die in dit hoofdstuk aan bod zijn gekomen, als niet-financiële risico's, waarop de volgende hoofdstukken uitgebreider ingaan. Aangezien geopolitieke ontwikkelingen via uiteenlopende en elkaar versterkende (risico)kanalen instellingen kunnen raken, is een integrale verankering belangrijk. Ook de ECB en de drie Europese toezichthoudende autoriteiten voor financiële instellingen hebben hier recent op gewezen.[33] Verankering vergt onder meer dat taken en verantwoordelijkheden rondom de monitoring en beheersing van geopolitieke risico's op passende wijze expliciet worden toegewezen binnen een organisatiestructuur, in overeenstemming met het risicoprofiel. Ook is belangrijk dat de beleidsbepalers van een instelling voldoende kennis, ervaring en vaardigheden hebben op het gebied van geopolitieke risico's. Zij moeten immers de blootstellingen aan deze risico's kunnen beoordelen en hier evenwichtige besluiten over kunnen nemen.

Vooruitblikkende instrumenten, waaronder stresstesten en scenario-analyses, zijn behulpzaam om (operationele) kwetsbaarheden, concentratierisico's en de doeltreffendheid van bedrijfsstrategieën in kaart te brengen. Het periodiek uitvoeren van stresstesten met geopolitieke scenario's waarin onder meer effecten op economische groei, inflatie en rente meegenomen worden, helpt om de impact van uiteenlopende geopolitieke risico's op de soliditeit van een instelling in kaart te brengen. Verschillende banken, verzekeraars en pensioenfondsen hebben hier de afgelopen jaren ook ervaringen mee opgedaan. De scenario's van deze stresstesten dienen zorgvuldig te worden gekozen, waarbij rekening wordt gehouden met de aard van de activiteiten en kwetsbaarheden

33 Zie ECB (2024) Global rifts and financial shifts: supervising banks in an era of geopolitical instability en het rapport van EBA, EIOPA en ESMA (2024) ESAs warn of risks from economic and geopolitical events.

van instellingen. Extreme, maar plausibele scenario's met zware economische tegenwind bieden instellingen hierbij veruit de meeste inzichten op potentiële kwetsbaarheden. Zo kan bijvoorbeeld gedacht worden aan een scenario van verdere escalatie van de spanningen tussen China en Taiwan. Door deze stresstesten aan te vullen met gerichte scenario-analyses kan ook zicht worden verkregen op risico's die zich niet in krediet- en marktrisicomodellen laten vatten, zoals scenario's waarin sancties tot het noodgedwongen stopzetten van operationele activiteiten leiden. Dit helpt om operationele kwetsbaarheden en de gevolgen van geopolitieke ontwikkelingen op de bestendigheid van het bedrijfsmodel in kaart te brengen. Toezichthouders hebben een rol om de stresstesten en scenario-analyses van instellingen te *challengen*. Door het uitvoeren van eigen stresstesten vergroten zij hun eigen inzichten, worden kwetsbaarheden in kaart gebracht en worden transparantie en marktdiscipline bevorderd.

Naast het identificeren van geopolitieke risico's, is het belangrijk dat financiële instellingen in staat zijn deze te beheersen. Beheersen van geopolitieke risico's vergt onder meer dat instellingen in hun beleggings- en kredietverstrekkingbeleid aandacht hebben voor de mate waarin bedrijven waaraan zij blootgesteld zijn geopolitieke risico's beheersen. Diversificatie – zowel in termen van geografische spreiding, als in de richting van verschillende sectoren, klantgroepen en aangeboden producten – blijft een essentieel onderdeel van een robuuste bedrijfsstrategie. Daarnaast dienen instellingen niet alleen geloofwaardige kapitaal-, liquiditeits- en financieringsplannen te ontwikkelen die rekening houden met onzekere vooruitzichten, maar ook in staat te zijn deze tijdig aan te passen aan veranderende risico's. In het verlengde hiervan zullen instellingen ook afbouwplannen gereed moeten hebben om activiteiten in kwetsbare jurisdicties op verantwoorde wijze af te kunnen bouwen. Dat vergt ook dat zij de over de benodigde capaciteit en middelen beschikken om dergelijke plannen, met de juiste prioriteit, uit te voeren. Tot slot is belangrijk dat instellingen over adequate buffers beschikken om materialiserende financiële risico's op te vangen. Schokbestendige en goed gekapitaliseerde instellingen zijn immers ook beter in staat markttoegang te behouden in tijden dat geopolitieke risico's zich materialiseren.

Veranderde cyberdreigings-landschap leidt tot risico's

Door een combinatie van geopolitieke ontwikkelingen en voortschrijdende digitalisering neemt de cyberdreiging toe en wordt het dreigingslandschap complexer. Financiële instellingen staan, ook via (kritieke) toeleveranciers, bloot aan operationele risico's, die via vertrouwensverlies en besmetting ook bredere gevolgen kunnen hebben voor het financieel systeem. Het veranderende dreigingslandschap onderstreept de noodzaak van operationele weerbaarheid van instellingen, hun ketenpartners en marktinfrastructuren. Naast het op orde houden van de cyberbeveiliging, vergen ook continuïteitsmaatregelen voor een vlot en veilig herstel aandacht.

3.1 Veranderde dreigingslandschap leidt tot toenemende cyberrisico's

De combinatie van geopolitieke ontwikkelingen en voortschrijdende digitalisering leidt tot een dynamischer dreigingslandschap. De afgelopen jaren is wereldwijd een toename te zien in zowel het aantal als de ernst van cyberaanvallen.[34] Verdergaande digitalisering van de samenleving en toegenomen technologische mogelijkheden zijn hier mede debet aan. Ook geopolitieke ontwikkelingen vertalen zich in een verhoogde cyberdreiging en een veranderd dreigingslandschap. Zo laat onderzoek van de ECB zien dat het aantal cyberaanvallen toeneemt in tijden van oplopende geopolitieke spanningen.[35] Daarnaast zijn cyberaanvallen door statelijke actoren, volgens de NCTV, het nieuwe normaal geworden.[36] Kader 3.1 gaat hier in meer detail op in.

Financiële instellingen zijn een potentieel doelwit van cyberaanvallen, ook van statelijke actoren. Financiële instellingen vormen vanwege hun bezittingen, gevoelige klantinformatie en centrale rol binnen de samenleving een aantrekkelijk doelwit voor cyberaanvallen. Op basis van data van het agentschap van de EU voor netwerk- en informatiebeveiliging (ENISA) over in de media gerapporteerde cyberaanvallen blijkt dat bijna 10% van alle cyberaanvallen op de financiële sector is gericht.[37] Veruit de meeste cyberaanvallen met potentieel grote impact op de financiële sectoren zijn financieel gemotiveerd en worden uitgevoerd door georganiseerde criminele groeperingen. Voorbeeld hiervan zijn aanvallen met *ransomware*, zoals de ransomware-aanval op de Amerikaanse dochter van de Industrial and Commercial Bank of China (ICBC) die tot een tijdelijke verstoring van clearing-diensten op de Amerikaanse treasury-

34 Zie de CISSM Cyber Attacks Database die inzicht geeft in cyberaanvallen sinds 2014. Hierbij zij opgemerkt dat in deze database aanvallen uitgevoerd op Amerikaanse ondernemingen oververtegenwoordigd zijn. De toename van het aantal cyberincidenten kan ook deels het gevolg zijn van dat meer incidenten gerapporteerd worden. Tegelijkertijd is aannemelijk dat het aantal daadwerkelijke cyber-incidenten onderschat wordt, onder andere vanwege terughoudendheid om incidenten te melden of doordat deze (nog) niet gedetecteerd zijn. Zie Harry, C. en Gallagher N. (2018) Classifying cyber events voor een nadere toelichting op deze database.
35 ECB (2022) Towards a framework for assessing systemic cyber risk.
36 NCTV (2023) Cybersecuritybeeld Nederland 2023.
37 ENISA (2024) Threat Landscape 2024.

markt heeft geleid.[38] Vanwege de potentieel grote impact die verstoringen kunnen hebben, vormt de financiële sector ook voor statelijke actoren en hacktivisten een interessant strategisch doelwit.[39] Een deel van de cyberaanvallen beoogt (maatschappelijke) ontwrichting teweeg te brengen en heeft disruptie tot doel. Veruit het grootste deel van dit type aanvallen wordt gevormd door DDoS-aanvallen, die niet of nauwelijks een effect sorteerden. De DDoS-aanvallen die pro-Russische hackers op Nederlandse en andere Europese banken uitvoerden zijn hier een voorbeeld van.

Kader 3.1
Statelijke actoren steeds actiever in het digitale domein

Statelijke actoren nemen een prominentere plek in het cyberdreigingslandschap in. Statelijke actoren en aan een staat-gelieerde actoren zetten, al dan niet als onderdeel van hybride conflict-voering, cybermiddelen in voor beïnvloeding, spionage, verstoring en sabotage – of het treffen van de voorbereidingshandelingen daartoe. Cybermiddelen zijn aantrekkelijk vanwege hun relatief lage kosten, potentieel langdurige effecten en doordat het lastig en complex kan zijn om na te gaan wie voor een cyberaanval verantwoordelijk was. Statelijke actoren maken vaak gebruik van geavanceerde aanvalstechnieken en hebben, doorgaans veel tijd, capaciteit en middelen tot hun beschikking.[40] Dit geeft ze ook de mogelijkheid aanvallen zorgvuldig te plannen en op strategische momenten toe te slaan. Zo ontdekte de FBI een slapend netwerk van Chinese hackers in de VS dat honderden routers had gecompromitteerd en stand-by stond om een aanval uit te voeren.[41] Het komt ook met regelmaat voor dat staten cybercriminelen in huren, hun activiteiten gedogen of ze aanmoedigen om zich op bepaalde doelwitten te richten. Hierdoor vervagen scheidslijnen tussen statelijke actoren en cybercriminelen.

Nederland wordt, net als andere Europese landen, doorlopend geconfronteerd met offensieve cyberaanvallen en -spionage, zo geven de MIVD en AIVD aan.[42] Hoewel voor Russische statelijke actoren het uitvoeren van cyberoperaties tegen Oekraïne - bijvoorbeeld om locaties van Oekraïens militaire materieel in kaart te brengen en de vitale infrastructuur te saboteren - de hoogste prioriteit heeft, geeft de MIVD aan dat in 2023 tevens sprake was van een toename in cyberoperaties door Russische statelijke actoren tegen Europese en NAVO-bondgenootschappelijke doelwitten.[43] Voornaamste motief is volgens de MIVD het bemachtigen van een digitale positie binnen de vitale infrastructuur.

38 The Banker (2023) The significance of the ICBC FS hack on the US Treasury market.
39 Statelijke actoren kunnen ook andere motieven hebben, zoals het vergaren van financiële middelen. De aan Noord-Korea toegeschreven cyberaanval op de centrale bank van Bangladesh, waarbij 81 miljoen dollar werd buitgemaakt, is hiervoor illustratief (Financial Times, 2019).
40 ENISA (2023) Threat landscape 2023.
41 New York Times (2024) F.B.I. Director Warns of China Hacking Threat.
42 AIVD (2023) Jaarverslag 2022 en MIVD (2024) Jaarverslag 2023.
43 MIVD (2024) Jaarverslag 2023.

Daarnaast probeert Rusland via cyberspionage zicht te krijgen op transporten van westerse militaire steun, zowel binnen als buiten Oekraïne. Ook de intensiteit waarmee Chinese statelijke hackersgroepen spionagecampagnes uitvoeren richting Nederland en andere EU-lidstaten is volgens de MIVD afgelopen jaar toegenomen. Chinese cyberactiviteiten richten zich vooral op het verzamelen van informatie over intellectueel eigendom, persoonsgegevens en voorkennis over politieke en bestuurlijke besluitvorming. In 2023 waren verschillende Nederlandse overheidsinstellingen en (defensie)bedrijven een spionagedoelwit van Chinese cybereenheden.[44]

Sinds de oorlog in Oekraïne is er sprake van een opleving van hacktivism, het vanuit ideologische overwegingen uitvoeren van cyberaanvallen. In veel gevallen gaat het, volgens het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), om DDoS-aanvallen. De impact daarvan is volgens ENISA veelal kortdurend en relatief beperkt, maar een deel van deze aanvallen is de afgelopen jaren wel groter en complexer geworden.[45] Illustratief zijn de DDoS-aanvallen van pro-Russische hackersgroepen op websites van overheden en bedrijven uit landen die Rusland sancties hebben opgelegd, waaronder de VS, Italië, Noorwegen en Japan en aanvallen op banken in onder andere Nederland, Duitsland, Tsjechië en Polen.[46] Ook hebben pro-Russische hacktivisten opgeroepen tot DDoS-aanvallen op Nederlandse ziekenhuizen. Enkele Nederlandse ziekenhuizen werden daadwerkelijk slachtoffer van dergelijke aanvallen, waarbij er soms korte tijd uitval van de publieke website was.[47] Ook elders in de wereld is sprake van een opleving van hacktivism. Zo kregen Taiwanese overheidswebsites te maken met een forse toename van DDoS-aanvallen in aanloop naar het bezoek van de voorzitter van het Amerikaanse Huis van Afgevaardigden.[48] De federale beveiligingsautoriteit van Duitsland waarschuwt dat het groeiende netwerk van hacktivistische groeperingen statelijke actoren in de kaart kan spelen, doordat het statelijke actoren de mogelijkheid biedt om zich in de toekomst als hacktivisten voor te doen.[49]

Ook via kritieke ICT-toeleveranciers staan financiële instellingen bloot aan cyberrisico's. Financiële instellingen maken in toenemende mate gebruik van derde partijen voor kritieke bedrijfsprocessen, zoals clouddienstverleners en andere ICT-bedrijven. Een gebrekkige uitvoering van kritieke diensten of processen kan materiële gevolgen hebben voor bijvoorbeeld de soliditeit, continuïteit of de reputatie van een instelling.

Hoewel vooral de grotere ICT-dienstverleners doorgaans veel expertise hebben en hoge normen voor cyber- en informatieveiligheid hanteren, resulteert de uitbesteding van kritieke diensten of processen door financiële instellingen in een verhoogde afhankelijkheid en extra complexiteit. Cyberaanvallers zijn zich bewust van deze ketenafhankelijkheden. De afgelopen jaren is, volgens ENISA, sprake van een verschuiving in

44 Ministerie van Defensie (2024) MIVD onthult werkwijze Chinese spionage in Nederland.
45 ENISA (2023) Threat landscape 2023.
46 Zie ENISA (2023), Reuters (2023) en Center for Strategic & International Studies (2024).
47 NCTV (2023) Cybersecuritybeeld Nederland 2023.
48 ENISA (2023) Threat landscape 2023.
49 BSI (2023) The state of IT security in Germany 2023.

cyberaanvallen die statelijke en aan staat-gelieerde actoren uitvoeren. Steeds vaker worden de pijlen gericht op derde partijen in de toeleveringsketen.[50] De aan Rusland toegeschreven hack op het Amerikaanse softwarebedrijf SolarWinds in 2020, waarvan verschillende Amerikaanse overheidsinstellingen en bedrijven diensten afnemen en slachtoffer werden, illustreert de potentiële gevolgen van dergelijke aanvallen.[51] Exemplarisch voor ketenafhankelijkheden is, ondanks dat dit geen cyberaanval betrof, ook de wereldwijde uitval van communicatietechnologie als gevolg van tekortkomingen in een software-update van het Amerikaanse CrowdStrike. Deze trof in de zomer van 2024 naar schatting 8,5 miljoen Windows-apparaten en leidde wereldwijd tot uitval van vluchten en uitstel van ziekenhuisoperaties.[52] Uitbesteding kan tot slot tot concentratierisico's leiden, doordat een beperkte groep ICT-dienstverleners een groot aantal financiële instellingen bedient en ICT-diensten vaak niet eenvoudig substitueerbaar zijn. In dit opzicht valt de sterke afhankelijkheid van Amerikaanse clouddienstverleners op, waarbij drie grote partijen uit de VS bijna driekwart van de Europese markt in handen hebben.[53]

In geval van besmetting of breder vertrouwensverlies, kunnen cyberincidenten ook gevolgen hebben voor het financiële systeem als geheel. In vergelijking met andere operationele risico's vallen cyberincidenten op door de hoge snelheid waarop en schaal waarmee ze zich binnen een instelling en tussen instellingen, sectoren en landen kunnen verspreiden. Illustratief is de snelle, wereldwijde verspreiding in 2017 van de NotPetya-malware. Hierdoor vielen overheidssystemen in Oekraïne uit, traden er problemen op in Oekraïense elektriciteitscentrales en liep de Deense containervervoerder Maersk forse schade op.[54] Ook in de financiële sector kunnen cyberincidenten potentieel in rap tempo verspreiden, bijvoorbeeld doordat veel instellingen afhankelijk zijn van onderliggende marktinfrastructuren en dezelfde systemen voor het betalings- en kapitaalmarktverkeer. Voor een individuele instelling kunnen cyberincidenten tot financieel verlies en reputatieschade leiden. Ze kunnen ook tot juridische risico's leiden, in het geval ongeoorloofde toegang tot data niet tijdig wordt gemeld of wanneer deze het gevolg blijkt te zijn van nalatigheid van een instelling. Cyberincidenten kunnen ook gevolgen voor andere instellingen hebben, bijvoorbeeld wanneer ze in een breder verlies van vertrouwen resulteren en tot een uitstroom van deposito's leiden. Ook via de onderlinge verbondenheid via het interbancaire betalingssysteem kunnen instellingen nadelige gevolgen ondervinden, bijvoorbeeld wanneer banken in liquiditeitsproblemen komen doordat andere banken als gevolg van een cyberincident hun betalingen niet uit kunnen voeren. Daarmee zijn cyberrisico's ook vanuit het perspectief van financiële stabiliteit relevant, zoals DNB recent uiteen heeft gezet in het Overzicht Financiële Stabiliteit.[55]

In andere sectoren, zoals de telecom- en energiesector, kunnen (cyber)incidenten potentieel verstrekkende gevolgen hebben

50 ENISA (2022) Threat landscape 2022.
51 ENISA (2021) Threat landscape for supply chain attacks.
52 Financial Times (2024) Companies around the world hit by Microsoft outage.
53 Gomes, A. en Okano-Heijmans, M. (2024) Too late to act? Europe's quest for cloud sovereignty.
54 Zie bijvoorbeeld NCTV (2018) en Wired (2018) en Maersk (2017).
55 Zie ook DNB (2024) Overzicht Financiële Stabiliteit najaar 2024.

voor de financiële sector. Evenals internet- en datadiensten en de productie en distributie van elektriciteit, wordt het betalingsverkeer in Nederland onder de vitale processen geschaard.[56] Uitval, (digitale) verstoring of manipulatie van de vitale infrastructuur, al dan niet moedwillig veroorzaakt, kan de nationale veiligheid schaden, of tot maatschappelijke ontwrichting leiden. Zo zijn in het geval van een langdurige uitval van de elektriciteitsvoorziening veel keteneffecten in andere sectoren te verwachten.[57] Ook in het geval van langdurige disruptie van telecomdiensten, waardoor gebruikers geen toegang tot internet- en telefoondiensten hebben, treden forse keteneffecten op, met potentiële doorwerking op de financiële sector.[58] Hoewel in Nederland tot op heden geen daadwerkelijke digitale verstoring of fysieke sabotage van de vitale infrastructuur is gerapporteerd, zijn volgens de AIVD, MIVD, NCTV vitale processen in Nederland potentieel kwetsbaar voor statelijke activiteiten.[59] Deze organisaties wijzen op de dreiging tegen onderzeese infrastructuur, zoals onderzeekabels en pijpleidingen, de activiteiten die Russische entiteiten ondernemen om deze infrastructuur in kaart te brengen en de voorbereidingshandelingen die zij treffen voor mogelijke verstoring en sabotage. Ook de Adviesraad voor Internationale Vraagstukken (AIV) wijst op de kwetsbaarheden die samenhangen met de grote hoeveelheden internet- en elektriciteitskabels en gaspijpleidingen in de Noordzee en de grote concentratie van datastromen via netwerken in Nederland.[60] Ook elders bestaan zorgen over de kwetsbaarheid van de vitale infrastructuur. Deze zijn mede ingegeven door verdachte incidenten zoals de sabotage van internetkabels in Frankrijk, GPS-verstoringen in Finland en het risico op slapende *hacker-cells* in de vitale infrastructuur in de VS waarop de FBI heeft gewezen.[61] Nederland kan, net als andere EU-landen, ook te maken krijgen met keteneffecten van sabotage van vitale processen in andere landen.

Naast cyberaanvallen kunnen financiële instellingen te maken krijgen met desinformatie, wat in potentie tot liquiditeitsrisico's kan leiden. Gedurende de COVID-19 pandemie, in aanloop naar en tijdens de oorlog in Oekraïne en bij recente verkiezingen is door verschillende statelijke actoren met regelmaat doelbewust misleidende informatie verspreid. Het is goed denkbaar dat de verspreiding van desinformatie in omvang en intensiteit de komende jaren verder toeneemt. Ontwikkelingen op het terrein van generatieve artificiële intelligentie dragen immers bij aan het sneller creëren en het op grotere schaal verspreiden van geloofwaardige desinformatie in de vorm van tekst, beeld en audio.[62] Ook financiële instellingen kunnen te maken krijgen met de verspreiding van desinformatie. Zo zouden kwaadwillende actoren nepnieuws kunnen verspreiden over de financiële positie van een bank of meerdere banken om

56 De beoordeling of een bepaald proces of dienst vitaal is, wordt gemaakt door de vakdepartementen in overleg met de NCTV gemaakt. Hierbij wordt geanalyseerd of bij verstoring, uitval of manipulatie van een proces of dienst dermate ernstige gevolgen kunnen optreden dat deze de nationale veiligheid kunnen schaden. Thans zijn de volgende processen en diensten als vitaal aangemerkt (zie hier), op dit moment wordt door het kabinet de zogenoemde beleidscyclus vitaal doorlopen om te kijken welke processen of aanbieders als vitaal aangemerkt worden (Rijksoverheid, 2024).
57 Zie bijvoorbeeld Analistennetwerk Nationale Veiligheid (2022) Themarapportage bedreiging vitale infrastructuur.
58 In box 2 van DNB (2024) Overzicht Financiële Stabiliteit najaar 2024 wordt geïllustreerd hoe een cyberaanval op de vitale infrastructuur systeemrisico's voor de financiële sector kan veroorzaken.
59 AIVD, MIVD en NCTV (2022) Dreigingsbeeld statelijke actoren 2.
60 Adviesraad Internationale Vraagstukken (2024) Hybride dreigingen en maatschappelijke weerbaarheid.
61 Pillai, H. (2023) Protecting Europe's critical infrastructure from Russian hybrid threats en Financial Times (2024) FBI warns Chinese malware could threaten critical US infrastructure.
62 Zie bijvoorbeeld AFM en DNB (2024) en Bontridder, N. en Poullet, Y. (2021).

onrust onder depositohouders aan te wakkeren, in een poging maatschappelijke ontwrichting te weeg te brengen. Zij zouden met name vruchtbare bodem bij depositohouders kunnen vinden wanneer het vertrouwen in een bank en/of de financiële sector al onder druk staat.[63] Illustratief voor de potentiële risico's, is de verspreiding van nepnieuws over de financiële gezondheid van Bulgaarse banken in 2014. Daarbij namen depositohouders in totaal zo'n 10% tot 20% van de totale waarde van de bezittingen bij twee grote Bulgaarse banken op.[64]

Tot slot vergen ook *insider threats* aandacht. Financiële instellingen hebben de afgelopen jaren hun cyberbeschermingsmaatregelen versterkt om externe aanvallen buiten te houden, wat de mogelijkheid vergroot dat via kwaadwillende *insiders* gepoogd wordt toegang te krijgen tot kritieke systemen en gevoelige data. Het rekruteren of plaatsen van medewerkers die bereid zijn kwaadwillende actoren toegang tot financiële instellingen te verschaffen vormt immers een alternatief voor de benodigde inspanningen om de cyberbeveiliging van een instelling te doorbreken. Dit risico is al zichtbaar in de *tech*-sector, waar *insider threats* veelal gemotiveerd zijn vanuit het verkrijgen van toegang tot hoogwaardig technologische kennis. Vanwege dit toegenomen risico, hebben *tech*-bedrijven in Silicon Valley aangekondigd hun personeelsscreening te intensiveren.[65]

3.2 Versterken operationele weerbaarheid vergt voortdurende inspanning

Het veranderde dreigingslandschap onderstreept de noodzaak van weerbaarheid van instellingen en hun ketenpartners. Het van toepassing worden van de Europese *Digital Operational Resilience Act* (DORA) is een welkome ontwikkeling. Hoewel de bestuurlijke aandacht voor cyberrisico's bij financiële instellingen groeit en de afgelopen jaren stappen zijn gezet om de weerbaarheid te verhogen, blijven inspanningen nodig om de informatie- en ICT-beveiliging op het gewenste volwassenheidsniveau te brengen. Zo blijkt uit toezichtonderzoeken dat banken, verzekeraars en pensioenfondsen nog stappen te zetten hebben om de basis cyberhygiëne-maatregelen – zoals het tijdig updaten en *patchen* van systemen – op orde te brengen. Ook is er ruimte voor verbetering in het beheersen van de risico's rondom de uitbesteding van kritieke processen en het testen met en voorbereiden op cyberaanvallen.[66] Met het van toepassing worden van DORA in januari 2025 beogen Europese beleidsmakers de digitale operationele weerbaarheid en ICT-beveiliging van financiële instellingen verder te versterken en hier op Europees niveau harmonisatie in aan te brengen. Zo verplicht DORA financiële instellingen om ernstige ICT-gerelateerde incidenten bij de toezichthouder te melden en voorziet het in een mechanisme om informatie over incidenten tussen toezichthouders uit te wisselen. Ook worden dreiging-gebaseerde cybertesten, zogenoemde *threat-led penetration testen*, voor de grootste financiële instellingen verplicht.

63 Bateman, J. (2020) Deepfakes and synthetic media in the financial system: assessing threat scenarios.
64 Merler, S. (2014) Fact of the week: A spam newsletter caused a bank run in Bulgaria.
65 Financial Times (2024) Sillicon Valley steps up staff screening over Chinese espionage threat.
66 Zie DNB (2023) voor de uitkomsten van deze toezichtonderzoeken voor banken en betaalinstellingen, DNB (2023) voor verzekeraars en DNB (2023) voor de pensioensector en DNB (2023) voor de cyberstrategie.

Daarnaast worden er scherpere eisen gesteld aan de beheersing van ICT- en cyberrisico's in uitbestedingsketens, onder meer doordat instellingen verplicht worden due diligence-onderzoeken te verrichten over toekomstige ICT-aanbieders en exit-strategieën op te stellen voor kritieke ICT-dienstverleners.[67] Tot slot worden onder DORA concentratierisico's in kaart gebracht en wordt een *oversight*-framework geïntroduceerd, waaronder Europese toezichthouders – samen met nationale toezichthouders – onderzoeken kunnen uitvoeren bij kritieke derde aanbieders van ICT-diensten. Toezichthouders, waaronder DNB en AFM, zullen erop toezien dat financiële instellingen de uit DORA voortvloeiende vereisten naleven.

Naast het op orde hebben en houden van ICT- en cyberbeveiliging en het met regelmaat testen daarvan, is het zaak dat instellingen over de benodigde veerkracht beschikken om na incidenten veilig en vlot hun dienstverlening op te starten en voort te zetten. Volledige digitale veiligheid bestaat niet. Het is daarom belangrijk dat instellingen over de benodigde wendbaarheid beschikken om veilig en vlot te kunnen reageren en herstellen na een incident, ook in het geval er sprake van disruptie van ICT-systemen. Dat draagt bij aan de continuïteit van dienstverlening en het beperken van potentieel vertrouwensverlies en eventuele besmettingsrisico's. Hoewel er in de financiële sector steeds meer aandacht voor het versterken van het herstelvermogen is en maatregelen worden genomen om de continuïteit van de meest essentiële dienstverlening zoveel mogelijk te borgen, laten resultaten uit de recente ECB cyber-stresstest zien dat er nog verbeterpotentieel is.[68] Belangrijke ingrediënten voor een effectieve response zijn een cultuur waarin cyberincidenten snel worden opgemerkt en gemeld en er duidelijke gedefinieerde rollen en verantwoordelijkheden binnen het management zijn. Ook is belangrijk dat er *playbooks* zijn opgesteld, die periodiek tegen het licht worden gehouden, waar nodig worden bijgesteld en waarmee ook wordt geoefend in de praktijk. Met de inwerkingtreding van DORA worden ook nieuwe vereisten aan de continuïteitsplannen en het back-upbeleid van instellingen opgelegd. Tegen de achtergrond van het veranderde dreigingslandschap is het tevens verstandig dat financiële instellingen – en in het verlengde daarvan ook toezichthouders en overheid – zich voorbereiden op scenario's waarin zij doelwit worden van desinformatie. Dit vergt ook dat nagedacht wordt over een passende communicatiestrategie voor dergelijke scenario's. Tot slot dragen instellingen ook indirecte verantwoordelijkheden voor de weerbaarheid van de gehele marktinfrastructuur. Financiële instellingen zijn vaak direct of indirect, hetzij via samenwerkingsverbanden dan wel dochters, verbonden aan kritieke partijen voor de marktinfrastructuur. Zodoende bestaat er via deze instellingen belangrijke weerbaarheidsverantwoordelijkheid, aangezien de marktinfrastructuur fundamenteel is voor het functioneren van het gehele financiële systeem. Gezien het veranderde dreigingslandschap, moedigt DNB instellingen dan ook aan prioriteit te blijven geven aan het vermogen om snel te herstellen, in het geval van al dan niet moedwillig veroorzaakte digitale of fysieke verstoringen.

67 Publicatieblad van de Europese Unie (2022) Verordening 2022/2554 betreffende digitale operationele weerbaarheid voor de financiële sector.
68 ECB (2024) ECB concludes cyber resilience stress test.

Een weerbare vitale infrastructuur vergt centrale regie vanuit de overheid en intensieve publiek-private samenwerking. Bedrijven en financiële instellingen zijn zelf verantwoordelijk voor de benodigde preventieve en mitigerende maatregelen om de continuïteit en weerbaarheid van hun processen en diensten te borgen. Dat geldt ook voor bedrijven en financiële instellingen die een onderdeel vormen van de vitale infrastructuur.[69] Tegelijkertijd kunnen de private inspanningen afwijken van het maatschappelijk gewenste beschermingsniveau en komen sector- en grensoverschrijdende informatie-uitwisseling, samenwerking en coördinatie niet vanzelf van de grond.[70] Versterken van de weerbaarheid vergt daarom ook regie vanuit de overheid, proactief beleid en het maken van tempo in de uitvoering.[71] In dat licht zijn recente Europese wetgevingsinitiatieven – waaronder de *Network and Information Security (NIS2)-richtlijn*, die een zorg- en meldplicht introduceert bij een veel groter aantal organisaties dan momenteel het geval is, de *Cyber Resilience Act* voor het verhogen van de cyberveiligheid van hard- en software en DORA dat zich specifiek op de financiële sector richt – belangrijke, positieve ontwikkelingen, die een voortvarende implementatie en operationalisering verdienen. Sectorale toezichthouders, waaronder DNB en AFM, hebben de taak om erop toe te zien dat de hieruit voortvloeiende verplichtingen adequaat worden nageleefd en zullen ook onderling intensief moeten samenwerken. Als onderdeel van haar cyberstrategie geeft DNB daaraan onder meer invulling door, waar passend binnen haar mandaat, ook de vitale sectoren die het meest kritiek zijn voor de financiële sector, zoals de energie- en telecomsector, te ondersteunen.[72] Voor de overheid ligt er tot slot ook een taak om het initiatief te nemen voor grootschalige oefeningen met scenario's waarin meerdere vitale sectoren gelijktijdig met incidenten te maken krijgen en activering van nationale crisisstructuren noodzakelijk is, waardoor operationele coördinatie vanuit het Nationaal Cyber Security Centrum (NCSC) plaatsvindt. Dit is eerder gedaan met verschillende ISIDOOR-crisisoefeningen.[73] Het is belangrijk dat de inzichten die met deze crisissimulaties worden opgedaan benut worden om de weerbaarheid te verhogen. Recente evaluaties laten zien dat een effectieve en efficiënte informatie-uitwisseling tussen aanbieders van vitale infrastructuur, de verdeling van rollen en verantwoordelijkheden in geval van opschaling naar een landelijke crisisstructuur en de wijze waarop schaarse cybersecuritykennis en -expertise in geval van grootschalige cyberincidenten gemobiliseerd kan worden belangrijke aandachtspunten zijn.[74]

69 Partijen die processen en diensten aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving worden vitale aanbieders genoemd. De ministeries zijn verantwoordelijk voor het aanwijzen van de vitale aanbieders (zie hier).
70 Specifiek voor de financiële sector bestaat in Nederland het Tripartiet Crisisoverleg (TCO). Dit richt zich op sector crisismanagement in geval van operationele verstoringen in het betalings- en effectenverkeer. Zie ook DNB (2023) Cyberstrategie.
71 Zie ook CSR (2024) Cyber Security Raad aan nieuw kabinet: Nederland moet meer investeren in digitale veiligheid.
72 DNB (2023) Cyberstrategie.
73 Aan de cyberoefening ISIDOOR deden in 2023 ruim 120 organisaties uit de publieke en private sector mee (zie NCSC, 2023).
74 Zie NCSC (2024) Het beoefenen van een cybercrisis maakt ons land weerbaarder. Ook in WRR (2024) Nederland in een fragmenterende wereldorde worden aanbevelingen gedaan ten aanzien van het versterken van de cyberweerbaarheid.

Veranderend sanctie-landschap: uitdagingen en risico's voor instellingen

Het aantal sancties dat (westerse) overheden oplegt neemt, door toegenomen geopolitieke spanningen, sterk toe. Dit geldt in het bijzonder voor financiële sancties. Financiële instellingen hebben een belangrijke verantwoordelijkheid bij de uitvoering van deze sancties, wat hen aan reputatie- en juridische risico's blootstelt. Deze risico's zijn groter wanneer sanctieregelgeving niet adequaat wordt nageleefd, wat het belang onderstreept van een goed ingerichte bedrijfsvoering. Het veranderde sanctielandschap leidt ook tot risico's vanwege de blootstellingen en operationele activiteiten die instellingen in potentieel kwetsbare jurisdicties hebben, de extraterritoriale werking van door de VS opgelegde sancties en mogelijke tegenreacties vanuit gesanctioneerde landen. Het is daarom ook zaak dat instellingen hun risicomanagement op orde hebben zodat zij de risico's die voortvloeien uit het groeiende aantal sancties adequaat kunnen identificeren en beheersen.

4.1 Veranderde sanctielandschap leidt tot intensievere rol voor financiële instellingen

Westerse overheden maken steeds intensiever gebruik van sancties, in het bijzonder van financiële sancties. Sancties vormen een aantrekkelijk beleidsinstrument voor overheden. Allereerst voor de handhaving van de internationale rechtsorde of om op te komen voor vrede en veiligheid, bijvoorbeeld wanneer diplomatieke inspanningen onvoldoende effect sorteren en militair ingrijpen niet wenselijk wordt geacht. In toenemende mate worden sancties ook ingezet om eigen (strategische) belangen na te streven en het beleid van andere jurisdicties te beïnvloeden.[75] Het aantal opgelegde sancties vertoont al jaren een opwaartse trend, zoals blijkt uit figuur 5. Deze ontwikkeling heeft grote impact, zowel op de financiële sector als op andere sectoren in Nederland.[76] Bovendien zijn sancties, met name sinds de aanslagen van 11 september 2001, steeds gerichter en van een meer financiële aard geworden.[77] Sanctiepakketten zijn sinds die tijd sterker gericht op het beperken van toegang tot financiële dienstverlening of het bevriezen van tegoeden om specifieke regimes te treffen. Sanctiepakketten daarvoor bestonden vooral uit embargo's tegen landen – die vaak schadelijke neveneffecten op de lokale bevolking hadden.[78] Ook in reactie op de Russische invasie

75 Zie bijvoorbeeld Wittmann & Teichmann (2022), Hoff & Hoff (2023) en Caytas (2017).
76 CBS (2023) Nederland Handelsland 2023: export, import en investeringen
77 Zie bijvoorbeeld Rodriguez F. (2023), Yotovm, Y. et al. (2020) en Drezner (2011).
78 Zie Ahn D. (2019), GIATOC (2023) en Drezner D.W. (2015).

van Oekraïne in 2022 hebben onder andere de EU, de VS en het VK een groot aantal financiële sancties tegen Rusland en Belarus opgelegd. Zo werden tegoeden van (rechts)personen bevroren en verboden op dienstverlening aan deze (rechts) personen opgelegd. Ook werden de tegoeden van de Russische centrale bank en andere Russische banken bevroren (via *Euroclear*), transacties met deze centrale bank verboden en werd een aantal Russische banken uitgesloten van het internationale berichtensysteem voor betalingen (SWIFT). Deze ontwikkeling, waarbij door groeiende mondiale competitie en internationale machtsuitoefening een deel van de financiële infrastructuur tot een wapen wordt gemaakt, wordt ook wel de *weaponisation of finance* genoemd.[79]

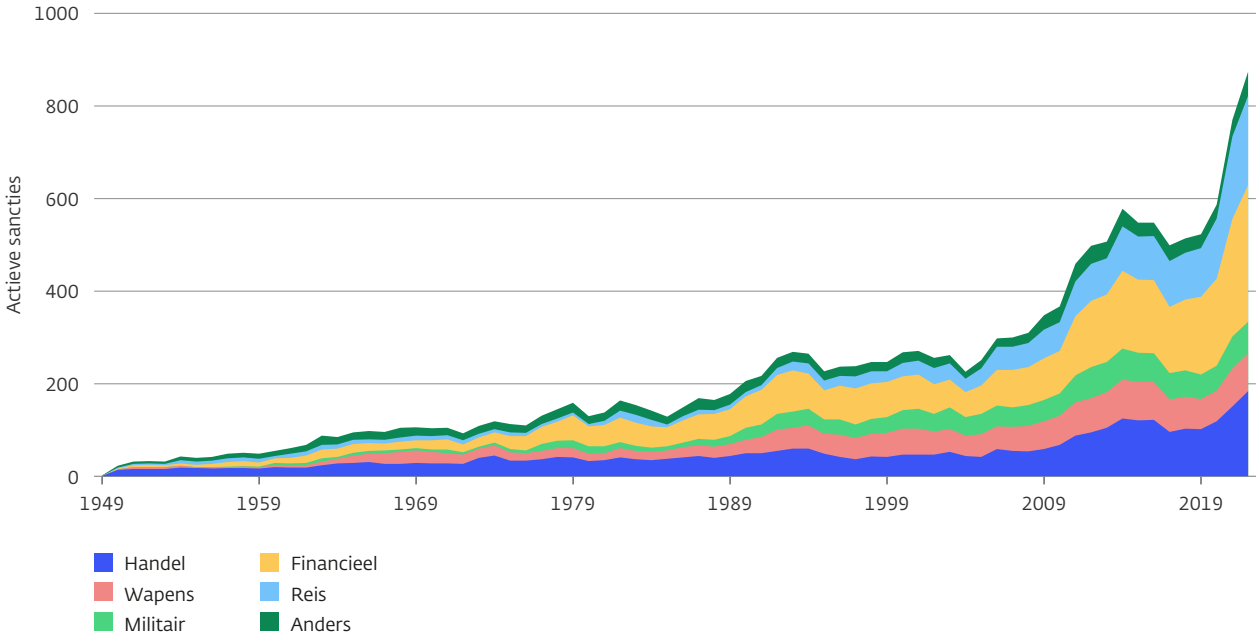
Financiële instellingen hebben een belangrijke verantwoordelijkheid bij de uitvoering van sancties vanwege hun sleutelrol in het betalingsverkeer, de toegang tot financiële diensten, en in hun rol als belegger. Financiële instellingen zijn wettelijk verplicht om continu te kunnen detecteren of klantrelaties dan wel partijen waarin ze beleggen onderwerp zijn van een sanctie. Ook moeten zij controleren of diensten en transacties die ze verzorgen betrekking hebben op personen, bedrijven of andere entiteiten die in sanctieregelingen zijn opgenomen. Dit geldt niet alleen op het moment dat een persoon of bedrijf klant wil worden of een nieuwe dienst afneemt, maar ook voor bestaande klanten. Indien uit klantonderzoek blijkt dat een klant op sanctielijsten staat, of transacties – zoals bijvoorbeeld een overboeking – naar gesanctioneerde partijen zijn gepland, moet een financiële instelling de sanctie onmiddellijk uitvoeren en een melding maken bij DNB. In niet alle gevallen is een snelle controle of een bepaalde klant op een sanctielijst staat mogelijk. Bij ondernemingen zal een financiële instelling bijvoorbeeld moeten nagaan wie de *ultimate beneficial owner* (UBO) is en wie er feitelijk zeggenschap over de onderneming heeft. Ook bij andersoortige sancties, zoals import- en exportrestricties, hebben financiële instellingen een rol. Instellingen mogen namelijk niet betrokken zijn bij transacties die niet in overeenstemming zijn met de sanctieregelingen. In de opeenvolgende sanctiepakketten tegen Rusland en Belarus hebben verboden en restricties op het verlenen van financiële diensten ten behoeve van militaire goederen, goederen voor binnenlandse repressie en *dual-use* goederen[80] een vlucht genomen, waardoor transactiescreening of andere detectiemaatregelen belangrijker zijn geworden. In het verlengde hiervan dienen financiële instellingen beducht te zijn op sanctie-omzeiling. Sanctie-omzeiling kan bijvoorbeeld plaatsvinden doordat goederen eerst naar andere landen worden geëxporteerd, alvorens zij bij gesanctioneerde partijen terecht komen.[81]

79 Zie Financial Times (2022) Weaponisation of finance: how the west unleashed 'shock and awe' on Russia. Het rapport van de WRR, (2024) Nederland in een fragmenterende wereldorde, laat zien dat de *weaponisation of finance* als onderdeel kan worden gezien binnen een wereldwijd proces van een algehele 'verbreding van gebieden van machtsuitoefening'. Op basis van andere rapporten benoemt de WRR dit fenomeen als: *weaponisation of everything*.

80 Dual-use goederen zijn goederen, diensten of technologieën die die zowel voor civiele als militaire doeleinden gebruikt kunnen worden. Zo worden bepaalde brandvertragers in de bouw gebruikt, die ook als grondstof voor gifgas kunnen dienen.

81 The Economist (2024) The mysterious middlemen helping Russia's war machine.

Figuur 5 Overheden leggen steeds vaker financiële sancties op



Toelichting: Figuur geeft een overzicht van de publiek afgekondigde van kracht zijnde sancties tussen de verschillende staten en organisaties per jaar. In de grafiek is een onderscheid gemaakt naar de aard van de sanctie.

Bron: The Global Sanctions Data Base (2023).

4.2 Gevolgen van veranderde sanctielandschap op financiële instellingen

Het toegenomen aantal opgelegde sancties gaat gepaard met verhoogde juridische- en reputatierisico's voor instellingen. Zowel door eigen actieve beslissingen, zoals het verstrekken van krediet aan een gesanctioneerde partij, als door het gedrag van klanten die bijvoorbeeld geld willen overboeken naar een gesanctioneerde partij, kan sprake zijn van een overtreding van de sanctieregelgeving. De gevolgen voor instellingen kunnen, afhankelijk van de specifieke omstandigheden, groot zijn. Indien instellingen onvoldoende adequaat intern beleid hebben om uitvoering te geven aan de sanctieregelgeving, kunnen DNB en AFM bestuursrechtelijk handhaven en boetes opleggen. Overtreding van de Sanctiewet is ook gekwalificeerd als economisch delict, wat strafrechtelijke vervolging mogelijk maakt en kan leiden tot boetes die oplopen tot 10% van de jaaromzet. Naast de impact die deze boetes hebben op de financiële positie van een instelling, kan betrokkenheid in een handhavings- of strafrechtelijke procedure ook tot reputatierisico's leiden. Tot slot kunnen ook juridische risico's ontstaan wanneer derde partijen die nadeel ondervinden van sanctie-uitvoering, bijvoorbeeld doordat transacties geen doorgang kunnen vinden, een gerechtelijke procedure tegen een financiële instelling starten. Dat risico wordt vergroot wanneer sancties niet eenduidig te interpreteren zijn. Ondanks dat sanctieverordeningen clausules bevatten

om de kans op aansprakelijkheid te beperken[82], kan de start van een procedure reputatierisico's opleveren voor een instelling. Zelfs in het geval een procedure weinig kans van slagen heeft.

Naast Europese sancties hebben ook door de VS opgelegde sancties impact op Nederlandse financiële instellingen. Niet-Amerikaanse partijen vallen in sommige gevallen onder de Amerikaanse sanctieregelgeving, bijvoorbeeld wanneer zij betrokken zijn bij transacties waarin Amerikaanse partijen betrokken zijn of in geval transacties betrekking hebben op Amerikaanse goederen.[83] Doordat een groot deel van de internationale transacties in dollars wordt afgewikkeld, hebben Amerikaanse sancties de facto extraterritoriale werking. Dit geeft de Amerikaanse autoriteiten een krachtig beleidsinstrument in handen, waar ze ook veelvuldig gebruik van maken.[84] De gevolgen van niet-naleving van Amerikaanse sanctiewetgeving kunnen fors zijn. Zo werd BNP Paribas in 2015 door de Amerikaanse autoriteiten veroordeeld, omdat het miljarden aan transacties in dollars via het Amerikaanse financiële systeem verwerkte namens Soedanese, Iranese en Cubaanse entiteiten die waren onderworpen aan Amerikaanse sancties. BNP Paribas verklaarde schuldig te zijn en werd geconfronteerd met een boete van bijna USD 9 miljard.[85] Ook verschillende Nederlandse grootbanken zijn eerder aan onderzoeken onderworpen en hebben schikkingen met de Amerikaanse autoriteiten getroffen. Naast boetes, bestaat het risico dat partijen die in overtreding van de Amerikaanse sanctiewetgeving handelen, de toegang tot de Amerikaanse financiële markten, en daarmee tot dollar-financiering, wordt ontzegd of dat zij zelf op sanctielijsten worden geplaatst.[86] Amerikaanse autoriteiten hebben recent aangegeven scherp in de gaten te houden of de Europese banken die nog in Rusland actief zijn de Amerikaanse sanctiewetgeving adequaat naleven. Daarbij is gewaarschuwd dat banken bij niet-naleving ook zelf sancties opgelegd kunnen krijgen of de toegang tot dollar-financiering wordt ontzegd.[87] De ECB heeft herhaaldelijk haar zorgen uitgesproken over de trage voortgang die een aantal banken maakt bij het afbouwen van de risico's die voorvloeien uit lopende activiteiten in Rusland. Deze banken zijn dan ook opgeroepen hun exit-strategieën en de afbouw van hun bezittingen in Rusland te versnellen.[88] Naast de eigen overwegingen van de ECB zijn deze ook deels gemotiveerd vanuit afwegingen rond de sanctierisico's van de VS.[89]

Het veranderde sanctielandschap gaat gepaard met financiële en niet-financiële risico's voor instellingen, die voorheen niet of nauwelijks op het netvlies stonden. Hoewel banken, pensioenfondsen en verzekeraars hun beleggingen in Rusland al grotendeels vóór de Russische inval in Oekraïne in het voorjaar

82 Zie in dit kader bijvoorbeeld artikel 10 van verordening 269/2014.
83 Zie Amar, Y. en Bennink S. (2020) voor een verdere toelichting op de werking van de Amerikaanse sanctieregelgeving.
84 Zie Farrell H. en Newman A. (2024) Underground Empire - How America weaponized the world economy, Penguin Random House en Caytas, J. (2017) Weaponizing finance: US and European options, tools and policies.
85 U.S. Department of Justice (2015) BNP Paribas sentenced for conspiring to violate the International Emergency Economic Powers Act and the Trading with the Enemy Act.
86 Zo kreeg in 2018 een Letse bank te maken met een forse uitstroom van deposito's en een gebrek aan toegang tot dollarfinanciering, nadat de Amerikaanse autoriteiten aankondigden deze bank aan te merken als een instelling waarbij er zorgen waren op het gebied van witwassen op basis van de Amerikaanse Patriot Act. Deze bank dreigde hierdoor om te vallen, waarna is besloten deze bank te liquideren (zie ook ECB, 2018).
87 Reuters (2024) European banks in Russia face 'awful lot of risk', Yellen says.
88 Enria, A. (2023) Letter to the members of the European Parliament.
89 Financial Times (2024) ECB pressures banks to speed up Russia exits on fear of US action.

van 2022 hadden afgebouwd, zagen zij zich na deze inval genoodzaakt hun beleggingen in Russische bedrijven onmiddellijk tot (vrijwel) nul af te schrijven. Vanwege Europese sancties mochten zij namelijk niet meer in Russische beleggingen handelen. Scenario's waarin beleggingen in een jurisdictie van de een op de andere dag illiquide en (vrijwel) waardeloos worden, stonden bij velen voorheen niet op het netvlies. Daarnaast is gebleken dat opgelegde sancties ook tot operationele problemen voor instellingen kunnen leiden, zoals het faillissement van de Amsterdam Trade Bank (ATB) in 2022 illustreert. Vanwege de sancties die autoriteiten in de VS en het VK oplegden aan bedrijven met Russische aandeelhouders, zagen IT-dienstverleners uit de VS en het VK zich genoodzaakt hun dienstverlening te beëindigen. ATB kon hierdoor niet langer over essentiële systemen beschikken om aan de verplichtingen richting rekeninghouders en andere tegenpartijen te voldoen en zag het zich genoodzaakt een faillissement aan te vragen.

In het verlengde hiervan kunnen financiële instellingen ook te maken krijgen met tegenreacties vanuit landen waaraan sancties zijn opgelegd. Europese banken die nog in Rusland actief zijn worden niet alleen scherp in de gaten gehouden door Europese en Amerikaanse toezichthouders (zie hierboven), maar ook door Russische autoriteiten. Deze hebben recent gedreigd beslag te leggen op de bezittingen van in Rusland actieve banken die zij als 'onvriendelijk' bestempelen, confronteren hen met additionele, onverwachte belastingheffingen en beperken de mogelijkheden om bezittingen zonder verlies van de hand te doen.[90] Tegenreacties kunnen ook andere vormen aannemen, bijvoorbeeld door druk op derde landen uit te oefenen en hen maatregelen te laten nemen die het verdienvermogen van westerse banken daar treft. Ook kunnen financiële instellingen doelwit worden van cyberaanvallen. Zo wijst bijvoorbeeld ENISA erop dat de westerse sancties op Rusland een additioneel motief voor Russische cybercriminelen vormen om cyberaanvallen op westerse organisaties uitvoeren, waarbij door deze groepen de vitale infrastructuur als potentieel doelwit wordt genoemd (zie ook hoofdstuk 3).[91]

Tot slot kan het veranderde sanctielandschap bredere gevolgen hebben voor de werking van het financiële stelsel als geheel. Financiële sancties die niet zozeer gericht zijn tegen (rechts)personen maar zich richten op de markt- of financiële infrastructuur waarvan zij gebruikmaken, zoals het berichtensysteem voor betalingen SWIFT en het bevriezen van centrale banktegoeden (door Euroclear) zijn illustratief voor de *weaponisation of finance*. Deze sancties kunnen in potentie ontwrichtend voor gesanctioneerde partijen zijn, aangezien voor grensoverschrijdende activiteiten toegang tot het internationale betalingssysteem een vereiste is. Het is niet ondenkbaar, en zelfs al zichtbaar, dat de inzet van dergelijke financiële sancties andere landen verder aanmoedigt om een eigen infrastructuur op te zetten om onderlinge grensoverschrijdende transacties af te wikkelen.[92] Zo ontwikkelde Rusland al in 2014

90 Zie The Economist (2024) European banks are making heady profits in Russia en Financial Times (2024) Western banks in Russia paid €800m in taxes to Kremlin last year.
91 ENISA (2022) Threat landscape 2022.
92 Cipriani, M. et al. (2023) Financial sanctions, SWIFT, and the architecture of the international payment system.

- na de dreiging van SWIFT afgesloten te worden - een eigen berichtensysteem voor betalingen waarop vooral banken uit Rusland en voormalig Sovjet-landen zijn aangesloten (System for Transfer of Financial Messages, SPFS). Ook China werkt aan een alternatief voor SWIFT, Chinese Cross-Border Interbank Payment System (CIPS), mede vanuit de ambitie om de Chinese valuta een steviger rol op het wereldtoneel te geven.[93] Daarnaast ontwikkelden Frankrijk, Duitsland en het VK het Instrument in Support of Trade Exchanges (INSTEX) om transacties met Iran uit te kunnen blijven voeren, nadat dat land de toegang tot SWIFT verloor vanwege Amerikaanse sancties.[94] Dergelijke initiatieven verminderen de interopabiliteit van marktinfrastructuren waardoor het omslachtiger wordt om handel en financiële transacties tussen verschillende landen en regio's plaats te laten vinden, met mogelijk negatieve effecten op wereldwijde kapitaalstromen, internationale handel en wereldwijde groei.[95] Ook het al dan niet inzetten van de gerealiseerde opbrengsten op Russische centrale banktegoeden of zelfs het inzetten van de bevroren tegoeden zelf, waarover eerder door Europese beleidsmakers werd gediscussieerd, kan potentieel verstrekkende gevolgen hebben. Zo heeft DNB op de economische en financiële implicaties van het inzetten van bevroren Russische tegoeden voor hulp aan Oekraïne gewezen, onder andere vanwege de gevolgen die dit kan hebben voor het vertrouwen in en de aantrekkelijkheid van de euro als handels- en reservevaluta en in euro-gedenomineerde activa voor publieke en private partijen buiten Europa.[96]

4.3 Adequate naleving sanctieregeling, scherp op potentiële neveneffecten

Ondanks recente verbeteracties, is een blijvende inspanning van financiële instellingen nodig voor adequate naleving van de sanctieregelgeving. Financiële instellingen zijn gehouden aan de Sanctiewet, wat vergt dat zij hun bedrijfsvoering dusdanig inrichten dat sanctieregelgeving wordt nageleefd. Uit toezichtonderzoeken die DNB in 2023 en 2024 heeft uitgevoerd blijkt dat instellingen de afgelopen jaren weliswaar de nodige stappen hebben gezet, maar dat er nog tekortkomingen worden vastgesteld op het gebied van screening, identificatie, risicobeheersing en rapportage van de sanctienaleving.[97] Bovendien valt op dat de volwassenheid van processen en ingezette systemen voor naleving van sanctieregelgeving tussen sectoren uiteenloopt. Zo blijkt dat de onderzochte banken het over het geheel genomen voldoende presteren, maar dat zij onder meer nog stappen te zetten hebben in het detecteren van *dual-use* goederen. Bij de onderzochte pensioenfondsen en verzekeraars zijn verschillende tekortkomingen vastgesteld. Zo is geconstateerd dat binnen de pensioensector sanctiescreening met regelmaat wordt uitbesteed, waarbij vervolgens te weinig waarborgen zijn of sanctieregelgeving daadwerkelijk wordt nageleefd en is bij meerdere verzekeraars vastgesteld

93 Zie bijvoorbeeld Eichengreen B. (2022) Sanctions, SWIFT, and China's Cross-Border Interbank Payments System en Eichengreen B. & Kawai M. (2015) Renminbi Internationalization: Achievements, Prospects, and Challenges.

94 Nadat de VS uit de Iran Nuclear Deal stapten, zochten de Europese landen naar manieren om buiten het Amerikaanse bancaire systeem transacties met Iran te blijven faciliteren (zie bijvoorbeeld Marineau, S. (2021) en CFR (2023)). Oorspronkelijk was INSTEX geen succes, maar gedurende de COVID-19 heeft het Europese bedrijven instaat gesteld om humanitaire goederen aan Iran te leveren (The Economist, 2024). Zie ook Batmanghelidj E. en Rouhi M. (2021) The Iran Nuclear Deal and Sanctions Relief: Implications for US Policy.

95 Zie bijvoorbeeld Greene, R. (2022) How Sanctions on Russia Will Alter Global Payments Flows en Cipollone, P. (2024) Why Europe must safeguard its global currency status.

96 DNB (2024) DNB schuift aan in Tweede Kamer over inzet van bevroren Russische tegoeden.

97 Zie DNB (2024) Integriteitstoezicht in beeld en DNB (2023) DNB onderzoek Sanctiewet voor een uitgebreidere toelichting.

dat de screening van UBO's niet naar behoren wordt uitgevoerd. UBO's worden namelijk niet altijd geïdentificeerd, en worden ook niet altijd gescreend tegen sanctielijsten. Ook bij cryptodienstverleners en in de trust-sector, waarbij het risico op sanctie-omzeiling groot is gezien het hoge aantal cliënten dat actief is in de energiesector, heeft DNB tekortkomingen geconstateerd. DNB verwacht van instellingen dat zij geconstateerde tekortkomingen voortvarend adresseren en goed reflecteren op de ervaringen die de afgelopen jaren met sanctienaleving zijn opgedaan, zodat zij beter in staat zijn in te spelen op veranderingen in het sanctielandschap. DNB zal scherp blijven toezien op adequate naleving van de sanctieregelgeving.

Naast adequate interne processen voor naleving van sanctieregelgeving, is belangrijk dat instellingen ook de potentiële risico's die voortvloeien uit sancties identificeren en beheersen. Toenemende geopolitieke spanningen leiden tot snelle ontwikkelingen in opgelegde sancties, waardoor ook neveneffecten van sancties – waaronder tegenreacties vanuit gesanctioneerde landen – in potentie snel kunnen optreden. Het is daarom belangrijk dat zij potentiële risico's die samenhangen met de uitvoering van sancties en daaruit voortvloeiende ongunstige neveneffecten identificeren en beheersen. Instellingen zullen daarbij in het bijzonder oog moeten hebben voor de blootstellingen die zij in potentieel kwetsbare jurisdicties hebben en operationele activiteiten die, al dan niet via uitbestedingsconstructies, in die jurisdicties plaatsvinden of die kwetsbaar zijn voor mogelijke tegenreacties uit gesanctioneerde landen. Scenario-analyses, waarmee bijvoorbeeld de gevolgen worden verkend van forse *haircuts* op eigen activa, die van belangrijke klantrelaties of verstoringen in kritieke diensten of operationele processen, kunnen behulpzaam zijn om kwetsbaarheden in kaart te brengen en aanknopingspunten geven voor het verder uitwerken van afbouw- en crisisplannen.

Instellingen zijn gebaat bij meer harmonisatie van het Europese sanctiebeleid. Sancties worden in Europese verordeningen neergelegd, terwijl het toezicht en beleid waarmee invulling aan sancties wordt gegeven een nationale aangelegenheid is. Dit leidt ertoe dat EU-lidstaten soms een andere interpretatie van sancties hebben, zoals bijvoorbeeld bij het vraagstuk wie de uiteindelijke controle over bepaalde activa heeft.[98] Ook hebben lidstaten de bevoegdheid om in bijzondere gevallen uitzonderingen op sancties te maken, waarbij de regels voor het maken van dergelijke uitzonderingen verschillend worden geïnterpreteerd.[99] Het ontbreken van een uniforme interpretatie van sancties binnen de EU leidt tot een ongelijk speelveld tussen Europese instellingen. Ook dienen instellingen die in meerdere lidstaten actief zijn rekening te houden met uiteenlopende interpretaties. Dit leidt tot additionele kosten voor instellingen en kan tot juridische en reputatierisico's leiden. Ook in het toezicht en de sanctiehandhaving bestaan verschillen tussen lidstaten. Zo verschillen onder meer de juridische kwalificatie van overtredingen en de maximale straffen die overtreders kunnen

98 Zie bijvoorbeeld aanbeveling 14 in Rijksoverheid (2022) Rapport van de nationaal coördinator sanctienaleving en handhaving en CEPA (2024) Europe's Russia Sanction Regime Cracks.
99 Zie aanbeveling 16 in Rijksoverheid (2022) Rapport van de nationaal coördinator sanctienaleving.

krijgen.[100] Het is daarom goed dat er recent prioriteit wordt gegeven aan de harmonisering van het Europese sanctiebeleid. De Europese richtlijn die in het voorjaar van 2024 is aangenomen, waarmee lidstaten verplicht worden om omzeilingen en schendingen van EU-sancties strafbaar te stellen, is een stap in de goede richting.[101] In het algemeen zijn instellingen gebaat bij meer harmonisatie van het sanctiebeleid, het toezicht en de handhaving. Een neveneffect van dergelijke harmonisatie is tevens dat sancties effectiever en sanctienaleving efficiënter kunnen worden. Het is daarom belangrijk dat het ministerie van Buitenlandse Zaken zich, samen met de Europese Commissie, inzet voor verdere harmonisatie van het Europese sanctiebeleid. In een ideaal scenario kan gedacht worden aan het onderbrengen van beleids- en handhavende taken bij een onafhankelijke Europese organisatie. Deze optie verdient dan ook om serieus onderzocht te worden. Indien blijkt dat hier onvoldoende draagvlak voor is, is een inzet op een formele Europese interpretatie van sancties gewenst. De Q&A's die de Europese Commissie eerder in dit kader heeft opgesteld, zijn een stap in de goede richting. Om deze Europese interpretatie voldoende effectief te maken dient dit verder geformaliseerd te worden.

Tot slot kan intensievere uitwisseling tussen publieke en private organisaties over sanctiemeldingen en -omzeilingen instellingen waardevolle informatie verschaffen voor het verbeteren van de naleving van sanctieregelgeving. Het wetsvoorstel internationale sanctiemaatregelen, dat in de zomer van 2024 ter internetconsultatie is aangeboden, breidt de meldplicht bij sancties uit naar meer beroepsgroepen - waaronder advocaten, notarissen en belastingadviseurs. Ook introduceert het een centraal meldpunt voor sanctiemeldingen.[102] Dit meldpunt heeft onder andere de taak meldingen te verzamelen en te analyseren waardoor, in combinatie met de uitbreiding van de meldplicht, een completer beeld ontstaat. Patronen in onder andere sanctie-ontwijking en omzeiling kunnen zo sneller en beter worden herkend. Het, waar mogelijk, delen van dergelijke informatie vanuit dit centraal meldpunt met financiële instellingen, is waardevol. Het biedt instellingen aanknopingspunten voor het verbeteren van de naleving van sanctieregelgeving, waardoor risico's voor instellingen worden verkleind. Doordat deze informatie geen betrekking heeft op persoonsgegevens, lijken er daartoe ook mogelijkheden te bestaan. Eenbijkomstigheidhiervan is tevens dat het voor gesanctioneerde partijen lastiger wordt sancties te omzeilen, waardoor de effectiviteit van sancties kan toenemen.

100 Deze verschillen bemoeilijken internationale samenwerking tussen opsporingsdiensten. Zo kan de opsporing in verschillende lidstaten alleen gegevens delen als de kwalificatie van het strafbare feit in beide lidstaten hetzelfde is. Daarnaast ontstaan ook problemen rondom gegevensuitwisseling als de mogelijke straffen die op delicten staan veel van elkaar verschillen in lidstaten.
101 Richtlijn (EU) 2024/1226
102 Rijksoverheid (2024) Wetsvoorstel Wet internationale sanctiemaatregelen.

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl

Volg ons op:

DeNederlandscheBank

EUROSYSTEEM