Digitale afhankelijkheid in de financiële sector

risico's, weerbaarheid en Europese autonomie

DeNederlandscheBank
EUROSYSTEEM

AFM

Inhoudsopgave

Samenvatting & hoofdboodschappen

De financiële sector is in toenemende mate afhankelijk van externe IT-dienstverleners voor het uitvoeren van zijn kernprocessen. De digitale infrastructuur vormt de ruggengraat van vrijwel alle bedrijfsprocessen: van klant-interactie en risicobeheer tot compliance en transactieverwerking. Artificiële intelligentie (AI) speelt hierbinnen een groeiende rol. Steeds meer instellingen besteden (delen van) hun IT uit aan externe leveranciers, waaronder clouddienstverleners, softwareaanbieders en leveranciers van AI-modellen. Deze trend wordt mede gedreven door toenemende complexiteit van IT en cyberbeveiliging, technologische vernieuwing en schaalvoordelen. Clouddienstverlening heeft een grote vlucht genomen, waarbij een steeds groter deel van de 'technologie stack' van instellingen wordt beheerd door externe IT-leveranciers.

De digitale afhankelijkheid van de financiële sector brengt aanzienlijke risico's met zich mee. Doordat instellingen veelal gebruikmaken van dezelfde aanbieders en infrastructuren zijn concentratie- en systeemrisico's ontstaan. Een paar grote, wereldwijd opererende digitale dienstverleners, de zogeheten hyperscalers, zijn de afgelopen jaren het hele speelveld gaan domineren. In het huidige gure geopolitieke klimaat bestaat het risico dat statelijke actoren de afhankelijkheid van digitale dienstverlening misbruiken als politiek pressiemiddel of instrument in een handelsconflict. Door complexe ketens van onderaannemers en gedeelde infrastructuren kunnen storingen en cyberincidenten bij IT-dienstverleners meerdere instellingen tegelijkertijd raken. Door deze complexe toeleveringsketens en beperkt zicht op onderliggende partijen ontstaat een ecosysteemrisico dat lastig te beheersen is. 'Vendor lock-in' maakt overstappen of spreiding van risico's voor instellingen moeilijk en kostbaar, waardoor hun onderhandelingspositie verzwakt en prijzen kunnen stijgen.

Financiële instellingen en IT-leveranciers zijn zich bewust van de risico's en nemen maatregelen om deze in te perken. Instellingen stellen exitstrategieën en continuïteitsplannen op en brengen ketenafhankelijkheden in kaart. 'Multi-vendor'-strategieën, containerisatie en het gebruik van open standaarden worden door een aantal instellingen als voorbeelden genoemd om flexibiliteit te vergroten. Toch blijven deze oplossingen kostbaar en technisch complex. Aan 'vendor lock-in' blijft daarmee moeilijk te ontkomen. IT-leveranciers bieden een hoge mate van continuïteit om hun diensten zo betrouwbaar mogelijk te maken. Ook bieden ze steeds vaker 'soevereine cloud'-oplossingen aan waarbij data, dienstverlening en beheer onder Europese wet- en regelgeving vallen. In hoeverre deze oplossingen echter daadwerkelijk effectief bescherming bieden tegen potentiële invloed van niet-Europese actoren, staat nog te bezien. Technische maatregelen zoals eigen beheer van encryptiesleutels dragen volgens een aantal instellingen bij aan dataveiligheid en continuïteit, maar bieden geen volledige bescherming tegen uitval of dataverlies.

Korte termijn: voorbereiden op ontwrichtende scenario's

Op korte termijn is de sterke afhankelijkheid van niet-Europese IT-aanbieders een gegeven. Het is belangrijk dat instellingen maatregelen nemen om zich voor te bereiden op disruptieve scenario's en om waar mogelijk de potentiële impact te mitigeren. Op korte termijn kunnen sancties of hybride aanvallen de dienstverlening ernstig verstoren.

- Instellingen kunnen samenwerken met andere instellingen, en met IT-leveranciers en autoriteiten in:
  - het ontwikkelen van dreigingsscenario's;
  - het uitwisselen van informatie over concrete dreigingen en aanvallen;
  - het op basis van scenario's uitvoeren van ketentests, inclusief 'real life' testen.

  De AFM en DNB zijn bereid waar nodig deze samenwerking te faciliteren.
- Voor instellingen is het van belang dat ze kunnen uitleggen welke keuzes ze hebben gemaakt om te waarborgen dat hun data soeverein en veilig zijn, eventueel door gebruik van 'soevereine cloud'-oplossingen van niet-Europese clouddienstverleners.
- Om te voorkomen dat belangrijke en gevoelige data in handen van derden komen, kunnen instellingen het beheer van encryptiesleutels zoveel mogelijk in eigen hand nemen.
- Instellingen kunnen hun afhankelijkheid verminderen door te streven naar een flexibele inrichting van de IT-dienstverlening. Voorbeelden zijn containerisatie van applicaties zodat deze leverancieronafhankelijk kunnen draaien, gebruik van open standaarden en open source oplossingen, en gebruik maken van meerdere leveranciers ('multi-vendor').

Langere termijn: vergroten van de strategische autonomie vergt een Europese aanpak

Op langere termijn is het van belang dat Europa minder afhankelijk wordt van niet-Europese IT-aanbieders, en een grotere mate van digitale autonomie bereikt. Scenario-analyse laat zien dat een sterkere Europese techsector nodig is, zelfs als geopolitieke spanningen zouden afnemen. Een sterke, autonome en innovatieve Europese techmarkt is wenselijk, zowel voor de weerbaarheid, als voor het behoud van Europese waarden zoals privacy en inclusiviteit.

Het vergroten van digitale autonomie overstijgt de competenties van financiële instellingen en nationale financiële toezichthouders, en vergt actie op Europees niveau.

- Het is van belang de structurele factoren die hebben geleid tot het ontstaan van digitale afhankelijkheid aan te pakken. Het Draghi-rapport reikt hiervoor concrete handvatten aan, die opvolging verdienen.
- Om afhankelijkheden van niet-Europese IT-dienstverleners te verminderen, zullen volwaardige Europese alternatieven moeten worden ontwikkeld. Waar Europese alternatieven al beschikbaar zijn kunnen financiële instellingen overwegen hiervan gebruik te gaan maken. Daarbij is het goed als instellingen samenwerken, om een mogelijk 'first mover disadvantage' te overwinnen, en kritische massa te creëren om de levensvatbaarheid van Europese leveranciers te bevorderen.
- Ten aanzien van (generatieve) AI-toepassingen zijn er reeds Europese toepassingen beschikbaar voor financiële instellingen. Het gebruik hiervan kan bijdragen aan het voorkomen van nieuwe 'vendor lock-ins'.

- De AFM en DNB ondersteunen de ontwikkeling van de Europese spaar- en investeringsunie. Voor de ontwikkeling van de Europese IT-sector is daarbij toegang tot financiering met het oog op schaalvergroting van innovatieve ondernemingen een belangrijk aandachtspunt.

Wetgeving en toezicht

Wetgevers en toezichthouders hebben al de nodige maatregelen genomen om risico's van digitale afhankelijkheden te beheersen. De implementatie van DORA versterkt de grip op risico's van digitale afhankelijkheden voor de continuïteit van dienstverlening, waaronder het risico van cyberaanvallen op derde partijen en geopolitieke risico's. Het DORA 'Register of information' vergroot het inzicht in derde-partijafhankelijkheden. Onder DORA worden kritieke IT-leveranciers onder een oversightkader geplaatst dat een vorm van direct Europees toezicht mogelijk maakt. Ook andere, cross-sectorale, Europese regelgeving richt zich op kritieke grote tech-partijen. Hoewel de huidige regelgeving een belangrijke bijdrage levert aan het beheersen van risico's rond derde partijen, blijven er kwetsbaarheden bestaan.

De AFM en DNB:

- verwachten dat instellingen risico's van derde-partijafhankelijkheden adequaat beheersen en zullen in hun toezicht in het bijzonder aandacht besteden aan de voorbereiding op ontwrichtende scenario's;
- vinden het wenselijk dat betrokken toezichthouders (naast de AFM en DNB bijvoorbeeld de ACM en de RDI) hun samenwerking ten aanzien van toezicht op IT-leveranciers intensiveren;
- voeren een analyse uit op de DORA 'Registers of information' die is gericht op het voor de Nederlandse financiële sector in kaart brengen van concentraties in het gebruik van IT-diensten. De verwachting is dat instellingen het informatieregister gebruiken als middel om hun eigen concentratierisico's en afhankelijkheden goed in kaart te brengen;
- onderzoeken in hoeverre financiële regelgeving (waaronder DORA) en toezicht belemmeringen bevat voor het gebruikmaken van Europese IT-leveranciers en innovatie. Geïdentificeerde issues kunnen aanleiding geven tot het nemen van beleidsinitiatieven in Europees verband, het aankaarten bij de wetgever, of het doorvoeren van aanpassingen in het toezicht. Dit om het voor instellingen mogelijk te maken dat soevereiniteit kan worden afgewogen ten opzichte van andere kenmerken bij de keuze van digitale dienstverlener;
- vragen de Europese overheden en toezichtautoriteiten te analyseren of DORA in voldoende mate bijdraagt aan de weerbaarheid tegen geopolitieke risico's – en als dit niet het geval is nadere guidance te overwegen. Op termijn kan vanuit geopolitiek perspectief ook worden gedacht aan een sectoroverstijgende Europese cloudtoezichthouder, die krachtig kan optreden om de risico's van digitale afhankelijkheden te mitigeren, bijvoorbeeld door het afdwingen van echt soevereine cloudoplossingen;
- zien mogelijkheden om op termijn DORA te versterken. Onder meer zou het oversightkader voor derde partijen zo nodig meer dwingend kunnen worden gemaakt en kunnen explicieter vereisten worden opgenomen voor de beheersing van geopolitieke risico's met voldoende oog voor innovatie.

Inleiding

Technologische innovatie en digitalisering hebben de financiële sector fundamenteel veranderd. Financiële instellingen zijn steeds afhankelijker van externe technologieleveranciers. Banken, verzekeraars en vermogensbeheerders leunen grotendeels op een handvol grote (veelal niet-Europese) techbedrijven voor de ondersteuning van kritieke processen. Recente geopolitieke ontwikkelingen en incidenten hebben deze afhankelijkheid scherper in beeld gebracht. We bevinden ons op een kruispunt waar digitalisering onmisbaar is, maar waar ook nieuwe risico's zijn ontstaan rond continuïteit, cybersecurity en zelfs soevereiniteit.

De Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB) vinden het van strategisch belang dat op termijn de afhankelijkheid van de financiële sector van niet-Europese IT-leveranciers wordt verminderd. Afhankelijkheid van één of enkele IT-leveranciers kan leiden tot systeemrisico's: een storing of incident bij zo'n leverancier kan hele delen van de financiële sector treffen en daarmee de stabiliteit van het stelsel of de belangen van consumenten in gevaar brengen. Het borgen van een stabiele, integere financiële markt vereist dat afhankelijkheidsrisico's inzichtelijk en beheersbaar zijn. Voor de korte termijn zijn de mogelijkheden om de afhankelijkheid van niet-Europese IT-leveranciers substantieel te verminderen beperkt, gezien het huidige gebrek aan volwaardige Europese alternatieven. Het is voor instellingen van belang dat zij zich op korte termijn richten op het vergroten van hun digitale weerbaarheid en zich zo goed mogelijk beschermen tegen de risico's die de afhankelijkheden met zich meebrengen. Voor de langere termijn is het noodzakelijk om de Europese techsector structureel te versterken en zo de afhankelijkheden daadwerkelijk te verminderen. Dit vraagt om tijdige en gerichte actie van publieke en private partijen. In dit rapport doen de AFM en DNB hiervoor een aantal aanbevelingen en worden vervolgstappen benoemd.

De opzet van het rapport is als volgt.
Hoofdstuk 1 schetst eerst de huidige stand van zaken: hoe diep vervlochten is de financiële sector met informatietechnologie van derde partijen? Vervolgens worden de belangrijkste risico's beschreven die voortvloeien uit deze digitale afhankelijkheden. We laten zien welke typen nieuwe kwetsbaarheden zijn ontstaan – van operationele incidenten tot strategische lock-in – en we verkennen aan de hand van scenario's hoe deze risico's zich op korte en lange termijn zouden kunnen manifesteren. In hoofdstuk 2 verschuift de focus naar de praktijk: op basis van gesprekken en analyses wordt inzichtelijk gemaakt hoe financiële instellingen en hun IT-leveranciers omgaan met de gesignaleerde afhankelijkheidsrisico's. Tot slot richt hoofdstuk 3 zich op het toezicht- en beleidskader: We inventariseren bestaande regelgeving en initiatieven, en doen een aantal aanbevelingen om afhankelijkheden te verminderen en de digitale autonomie van de financiële sector te versterken.

1 De ontwikkeling van digitale afhankelijkheidsrisico's

De financiële sector is in hoge mate afhankelijk van informatietechnologie (IT) voor het uitvoeren van zijn kernprocessen, vaak uitgevoerd door derde partijen. De digitale infrastructuur vormt de ruggengraat van vrijwel alle bedrijfsprocessen: van klantinteractie en risicobeheer tot compliance en transactieverwerking. Steeds meer instellingen besteden (delen van) hun IT uit aan externe leveranciers. Deze trend wordt mede gedreven door toenemende complexiteit van IT en cyberbeveiliging, technologische vernieuwing en schaalvoordelen. In de volgende paragrafen wordt uiteengezet hoe deze afhankelijkheden zich hebben ontwikkeld (1.1) en welke risico's zich manifesteren (1.2). Tot slot kijken we met een scenario-analyse naar mogelijke toekomstbeelden voor deze risico's (1.3).

1.1 De financiële sector draait op IT

De digitalisering van financiële processen is ingegeven door zowel de wens om processen efficiënter en sneller uit te voeren, als door externe factoren zoals regelgeving en klantverwachtingen. Digitalisering biedt instellingen voordelen, zoals verbeterde datakwaliteit, realtime inzicht in financiële stromen en geautomatiseerde rapportages die de besluitvorming ondersteunen. Deze technologische verbeteringen maken het mogelijk om processen schaalbaar en flexibel in te richten, wat bij kan dragen aan bijvoorbeeld internationale samenwerking en concurrentiekracht. Klantinteractie verloopt grotendeels via apps, webportalen en geautomatiseerde chatdiensten, terwijl ook risicobeheer en compliance draaien op technologie. De hogere verwachtingen op het gebied van snelheid, kostenbesparing en servicekwaliteit zetten instellingen ertoe aan om hun digitale transformatie verder te versnellen. Dit was voor toezichthouders aanleiding om strengere eisen te stellen aan transparantie, controleerbaarheid en risicobeheersing. De toenemende afhankelijkheid van IT creëert ook nieuwe kwetsbaarheden, zoals cyberaanvallen en systeemstoringen, die op hun beurt vragen om beveiligingsmaatregelen en effectieve incidentrespons. Er is sprake van een wederkerige dynamiek: IT is zowel een middel om aan externe eisen te voldoen als een factor die deze eisen mede vormgeeft.

Steeds meer instellingen besteden (delen van) hun IT uit aan externe IT-leveranciers. Instellingen profiteren van de expertise, de innovatiekracht en de voordelen qua schaal en scope van gespecialiseerde leveranciers, die innovatieve toepassingen sneller en goedkoper kunnen implementeren dan interne teams. Daarbij brengt het zelf beheren van 'on-premises' IT-infrastructuur risico's en inefficiënties met zich mee, zoals het zelf regelen van fysieke beveiliging, back-ups en cyberweerbaarheid. In de publieke cloud zijn deze aspecten geborgd door gespecialiseerde aanbieders, wat de algehele veiligheid en continuïteit ten goede komt. De uitbesteding aan derde partijen betreft niet enkel ondersteunende processen, maar raakt ook aan de kern van financiële dienstverlening. Er is een aantal kritieke infrastructuren waarop financiële instellingen in hoge mate vertrouwen, zoals publieke cloud, datacenters voor veilige opslag en hosting, technische netwerken voor realtime transacties en geavanceerde cyberverdedigingssystemen. Een inventarisatie van de Europese toezichthoudende autoriteiten in de financiële sector uit 2022 liet zien dat 9.000 van de 15.000 ICT-dienstverleners die hun diensten direct leveren aan financiële instellingen, kritieke of belangrijke functies van deze instellingen ondersteunden.[1]

1 ESMA, ESAs report on the landscape of ICT third-party providers

Artificiële intelligentie (AI) speelt binnen financiële instellingen een steeds grotere rol bij het verbeteren van efficiëntie, nauwkeurigheid en klantgerichtheid. Waar IT traditioneel werd ingezet voor het automatiseren van processen en het beheren van data, stelt AI-organisaties in staat om deze data op een geavanceerdere manier te interpreteren en toe te passen. Dit opent nieuwe mogelijkheden voor het verbeteren van operationele processen, het verhogen van klantgerichtheid, en het versterken van risicobeheersing. AI wordt toegepast voor uiteenlopende doelen, zoals geautomatiseerde fraudedetectie, het monitoren van marktrisico's, kredietrisicoanalyse, klantsegmentatie, transactie- en incidentmonitoring en cyberweerbaarheid. Chatbots en virtuele assistenten kunnen zorgen voor snellere en gepersonaliseerde klantinteractie, terwijl machine learning algoritmen worden ingezet om patronen in grote hoeveelheden financiële data te herkennen. Ook compliance-toepassingen bevatten AI: regels rond anti-witwas-praktijken (AML) en Know Your Customer (KYC) kunnen efficiënter worden nageleefd door intelligente dataverwerking, mits de privacy geborgd is en er niet wordt gediscrimineerd.

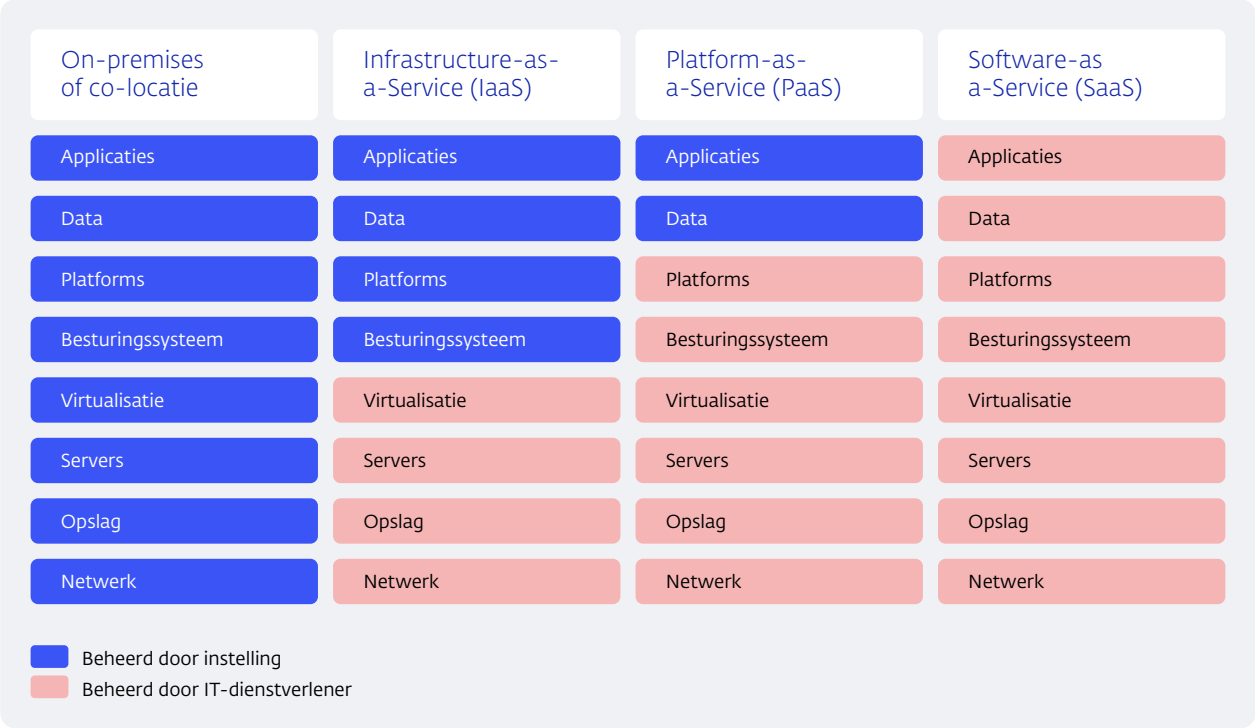
Clouddienstverlening heeft een grote vlucht genomen. De opkomst van virtualisatie-technieken[2] maakte het mogelijk voor bedrijven om een geleidelijke stap van eigen datacenters naar cloudoplossingen te maken. De belofte van schaalvoordelen, kostenbesparing en snellere innovatie maakte cloud aantrekkelijk, vooral voor minder kritieke toepassingen zoals testomgevingen en klantportalen. Grote Amerikaanse aanbieders begonnen gestan-daardiseerde infrastructuurdiensten aan te bieden en konden daardoor de markt domineren.

De verschuiving van interne IT-omgevingen naar uitbesteding en externe cloudoplossingen markeert een belangrijke ontwikkeling, ook binnen de financiële sector. Hoewel veel instellingen nog gebruikmaken van 'on-premises' datacenters, soms in eigen beheer, maar vaak ook via gehuurde of gedeelde faciliteiten zoals co-locatie, wordt ook steeds vaker gekozen voor hybride modellen waarin externe cloud-omgevingen een steeds grotere rol spelen.

De transitie van traditionele 'on-premises' IT-infrastructuren naar cloudgebaseerde diensten weerspiegelt een structurele verschuiving in de manier waarop organisaties technologie beheren en inzetten. Binnen het clouddienstverleningsmodel onderscheiden we drie hoofdvormen: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) en Software-as-a-Service (SaaS). Deze modellen lopen op in mate van uitbesteding en overdracht van operationeel beheer van de instelling aan de IT-dienstverlener (zie figuur 1). Instellingen kunnen voor verschillende processen hoger of minder hoog in de 'technologie stack' gaan qua mate van uitbesteding. Soms blijven kritieke processen, zoals transactieverwerking of klantdata, intern zonder verbinding met het open internet. Minder gevoelige functies, zoals e-mail of HR-systemen, worden uitbesteed aan een clouddienstverlener. Andere instellingen hanteren een volledige cloudstrategie, waarbij ze hun informatievoorziening grotendeels (gaan) realiseren met de inzet van clouddiensten. Innovatieve en gespecialiseerde diensten worden vaak 'cloud native' ontwikkeld, soms door de clouddienstverlener zelf, maar vaak ook door gespecialiseerde dienstverleners. Dergelijke diensten zijn dus alleen als 'SaaS-oplossing' te

2 Hiermee kunnen softwarematig meerdere 'virtuele' computers worden gecreëerd op één fysieke computer, zodat de hardware optimaal wordt benut.

Figuur 1 Modellen van clouddienstverlening



gebruiken, draaiend op een public-cloudplatform. Soms kan wel gekozen worden voor het gebruik van de eigen infrastructuur van de instelling, of een alternatieve clouddienstverlener, maar doorgaans tegen hogere kosten of verminderde functionaliteit. Een alternatief is dat instellingen zelf diensten ontwikkelen op het platform van de clouddienstverlener (PaaS), of indien beschikbaar kiezen voor diensten die niet (alleen) als SaaS-oplossing beschikbaar zijn.

1.2 Risico's bij digitale afhankelijkheid

De toenemende afhankelijkheid van externe IT-dienstverleners en cloudomgevingen binnen de financiële sector leidt tot concentratie- en systeemrisico's. Er zijn weliswaar veel dienstverleners actief, maar naarmate meer instellingen gebruikmaken van dezelfde infrastructuren en aanbieders, ontstaat een concentratierisico. Een paar grote, globaal opererende digitale dienstverleners, de zogeheten hyperscalers, zijn de afgelopen jaren het hele speelveld gaan domineren door hun voordelen van schaal en scope en het brede functionele palet van diensten. Waar instellingen eerder

werkten met meerdere leveranciers, vertrouwen zij de IT-stack nu vaak volledig toe aan één hyperscaler. Tegelijkertijd groeit het systeemrisico, doordat de stabiliteit van het financiële stelsel mede afhankelijk wordt van de robuustheid en beschikbaarheid van de externe IT-leveranciers. Een storing of (cyber)incident bij één aanbieder kan meerdere financiële instellingen tegelijkertijd treffen. Afhankelijkheden beperken zich niet langer tot individuele instellingen, maar kunnen zich, mede via ketens van dienstverleners, opstapelen tot risico's op systeemniveau. Fallback- en herstelmechanismen kunnen ontoereikend zijn als meerdere partijen dezelfde afhankelijkheden hebben.

Ook de hardware waarop de systemen draaien wordt doorgaans geleverd door een selecte groep niet-Europese leveranciers. Veel van deze servers, netwerkcomponenten, beveiligingsvoorzieningen en opslagapparatuur zijn afkomstig van een klein aantal mondiale leveranciers. Naast de fysieke bouwstenen leveren enkele leveranciers vaak ook de firmware en beheersoftware die essentieel zijn voor het functioneren van deze systemen. Een bijzonder aandachtspunt is de opkomst van gespecialiseerde hardware voor kunstmatige intelligentie. Specifieke chips zijn cruciaal voor het trainen en uitvoeren van machine learning modellen, bijvoorbeeld voor realtime fraudedetectie of geautomatiseerde klantinteractie. De productie en innovatie van dergelijke hardware is sterk geconcentreerd in bepaalde regio's, wat vragen oproept over leveringszekerheid, strategische afhankelijkheid en technologische soevereiniteit. Ook de voor de productie benodigde grondstoffen creëren een afhankelijkheid.

In het huidige gure geopolitieke klimaat bestaat het risico dat statelijke actoren de afhankelijkheid van digitale dienstverlening misbruiken als politiek pressiemiddel of instrument in een handelsconflict.[3] De grote afhankelijkheid van de Europese financiële instellingen van vooral Amerikaanse IT-leveranciers, inclusief de grote clouddienst-verleners, plaatst ze in een kwetsbare positie. Dit risicobeeld gaat uit van het scenario dat de betreffende niet-Europese IT-dienstverleners op last van statelijke actoren hun dienstverlening (selectief) aan hun klanten staken, onderbreken of op een lager serviceniveau brengen. Dit risico is één van de drijfveren van de niet-Europese dienstverleners om 'soevereine' oplossingen te ontwikkelen voor de Europese markt. 'Soevereine' oplossingen voor clouddiensten vormen als mitigerende maatregel een reële optie. Het ontwikkelen en implementeren van deze 'soevereine' oplossingen vergt echter veel tijd en investeringen, terwijl de dreiging en de mogelijke impact van deze risico's juist op korte termijn al acuut kunnen zijn. Hierdoor ontstaat een spanningsveld tussen de urgentie van de problematiek en het tempo waarmee structurele oplossingen gerealiseerd kunnen worden.

De complexiteit van de toeleveringsketen neemt toe, met gelaagde afhankelijkheden die moeilijk te overzien zijn. Een instelling kan bijvoorbeeld een bepaald tech-platform afnemen van een fintechbedrijf, dat zelf draait op een ander cloudplatform dan de instelling, en ook weer gebruikmaakt van application programming interfaces (API's) van andere derde partijen.[4] Incidenten bij toeleveranciers dieper in de keten kunnen daardoor onverwacht grote gevolgen

3 Zie ook: DNB, Weerbaar in een gure wereld.

4 API: Application Programming Interface, de technische verbinding tussen IT-applicaties.

hebben. Instellingen zijn afhankelijk van de snelheid en zorgvuldigheid waarmee elke schakel in de keten reageert. Dit ecosysteemrisico is moeilijk te beheersen, omdat het zicht op onderliggende partijen vaak ontbreekt. De financiële instelling is weliswaar altijd eindverantwoordelijk, maar heeft niet altijd goed zicht op de onderliggende lagen en het belang van partijen die daar actief zijn. Instellingen die hun keten van toeleveranciers inzichtelijk hebben, kunnen veelal geen invloed uitoefenen op de interne beheersing van deze partijen.

'Vendor lock-in' is een tastbaar risico, doordat migreren of 'multi-sourcing' moeilijker wordt naarmate men dieper in een specifiek ecosysteem zit. Applicaties en data zijn afgestemd op specifieke technologieën van de platformaanbieder waardoor migratie naar een ander platform aanzienlijke investeringen vereist en doorgaans gepaard gaat met een kostbaar meerjaren transitieplan. 'Multi-sourcing', het parallel gebruiken van meerdere leveranciers, blijkt hierdoor in de praktijk vrijwel altijd (te) kostbaar en (te) complex. Dit maakt het lastig om een vorm van risicospreiding te realiseren. Een 'multi-vendor'-strategie, waarbij een deel van de (kritieke) processen bij de ene leverancier is ondergebracht en een ander deel bij een andere, wordt vaker gehanteerd, maar ondervangt het risico maar ten dele. Het gevolg hiervan is dat het machtsevenwicht verschuift in contractonderhandelingen tussen leveranciers en financiële instellingen, met risico's op prijsstijgingen.[5]

Door de verdere digitalisering worden ook cyberdreigingen steeds prominenter en de aanvallen geavanceerder, met grotere potentiële impact dan voorheen. Waar voorheen een cyberaanval vaak op één instelling direct gericht was, kan een aanval op een externe leverancier nu indirect meerdere instellingen treffen. Financiële instellingen beseffen dat hun cyberweerbaarheid afhankelijk is van de zwakste schakel in hun digitale keten. Tegelijkertijd neemt het aantal cyberaanvallen toe. Autoriteiten zoals AFM, DNB en ECB voeren zogeheten vrijwillige TIBER-testen (Threat Intelligence Based Ethical Red teaming) en ART-testen (Advanced Red Teaming) uit, waarbij financiële instellingen en hun leveranciers door ethische hackers worden getest op kwetsbaarheden. Door de invoering van de Digital Operational Resilience Act (DORA), een Europese verordening die digitale weerbaarheid bij financiële instellingen verplicht stelt, is ook de verplichte variant genaamd TLPT (Threat Led Penetration Testing) in het leven geroepen voor de grootste, kritieke financiële entiteiten. Bij deze testen komt ook steeds meer aandacht voor het (mee)testen van derde partijen.

Door de uitbesteding van dataopslag en verwerking aan clouddienstverleners ontstaan vraagstukken rondom gegevensbescherming, toezicht en compliance. Financiële instellingen opereren binnen strikte privacy- en beveiligingsregels, en het gebruik van publieke cloudoplossingen wringt soms met bestaande regelgeving. Dit brengt juridische risico's met zich mee, vooral wanneer de data onderhevig worden aan niet-Europese wetgeving. Denk hierbij aan de Amerikaanse CLOUD Act, die Amerikaanse autoriteiten het recht geeft om data van personen en organisaties op te vragen

5 Zie ook ACM, Markstudie clouddiensten, die uitgebreid ingaat op de (potentiële) gebreken in de werking van de markt voor clouddiensten.

bij Amerikaanse technologiebedrijven, ongeacht waar die data fysiek zijn opgeslagen. Dit staat op gespannen voet met de Europese privacyregels, zoals vastgelegd in de Algemene Verordening Gegevensbescherming (AVG). De afhankelijkheid van buitenlandse infrastructuur is dus een kwetsbaarheid, die niet alleen de beschikbaarheid raakt, maar ook de controle over wie toegang heeft tot welke data, en onder welke jurisdictie.

1.3 Scenario-analyse

Ook op korte termijn kan de financiële sector worden geconfronteerd met gebeurtenissen waarbij afhankelijkheden van derde partijen voor problemen voor financiële instellingen zorgen. Sommige negatieve scenario's zijn extreem, maar niettemin plausibel. Ze hebben een kleine kans maar een grote impact en kunnen zich in een kort tijdbestek manifesteren (zie figuur 2). Zo is het niet ondenkbaar dat belangrijke IT-leveranciers van financiële instellingen door overheden gedwongen worden hun dienstverlening te staken (scenario 'Geopolitieke sancties'). Ook kunnen die leveranciers slachtoffer worden van hybride aanvallen, die indirect de financiële sector raken (scenario 'Hybride aanval'). Deze scenario's kunnen leiden tot grote problemen binnen en buiten de financiële sector. Hoewel het handelingsperspectief op dat moment beperkt is kunnen er wel mitigerende maatregelen worden getroffen die instellingen helpen om zich op een dergelijke crisissituatie voor te bereiden. Voorbeelden zijn de samenwerking versterken door het delen van informatie, gezamenlijke oefeningen en het gezamenlijk ontwikkelen van dreigingsscenario's.

Figuur 2 Snelle disruptieve scenario's

Geopolitieke sancties

Essentiële derde partijen mogen ineens geen diensten meer leveren.
Gevolg: massale uitval van financiële dienstverlening. Vanwege het tekort aan uitwijkmogelijkheden naar EU-datacenters lukt het niet om de kernapplicaties van financiële instellingen blijvend te ondersteunen. Voor het merendeel van de applicaties is geen direct alternatief.

Mogelijke maatregelen nu

Omkeer: start direct een transitie naar Europese 'soevereine cloud'-oplossingen, die een 'minimal viable organisation' ondersteunen.
Harmoniseer: initieer en participeer, in een EU-platform voor standaardisatie en harmonisatie van IT-diensten.
Formaliseer: leg de samenwerking intra-EU vast. Maak duidelijk welke IT-diensten geleverd worden, en wie garant staat.

Hybride aanval

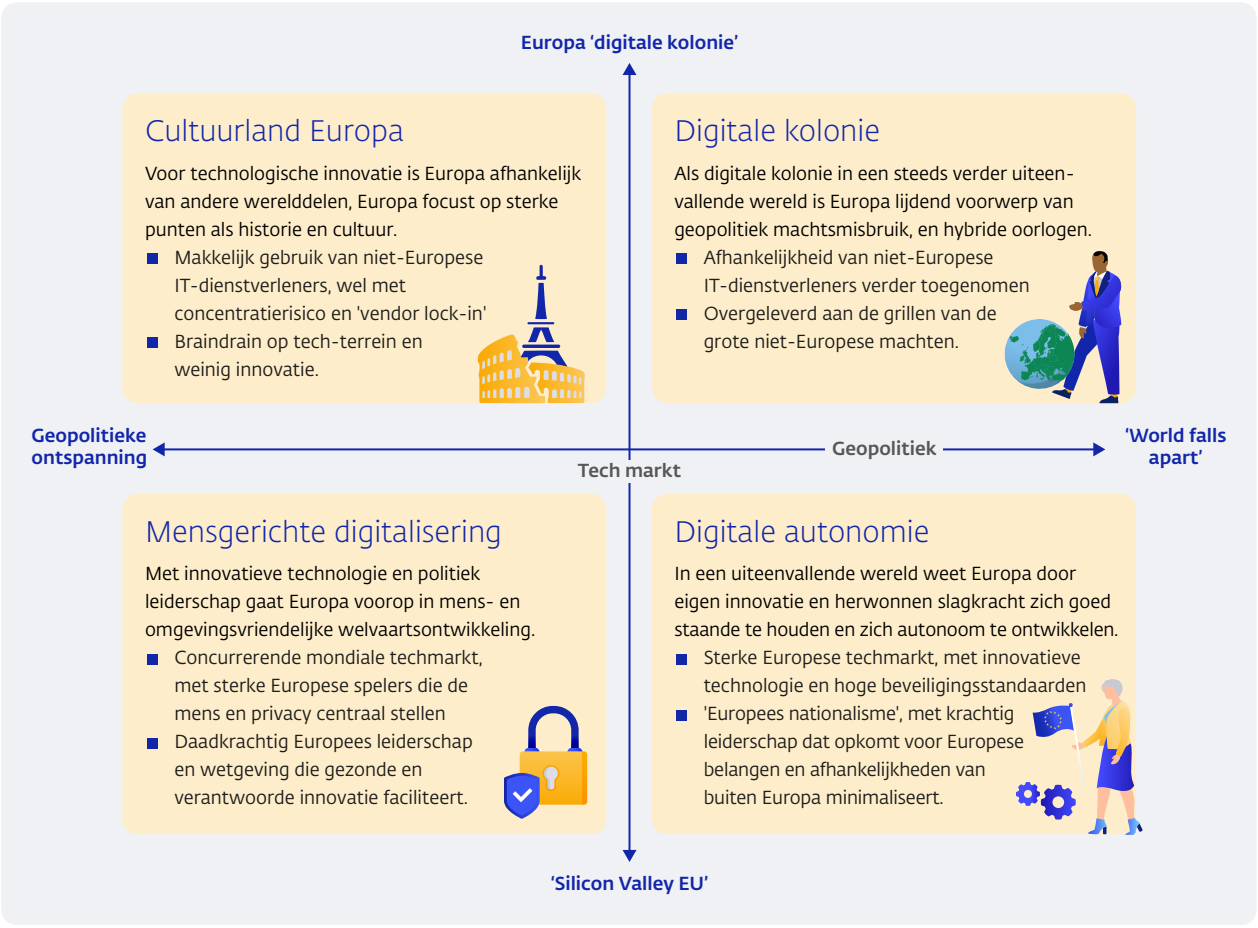
Intensieve aanval gericht op ontwrichting, door statelijke actor. Cyberaanvallen en fysieke schade aan kritieke infrastructuur, bijvoorbeeld aanvallen op nutsvoorzieningen. Hierdoor uitval van kritieke technologieleveranciers.
Gevolg: kritieke processen van financiële instellingen vallen uit.

Mogelijke maatregelen nu

Samenwerking: informatie delen over dreigingen, gezamenlijk oefenen met leveranciers (ketentesten).
Ontwikkelen dreigingsscenario's: overkoepelende dreigingsscenario's, met overeenkomstige mitigerende maatregelen.
No-IT situatie: voorbereiden op een situatie zonder IT – haalbaarheid alternatieve verwerkingsmethoden in kaart brengen.

Op de langere termijn kunnen ontwikkelingen uitmonden in uiteenlopende scenario's. De geopolitieke fragmentatie kan geleidelijk verder doorzetten, waarbij het van de slagkracht van Europa afhangt hoe digitale afhankelijkheden zich ontwikkelen. Maar ook een terugkeer naar een situatie met minder geopolitieke spanningen kan niet worden uitgesloten. Ook de markt voor IT-dienstverlening kan zich op uiteenlopende manieren ontwikkelen. Niet-Europese spelers kunnen dominant blijven, ook ten aanzien van nieuwe technologieën zoals AI en in de verdere toekomst quantum computing. Maar het kan ook zijn dat de Europese techindustrie, bijvoorbeeld juist onder druk van negatieve korte-termijnscenario's, zich opricht en op lange termijn Europese techpartijen zich tot sterke spelers ontwikkelen. Zie figuur 3 voor de scenario's die zich aldus op lange termijn kunnen ontvouwen.

Figuur 3 Afhankelijkheidsscenario's op lange termijn



Uit de scenario-analyse komt naar voren dat een sterkere Europese techsector nodig is.
Als de geopolitieke situatie verder verslechtert zal Europa zonder een eigen ontwikkelde techsector een speelbal worden van de grillen van de andere machtsblokken ('Digitale kolonie'). Door het zich richten op een sterke eigen techsector kan Europa de digitale afhankelijkheden verminderen zodat de financiële sector minder kwetsbaar wordt voor disruptieve gebeurtenissen ('Digitale autonomie'). Als geopolitieke spanningen zijn afgenomen maar de Europese techsector onderontwikkeld blijft, blijven digitale afhankelijkheden van niet-Europese partijen in de financiële sector groot of nemen deze zelfs verder toe, bijvoorbeeld op het gebied van AI. De Europese economie kan zich op andere terreinen focussen ('Cultuurland Europa'). Europa blijft dan wel in een afhankelijke positie, die nadelig is wanneer in een verdere toekomst de geopolitieke situatie alsnog weer verslechtert. In een scenario waarin zich wel een sterke en innovatieve Europese techmarkt ontwikkelt kan die 'Europese waarden' zoals privacy en inclusiviteit incorporeren ('Mensgerichte digitalisering'). De Europese financiële sector heeft dan de keuze om Europese alternatieven te gebruiken, en kan daarmee de afhankelijkheid van niet-Europese partijen verminderen. Om in de scenario's waarin de kwetsbaarheid voor disrupties is verminderd en een grotere mate van digitale autonomie wordt bereikt te komen zijn wel inspanningen van de publieke en private sector nodig. Hier wordt in de volgende hoofd-stukken op ingegaan.

2 Risicobeheersing bij financiële instellingen en leveranciers

Zowel financiële instellingen als leveranciers zijn zich bewust van de risico's die gepaard gaan met de kritische afhankelijkheid van niet-Europese techbedrijven. In het kader van dit rapport spraken we met verschillende financiële instellingen zoals banken, verzekeraars, betaaldienstverleners en vermogensbeheerders over hoe zij omgaan met de risico's van de afhankelijkheden op technologisch gebied. Daarnaast spraken we met diverse leveranciers, van BigTechs tot gespecialiseerde digitale beveiligingsbedrijven. Ook zij hebben de laatste tijd fors ingezet op maatregelen om de afhankelijkheidsrisico's, met name op geopolitiek gebied, te beheersen. In dit hoofdstuk gaan we nader in op de beheersmaatregelen die instellingen (2.1) en leveranciers (2.2) nemen.

2.1 Financiële instellingen zijn zich bewust van afhankelijkheidsrisico's

Instellingen geven om te beginnen aan dat de concentratie bij hyperscalers deels onvermijdelijk is, omdat Europese alternatieven van dezelfde kwaliteit op veel terreinen vooralsnog ontbreken. Er zijn bijvoorbeeld wel Europese clouddienstverleners, maar die kunnen momenteel niet concurreren met hyperscalers: ze leveren de basale clouddiensten, maar missen de geavanceerdere functionaliteiten en de schaal. De hyperscalers bieden wereldwijde dekking met directe schaalbaarheid, een grote mate van redundantie[6], een hoog niveau van beveiliging, toegang tot geavanceerde databasetechnologie en analyse-instrumenten. Ook worden via hun platforms veel innovatieve diensten van andere derde partijen aangeboden. Factoren als een tekortschietend innovatie- en investeringsklimaat, de fragmentatie van de markt en effecten van belemmerende regelgeving, dragen eraan bij dat Europa op dit vlak nog niet concurrerend is.[7]

Instellingen kiezen bewust voor de Amerikaanse hyperscalers vanwege de voordelen die zij bieden, maar beseffen dat daarmee nieuwe kwetsbaarheden ontstaan. Bestuurders en IT-riskmanagers van financiële instellingen geven aan dat zij de risico's van deze afhankelijkheden op het netvlies hebben. Zij zien een duidelijk trade-off: moderne cloud- en softwarediensten leveren schaalvoordelen, innovatie en flexibiliteit op, maar leiden ertoe dat IT-ondersteuning voor kritieke processen buiten de eigen instelling komt te liggen. Tegelijkertijd verschuift de macht over de IT-infrastructuur steeds meer naar deze externe partijen: meerdere grote aanbieders bewegen zich "steeds hoger in de technologie stack". Ze leveren naast basisonderdelen ook platform- en softwarediensten en dringen daarmee dieper door in de haarvaten van de bedrijfsvoering van financiële instellingen.

Instellingen zijn zich ervan bewust dat dit hun operationele afhankelijkheid steeds verder vergroot en maken daarom bij elke uitbestedingsbeslissing een afweging. Extra diensten afnemen van een clouddienstverlener kan functioneel aantrekkelijk zijn en betere beveiliging bieden, maar versterkt de 'vendor lock-in'. Instellingen streven ernaar lock-in te beperken door het gebruik van open standaarden en containerisatie, waarmee ze de workloadportabiliteit vergroten en applicaties eenvoudiger kunnen verplaatsen indien nodig. Containerisatie houdt in dat softwaretoepassingen worden

6 Redundantie is het inzetten van extra capaciteit om uitval op te vangen en de beschikbaarheid en continuïteit van diensten te waarborgen.

7 Zie hiervoor uitgebreid The Draghi report on EU competitiveness.

verpakt in geïsoleerde, overdraagbare (virtuele) containers, waardoor ze onafhankelijk van de onderliggende IT-infrastructuur overal kunnen draaien. Sommige partijen geven aan dat voor latency-gevoelige transacties en data, waarvoor een snelle reactietijd nodig is tussen het moment dat de opdracht wordt gegeven en het moment dat het resultaat bekend is, zoals bijvoorbeeld handelsdata, veelal geen gebruik wordt gemaakt van de cloud maar van eigen 'on-premises' systemen.

De afhankelijkheden op het gebied van generatieve AI lijken op dit moment nog niet zo groot, maar dat kan snel veranderen. Veel financiële instellingen gebruiken generatieve AI-tools om het werk efficiënter te maken. Deze AI-toepassingen worden vooralsnog vooral ingezet als hulpmiddel voor medewerkers. Instellingen geven aan dat ze hooguit enigszins aan efficiëntie zouden verliezen als op dit moment een generatieve AI-tool zou wegvallen. Tegelijkertijd zal deze tooling in de toekomst waarschijnlijk net zo onmisbaar worden als andere technologie. Om een sterke afhankelijkheid van niet-Europese leveranciers te voorkomen, wordt ook bewust gekeken naar Europese leveranciers, al zijn die er nog maar in beperkte mate. Het is dan wel van belang dat die zich in de nabije toekomst verder gaan ontwikkelen.[8]

Instellingen kiezen voor meerdere toeleveranciers waar dat kan. Hoe hoger in de 'technologie stack', hoe vaker men afhankelijk is van één leverancier. Voor de levering van hardware kan men relatief makkelijk kiezen voor twee leveranciers, en gebeurt dit ook. Voor cloud kiest men in de praktijk vaak één primaire leverancier. Een enkele instelling hanteert een 'dual-vendor'-strategie voor cloud, waarbij workloads snel van de ene naar de andere aanbieder kunnen worden overgezet. Dat vermindert de afhankelijkheid aanzienlijk. Andere instellingen hebben een dergelijke strategie niet of weer losgelaten. Hoewel een multicloud-strategie in theorie wel een uitweg biedt bij problemen, is dit door de complexiteit en de kosten voor veel instellingen lastig of niet haalbaar. Een aantal grotere instellingen gebruikt wel meerdere clouddienstverleners, maar voor verschillende toepassingsgebieden. Workloads snel van de één naar de ander overzetten kan dan niet, maar het spreidt wel de afhankelijkheid en vergroot de onderhandelingsruimte. Andere, vaak kleinere, instellingen kiezen één primaire clouddienstverlener en hebben bijvoorbeeld een beperkte uitwijkmogelijkheid achter de hand gehouden in een datacenter of private cloudomgeving. Redundantie wordt met name binnen één leverancier gerealiseerd, bijvoorbeeld door IT-systemen over meerdere datacenterregio's van dezelfde clouddienstverlener te spreiden.

Overstappen (of in sommige gevallen "terug") naar eigen datacenters of co-locatie ('on-premises') beschouwen veel instellingen niet als een realistische strategie. Met name de complexiteit en kosten om een 'on-premises' datacenteromgeving tegen moderne cyber-aanvallen te wapenen zijn hoog, en veel organisaties hebben niet meer de expertise in huis om dit goed te doen. Bovendien zijn de afhankelijkheden bij het gebruik van eigen datacenters niet weg: ook dan is men afhankelijk van bijvoorbeeld hardware en zeekabels. Om deze redenen leggen instellingen de focus op het beheersen van risico's binnen het werken met

8 Er zijn nu veel ontwikkelingen op dit terrein. Zie bijvoorbeeld ASML, Mistral AI enter strategic partnership, Nebul at the NVIDIA GTC 2025, en beleidsmatig vanuit de Europese Commissie: AI Continent – new cloud and AI development act.

externe partijen, in tegenstelling tot het vermijden van alle afhankelijkheden, want dat lijkt op dit moment onrealistisch.

Financiële instellingen doen aan intensief risicomanagement om de risico's van afhankelijkheid te beheersen, bijvoorbeeld door scenario-analyses te doen. Voor financiële instellingen vormen technologische afhankelijkheidsrisico's een vast onderdeel van hun risicobeheersing. Deze risico's komen expliciet terug in periodieke risicoanalyses en in strategische IT-plannen. Zo analyseren financiële instellingen verschillende scenario's: wat als een belangrijke provider langdurig uitvalt of bepaalde diensten niet langer levert? Instellingen hanteren dit soort scenario's om maatregelen voor te bereiden. Zij zijn ook bereid om scenario's en inzichten uit deze exercities waar mogelijk met elkaar te delen, en doen dit soms al. Hoewel mitigerende maatregelen lastig zijn, heeft het doordenken van ontwrichtende scenario's wel toegevoegde waarde om het dan resterende handelingsperspectief in kaart te brengen.

Ook brengen financiële instellingen in kaart met welke onderaanbieders en ketenpartijen hun primaire leveranciers werken, zoals DORA vereist (zie ook hoofdstuk 3). Die inzichten maken het (voor grote financiële instellingen) mogelijk om bijvoorbeeld in contracten met grote IT-leveranciers voorwaarden op te nemen over diversiteit in toeleveringsketens, of door recht van audit te bedingen om te kunnen controleren hoe een leverancier zijn eigen continuïteit en veiligheid waarborgt.

Daarnaast zijn er exit-plannen en business-continuïteitsplannen aanwezig voor kritieke derde partijen. In zulke plannen is beschreven hoe men zou overschakelen als één technologieleverancier uitvalt. Zo'n plan voorziet bijvoorbeeld in het overzetten van workloads naar een andere omgeving, binnen een bepaalde tijdsperiode. De mate waarin deze plannen realistisch zijn hangt af van het toepassingsgebied. Het wegvallen van een grote clouddienstverlener zou zeker grote problemen opleveren, terwijl voor meer specialistische diensten sneller op alternatieven kan worden overgestapt, mits die beschikbaar zijn. Soms kan in noodgevallen mogelijkerwijs sneller worden overgestapt dan exit-plannen aangeven, omdat men in crisistijd bereid zal zijn normale procedures en governance los te laten om de bedrijfsvoering zo snel mogelijk te herstellen. Financiële instellingen testen deze plannen ook periodiek om te beoordelen of herstel inderdaad mogelijk is. Op basis van de uitkomsten van deze tests worden de plannen indien nodig vervolgens weer aangepast.

Een scenario waarin meerdere grote IT-dienstverleners tegelijkertijd onbeschikbaar zijn voor Europa, bijvoorbeeld door een geopolitiek conflict, is veel lastiger op te vangen en valt buiten de meeste plannen. Dit is een scenario met een heel kleine kans, maar wel een extreem grote impact. Het economisch belang van de levering van technologiediensten aan Europa is groot. Dit zal inzet als geopolitiek wapen ontmoedigen, maar sluit het niet geheel uit. Financiële instellingen houden ook rekening met een realistischer scenario waarin één bedrijf of een kleine groep personen bij wijze van sanctie wordt uitgesloten van dienstverlening, vergelijkbaar met de situatie zoals die zich voordeed bij het faillissement van

de Amsterdam Trade Bank.[9] Instellingen proberen proportioneel met dit soort scenario's om te gaan; ze maken een afweging van voor- en nadelen, en kiezen ervoor om niet alle voordelen mis te lopen.

In hun risico-inschatting relativeren instellingen ook het risico voor een enkele instelling: een storing bij een hyperscaler zou een systeembrede impact hebben, en daarmee niet alleen de instelling maar ook hun klanten treffen. Het maakt uit of een financiële instelling als enige wordt geraakt door een storing, of dat de hele sector en hun klanten worden getroffen. De uitval van een toonaangevende clouddienstverlener treft zoveel bedrijven tegelijk dat het voor geen enkele individuele instelling een uniek probleem oplevert. Tegelijkertijd zou dit laatste scenario betekenen dat de maatschappelijke en economische ontwrichting groot is. Wanneer dit zich voordoet is een gecoördineerde aanpak noodzakelijk, waarbij naast de financiële instellingen en hun IT-leveranciers, ook de overheid en toezichthouders betrokken worden.

De sector zoekt daarom actief samenwerking en kijkt naar de AFM en DNB voor sturing bij het beperken van externe IT-risico's en het op termijn verminderen van afhankelijkheden. Vrijwel alle financiële partijen benadrukken het belang van kennisuitwisseling en gezamenlijke voorbereidingen om afhankelijkheidsrisico's te beheersen. Zij pleiten ervoor om scenario's en best practices op het gebied van derde partij risico's met elkaar te delen, omdat iedereen uiteindelijk tegen dezelfde problemen aanloopt en met dezelfde leveranciers te maken heeft. Een significant deel van de geïnterviewden stelt dat de AFM en DNB een faciliterende rol kunnen spelen en samenwerking kunnen organiseren om afhankelijkheden te managen. Met name clouddiensten worden gezien als een 'commodity' die prima Europees ontwikkeld kunnen worden. Het bereiken van schaal is daarbij eerder een knelpunt dan de beschikbaarheid van investeringskapitaal. Gezamenlijk kan hier meer worden bereikt. DNB en AFM zouden dit kunnen faciliteren, in een sfeer van "community building". Ook zouden DNB en AFM gezamenlijke ketentesten kunnen coördineren, waarin financiële instellingen en hun belangrijkste IT-leveranciers een scenario oefenen. De behoefte aan publiek-private samenwerking is groot.

Tegelijkertijd willen de instellingen dat Europese regels en normen pragmatisch blijven: de roep is om te focussen op wat écht nodig is. Sommige instellingen signaleren dat DORA prikkels geeft die kunnen leiden tot meer concentratie van dienstverleners. Zo hebben zij ervaren dat kleine IT-leveranciers afhaken als leverancier voor de financiële sector omdat ze niet aan alle DORA-eisen willen of kunnen voldoen. Hierdoor bestaat het risico dat grote bestaande IT-leveranciers nog dominanter worden. Ook merken instellingen dat DORA prikkels geeft om minder leveranciers te gebruiken, dus om diensten van één leverancier af te nemen in plaats van veel verschillende: "hoe minder aanbieders, hoe minder papierwerk". Dit is niet bevorderlijk voor de diversiteit, en daarmee voor de weerbaarheid. DORA en andere wetgeving zou volgens instellingen flexibel en proportioneel moeten worden toegepast, afgestemd op verschillende typen instellingen en gericht op de praktijk. Ongewenste neveneffecten moeten worden beperkt, bijvoorbeeld door uitvragen te standaardiseren. Ook moeten er duidelijke

9 Brief DNB over faillissement ATB aan minister van Financiën

definities gebruikt worden, waardoor verschillende interpretaties worden voorkomen. De AFM en DNB kunnen zich hier goeddeels in vinden.

2.2 Leveranciers ontplooien initiatieven om afhankelijkheidsrisico's te beperken

Grote technologieleveranciers beseffen dat de financiële sector in hoge mate van hen afhankelijk is en nemen maatregelen die erop gericht zijn de soevereiniteit te vergroten. Sommige leveranciers ervaren druk vanuit hun klanten om maatregelen te nemen. Vooral hun klanten uit de financiële sector, de defensie-industrie en andere sectoren waar beschikbaarheid en dataveiligheid cruciaal zijn, stellen steeds vaker vragen over geopolitieke risico's. Zij eisen, mede door de inwerkingtreding van DORA, contractuele garanties met betrekking tot beschikbaarheid, exit-mogelijkheden en auditrechten. Leveranciers spelen hierop in en zoeken actief naar manieren om het vertrouwen van hun klanten in dataveiligheid te versterken.

Een aantal clouddienstverleners biedt financiële instellingen de mogelijkheid om hun diensten in Europa via aparte juridische entiteiten af te nemen, aangeduid als Europese 'soevereine cloud'-oplossingen. De precieze invulling verschilt per leverancier, maar in het algemeen zetten clouddienstverleners daarbij structuren op die operationeel en juridisch onder Europese jurisdictie vallen en in dat opzicht zoveel als mogelijk zijn gescheiden van het moederbedrijf buiten Europa. Data, dienstverlening en beheer vallen onder Europese wet- en regelgeving, bijvoorbeeld door het inrichten van Europese dochterondernemingen, het aanstellen van lokale teams en het implementeren van governance-maatregelen die gericht zijn op het minimaliseren van de invloed van niet-Europese regelgeving. In sommige gevallen is zelfs contractueel vastgelegd dat sleutelfunctionarissen geen instructies mogen aannemen van buiten de EU. Het is hierbij belangrijk dat alle data binnen de EU-grenzen blijven en uitsluitend worden beheerd door Europese teams. Voorbeelden van de vormen waarin 'soevereine cloud'-oplossingen door clouddienstverleners worden aangeboden zijn: het lokaal bij de financiële instelling draaien van workloads ondersteund door cloudinfra-structuur, samenwerking met Europese partners voor het leveren van clouddiensten, volledig gescheiden cloudregio's binnen Europa, en geïsoleerde cloudomgevingen die tijdelijk autonoom functioneren in een lokaal datacenter, zonder internetverbinding of tussenkomst van de leverancier. Hoewel deze oplossingen vooral worden ingezet in sectoren als defensie, nationale veiligheid en overheden, groeit ook de interesse vanuit de financiële sector hiervoor. Wel gaan dergelijke vormen veelal gepaard met enige beperkingen in resilience en functionaliteit, en met hogere kosten.

Deze 'soevereine' oplossingen zijn bedoeld om het vertrouwen te geven dat niet-Europese (statelijke) actoren en besluitvormers geen invloed kunnen uitoefenen op de werking van de diensten. De juridische, operationele en organisatorische schotten zijn erop gericht om druk van buitenaf te weerstaan, bijvoorbeeld bij verzoeken om toegang tot data via buitenlandse wetgeving of bij geopolitieke incidenten ("red-button scenario"). Clouddienstverleners stellen dat zij in zulke gevallen juridische stappen zullen ondernemen om dergelijke verzoeken af te wijzen. Er dient nog te worden vastgesteld in hoeverre de getroffen maatregelen daadwerkelijk effectief bescherming bieden tegen potentiële invloed van niet-Europese actoren.

Clouddienstverleners vergroten de controle van hun klanten over hun data door ze de mogelijkheid te geven het beheer van de encryptiesleutels in eigen handen te nemen. Met deze sleutels wordt de aan de dienstverleners toevertrouwde informatie versleuteld. De betreffende leveranciers faciliteren het gebruik van het door klanten beheren van encryptiesleutels, wat betekent dat hun afnemers hun sleutels zelf beheren en veilig opbergen in hun eigen hardware-beveiligingsmodules ('hardware security module', HSM), in plaats van dat over te laten aan de dienstverleners. Uitbesteden van de HSM-diensten aan een gespecialiseerde dienstverlener is hierbij een alternatief. Door het 'uitplaatsen' van het sleutelmateriaal heeft de clouddienstverlener geen ongeautoriseerde toegang tot het sleutelmateriaal van zijn afnemers en kunnen de betreffende data niet in ontsleutelde vorm onvrijwillig worden overgedragen aan een niet-Europese actor. Het brengt echter wel met zich mee dat instellingen zelf verantwoordelijk zijn voor het genereren, beveiligen en niet kwijtraken van de sleutels. De complexiteit en het afbreukrisico hiervan zijn groot. Bovendien beschermt deze maatregel uitsluitend de privacy van de data, zoals de onderhevigheid aan de CLOUD Act. Voor risico's als onbeschikbaarheid van diensten, corruptie of verlies van data biedt deze maatregel geen bescherming.

Clouddienstverleners bieden een hoge mate van continuïteit om hun diensten zo betrouwbaar mogelijk te maken. Grote clouddienstverleners weten dat uitval grote gevolgen heeft, en besteden daarom veel aandacht aan het voorkomen daarvan en het snel kunnen herstellen als er toch iets misgaat. Cloud- en netwerkleveranciers leggen sterk de nadruk op redundantie: alle cruciale componenten (inclusief zeekabels) zijn minstens dubbel uitgevoerd en vaak verspreid over verschillende geografische locaties. Cloudleveranciers bieden uitgebreide uitwijkmogelijkheden, waarbij systemen en data bij een verstoring snel kunnen worden overgezet naar alternatieve datacenters, binnen de regio of in andere landen. Dit zorgt ervoor dat dienstverlening en beschikbaarheid ook bij grote incidenten gewaarborgd blijven. Voor financiële instellingen is het van belang dat deze uitwijkprocedures regelmatig worden getest en dat er duidelijke afspraken zijn over de maximale hersteltijd en het behoud van data-integriteit. De grote clouddienstverleners hebben doorgaans een (veel) hogere mate van redundantie ingebouwd dan individuele financiële instellingen zelf zouden kunnen bereiken. Ze stellen dan ook dat de kans op volledige uitval van hun dienstverlening door een storing niet waarschijnlijk is, gezien de robuustheid van hun infrastructuur. Bovendien doen ze continuïteitstesten om voorbereid te zijn op noodgevallen.

Clouddienstverleners bieden mogelijkheden voor workload-portabiliteit als open standaarden, containertechnologie en multicloud-architecturen. Migratie van kritische IT-workloads tussen clouddienstverleners blijft echter complex en vereist diepgaande kennis, afstemming en aandacht voor continuïteit. Een focus op open standaarden, open source software en interoperabiliteit kan bijdragen aan een hogere portabiliteit van workloads. Tegelijkertijd geldt: hoe intensiever een financiële instelling gebruikmaakt van het brede aanbod aan PaaS- en SaaS-diensten van een bepaalde clouddienstverlener – en profiteert van voordelen zoals snelle ontwikkeling, minder beheerlast en geen zorgen over onderliggende infrastructuur – hoe beperkter de portabiliteit van workloads wordt. Dit vraagt om een zorgvuldige balans,

waarbij het risico bestaat dat risico's met een kleine kans en lange-termijnoverwegingen te weinig gewicht krijgen.

De maatregelen van niet-Europese leveranciers dragen bij aan het beperken van geopolitieke risico's rond beschikbaarheid en dataveiligheid, maar kunnen deze risico's niet uitsluiten. Zowel financiële instellingen als de niet-Europese technologiebedrijven zelf erkennen dat ondanks alle maatregelen die ze nemen er risico's blijven bestaan. Zo is de afhankelijkheid niet weg: instellingen zijn ondanks de maatregelen nog steeds aangewezen op externe leveranciers voor de levering van IT-diensten ter ondersteuning van kritieke processen. Maatregelen van leveranciers zijn vooral gericht op het vergroten van de soevereiniteit van hun klanten, en begrijpelijkerwijs minder op het verkleinen van de 'vendor lock-in'. Als tegenwicht hiervoor kan een financiële instelling bewust kiezen voor een grote mate van portabiliteit van workloads. De daadwerkelijke uitwijkmogelijkheden bij langdurige uitval blijven echter beperkt: overschakelen naar een ander platform of een eigen omgeving blijft tijdrovend en complex.

3 Toezicht en beleid

Versterking van de digitale weerbaarheid en digitale autonomie binnen de financiële sector krijgen in toenemende mate aandacht van wetgevers en toezichthouders. Geopolitieke spanningen hebben de kans op ontwrichtende scenario's aanzienlijk vergroot, en financiële instellingen en autoriteiten moeten daarop zo goed mogelijk voorbereid zijn. Voor de langere termijn is het van belang te streven naar vermindering van de afhankelijkheid van niet-Europese IT-dienstverleners en vergroting van de digitale autonomie. Dit hoofdstuk opent met een typering van de bestaande wet- en regelgeving die raakt aan digitale autonomie, waarbij duidelijk wordt dat deze kaders niet altijd toereikend zijn om de risico's van afhankelijkheid goed te beheersen en hiermee samenhangend de digitale autonomie te vergroten (3.1). Vervolgens doen AFM en DNB in dit hoofdstuk suggesties voor vervolgacties om de weerbaarheid te vergroten en om met een gecoördineerde Europese aanpak digitale afhankelijkheden te verkleinen en zo de grip op kritieke digitale processen te versterken (3.2).

3.1 Bestaande regelgeving en structuren

De EU-regelgeving gericht op de beheersing van IT- en derde-partijenrisico's is in de afgelopen periode versterkt. Voor de financiële sector gaat het met name om de in januari 2025 van toepassing geworden Europese DORA-verordening. DORA geldt voor de financiële sector in Europa en heeft als doel het versterken van de digitale weerbaarheid van financiële instellingen. De AFM en DNB houden toezicht op de naleving van DORA.

Een belangrijk onderdeel van DORA richt zich op het beheersen van de risico's die verbonden zijn aan het afnemen van IT-diensten van derde partijen. Uitgangspunt is daarbij dat financiële instellingen die diensten van derde partijen afnemen te allen tijde eindverantwoordelijk blijven voor de financiële diensten die zij verlenen. DORA stelt eisen aan contracten met derde partijen, waarbij onder andere specifiek aandacht wordt gevraagd voor exit-strategieën en het borgen van de continuïteit van de IT-dienstverlening die kritieke financiële diensten ondersteunt. Daarbij schrijft DORA voor dat instellingen in hun risicoanalyses rekening houden met het risico van beperkende maatregelen zoals embargo's en sancties, die van invloed kunnen zijn op het vermogen van de aanbieder om de diensten te verlenen of de instelling om die te ontvangen. Aanvullend bevat DORA voorschriften voor de inrichting van de informatiebeveiliging. Deze gelden voor zowel de eigen dienstverlening als voor de IT-diensten die derde partijen leveren. Ook het periodiek uitvoeren van weerbaarheidstesten, waaronder ethische hacktesten, vormt een belangrijk onderdeel van DORA.

Wanneer sprake is van derde partij afhankelijkheden dan moeten financiële instellingen onder DORA niet alleen kijken naar partijen met wie zij directe contracten hebben afgesloten, maar ook naar contracten die deze derde partijen op hun beurt hebben afgesloten met derde partijen. Financiële instellingen zijn op grond van DORA verplicht om een register bij te houden dat informatie bevat over de gehele keten van leveranciers van IT-diensten (zogeheten DORA 'Registers of Information'). De verwachting is dat instellingen het informatieregister gebruiken als middel om hun eigen concentratierisico's en afhankelijkheden goed in kaart te brengen. Deze registers worden gebruikt door de drie Europese

financiële toezichtautoriteiten (EBA, EIOPA en ESMA) om op Europees niveau de IT-leveranciers te identificeren die het meest kritiek zijn, onder andere gebaseerd op hun systeemimpact en het aantal kritieke financiële instellingen waaraan ze IT-diensten verlenen. De AFM en DNB zullen de registers ook gaan analyseren om voor hun toezicht op de Nederlandse financiële sector meer inzicht te krijgen in de afhankelijkheden van instellingen, en in mogelijke concentratierisico's.

De meest kritieke IT-leveranciers op Europees niveau worden op grond van DORA onder een oversightkader gebracht. Deze IT-dienstverleners zullen daarmee vanaf 2026 onder een vorm van direct Europees toezicht komen te staan. Het oversight richt zich op de beoordeling van het beheer van de IT-risico's die samenhangen met het gebruik van deze dienstverleners door financiële instellingen. Wanneer nodig kunnen de toezichthouders ('overseers') inspecties verrichten en aanbevelingen uitvaardigen. Wanneer een kritieke IT-leverancier deze aanbevelingen niet opvolgt kunnen financiële instellingen in het uiterste geval worden verplicht het gebruik van een dienst van de betreffende IT-dienstverlener te staken.

Voor instellingen die niet onder DORA vallen gelden andere raamwerken die beogen risico's van het gebruik van IT-dienstverleners te beperken. Voor een beperkt aantal van deze instellingen, die niet onder direct toezicht van de AFM of DNB vallen, geldt dat ze onder oversight staan van DNB als centrale bank. Hiervoor gelden internationale standaarden: de Principles for Financial Market Infrastructures (PFMI) en, binnen de EU, de hiervan afgeleide Payment Instruments, Schemes and Arrangements (PISA). Omdat deze standaarden en vereisten relatief hoog over zijn beschreven geven in de praktijk instellingen hieraan invulling met de vereisten vanuit DORA.

Voor bepaalde financiële ondernemingen, zoals afwikkelondernemingen en 'basic' verzekeraars, die eveneens niet onder DORA vallen, stelt de Wet op het Financieel Toezicht eisen aan de inrichting van de bedrijfsvoering, waaronder het beheersen van uitbestedingsrisico's. Ondernemingen moeten aantoonbaar beschikken over een beheerste en integere bedrijfsvoering, inclusief functiescheiding en risicobeheersing.

Naast regelgeving specifiek voor de financiële sector is er in Europa ook bredere regelgeving die raakt aan digitale weerbaarheid en de rol van grote IT-leveranciers. Sinds september 2025 is in Europa de Data Act van kracht, met toezicht door de Autoriteit Consument en Markt (ACM). Deze verordening heeft onder meer tot doel de interoperabiliteit van de dataverwerkingsdiensten van clouddienstverleners te bevorderen. Hiermee worden drempels voor het overstappen naar een andere IT-leverancier verlaagd, en wordt de mogelijkheid gecreëerd om stapsgewijs bepaalde dienstverlening bij een andere IT-leverancier te plaatsen. Deze bepalingen in de Data Act kunnen daarmee bijdragen aan vermindering van 'vendor lock-in' situaties. Op het terrein van informatiebeveiliging is de Network and Information Security Directive 2 (NIS2) van kracht (met als toezichthouder de Rijksinspectie Digitale Infrastructuur, RDI). NIS2 is gericht op het verhogen van de digitale weerbaarheid van een groot aantal verschillende sectoren waaronder een aantal verschillende typen financiële instellingen. Voor de bescherming van persoonsgegevens is er de AVG (toezichthouder Autoriteit Persoonsgegevens, AP), die ook regels bevat voor situaties waarbij opslag en verwerking door derde partijen wordt uitgevoerd. Ook stelt de AVG strikte voorwaarden aan de doorgifte van persoonsgegevens buiten de EU. De verschillende betrokken toezichthouders werken nauw samen.

Europese en nationale wetgeving wordt verder ingevuld door diverse financieel toezichthouders, zoals de EBA, EIOPA, ESMA en de ECB, met aanvullende richtlijnen, frameworks, toolkits en Q&A's. Deze zijn bedoeld om financiële instellingen te ondersteunen bij het beheerst inzetten van IT-diensten, waaronder clouddiensten. Een voorbeeld is de ECB Guide on Outsourcing Cloud Services. De Nederlandse beroepsvereniging voor IT-auditors heeft de International Digital Reporting Standards (IDRS) ontwikkeld. Deze standaard heeft tot doel tot een eenduidige manier te komen waarop organisaties kunnen rapporteren inclusief het afleggen van verantwoording over hoe ze hun digitale processen en IT-risico's beheersen.

Hoewel de huidige regelgeving en aanvullende guidance een belangrijke bijdrage leveren aan het beheersen van risico's rond derde partijen, blijven er kwetsbaarheden bestaan. De concentratie bij een beperkt aantal IT-leveranciers en het gevaar van 'vendor lock-in' zijn met de bestaande kaders nog onvoldoende te beheersen. Dit geldt niet alleen voor de afhankelijkheid van veelal niet-Europese partijen, maar ook voor potentiële Europese alternatieven. Doordat steeds meer essentiële bedrijfsprocessen en data worden uitbesteed aan externe IT-dienstverleners verliezen financiële instellingen een deel van hun directe controle. Dit maakt hen kwetsbaar voor verstoringen als gevolg van geopolitieke spanningen, handelsgeschillen of onverwachte marktontwikkelingen, met directe impact op de betrouwbaarheid en veiligheid van hun digitale diensten. Deze risico's zijn niet louter denkbeeldig, maar vragen om concrete, structurele maatregelen. Het is daarom noodzakelijk om versneld te investeren in alternatieven die de digitale autonomie en weerbaarheid van Europa versterken, met blijvende aandacht voor het voorkomen van nieuwe concentratie- en lock-in risico's.

3.2 Mogelijkheden om de risico's van afhankelijkheden te verkleinen

Een breed pakket aan acties en maatregelen is nodig om de risico's van ontwrichtende scenario's te mitigeren en de afhankelijkheid van IT-gerelateerde derde partijen te verminderen. Sommige van deze stappen kunnen al op korte termijn worden gezet, andere vereisen meer tijd en kunnen daarom pas op langere termijn hun vruchten afwerpen. Wel is het van belang nu in actie te komen.

Op korte termijn is de sterke afhankelijkheid van niet-Europese IT-leveranciers een gegeven, en is het belangrijk dat instellingen maatregelen nemen om zich voor te bereiden op disruptieve scenario's en om waar mogelijk de potentiële impact te mitigeren. Door te voldoen aan de DORA-vereisten versterken instellingen hun digitale weerbaarheid. Daarnaast is het van belang dat instellingen zich voorbereiden op de risico's die geopolitieke ontwikkelingen met zich meebrengen. Een manier om dit te doen is door het ontwikkelen van dreigingsscenario's, en daarin samen te werken met andere instellingen en autoriteiten. Waar mogelijk is het aan te bevelen om informatie over concrete dreigingen en aanvallen binnen de sector en met autoriteiten uit te wisselen. Op basis van vergaande, maar realistische scenario's kunnen ketentesten worden uitgevoerd. Instellingen, IT-leveranciers en publieke autoriteiten kunnen samenwerken in 'real life' testen. Dit kan de basis vormen voor het nemen of versterken van mogelijke mitigerende maatregelen. Hoewel deze acties nu al plaatsvinden, is het wenselijk om geopolitieke risico's hierin nog nadrukkelijker mee te nemen, en IT-dienstverleners nog vaker te betrekken. De AFM en DNB zijn bereid verdere samenwerking op dit terrein te faciliteren.

Ook andere maatregelen kunnen al op korte termijn helpen om de effecten van negatieve scenario's te verminderen. Financiële instellingen kunnen, waar mogelijk, beginnen met het realiseren van een 'multi-vendor'-strategie. Het is van belang dat financiële instellingen helder hebben welke alternatieve leveranciers er zijn voor de ondersteuning van essentiële of belangrijke diensten. Daarnaast is het belangrijk dat financiële instellingen mogelijkheden onderzoeken voor het gebruik van open standaarden en open source-oplossingen. Dit type oplossing helpt bij het verminderen van de afhankelijkheid van specifieke leveranciers, en verhoogt de flexibiliteit van het gebruik van IT-diensten van derden. Andere technische maatregelen, zoals containerisatie maken het mogelijk om workloads flexibel te verplaatsen tussen platforms van verschillende dienstverleners en de eigen infrastructuur. Encryptie van financiële data inclusief klantgegevens met sleutels in eigen beheer versterkt, mits goed beheerd, de controle over data en draagt bij aan datasoevereiniteit.

Een aantal niet-Europese clouddienstverleners biedt 'soevereine cloud'-oplossingen aan, die de impact van bepaalde geopolitieke risico's mogelijkerwijs mitigeren. Dit roept wel de vraag op of deze oplossingen 'echt' soeverein zijn. Recent is vanuit een Europese taskforce een voorstel gedaan voor een 'sovereignty scoring system' waarmee aan de hand van criteria (juridisch, technologisch, operationeel, economisch, cultureel) kan worden bepaald of een geboden clouddienst daadwerkelijk 'soeverein' is.[10] Voor instellingen en toezichthouders kunnen deze criteria handvatten bieden om te bezien in hoeverre 'soevereine cloud'-oplossingen de afhankelijkheidsrisico's daadwerkelijk beperken. Hoewel de vraag blijft in hoeverre dergelijke oplossingen uiteindelijk standhouden, kan door het zoveel mogelijk verzelfstandigen van de Europese operaties van hyperscalers op zijn minst tijd worden gewonnen in bijvoorbeeld situaties waarin derde landen data opeisen. Die tijd kan worden benut om hetzij in het geweer te komen tegen dergelijke acties, dan wel naar alternatieve oplossingen te zoeken. Instellingen maken hierin hun eigen keuzes. Voor instellingen is het van belang dat ze kunnen uitleggen welke keuzes ze hebben gemaakt om te waarborgen dat hun data soeverein en veilig zijn.

Op langere termijn is het van belang dat Europa minder afhankelijk wordt van niet-Europese IT-aanbieders, en een grotere mate van digitale autonomie bereikt. Een sterke, autonome en innovatieve Europese techmarkt is wenselijk, zowel voor de weerbaarheid, als voor het behoud van Europese waarden zoals privacy en inclusiviteit. Het vergroten van digitale autonomie overstijgt de competenties van financiële instellingen en nationale financiële toezichthouders, en vergt actie op Europees niveau.

Om de strategische autonomie te versterken is het nodig dat de Europese digitale infrastructuur wordt versterkt. Daarvoor zullen de structurele factoren die hebben geleid tot het ontstaan van digitale afhankelijkheid moeten worden aangepakt. Het Draghi-rapport reikt hiervoor concrete handvatten aan. Onder meer gaat het om het verbeteren van het innovatieklimaat, het investeringsklimaat, stimuleren van de ondernemingscultuur en beslechten van belemmeringen door wet- en

10 Drafting European Sovereignty Criteria for Software and Digital Systems | EuroStack Directory Project. Het voorstel moet wel verder worden geoperationaliseerd om concreet toepasbaar te zijn.

regelgeving. Het Draghi-rapport wijst erop dat in Europa geen gebrek bestaat aan goede innovatieve ideeën en ambities, maar dat die onvoldoende worden omgezet in commercieel succesvolle producten en diensten. Het gemis van een voldoende innovatiestimulerend ondernemersklimaat is het grote verschil met de VS. Voor het streven naar digitale autonomie is innovatie (en alles wat nodig is om dat te ondersteunen) cruciaal. In potentie ontbreekt het volgens het Draghi-rapport niet aan investeringskapitaal. Om voldoende kapitaal te mobiliseren is een belangrijke rol weggelegd voor de door AFM en DNB ondersteunde 'spaar- en investeringsunie'. Toegang tot financiering met het oog op schaalvergroting van innovatieve ondernemingen is daarbij een belangrijk aandachtspunt.[11]

Ter vermindering van de afhankelijkheid van niet-Europese IT-dienstverleners zullen volwaardige Europese alternatieven moeten worden ontwikkeld. Financiële instellingen kunnen overwegen gebruik te gaan maken van Europese IT-leveranciers waar die beschikbaar zijn. Om kritische massa te bereiken kunnen financiële instellingen de krachten bundelen gericht op het opstellen van specificaties voor cloudtoepassingen, testen van toepassingen (door onder andere accountants en IT-auditors) en bieden van afnamegaranties. Hierdoor kan de ontwikkeling van een aantal Europese hyperscalers worden bevorderd. Wat betreft investeringen door financiële instellingen kan samenwerking borgen dat de partijen die als eerste deze stap zetten niet in het nadeel zijn ten opzichte van partijen die niet of pas later overgaan tot investeringen (en hiermee slachtoffer worden van een zogeheten 'first mover disadvantage').

Hoewel het versterken van de Europese techsector op de lange termijn kan bijdragen aan het verminderen van digitale afhankelijkheden, is dit slechts één aspect van een het bredere en complexere vraagstuk van digitale autonomie. Het aanpakken van afhankelijkheden vraagt om meer dan alleen het stimuleren van Europees aanbod. Europese leveranciers bieden niet per definitie een oplossing voor alle risico's (zoals 'vendor lock-in' en concentratierisico's); hiervoor moeten zij ook concurrerend zijn op het gebied van prijs, kwaliteit, leveringszekerheid en cybersecurity. Zonder deze randvoorwaarden kan het stimuleren van Europees aanbod zelfs leiden tot suboptimale keuzes voor financiële instellingen, bijvoorbeeld op het gebied van kwaliteit en gebruiksvriendelijkheid.

De opkomst van AI verlangt beleidsmatige aandacht om concentratierisico's in deze markt te mitigeren. AI-systemen zijn nog volop in ontwikkeling, en de afhankelijkheidsrisico's op het vlak van generatieve AI zijn nu nog niet zo groot. Er zijn ook Europese AI-systemen actief. Wel zijn factoren, zoals het ongunstige investeringsklimaat, die op andere terreinen hebben geleid tot grote afhankelijkheid van niet-Europese spelers, ook hier aanwezig. Ook op dit terrein is het stimuleren van de opkomst van echte Europese alternatieven wenselijk en zal er gewerkt moeten worden richting een schaalgrootte die zich laat meten met niet-Europese AI-diensten, om een concurrerende markt te bereiken en nieuwe 'vendor lock-ins' te voorkomen.

11 Zie hiervoor ook: Kamerbrief kabinetsinzet kapitaalmarktunie | Kamerstuk | Rijksoverheid.nl.

De AFM en DNB onderzoeken in hoeverre financiële regelgeving (waaronder DORA) en toezicht belemmeringen bevat voor het gebruik maken van Europese IT-leveranciers en innovatie. Geïdentificeerde issues kunnen aanleiding geven tot het nemen van beleidsinitiatieven in Europees verband, het aankaarten bij de wetgever, of het doorvoeren van aanpassingen in het toezicht. Dit om het voor instellingen mogelijk te maken dat soevereiniteit kan worden afgewogen ten opzichte van andere kenmerken bij de keuze van digitale dienstverlener.

Waar nodig kan regelgeving worden verbeterd. EU-wetgeving, en dan in het bijzonder de DORA-verordening, gaat uitgebreid in op de risico's die gepaard gaan met het afnemen van IT-diensten van derde partijen, maar kent ook beperkingen. Hoewel in DORA aandacht wordt gevraagd voor concentratierisico's en onder meer de risico's van sancties, is op deze punten versterking mogelijk. Ecosysteemrisico's worden niet volledig belicht onder DORA. Ook stelt DORA geen eisen aan de geografische locatie waar data ligt opgeslagen en wordt bewerkt. Dit zou kunnen worden heroverwogen. Naast het doorvoeren van verbeteringen, kan ook de reikwijdte van bestaande wetgeving worden geëvalueerd en kunnen desgewenst ook andere organisaties onder bestaande wetgeving worden gebracht. De AFM en DNB zullen de Europese toezichthouders vragen om een analyse te maken gericht op de vraag of DORA in voldoende mate bijdraagt aan de weerbaarheid tegen geopolitieke risico's, en als dit niet het geval is nadere guidance te overwegen. Het DORA oversightkader voor grote pan-Europees opererende IT-leveranciers kan de opstap zijn naar nadrukkelijker toezicht. Hoewel het huidige toezicht een goede eerste stap is, zal moeten blijken hoe effectief de mogelijkheden zijn om naleving af te dwingen.

De AFM en DNB willen de Europese beleidsmakers in overweging geven om op termijn een cross-sectorale Europese cloudtoezichthouder op te richten. Er is inmiddels een uitgebreid Europees raamwerk van regelgeving ontstaan op deelaspecten van de activiteiten van grote IT-dienstverleners. Het is voor afzonderlijke, gespecialiseerde toezichthouders lastig om op de vele verschillende activiteiten en risico's van deze partijen toe te zien. Een mogelijke oplossing hiervoor zou het vormen van een nieuwe gecentraliseerde Europese cloudtoezichthouder met een generiek cross-sectoraal mandaat kunnen zijn.[12] Zo'n toezichthouder zal een breder en sterker mandaat moeten hebben, met meer capaciteit, dan nu is geregeld via het DORA oversightkader. Deze cloudtoezichthouder zou ook mandaat kunnen krijgen op het terrein van geopolitieke risico's, om daarmee bijvoorbeeld echt soevereine cloudoplossingen te kunnen afdwingen.

AFM en DNB kunnen op nationaal niveau sectoroverstijgend contact zoeken en samenwerken met andere autoriteiten. Bij nationale autoriteiten valt te denken aan de ACM en de RDI. Door gezamenlijk op te trekken in het stimuleren van veilige, betrouwbare en soevereine digitale infrastructuur, kunnen toezichthouders invloed uitoefenen op marktontwikkelingen en technologische keuzes. Dit vereist een gedeelde visie op risico's, afhankelijkheden en publieke belangen, en kan worden vormgegeven via gezamenlijke werkgroepen, beleidsafstemming en het delen van toezichtsinzichten. Tegelijkertijd overstijgt het realiseren van digitale autonomie de

12 Zie ook DNB, Veranderend landschap, veranderend toezicht.

nationale competenties. De afhankelijkheid van niet-Europese technologieaanbieders en infrastructuur vraagt om een gecoördineerde Europese aanpak. Nationale toezichthouders kunnen wel richting geven en signalen afgeven, maar het daadwerkelijk versterken van digitale soevereiniteit vereist Europese beleidsvorming, investeringen en normstelling. Alleen door samenwerking binnen de Europese Unie kunnen structurele stappen worden gezet richting een minder kwetsbare en meer autonome digitale toekomst.

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

Volg ons op:
Instagram
LinkedIn
X

Autoriteit Financiële Markten
Postbus 11723
1001 GS Amsterdam
afm.nl

Volg ons op:
Facebook
LinkedIn
X

DeNederlandscheBank
EUROSYSTEEM

AFM