

KPMG RAAD Board Program GeoPulse

**84,75% van Nederlandse C-suite
ervaart geopolitieke impact na
aantreden Trump**



Februari 2025

kpmg.nl

Managementsamenvatting

Het Trump 2-presidentschap zorgt voor veel onrust in de wereld sinds de start op 20 januari. De toename in protectionistische maatregelen en onzekerheden over geopolitieke allianties en doelen leiden ertoe dat het niet meer *business as usual* is.



Zo ervaart **84,75%** van de ondervraagde Nederlandse C-suite een geopolitieke impact sinds het aantreden van Trump. Maar liefst **96,61%** zet zich de komende twaalf maanden schrap voor een nog grotere geopolitieke impact op de bedrijfsvoering. Hierbij worden vooral protectionistische maatregelen genoemd. Van de respondenten neemt **72,88%** maatregelen om de risico's te managen.

Dit blijkt uit de meest recente KPMG GeoPulse over geopolitieke veranderingen, deze onder Nederlandse bedrijfsleiders en commissarissen in onder meer de financiële sector en de energiesector.

Aangezien **49,15%** van de 59 respondenten afkomstig zijn van organisaties die meer dan 1.000 medewerkers kennen, geeft het resultaat een goed beeld van de impact op het Nederlandse grootbedrijf.



Van dit percentage ziet **64,41%** regiospecifieke gevaren, waaronder risico's in Oost-Azië, Oost-Europa en de VS zelf. Het grootste deel van de respondenten die in deze regio's werken, zegt dat de spanningen op het wereldtoneel invloed hebben op zijn investeringsplannen in het buitenland.

Interessant detail:

74,58% van de respondenten geeft aan dat de veranderende geopolitieke situatie invloed heeft op zijn cybersecuritybeleid.

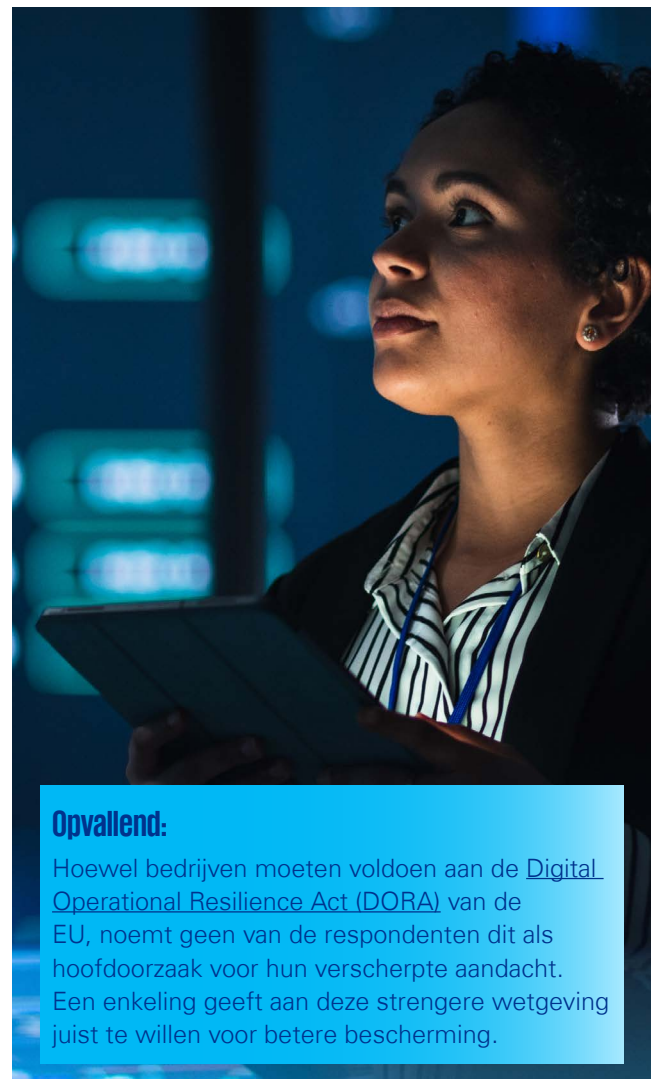
We lichten een aantal interessante zaken uit.

Focus op cybersecurity

Logisch dat de focus hierop is gericht. Allerlei (gevoelige) informatie en systemen zijn online te benaderen, en dat is iets waar naast cybercriminelen ook staatsoverheden sinds jaar en dag mee bezig zijn. [Tech Crunch](#) wijst bijvoorbeeld op de aanhoudende hacks in onder meer de telecomsector in de VS en Europa door 'Salt Typhoon', een hackerscollectief dat door Tech Crunch gelinkt wordt aan de Chinese overheid. In december 2024 gingen de FBI en CISA zelfs zo ver om Amerikanen [publiekelijk te waarschuwen](#) dat ze beter apps zoals [Signal](#) voor hun communicatie kunnen gebruiken. Deze heeft end-to-end encryptie, zodat alle informatie versleuteld is.

Respondenten geven zelf aan dat de dreiging op het gebied van cybersecurity een hot topic is. Maatregelen variëren van grotere waakzaamheid tot het volop investeren in digitale transformatie op dit gebied.

Het gaat dan om het beschermen van uiteenlopende zaken zoals IP, gevoelige kennis of toegang tot systemen om potentieel toeleveringsketens te (kunnen) verstoren. Hierbij worden met name de Russische Federatie, Noord-Korea en China als boosdoeners genoemd. Respondenten zien op dit gebied ook meer activiteit van hackers uit deze landen. Een persoon omschreef de situatie als het nieuwe normaal, een ander gaf aan dat de huidige hoeveelheid van cyberaanvallen al sinds de start van de Russische inval in Oekraïne aan de gang is. Een enkeling geeft aan zelf ooit slachtoffer te zijn geweest van een hack en daar sindsdien heel scherp op te zijn.



Opvallend:

Hoewel bedrijven moeten voldoen aan de [Digital Operational Resilience Act \(DORA\)](#) van de EU, noemt geen van de respondenten dit als hoofdoorzaak voor hun verscherpte aandacht. Een enkeling geeft aan deze strengere wetgeving juist te willen voor betere bescherming.



Voor nu afwachtende houding ten aanzien van reshoring

Hoewel **64,41%** van de bedrijfsleiders regiospecifieke gevaren zien en **72,88%** van de respondenten maatregelen neemt om risico's te managen, is er een afwachtende houding als het aankomt op 'reshoring': het terughalen van activiteiten naar Nederland of het verplaatsen daarvan naar Europa. Van de respondenten zegt **93,22%** niet van plan te zijn om voor het laatste te kiezen en voor nu af te wachten wat er gaat gebeuren. Een houding die was te verwachten, aangezien Trump 2 ten tijde van de survey nog maar net twee weken oud was.

Daar staat wel tegenover dat **96,61%** van de respondenten verwacht dat de geopolitieke impact groter gaat zijn in de komende twaalf maanden. Er zijn dus wel degelijk zorgen over wat er ons staat te wachten, waarbij vooral de onvoorspelbaarheid een punt is.

Risicomanagement is een aandachtspunt

Qua risicomanagementmaatregelen gaat het onder meer om het in kaart brengen van risico's, het doorlopen van scenario's, het uitvoeren van stresstesten en het uitstippelen van alternatieve strategieën. Er is niet zozeer een uniforme strategie, ook omdat veel afhangt van de desbetreffende organisatie, sector en afzetmarkt. Zo is een aantal respondenten van plan isolationistische landen te mijden, terwijl anderen schulden en investeringen strategisch willen verminderen, en weer anderen kijken juist naar het uitbreiden van investeringen om daarmee te diversificeren.

Vertrouwen in langetermijnvoordelen ESG en klimaatdoelen blijft

Ondanks de geopolitieke instabiliteit blijft **69,46%** van de ondervraagden vertrouwen houden in ESG. Ze zien het vooral als langetermijnprogramma met idem doelstellingen. Een aantal geeft aan dat ESG strategisch belangrijk is voor de organisatie, en dat ze hier in de voorhoede zijn en daar willen blijven. Toch is de algemene tendens dat de meesten verwachten dat er de komende tijd wat minder nadruk op ESG komt te liggen of dat het vertraging op gaat lopen, ook met het oog op recentelijk voorgestelde wijzigingen van de wetgeving op dit gebied.

Op de vraag of Europa concurrentiekracht verliest door vast te houden aan de Europese klimaatdoelen kwamen interessante genuanceerde antwoorden. Van de respondenten zei **52,54%** nee, de rest ja. Het nee-kamp onderstreepte de langetermijnvoordelen en het 'first-mover advantage' als Europa eenmaal de transitie naar een groene economie maakt. Als voorbeeld werd China genoemd, dat sterk inzet op groene energie, een streven waarbij binnenlandse bedrijven volop kunnen innoveren. Het ja-kamp, maar ook een deel van het nee-kamp, stelde dat het langer vasthouden aan de doelen op de korte termijn wel schadelijk kan zijn. Daarbij werd ook de komende hernieuwde focus van de VS op fossiele brandstoffen genoemd en er werd aangegeven dat energie relatief duur is binnen de EU.

AI zorgt voor discussie

De ontwikkelingen op het gebied van AI, LLM's in het bijzonder, houden ook in het Nederlandse bedrijfsleven de gemoederen bezig. Van de respondenten denkt **57,64%** dat onze maatschappij in staat is om de snelle technologische ontwikkelingen op dit gebied bij te benen.

De bedrijfsleiders gaven verder zeer uiteenlopende antwoorden. Van sceptisch tot enthousiast, van "We zijn er al mee bezig" tot "We moeten waarschijnlijk wel". Er werden ook zorgen geuit over een vermeende achterstand van Europa ten opzichte van China en de VS. Hierbij moet opgemerkt worden dat ten tijde van de survey de aankondiging van Mistrals Le Chat nog niet was gedaan. Daarmee lijkt de EU wel een goede challenger in huis te hebben. Maar gezien de snelheid van mondiale ontwikkelingen op dit gebied is het zeer lastig te voorspellen hoe alles gaat lopen. Nog een kanttekening is te ontwaren in de recente opmerkingen van Yann LeCun, de AI-tsaar van Meta, in de Financial Times. Hij gaf juist aan dat hij geen toekomst ziet in LLM's vanwege de vele beperkingen van dit type AI, zoals het relatief beperkte langetermijngeheugen, de hallucinaties en de enorme hoeveelheid trainingsdata die het nodig heeft.

Tot slot enige aanbevelingen

De geopolitieke gevolgen van Trump 2 zijn zeer reëel voor het Nederlandse grootbedrijf, vooral het deel dat internationaal opereert, al was het maar vanwege de afhankelijkheid van buitenlandse leveranciers.

Het grootste probleem is hierbij de onvoorspelbaarheid. Vandaar dat er slim met risicomanagement omgesprongen moet worden.

Voor vergelijkbare bedrijven die zoeken naar oplossingen over hoe ze hiermee om kunnen gaan, raden we het volgende aan:



Versterk cybersecurity en houd de focus scherp op dit gebied.

Lang niet iedereen is een doelwit van een staatsoverheid, maar een mogelijke hack door cybercriminelen kan net zo verstorend werken. Daarnaast voldoet u met de juiste maatregelen ook aan Europese regelgeving. Dat is een win-winsituatie.



Digitale transformatie is van belang voor zowel de (eventuele) adoptie van AI (in welke vorm dan ook) en cybersecurity.

Legacy-systemen zorgen vaak voor problemen. Kijk samen met IT wat er op welke termijn kan of moet worden vernieuwd. Daarbij is het verstandig om externe experts in te schakelen, al was het maar voor een second opinion over de plannen.



Breng geopolitieke risico's in kaart en stel scenario's en snel uitvoerbare plannen op.

Mocht er iets voorvallen, dan kan er direct ingegrepen worden. Het kan ook verstandig zijn om iemand verantwoordelijk te maken voor het in de gaten houden van de situatie, eventueel in samenwerking met externe partners als de interne capaciteit er niet is.



In lijn met het langetermijnvertrouwen van de respondenten in ESG **raden we aan om hier blijvend in te investeren**, zelfs als plannen op EU-niveau eventueel gewijzigd worden. Dat is ook verstandig met het oog op een gezonde, toekomstige bedrijfsvoering en een blijvend concurrerend vermogen ten opzichte van bijvoorbeeld China. Schakel gerust een ESG-expert in die hierin kan adviseren.

Contact



Tom van der Heijden

Voorzitter KPMG RAAD Board Program

vanderheijden.tom@kpmg.nl

020 6 567 520