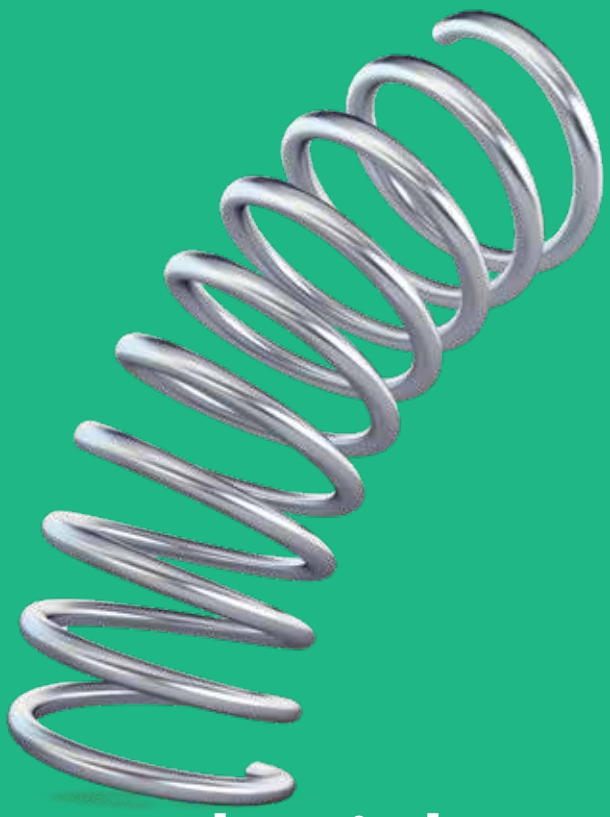
Voka

paper

Een uitgave van Voka vzw | april 2026
Verschijnt niet in juli en augustus | Afgiftekantoor
Brugge - Erkenningsnummer P708123



Weerbaarheid versterken, groei beschermen

Van kwetsbaarheid naar weerbaarheid in een veranderende veiligheidsomgeving

Hendrik Caluwé

VOKA KENNIS- en LOBBYCENTRUM

Hendrik Theunissen
Directeur Kennis- en Lobbycentrum

Bart Van Craeynest
Hoofdeconoom

Sonja Teughels
Arbeidsmarkt

Veerle Van Nieuwenhuysen
Arbeidsmarkt

Gianni Duvillier
Werk en Sociale zekerheid

Julie Beysens
Onderwijs

Daan Aeyels
Welzijns- en gezondheidsbeleid

Freija Fonteyn
Mobiliteit en logistiek

Jasmine De Rop
Milieu

Yannick Van den Broeck
Energie en klimaat

Robin Verbeke
Ruimtelijke ordening en omgeving

Dieter Somers
Digitale transformatie en competitiviteit

Philippe Nys
Economie, industrie en innovatie

Karl Collaerts
Fiscaliteit en begroting

Maarten Libeer
Europees beleid

Hendrik Caluwé
Europees beleid, handel en defensie

COLOFON

Eindredactie
Alessandra Magnus, Sandy Panis

Foto's
Adobe Stock

Vormgeving
Capone

Concept
Buro Knal

Cover
The Fat Lady

Druk
INNI Group, Heule

Verantwoordelijke uitgever
Frank Beckx i.o.v. Voka vzw,
Koningsstraat 154-158
1000 Brussel
info@voka.be - www.voka.be

Inhoud

Ontdek hier
alle Voka Papers.

WIE?
Hendrik Caluwé
Expert Europees beleid,
Handel & Defensie
Kennis- en lobbycentrum Voka
Hendrik.caluwe@voka.be

DE ESSENTIE

Weerbare ondernemingen als basis voor een weerbare samenleving

Vlaanderen en België staan voor een nieuwe realiteit. De continue hybride dreiging, van cyberaanvallen en sabotage tot economische druk en desinformatie, treft vandaag niet alleen overheden, maar de volledige economie. Toch krijgt ondernemingsweerbaarheid geen centrale plaats binnen het nationale veiligheidsbeleid. Dat is een structurele kwetsbaarheid. Bedrijven zijn geen randactoren, maar essentiële schakels in onze economische veiligheid en militaire paraatheid. Zonder weerbare ondernemingen is er geen weerbare samenleving. Deze Voka Paper vertrekt vanuit die vaststelling en reikt, in het kader van het Nationaal Weerbaarheidsplan, gerichte aanbevelingen aan om de weerbaarheid van België structureel te versterken.

Centraal in deze Voka Paper staat een analyse van het veranderende veiligheidslandschap en de toenemende kwetsbaarheden voor onze economie en ondernemingen. In een context van toenemende geopolitieke onzekerheid, hybride dreigingen en oplopende economische kosten van cyberaanvallen, spionage en verstoringen van kritieke infrastructuur wordt weerbaarheid een strategische voorwaarde voor economische stabiliteit en nationale veiligheid. Vervolgens schuift de paper drie hefbomen naar voren om de weerbaarheid van België en zijn bedrijven structureel te versterken: een sterkere verankering van publiek-private samenwerking in het nationale weerbaarheidsbeleid, een gerichte technologiestrategie om strategische afhankelijkheden te verkleinen en innovatie te versterken, en een concreet vierstappenplan waarmee ondernemingen weerbaarheid kunnen vertalen naar praktische acties.

1 België opereert in een snel veranderend veiligheidslandschap

België bevindt zich in een fundamenteel gewijzigde veiligheidsomgeving waarin hybride dreigingen structureel zijn geworden en digitale, economische en fysieke kwetsbaarheden elkaar versterken. Door zijn open economie, strategische ligging en geconcentreerde infrastructuur kunnen verstoringen zich snel verspreiden en aanzienlijke maatschappelijke en economische schade veroorzaken. Cyberaanvallen, spionage, desinformatie, verstoringen van vitale infrastructuur en geopolitieke spanningen treffen zowel de overheid als ondernemingen en toeleveringsketens, met daarenboven een snel oplopende financiële impact. Daarom ontwikkelt België een Nationaal Verdedigings-, Enablement- en Weerbaarheidsplan. Weerbaarheid wordt hierbij benaderd als een gedeelde verantwoordelijkheid van de overheid, het bedrijfsleven en de samenleving, om economische continuïteit en strategische geloofwaardigheid te waarborgen in een steeds onzekerdere internationale omgeving.

2 Ondernemingsweerbaarheid structureel verankeren in beleidsplannen

België kan ondernemingsweerbaarheid versterken door inspiratie te halen uit Finse, Duitse en Nederlandse initiatieven en publiek-private samenwerking structureel te verankeren in het Nationaal Weerbaarheidsplan. Centraal staat een permanent en gelijkwaardig partnerschap tussen de overheid en het bedrijfsleven, gericht op gezamenlijke voorbereiding op hybride dreigingen via risicomonitoring, ketenanalyses, scenarioplanning, strategische voorraden en oefeningen. Aangezien het merendeel van de kritieke infrastructuur in private handen is, is structurele betrokkenheid van ondernemingen essentieel. Dit vraagt ook een gerichte investeringsagenda met fiscale stimulansen, weerbaarheidsfondsen en Europese financiering om publieke en private investeringen te versnellen.

3 Een technologiestrategie ter versterking van groei en onafhankelijkheid

Vlaanderen heeft door geopolitieke spanningen, hybride dreigingen en mondiale concurrentie nood aan een samenhangende technologiestrategie. Door te focussen op een beperkte set sleuteltechnologieën zoals cybersecurity, artificiële intelligentie en quantumtechnologie kan het zijn innovatiekracht bundelen, strategische afhankelijkheden verkleinen en investeringen efficiënter inzetten. Internationale voorbeelden tonen aan dat focus en schaal technologische autonomie versterken. Een duidelijke samenwerking tussen overheid, ondernemingen en defensie is daarbij essentieel om veiligheid, soevereiniteit en duurzame welvaart op lange termijn te kunnen waarborgen.

4 Vierstappenplan voor sterkere weerbaarheid bij ondernemingen

Met een vierstappenplan helpen we ondernemingen om strategische weerbaarheid om te zetten in concrete actie. Het biedt een praktisch kader dat start bij verankering op bestuursniveau en inzet op scenariodenken, horizon scanning en vroegtijdige waarschuwing om externe signalen tijdig te vertalen naar besluitvorming. Door te focussen op vitale functies en afhankelijkheden kunnen duidelijke prioriteiten worden gesteld, terwijl stressscenario's en crisisoefeningen plannen versterken. Zo wordt weerbaarheid een hefboom voor innovatie, vertrouwen en duurzame groei.

Inleiding

Weerbaarheid is het vermogen om vitale functies en maatschappelijke continuïteit te waarborgen bij fouten, incidenten of doelgerichte aanvallen. In een context van toenemende hybride dreigingen, krijgt dat begrip een brede invulling, maar deze paper focust specifiek op de weerbaarheidsuitdagingen die raken aan de private sector en prioritair aangepakt moeten worden. Het versterken van economische en maatschappelijke weerbaarheid begint bij de onderneming zelf, maar veronderstelt tegelijk een ruimer beleidskader waarin overheid en bedrijfsleven samen optrekken.

Het eerste hoofdstuk schetst de fundamenteel gewijzigde veiligheidsomgeving waarin België zich bevindt. Het analyseert de impact van geopolitieke spanningen, cyberdreigingen en andere hybride aanvallen, belicht de specifieke kwetsbaarheden van ons land en bespreekt de stijgende economische kosten van verstoringen. Daarbij wordt ook ingegaan op de ontwikkeling van drie nationale plannen: het Nationaal Verdedigingsplan, het Nationaal Enablementplan en het Nationaal Weerbaarheidsplan.

Het tweede hoofdstuk vertaalt deze context naar de nood aan structurele verankering van ondernemingsweerbaarheid binnen een interfederaal publiek-privaat samenwerkingsmodel. Het bespreekt waarom vaste partnerschappen, gedeelde verantwoordelijkheid en materiële paraatheid essentieel zijn in een omgeving waarin een groot deel van de kritieke infrastructuur in private handen is en verkent ook de rol van samenwerking tussen defensie en industrie, gezamenlijke oefeningen en een gerichte investeringsagenda.

Het derde hoofdstuk zoomt in op Vlaanderen en onderbouwt waarom een samenhangende technologiestrategie noodzakelijk is om groei, strategische autonomie en veiligheid te verbinden. Met focus op sleuteltechnologieën zoals cybersecurity, artificiële intelligentie en quantumtechnologie wordt toegelicht hoe gerichte keuzes kunnen bijdragen aan innovatiekracht en weerbaarheid.

“
Het versterken van economische en maatschappelijke weerbaarheid begint bij de onderneming zelf, maar veronderstelt tegelijk een ruimer beleidskader waarin overheid en bedrijfsleven samen optrekken.

Tot slot maakt het vierde hoofdstuk de vertaalslag naar de praktijk met een concreet vierstappenplan voor ondernemingen. Het reikt een gestructureerd kader aan om weerbaarheid strategisch te verankeren, dreigingen tijdig te detecteren, vitale functies en afhankelijkheden te beschermen en paraatheid te testen via scenario’s en oefeningen. Zo positioneert deze paper niet alleen als beschermingsmechanisme, maar ook als hefboom voor vertrouwen, innovatie en duurzame welvaart.

Hoofdstuk 1. België in een veranderende veiligheidsomgeving

België bevindt zich in een snel veranderende veiligheidscontext waarin digitale, economische en fysieke dreigingen elkaar versterken en hybride actoren steeds vaker inspelen op kwetsbaarheden in onze open en sterk verweven economie.[1] Door zijn strategische ligging, geconcentreerde infrastructuur en complexe staatsstructuur kunnen verstoringen zich snel verspreiden en disproportionele effecten veroorzaken. Drie nationale plannen zijn in opbouw om met deze nieuwe context om te kunnen gaan: het Nationaal Verdedigingsplan, het Nationaal Enablementplan en het Nationaal Weerbaarheidsplan.

Ook Europa bevindt zich vandaag in een veiligheidsomgeving die fundamenteel veranderd is.[2] Conflicten worden niet langer uitsluitend met klassieke militaire middelen uitgevochten. Steeds vaker maken statelijke en niet-statelijke actoren gebruik van een combinatie van digitale aanvallen, spionage, manipulatie van de publieke opinie, economische druk en subtiele verstoringen van infrastructuur.[3] Dit geheel noemen we 'hybride oorlogsvoering'. Het bijzondere aan deze aanpak is dat ze meestal net onder de drempel van een open militaire aanval blijft, maar toch een aanzienlijke impact kan hebben op de stabiliteit van landen. Door digitalisering, sociale media en de nauwe economische verwevenheid binnen Europa reikt deze vorm van beïnvloeding vandaag veel verder dan vroeger tijdens de Koude Oorlog bijvoorbeeld.

De NAVO erkent deze evolutie uitdrukkelijk in haar recente analyses. Sinds 2022 spreekt het bondgenootschap over een '360-graden dreigingslandschap'[4]: risico's komen niet alleen van militaire tegenstanders, maar ook uit cyberspace, de ruimte, internationale handel, energie-afhankelijkheden en desinformatiecampagnes. Een klassieke militaire aanval onder Artikel 5[5] (van de NAVO) is daarmee niet verdwenen, maar wordt in toenemende mate voorafgegaan door acties die bedoeld zijn om een samenleving te verzwakken nog vóór er sprake is van fysieke escalatie. Veiligheid draait dus niet langer enkel om de verdediging van fysieke grenzen.

Tegelijk ziet de Europese Unie een sterke toename van maatschappelijke en economische schokken.

Handelsconflicten, energiecrisissen, verstoringen in internationale toeleveringsketens, cyberdreigingen en extreem weer beïnvloeden steeds vaker de werking van bedrijven. In haar Financial Stability Review (2025) wijst de Europese Centrale Bank (ECB) op uitzonderlijk hoge geopolitieke onzekerheid, met gevolgen voor de industrie en de financiële stabiliteit. Ander ECB-onderzoek toont aan dat verstoringen in de aanvoer van essentiële buitenlandse inputs, waaronder voor België belangrijke grondstoffen en componenten, in alle lidstaten leiden tot een aantoonbare daling van economische activiteit. De logica is eenvoudig: hoe meer geopolitieke spanning of afstand, hoe moeilijker handel en investeringen verlopen.

Ook België voelt deze nieuwe realiteit. Digitale aanvallen hebben de voorbije jaren overheden, banken, havens en mediaplatformen getroffen terwijl op sociale media buitenlandse accounts probeerden maatschappelijke discussies te beïnvloeden.[6] Daarnaast zijn in en rond de Noordzee verschillende signalen opgedoken van verkenning van vitale infrastructuur. Elk incident afzonderlijk lijkt beperkt, maar samen tonen ze een patroon van systematische druk: het testen van onze systemen, het verzamelen van informatie en het aftasten van onze weerbaarheid. De drone-incidenten uit november 2025 passen hierbij: ze veroorzaken weinig fysieke schade, maar creëren onzekerheid en ondermijnen het vertrouwen in onze reactiesnelheid.

De kwetsbaarheid van België

België is kwetsbaar voor verschillende soorten verstoringen tegelijk. Problemen in computersystemen, pogingen om de publieke opinie te beïnvloeden, zwakke plekken in belangrijke infrastructuur en risico's voor de fysieke veiligheid kunnen elkaar versterken. Daardoor kan zelfs een klein incident snel grotere gevolgen krijgen. Bovendien maakt onze ligging en economische structuur het voor kwaadwillende spelers makkelijker om zwakke punten te vinden en daar druk op uit te oefenen.

Ons land ligt op een uniek kruispunt in Europa, met grote havens, belangrijke energieverbindingen, datakabels en knooppunten voor militair transport. Deze infrastructuur is essentieel voor zowel onze economie als voor die van Europa. Doordat alles zo dicht bij elkaar ligt, kan één probleem zich snel verspreiden naar andere sectoren of zelfs naar andere landen. Een kleine verstoring kan daardoor onverwacht grote schade veroorzaken.

België is ook sterk afhankelijk van internationale handel, waardoor we extra hard worden getroffen wanneer toeleveringsketens of markten verstoord raken. Tegelijk worden veiligheidstaken verdeeld over verschillende bestuursniveaus, wat snelle en gecoördineerde actie moeilijker maakt. In combinatie met onze rol als locatie voor Europese instellingen en als logistiek centrum binnen de NAVO maakt dit België aantrekkelijk voor actoren die onrust willen zaaien of invloed willen uitoefenen.

De kosten verbonden aan hybride aanvallen stijgen

De kosten van hybride aanvallen zijn divers en situeren zich op meerdere niveaus. Ze kunnen worden onderverdeeld in verschillende categorieën, waaronder kosten verbonden aan cyberaanvallen, aanvallen op vitale fysieke infrastructuur, aantasting van kennis en intellectueel kapitaal, verstoringen in toeleveringsketens en economische schade door informatie- en beïnvloedingsoperaties. Samen illustreren deze categorieën de brede financiële impact van hybride dreigingen.

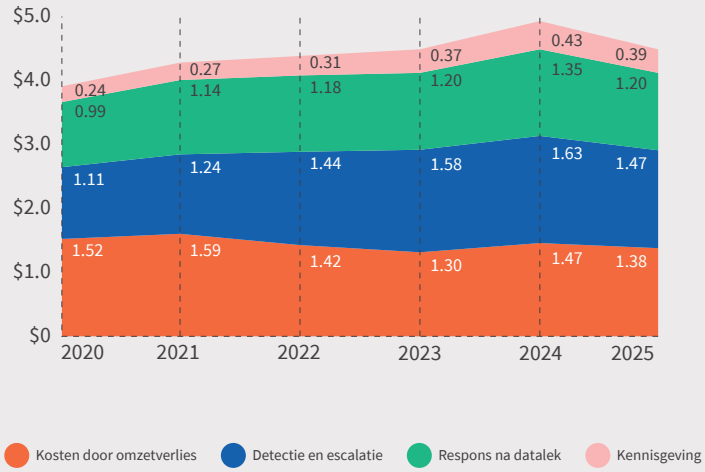
Figuur 1 De geschatte economische impact van de verstoring van kritieke overzeese infrastructuur

Infrastructuurtype	Kost per dag (miljoen euro)	Hersteltijd	Totale geschatte kost
Telecomkabel (subsea)	> 24	Tot 3 weken (~21 dagen)	≥ 504 miljoen euro
Elektriciteitsinterconnector	~ 12	Tot 60 dagen	~ 720 miljoen euro
Olie- en gaspijpleiding	n.v.t. (varieert)	Tot 9 maanden	Tientallen miljarden euro

Bron: RAND Europe (2024), Critical Undersea Infrastructure Perspective. Bewerking door auteur.

Figuur 2 **De verdeling en evolutie van datalek-kosten**

Gemeten in miljoenen USD



Bron: Cost of a Data Breach Report 2025, IBM (2025)

Figuur 3 **De internationale vergelijking van datalek-kosten (2024 vs. 2025)**

Gemiddelde kostprijs van een datalek in miljoenen USD

Land / Regio	2025	2024
1. Verenigde Staten	$10,22	$9,36
2. Midden-Oosten	$7,29	$8,75
3. Benelux	$6,24	$5,90
4. Canada	$4,84	$4,66
5. Verenigd Koninkrijk	$4,14	$4,53
6. Duitsland	$4,03	$5,31
7. Latijns-Amerika	$3,81	$4,16
8. Frankrijk	$3,73	$4,17
9. ASEAN	$3,67	$3,23
10. Japan	$3,65	$4,19
11. Italië	$3,44	$4,73
12. Zuid-Korea	$2,84	$3,62
13. Australië	$2,55	$2,78
14. India	$2,51	$2,35
15. Zuid-Afrika	$2,37	$2,78
16. Brazilië	$1,22	$1,36

Bron: Cost of a Data Breach Report 2025, IBM (2025)

Hybride aanvallen op vitale infrastructuur veroorzaken snel zeer hoge kosten: sabotage in Europa leidde sinds 2022 al tot honderden miljoenen euro schade, terwijl de uitval van onderzeese telecom- en energieverbindingen dagelijks 12 tot 75 miljoen euro kan kosten.[7] Het herstel van grote incidenten loopt soms op tot boven een miljard euro. Zelfs kleine fysieke verstoringen, zoals drone-incidenten aan luchthavens, genereren in korte tijd economische verliezen van honderdduizenden tot meerdere miljoenen euro.

Volgens IBM bedraagt de gemiddelde financiële schade van een cyberaanval inclusief datalek wereldwijd 4,44 miljoen dollar. In 2025 daalde deze kost voor het eerst, vooral door snellere detectie en kortere onderzoeks- en escalatiefases, al blijft de gemiddelde hersteltijd van 241 dagen hoog. De kosten dalen in alle vier categorieën: detectie en escalatie, notificatie, post-breachrespons en verloren business. In de Benelux is de impact duidelijk groter met een gemiddelde kost van 6,24 miljoen dollar per datalek. Dat cijfer ligt 6% hoger dan in 2024, en ruim boven het wereldgemiddelde. Daarenboven is slechts een derde van de Vlaamse bedrijven verzekerd tegen een cyberaanval.[8]

De kosten van een IP-diefstal zijn aanzienlijk groot en raken bedrijven op verschillende niveaus. In de Verenigde Staten wordt de jaarlijkse economische schade geschat op 225 tot 600 miljard dollar (1-5% van het bbp) volgens de Commission on the Theft of American Intellectual Property (2017). Individuele bedrijven kunnen zware financiële verliezen lijden: zo verloor American Superconductor 100 miljoen dollar per jaar nadat hun broncode werd gestolen. Daarnaast zijn juridische kosten hoog: patentzaken kosten gemiddeld 2 tot 9 miljoen dollar[9] en reputatieschade bedraagt gemiddeld 1,57 miljoen dollar per incident.[10] Ook de bredere economie wordt getroffen. De handel in

namaakgoederen vertegenwoordigde in 2021 wereldwijd 467 miljard USD (2,3% van de import), en 117 miljard USD in de EU (4,7%).[11]

Daarnaast zijn er ook nog de kosten van informatie-oorlog en beïnvloeding. Die zijn moeilijk precies te berekenen, omdat ze vooral voortkomen uit indirecte economische schade zoals reputatieverlies, dalend consumentenvertrouwen en de verstoring van markten. Duidelijk is wel dat de impact snel toeneemt. Volgens Cavazos (2021)[12] veroorzaken 'fake reviews' en andere vormen van misleidende online-informatie wereldwijd al 152 miljard dollar schade per jaar. Ook in België wordt dit steeds zichtbaarder: horeca-zaken, zorginstellingen en lokale ondernemingen verliezen soms plots klanten door viraal verspreide onjuiste verhalen of nepklachten.[13]

Artificiële intelligentie versterkt deze dynamiek drastisch. Onderzoek van het MIT (2018)[14] toont dat valse berichten 70% vaker worden gedeeld dan echte, waardoor desinformatie zich razendsnel verspreidt. De Edelman Crisis & Risk-studie (2024)[15] bevestigt dat acht op de tien bedrijfsleiders vrezen voor AI-gedreven reputatieschade, terwijl meer dan een derde toegeeft daar onvoldoende op voorbereid te zijn. De opkomst van deepfakes verdiept het risico verder: in 2024 werd naar schatting de helft van alle bedrijven wereldwijd geconfronteerd met deepfake-aanvallen, goed voor gemiddeld 450.000 dollar schade per incident. Het meest sprekende voorbeeld is een deepfake-videocall waarbij een medeweker van een financiële speler in Hong Kong werd misleid om 25 miljoen dollar over te maken.[16]

Tot slot lopen wereldwijd de kosten van verstoringen in toeleveringsketens snel op: volgens het Held Global Risk Report[17] gaat het inmiddels om meer dan 180 miljard dollar per jaar. Geopolitieke spanningen, cyberaanvallen, extreme weersomstandigheden en strengere regelgeving spelen daarin een grote rol. Voor België stelde de studie van de Nationale Bank[18] in 2022 vast dat hogere kosten voor grondstoffen en vertraagde leveringen de productie gemiddeld met 7% deden dalen en bedrijven ertoe aanzetten hun investeringen met ongeveer 12% terug te schroeven.

Drie nationale veiligheidsplannen

Om een antwoord te bieden op deze veranderende veiligheidsomgeving besliste de NAVO in 2025 om de defensie-uitgaven per land in termen van het bbp te verhogen. Hierbij maakte ze een onderscheid tussen strikte militaire uitgaven ten belope van 3,5% van het bbp en 1,5% veiligheidsuitgaven ter versterking van de algemene weerbaarheid.

Weerbaarheid is het vermogen om vitale functies en maatschappelijke continuïteit te blijven garanderen bij fouten, incidenten of aanvallen. Sterke weerbaarheid verhoogt niet alleen onze capaciteit om crisissen op te vangen, te beheersen en te herstellen, maar verkleint ook de kansen voor tegenstanders om kwetsbaarheden uit te buiten. Daarmee wordt weerbaarheid een essentieel onderdeel van afschrikking: een mogelijke aanval wordt ontmoedigd omdat ze weinig kans op slagen heeft.

In deze context actualiseren de Belgische overheden momenteel de drie onderling afhankelijke en complementaire plannen: het Nationaal Verdedigingsplan, het Nationaal Enablementplan en het Nationaal Weerbaarheidsplan. Het Nationaal Verdedigingsplan vormt het 'kaderplan' voor de twee andere plannen. De weerbaarheidsuitdagingen zijn enorm breed te beschouwen, van klimaatuitdagingen, over hybride dreiging tot gezondheidscrisissen. De scope van deze paper beperkt zich echter tot de nieuwe context van de hybride dreigingen en de uitdagingen in het weerbaarheidsplan en het enablementplan die betrekking hebben tot spelers in de private sector en prioritair zijn om aan te pakken.

Drie plannen[1]

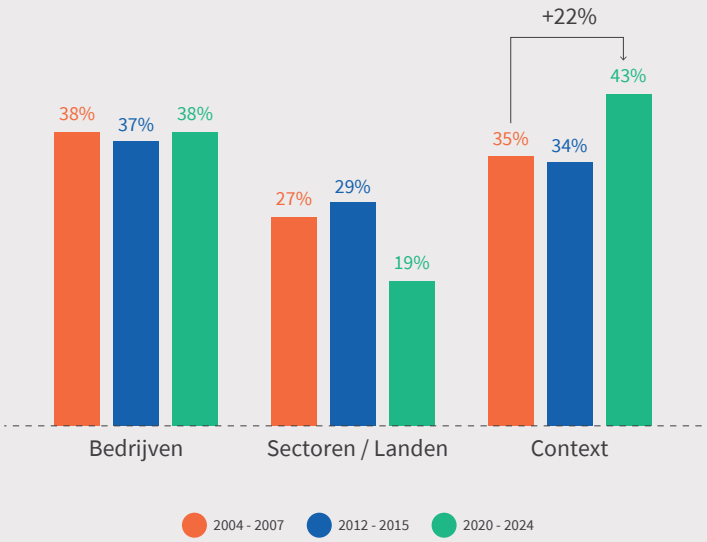
Het **Nationaal Verdedigingsplan** vormt het overkoepelende kader voor de bescherming van België tegen fysieke, digitale en cognitieve dreigingen. Het legt de strategische keuzes, doelen en middelen vast om de veiligheid van het grondgebied en de vitale belangen te waarborgen.

Het **Nationaal Enablementplan** beschrijft hoe België zijn rol vervult wanneer geallieerde troepen ons grondgebied moeten betreden, doorkruisen of gebruiken om verder te reizen. Diezelfde voorbereidingen maken het mogelijk dat België ook zijn eigen strijdkrachten snel kan ontplooien. Door zijn strategische ligging en havens speelt België een sleutelrol in de militaire mobiliteit richting Centraal- en Oost-Europa.

Het **Nationaal Weerbaarheidsplan** heeft negen strategische objectieven: decontinuïteit van overheid en essentiële diensten, de bescherming van energievoorziening, het beheersen van bevolkingsstromen, de beschikbaarheid van voedsel en water, de opvang van massaslachtoffers of gezondheidscrisissen en de robuustheid van communicatie, transport, financiële systemen en het bredere economische weefsel. Vijf horizontale thema's bepalen het volledige kader: cyber, hybride, klimaat, kritieke infratsructuur en maatschappelijke weerbaarheid. Kortom, het Weerbaarheidsplan moet garanderen dat vitale functies blijven werken tijdens grote verstoringen.

Figuur 4 Wat bepaalt winstgevendheid?

Hoe beïnvloedt wereldwijde volatiliteit de bedrijfsresultaten? Volgens een analyse van het BCG Henderson Institute worden verschillen in winstgevendheid tussen bedrijven steeds vaker bepaald door factoren buiten hun directe controle. Contextfactoren zoals geopolitiek, politiek, technologie en klimaat verklaren 43% van de variatie in winstgevendheid tussen bedrijven in de periode 2020-2024. Figuur 4 toont de variatie in nettowinstmarge opgesplitst naar bedrijfs-, land-, sector- en contextfactoren.



Noot: Deze figuur toont welke factoren schommelingen in de nettowinstmarge van bedrijven veroorzaken. Met een statistisch model wordt nagegaan welk deel van die schommelingen te maken heeft met kenmerken van het bedrijf zelf – zoals verkoop, verkoopgroei, marktkapitalisatie en aandeelhoudersrendement en welk deel door andere factoren wordt beïnvloed. Het resterende deel, aangeduid als 'context', is de variatie die overblijft nadat rekening is gehouden met verschillen tussen bedrijven, sectoren en landen in een bepaald jaar. Dit deel weerspiegelt de impact van bredere externe factoren, zoals geopolitieke ontwikkelingen, technologische veranderingen en klimaatrisico's, op de winstgevendheid van bedrijven. De analyse is gebaseerd op een steekproef van ongeveer 78.000 observaties van 6.800 bedrijven in de periode 2004–2024.

De impact van externe factoren op de bedrijfsvoering

Ondernemingen zijn in de eerste plaats zelf het best geplaatst om hun weerbaarheidsstrategie te ontwikkelen. Een analyse van het BCG Henderson Institute toont aan dat in de periode 2020-2024 ongeveer 43% van de verschillen in winstmarges tussen bedrijven niet kan worden verklaard door bedrijfsspecifieke keuzes of sector- en landeffecten, maar samenhangt met bredere contextfactoren zoals geopolitiek, technologie en klimaat. Dat aandeel is met circa 8 procentpunt gestegen tegenover twintig jaar geleden, wat erop wijst dat ondernemingen vandaag minder directe controle hebben over hun financiële resultaten.

Een klassieke strategie die louter focust op interne optimalisatie volstaat daardoor niet langer. Het wordt cruciaal om een weerbaarheidsstrategie te ontwikkelen die expliciet rekening houdt met externe factoren waar ondernemingen weinig vat op hebben, maar die wel steeds zwaarder doorwegen. In dat kader is samenwerking met publieke instanties een noodzaak geworden van een holistische weerbaarheidsaanpak. In de volgende hoofdstukken wordt dan ook dieper ingegaan op de beleidsaanbevelingen voor overheden om ondernemingen te ondersteunen in hun weerbaarheidsstrategie.

1. Wannes Verstraete et al., Will the New Government Safely Navigate Belgium through Turbulent International Waters? (2025)
2. Sapir et al., Geopolitical shifts and their economic impacts on Europe: short-term risks, medium-term scenarios and policy choices (2025)
3. Baumann & Pynnöniemi, European Security in the Era of Hybrid Warfare (2025)
4. Nato, Strategic Concepts (2022)
5. Artikel 5 van het Noord-Atlantisch Verdrag is de kernbepaling van de NAVO, waarin is vastgelegd dat een gewapende aanval op één lidstaat wordt beschouwd als een aanval op alle leden.
6. Vrt, Hybride oorlogsvoering uitgelegd en in kaart gebracht (2024)
7. RAND Europe (2024), Critical Undersea Infrastructure Perspective.
8. Wewis, CS-barometer: maturiteit in cybersecurity bij Vlaamse bedrijven (2023)
9. AIPLA, 2019
10. Ponemon Institute, 2020
11. EUIPO–OECD, 2025
12. THE ECONOMIC COST OF BAD ACTORS ON THE INTERNET FAKE ONLINE REVIEWS 2021
13. HLN (2022)
14. Dizikes, Study: On Twitter, false news travels faster than true stories (2018)
15. Navigating the AI Readiness Gap (2024)
16. FT, Arup lost $25mn in Hong Kong deepfake video conference scam (2024)
17. J.S. Held, 2025 Global Risk Report, 2025
18. https://www.ori.be/upload/nieuws_docs/120/file/perscommunique-ad-hoc-enquete-7-april-2022.pdf

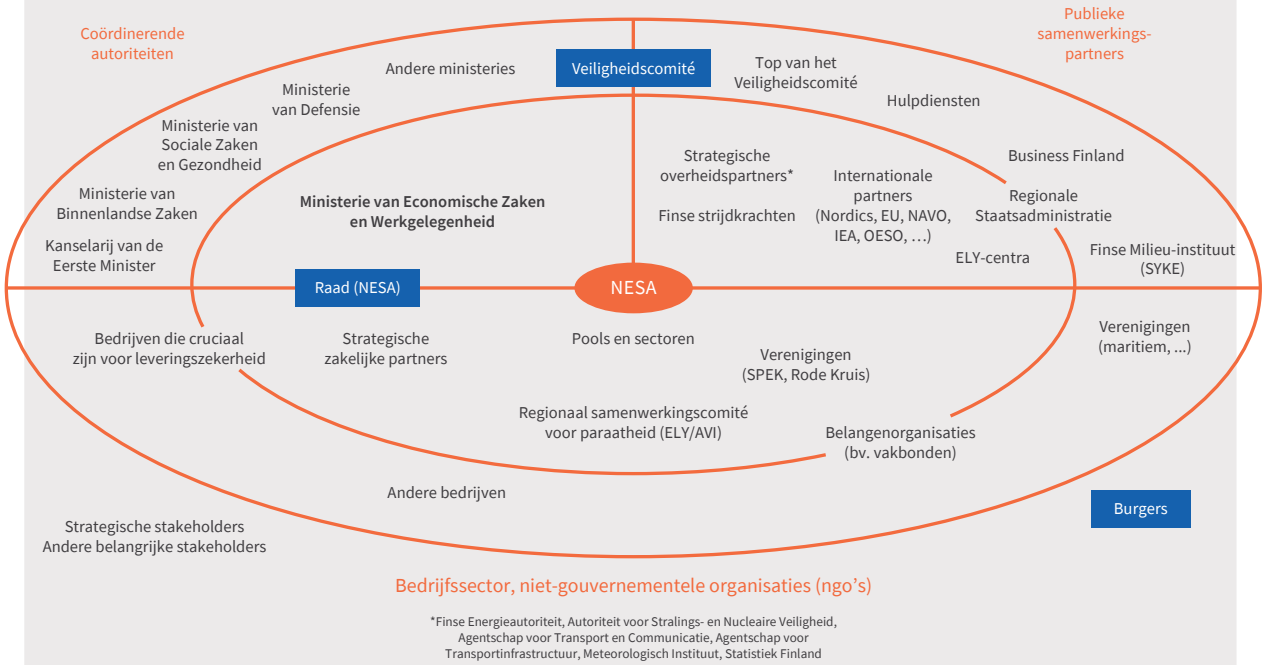
Hoofdstuk 2. Ondernemingsweerbaarheid structureel in beleidsplannen verankeren

Vitale infrastructuur en toeleveringsketens zijn steeds vaker in private handen, terwijl hybride dreigingen steeds vaker sectoroverschrijdend doorwerken. Dat maakt een gedeelde verantwoordelijkheid tussen publieke en private actoren, meer dan ooit cruciaal. Aan de hand van internationale voorbeelden uit Finland, Duitsland en Nederland, illustreert dit hoofdstuk hoe publiek-private partnerschappen kunnen uitgroeien tot een pijler van nationale weerbaarheid. Tot slot vertaalt het deze inzichten naar de Belgische en Vlaamse context, met aandacht voor governance, investeringen en gezamenlijke oefeningen.

Publiek-private samenwerkingsstructuur centraal in buitenlandse modellen

Het Fins weerbaarheidsmodel staat onder leiding van de National Emergency Supply Agency (NESA), dat is opgericht in 1993. De figuur toont hoe Finland weerbaarheid organiseert als een netwerk, met de NESA[19] als spil. NESA opereert onder het ministerie van Economische Zaken en Werkgelegenheid en is verantwoordelijk voor wat Finland 'security of supply' noemt: het garanderen dat vitale maatschappelijke functies blijven werken in ernstige crisissen. Finland gaat hier uit van een whole-of-society approach aangezien noch de overheid, noch de

Figuur 5 **Belangrijkste netwerken en stakeholders van het Fins Nationaal Agentschap voor Noodvoorzieningszekerheid (NESA)**



*Finse Energieautoriteit, Autoriteit voor Stralings- en Nucleaire Veiligheid, Agentschap voor Transport en Communicatie, Agentschap voor Transportinfrastructuur, Meteorologisch Instituut, Statistiek Finland

private sector voldoende capaciteiten hebben om de uitdagingen zelf aan te gaan.[20]

Centraal in dit model staan publiek-private samenwerkingsstructuren (PPS'en), georganiseerd in zogenaamde sectorale pools. Deze pools bestrijken alle sectoren die essentieel zijn voor het functioneren van de samenleving, waaronder kritieke infrastructuur, energie, logistiek, industrie (inclusief defensie-industrie), bouw, voedselproductie en -distributie, gezondheidszorg, digitale veiligheid en media. In totaal gaat het om zeven hoofdsectoren en 22 pools, gecoördineerd door NESA.

Elke pool wordt geleid door een niet-gouvernementele organisatie, op basis van formele samenwerkingsovereenkomsten met NESA. Dat is een cruciaal element: de overheid stuurt en coördineert, maar laat de private actoren zelf eigenaar zijn van hun voorbereiding. In de pools zitten samen ongeveer 1.500 publieke en private actoren die als kritisch worden beschouwd voor bevoorradingszekerheid en paraatheid. De pools hebben een zeer concreet mandaat: risico's monitoren, ketenafhankelijkheden analyseren, scenario's uitwerken en maatregelen voorbereiden om de continuïteit binnen hun sector te garanderen.[21]

Rond deze kernstructuur zie je in figuur 5 een brede schil van actoren: ministeries, regionale overheden,

> **België kan inspiratie halen uit goede voorbeelden uit Finland, Duitsland en Nederland, door sterker in te zetten op publiek-private samenwerking.**

hulpdiensten, bedrijven, ngo's (zoals het Rode Kruis), kennisinstellingen en burgers. Weerbaarheid wordt dus niet benaderd als een veiligheidsvraagstuk in enge zin, maar als een samenlevingsopdracht waarin overheid, markt en samenleving structureel samenwerken.[22]

Niinistö, niet toevallig een voormalige Finse president, focust in zijn rapport[23] ook op de implementatie van publiek-private partnerschappen:

- Ad-hocsamenwerkingen uit eerdere crisissen moeten worden omgezet in vaste partnerschappen voor voorbereiding en respons;
- Strategische paraatheidsdoelen moeten expliciet worden opgenomen in overheidsopdrachten, zodat marktmechanismen investeringen in veerkracht,

leveringszekerheid en dual-use-infrastructuur stimuleren;

» Privaat kapitaal moet worden gemobiliseerd via nieuwe financieringsinstrumenten (bijvoorbeeld een European Preparedness Bond Standard en een toekomstig EU-Competitiveness Fund).

België kan inspiratie halen uit praktijken uit landen zoals Finland, maar ook uit Duitsland en Nederland, door sterker in te zetten op structurele publiek-private samenwerking. Een belangrijk element daarbij is het uitbouwen van vaste netwerken in plaats van ad-hocoverleg tijdens crisissen. In dergelijke netwerken kennen bedrijven, overheden en maatschappelijke organisaties elkaar vooraf, delen zij informatie en werken zij gezamenlijk scenario's en voorbereidingsmaatregelen uit nog vóór zich een crisis voordoet.

Binnen het Nationaal Weerbaarheidsplan kunnen de weerbaarheidscomités per strategisch objectief worden gezien als een Belgische tegenhanger van de Finse sectorale pools. Hun rol hierin is het coördineren van gezamenlijke voorbereidingsinspanningen en het uitwerken van plannen om de weerbaarheid te versterken. Dit staat los van de taken die sectorale overheden uitvoeren in het kader van de Critical Entities Resilience (CER)-wetgeving, zoals risicoanalyses, identificatie van kritieke entiteiten en toezicht.

Met respect voor de verantwoordelijkheden van de sectorale overheden en de coördinerende rol van het Nationaal Crisiscentrum binnen het Nationaal Weerbaarheidsplan, kan een structurele PPS-structuur verder worden ontwikkeld waarin publieke en private actoren gezamenlijk werken aan de voorbereiding en versterking van de maatschappelijke weerbaarheid. Zo wordt vermeden dat samenwerking beperkt blijft tot consultatie en worden private actoren mede-eigenaar van de voorbereiding en uitvoering van weerbaarheidsmaatregelen. Een aansluiting bij de samenwerkingsstandaarden van de Preparedness Task Force binnen de Europese Preparedness Union Strategy kan deze publiek-private samenwerking verder versterken.

Voor de Belgische context is het belangrijk te benadrukken dat, in tegenstelling tot tijdens de Koude Oorlog, toen nutsvoorzieningen grotendeels in overheidshanden waren en digitale infrastructuur nauwelijks bestond, vandaag het merendeel van de kritieke infrastructuur in private handen is. Daardoor is het volume aan privaat beheerde en tegelijk kwetsbare systemen sterk toegenomen. De Belgische Nationale Risicoanalyse toont bovendien aan dat verstoringen in deze infrastructuren vrijwel onmiddellijk domino-effecten veroorzaken in andere sectoren, zoals de gezondheidszorg, voedselketens, drinkwatervoorziening, mobiliteit en openbare orde.

Hoe werkgeversorganisaties en private bedrijven ingebed zijn in de Duitse weerbaarheidsstrategie

In Duitsland vormen werkgeversorganisaties en private bedrijven een structureel onderdeel van het nationale veiligheids- en weerbaarheidsbeleid. Dit komt omdat het grootste deel van de kritieke infrastructuur in private handen is. Daarom is samenwerking tussen de overheid en het bedrijfsleven niet facultatief, maar een fundament van het systeem. Dat gebeurt via drie belangrijke kaders: de Nationale Sicherheitsstrategie, UP KRITIS, en de Sektorenarbeitskreise (SAK).

1. Nationale Sicherheitsstrategie

De Duitse Nationale Veiligheidsstrategie beschouwt veiligheid als een gezamenlijke verantwoordelijkheid van overheid, burgers en bedrijven. De strategie stelt expliciet dat de economie een onmisbare partner is voor het veilig houden van toeleveringsketens, energievoorziening, digitale infrastructuur en logistieke netwerken. Werkgevers- en sectororganisaties fungeren hierbij als centrale gesprekspartners tussen de overheid en ondernemingen.

2. UP KRITIS – publiek-private samenwerking voor kritieke infrastructuur

UP KRITIS is het nationale publiek-private samenwerkingsplatform voor bescherming van Kritische Infrastructuur. Het brengt samen:

» private infrastructuurbeheerders

» sectorfederaties en werkgeversorganisaties

» federale instanties

De samenwerking richt zich op gezamenlijke risicoanalyses, beveiligingsstandaarden, informatie-uitwisseling, incidentrespons en oefeningen. Omdat ±85% van KRITIS in private handen is, zijn werkgeversorganisaties hier vaste en structurele partners.

3. Sektorenarbeitskreise (SAK) – operationele samenwerking per sector

Rond elke KRITIS-sector bestaan Sektorenarbeitskreise (SAK): vaste werkgroepen waarin de overheid, bedrijven en sectorfederaties operationeel samenwerken. Hier worden sectorale risico's in kaart gebracht, dreigingsbeelden gedeeld, maatregelen en normen ontwikkeld, en continuïteitsplannen afgestemd. De technische en operationele kennis van bedrijven en hun organisaties is hierbij cruciaal.

Materiële weerbaarheid

Een tweede kernpunt is dat Finland de materiële weerbaarheid institutioneel verankert via het National Emergency Supply Fund. Dit fonds ondersteunt verplichte en vrijwillige strategische voorraden, beheerd door private bedrijven, onder meer voor energie, voedsel, geneesmiddelen en vitale industriële producten. De overheid bepaalt de doelstellingen en controleert, maar de voorraden blijven in handen van de markt, wat efficiëntie en realiteitszin bevordert.[24]

Het Finse systeem toont aan hoe strategische voorraden en ketenweerbaarheid effectief kunnen worden georganiseerd via een duidelijke taakverdeling tussen overheid en private instanties. Dit model is bijzonder relevant voor België, zeker in sectoren met grote internationale afhankelijkheden. Binnen het Nationaal Weerbaarheidsplan is het daarom essentieel om een duidelijke strategie uit te werken voor het beheer van kritieke voorraden door private actoren. Daarnaast is het wenselijk dat de strategie ook steunt op de Preparedness Union Strategy van de Europese Commissie, waarin een Europese aanpak voor strategische voorraden van bijvoorbeeld zeldzame grondstoffen en vitale inputs wordt opgemaakt.

EU Prepardness Union Strategy

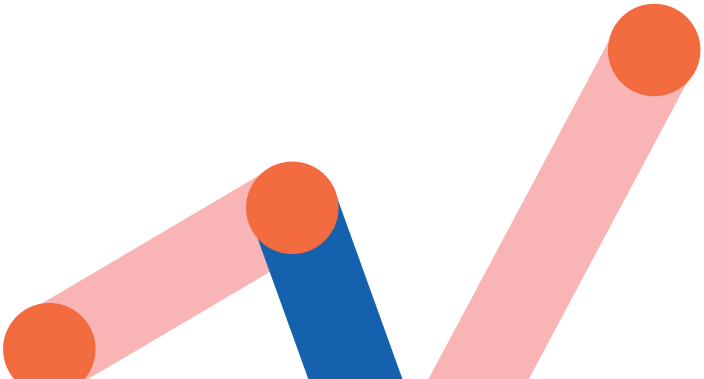
De EU-strategie voor paraatheid en weerbaarheid versterkt de civiele en militaire voorbereiding op toekomstige crisissen door nationale inspanningen beter op elkaar af te stemmen via een geïntegreerde overheidsbenadering (whole-of-government). Daarnaast wordt, samen met maatschappelijke actoren volgens een brede samenlevingsaanpak (whole-of-society), ingezet op het uitbouwen van een cultuur van weerbaarheid. Daarbij hanteert de EU een risico-overkoepelende benadering. Dit is een aanpak die vertrekt vanuit het principe dat men zich voorbereidt op uiteenlopende dreigingen (van natuurrampen tot cyberaanvallen en hybride dreigingen) binnen één geïntegreerd kader, in plaats van per risico afzonderlijk.

Samenwerking Defensie en industrie

Finland compenseert zijn beperkte binnenlandse defensie-industrie door civiele ondernemingen structureel te betrekken bij defensievoorbereidingen. Omdat het land relatief weinig gespecialiseerde defensiebedrijven heeft, sluit het logistieke commando van de Finse defensiemacht productiereserveringsovereenkomsten af met meer dan duizend niet-militaire private ondernemingen voor de productie van essentieel oorlogsmaterieel, zoals munitie. Deze afspraken worden gecoördineerd[25] in nauwe samenwerking met de NESA. Na de Russische invasie van Oekraïne activeerde Finland een deel van deze overeenkomsten om de werking ervan in crisistijd te testen en verder te verfijnen. De overeenkomsten zijn vrijwillig. Bedrijven engageren zich om bij te dragen aan de nationale defensie, terwijl Defensie gericht investeert in productiefaciliteiten en uitrusting die in noodsituaties kunnen worden ingezet. Daarnaast maakt de samenwerking met de overheid het mogelijk dat bedrijven in deze pools uitzonderingen kunnen aanvragen voor sleutelmedewerkers, zodat zij tijdens crisissen vrijgesteld worden van militaire dienst en de continuïteit van kritieke bedrijfsactiviteiten gewaarborgd blijft.

De defensie-industrie in dit land heeft gelijkenissen met die van Finland. Hoewel die aan het groeien is, is het te beperkt om alle capaciteiten van een defensiemacht te kunnen voorzien. Het is daarom ook belangrijk om naar Fins voorbeeld structuren en overeenkomsten af te sluiten die passen binnen de Nationale Verdedigingsplannen. Staten claimen formeel nog steeds een monopolie op het legitieme gebruik van geweld, maar de toenemende betrokkenheid van private actoren in defensie en veiligheid ondergraaft die aanname. Overheden kunnen zich daarom niet langer beperken tot louter ‘command and control’ van hun strijdkrachten, maar moeten actief nadenken over hoe zij samenhang en samenwerking organiseren met commerciële spelers. Dat geldt in het bijzonder voor bedrijven met internationale verankering, die belangen hebben buiten de Belgische grenzen.[26]

Bij de ontwikkeling van het Belgische Nationaal Enablementplan wordt de logistieke sector al sterk betrokken, omdat Defensie zelf niet over voldoende capaciteit beschikt om militair materieel te lossen en over het grondgebied te vervoeren. Diezelfde samenwerking met ondernemingen zou ook in andere onderdelen van het Nationale Verdedigingsplan en Nationaal Weerbaarheidplan moeten worden toegepast. Net zoals in Finland is het daarbij belangrijk dat de samenwerking vrijwillig blijft en niet gepaard gaat met verplichte rapportering.



Trainingen en oefeningen

Tot slot investeren Finland en Duitsland sterk in gezamenlijke training en oefeningen. Het Finse NESA organiseert sectoroverschrijdende oefeningen waarbij bedrijven samen trainen met ministeries, ngo's en andere sleutelactoren. Deelname is vrijwillig, maar sterk ingebed in een cultuur van collectieve verantwoordelijkheid. Bedrijven nemen deel omdat ze hun eigen paraatheid kunnen benchmarken, sectorbrede standaarden helpen ontwikkelen en samenwerken in een neutrale, vertrouwelijke omgeving.

Het Niinistö-rapport adviseert dat bedrijven systematisch zouden moeten deelnemen aan opleidingen en crisisoefeningen. In België zou het organiseren van cross-sectorale crisisoefeningen ter versterking van de weerbaarheid met bedrijven, overheden en hulpdiensten, een snelle hefboom zijn om maturiteit, vertrouwen en paraatheid te verhogen, zonder zware institutionele hervormingen. Een gedeeld plichtsbesef, de mogelijkheid om de eigen paraatheid te benchmarken, bij te dragen aan de versterking van de weerbaarheid van de hele sector en samen te werken in een neutrale omgeving, zijn factoren die ondernemingen motiveren om deel te nemen. Via een PPS kunnen gezamenlijke trainingen efficiënt georganiseerd worden.

Start met een investeringsagenda

Gezien de toenemende en structurele weerbaarheidsuitdagingen, is het aangewezen om een gerichte investeringsagenda voor weerbaarheidskosten uit te werken, die zowel publieke als private ondernemingen ondersteunt. Net als bij andere strategische investeringsdomeinen vraagt weerbaarheid om een samenhangende aanpak, met duidelijke prioriteiten, een coherent instrumentarium en afstemming tussen beleidsniveaus. Een dergelijke investeringsagenda moet vermijden dat weerbaarheidsinvesteringen versnipperd of ad hoc gebeuren, en moet ondernemingen stimuleren om tijdig en structureel te investeren in preventie, paraatheid en aanpassingsvermogen.

Voor wat is er aandacht nodig bij het opstellen van de investeringsagenda?

» **Gerichte O&O-investeringen op Vlaams niveau:** de Vlaamse Innovatie- en Industriestrategie voor Veiligheid en Defensie (VISD), die in februari 2026 is gelanceerd, biedt innovatieve kmo's en scale-ups ondersteuning bij projecten in strategische veiligheidssectoren zoals maritieme toepassingen, luchtvaart en (counter-)unmanned aircraft systems (UAS), ruimtevaart, AI, cyberveiligheid, biotechnologie, autonome systemen en energie/omgeving/geo-intelligentie. Door deze sectoren expliciet te positioneren en te verankeren, versterkt Vlaanderen niet alleen de weerbaarheid van individuele ondernemingen, maar bouwt het ook doelgericht aan een eigen weerbaarheidsindustrie. Deze aanpak

Lessen uit Nederland: Een structurele rol voor het bedrijfsleven in veiligheids- en weerbaarheidsbeleid

In het regeerakkoord van de regering Jetten vermeldt de nieuwe Nederlandse regering expliciet dat de weerbaarheid moet worden versterkt in nauwe samenwerking met de private sector. Er wordt ingezet op samenwerking met (innovatieve) technologiebedrijven, het delen van data met private partijen en een gecoördineerde aanpak tussen overheid, veiligheidsdiensten en bedrijfsleven om cyberdreigingen beter te detecteren en te bestrijden. Daarnaast wordt via samenwerkingsplatformen zoals Defport overheid, bedrijfsleven en kennisinstellingen samengebracht om de productiecapaciteit van de Nederlandse Defensie-Industrie aanzienlijk te verhogen.

In Nederland bestaat er bij de Rijksdienst voor Ondernemen een afdeling die zich specifiek bezig houdt met weerbaar ondernemen. Onderstaande omschrijving kan gelezen worden op de website: "Bent u werkzaam in een hightech vakgebied? Of heeft uw bedrijf waardevolle of sensitieve kennis? Houd dan rekening met specifieke risico's. Speciaal voor u zitten medewerkers klaar bij het Ondernemersloket Economische Veiligheid (OLEV)."

vergroot de strategische autonomie van de economie en creëert schaal in kennis, technologie en talent.

» **Federale fiscale stimulansen als hefboom voor private investeringen in weerbaarheid:** het federaal regeerakkoord voorziet de mogelijkheid om bepaalde investeringen, bijvoorbeeld in onderzoek en ontwikkeling, defensie en de energietransitie, tijdelijk versneld af te schrijven. Ondernemingen met meer dan vijftig werknemers, zouden die activa meer bepaald gedurende het eerste jaar kunnen afschrijven aan 40%.[27] De duurtijd waarbinnen deze activa zouden worden afgeschreven, vermindert door deze versnelde afschrijvingsannuïteit in het eerste jaar, wat een liquiditeitsvoordeel oplevert. Door deze regeling goed af te stemmen op investeringen die aansluiten bij de negen strategische doelstellingen van het Nationaal Weerbaarheidsplan, zou een directe fiscale prikkel ontstaan om sneller te investeren in weerbaarheid.

» **Een verbreding en versterking van bestaande defensiefondsen tot een breed weerbaarheids- en veerkrachtfonds, voortbouwend op de initiatieven die PMV vandaag al neemt:** voor ondernemingen die oplossingen ontwikkelen om de weerbaarheid van andere bedrijven en sectoren te versterken, zoals cybersecurityaanbieders, ontwikkelaars van beveiligingstechnologie en dual-use toepassingen, vormt dit een cruciale financieringshefboom. Door de defensiefondsen van PMV, LRM en SFPIM optimaal op elkaar af te stemmen en systematisch af te toetsen aan de prioriteiten van het Nationaal Weerbaarheidsplan, kan de impact van investeringen in cyberveiligheid, vitale infrastructuur en kennisbescherming maximaal worden versterkt, ten dienste van zowel ondernemingen als de bredere economie.

Daarnaast kan ook de Europese Investeringsbank (EIB) een belangrijke aanvullende rol spelen. De EIB kan voortaan investeren in veiligheid en defensie via publiek-private samenwerkingen, onder meer voor de bescherming van vitale infrastructuur, de versterking van nood- en communicatiesystemen en de modernisering van civiele infrastructuur met militair gebruik in crisistijd. Dit opent bijkomende financieringsmogelijkheden voor projecten die economische groei combineren met strategische en veiligheidsdoelstellingen, en versterkt zo de impact van de investeringsagenda op Europees niveau.

Beleidsaanbevelingen

Implementeer een weerbaarheidsmodel waarbij ondernemingen structureel worden betrokken ter voorbereiding van een crisis in fases, via een interfederaal publiek-privaat partnerschap die volgende doelstellingen heeft:

» Risico's monitoren, ketenafhankelijkheden analyseren, scenario's uitwerken en maatregelen voorbereiden om de continuïteit te verzekeren;

» Een samenwerkingsmodel uitwerken waarin de overheid en Defensie een ondernemersreflex ontwikkelen en verder gaan dan eenzijdige consultatie met commerciële spelers;

» Een duidelijke strategie uitwerken voor het beheer van kritieke voorraden in samenwerking met private actoren;

» Sectoroverschrijdende oefeningen organiseren waarbij bedrijven samen trainen met ministeries, ngo's en andere sleutelactoren;

» De aansluiting verzekeren met de Preparedness Task Force binnen de EU Preparedness Union Strategy;

Daarnaast bevelen wij aan:

» België kan binnen de opgerichte defensiefondsen van PMV en SFPIM de investeringen laten aftoetsen met de 9 strategische objectieven van het Nationaal Weerbaarheidsplan om zo tot een Weerbaarheid- en veerkrachtsfonds te komen;

» Maak werk van de versnelde afschrijvingsmogelijkheid voor specifieke investeringen in O&O, defensie en energietransitie, en breid de mogelijkheden uit naar bredere weerbaarheidsinvesteringen overeenkomstig met de negen strategische objectieven van het Nationaal Weerbaarheidsplan.

19. The National Emergency Supply Agency (2026)
20. Ruggiero et al., Enhancing societal resilience through the whole-of-society approach to crisis preparedness: Complex adaptive systems perspective – The case of Finland (2024)
21. Kähkönen, Preparing for a rainy day: What can EU member states learn from Finland's approach to resilience? (2024)
22. Finland Security Committee (2026)
23. European Commission, Safer together:A path towards a fully prepared Union (2024)
24. Kähkönen, Preparing for a rainy day: What can EU member states learn from Finland's approach to resilience? (2024)
25. Forsberg et al., Implications of a Finnish and Swedish NATO Membership for Security in the Baltic Sea Region (2022)
26. Rand Europe, Maneuver in the Marketplace: The Changing Economic Dimension of Warfare (2025)
27. Voor kleine ondernemingen wordt de herinvoering van het degressieve afschrijvingsregime voorzien.

Hoofdstuk 3. Een technologiestrategie ter versterking van groei en onafhankelijkheid

Dit hoofdstuk onderbouwt waarom Vlaanderen nood heeft aan een samenhangende technologiestrategie in een context van toenemende geopolitieke spanningen, hybride dreigingen en verscherpte mondiale concurrentie. Het onderzoekt hoe technologische keuzes steeds belangrijker worden voor onze economische slagkracht, innovatie en maatschappelijke weerbaarheid en waarom losse beleidsinitiatieven daarvoor onvoldoende richting geven.

De nood aan een technolgiestrategie

Vlaanderen heeft momenteel bestaande plannen voor AI, cybersecurity, cloud, … maar er ontbreekt een geïntegreerd overzicht van waar Vlaanderen technologisch staat en waar we naartoe willen. Andere landen zoals Nederland en Duitsland tonen hoe een nationale technologiestrategie richting geeft aan keuzes, innovatie verankert en Europese hefboomwerking mogelijk maakt. Voor Vlaanderen, met beperkte middelen, is zo'n strategie essentieel om sterktes in academische instellingen en bedrijven te bundelen tot één samenhangende technologische agenda.

Vlaanderen heeft nood aan een duidelijke technologiestrategie. Vlaanderen en Europa kunnen niet in alle technologieën tegelijk een leidende positie innemen, terwijl technologische concurrentie steeds bepalender wordt voor economisch verdienvermogen, het oplossen van maatschappelijke uitdagingen en de nationale veiligheid.[28] Door gericht te investeren in een beperkte set sleuteltechnologieën waarin Vlaanderen al sterke

wetenschappelijke, technologische en economische uitgangsposities heeft, kan de overheid innovatie versnellen, strategische afhankelijkheden verkleinen en de weerbaarheid van economie en samenleving versterken.

Lees hier de Voka Paper 'Drie wegen naar productiviteitsgroei'

De uitwerking van een technologiestrateige houdt daarmee gelijke tred met internationale innovatie, zoals de aanbeveling in de Voka Paper 'Drie wegen naar productiviteitsgroei'.

Tegelijk blijft een brede basis voor innovatie belangrijk om blinde vlekken te vermijden en samenwerking tussen technologieën mogelijk te maken. Net die combinatie van verschillende technologieën leidt vaak tot echte doorbraken.

Zo zorgen publieke en private investeringen samen voor duurzaam technologisch leiderschap, meer strategische autonomie en welvaart op lange termijn. Deze paper focust alvast op drie sleuteltechnologieën die, in het licht van de toegenomen hybride dreigingscontext, bijzonder relevant zijn voor de verdere economische uitrol van de Vlaamse technologiestrategie. Aanvullend kunnen ook andere technologieën in aanmerking komen, maar die vallen buiten het bestek van deze paper.

Cybersecurity als een van de prominente sleuteltechnologieën

Cybersecurity neemt een steeds belangrijkere plaats in binnen de economische en maatschappelijke weerbaarheid van Vlaanderen, onder meer door de toenemende digitale afhankelijkheid en hybride dreigingen. Dit maakt het aangewezen om cybersecurity expliciet te beschouwen als een sleuteltechnologie binnen een Vlaamse technologiestrategie en de beschikbare kennis en instrumenten beter op elkaar af te stemmen.

Een Vlaamse technologiestrategie moet niet alleen bepalen in welke technologische domeinen Vlaanderen wil uitblinken, maar ook het bestaande cybersecurity-instrumentarium van overheden overzichtelijk bundelen. Er is ruimte om bestaande initiatieven verder te versterken door ze toegankelijker en beter vindbaar te maken voor bedrijven. Een helder en geïntegreerd overzicht kan hen helpen gerichter gebruik te maken van beschikbare ondersteuning. VLAIO speelt hierin een centrale rol: via begeleidingstrajecten van haar partners, scaninstrumenten en steunprogramma's versterkt het de digitale en cyberweerbaarheid van ondernemingen. Het technologisch onderzoek in Vlaanderen is sterk, maar de valorisatie kan beter. Door VLAIO verder te positioneren als toegangspoort en gids kan Vlaanderen innovatie in cybersecurity sneller omzetten in concrete groeikansen en verhoogde bedrijfsweerbaarheid. Daarnaast loont het om een interfederale aanpak te ondersteunen waarbij initiatieven van het Centre for Cybersecurity Belgium (CCB) en VLAIO beter afgestemd zijn op elkaar.

Nederland leidt de weg: identificeren van sleuteltechnologieën

De Nederlandse technologiestrategie vertrekt vanuit de vaststelling dat het onmogelijk is om in alle technologieën tegelijkertijd leidend te zijn en kiest daarom voor focus en schaal.

Nederland identificeerde eerst 44 sleuteltechnologieën waarin het over een sterke kennis- en innovatiebasis beschikt en die op middellange termijn brede economische en maatschappelijke impact kunnen hebben. Op basis van een afwegingskader rond economisch verdienvermogen, maatschappelijke uitdagingen, nationale veiligheid en bestaande sterktes werd daaruit een selectie van tien prioritaire sleuteltechnologieën gemaakt, waaronder onder meer cybersecurity, artificiële intelligentie, quantumtechnologie, halfgeleiders, mechatronica en optische en fotonische systemen.

Voor deze prioriteiten zijn technologieagenda's uitgewerkt die telkens de definitie en strategische relevantie van de technologie, de huidige positie van Nederland en een concrete ambitie richting 2035 beschrijven, inclusief knelpunten, ecosystemen, betrokken spelers en opschalingsuitdagingen. Zo bepaalt het regeerakkoord van de Regering-Jetten dat de uitvoering van de Nationale Technologiestrategie wordt ondersteund door investeringen in regionale innovatieclusters, deelname aan Europese innovatieprogramma's en publiek-private innovatieprogramma's.

België wordt Europees en internationaal gezien als een land met een sterk ontwikkeld cybersecuritybeleid. In de National Cyber Security Index (NCSI) behoort België in 2025 tot de wereldwijde kopgroep met een vijfde plaats, dankzij solide beleidsmaatregelen, wetgeving en goed georganiseerde structuren. De vroege en coherente implementatie van de NIS2-richtlijn versterkt deze positie: België was de eerste lidstaat met een volledig wettelijk kader dat de beveiligingsverplichtingen voor ondernemingen verduidelijkt en de samenwerking tussen overheid, toezichthouders en vitale sectoren structureert. Andere lidstaten nemen deze aanpak intussen als referentie. Ook het bredere technologische ecosysteem

> **66% van de ondernemingen wil bijkomende maatregelen nemen om hun cyberveiligheid te versterken.**

draagt bij aan deze sterke positie. Het CCB geldt binnen Europa als voorbeeld, terwijl onderzoekscentra zoals COSIC en Distrinet tot de mondiale top behoren. Via VLAIO wordt bovendien geïnvesteerd in digitale autonomie en innovatie.

De algemene cyberveiligheidssituatie in België is echter minder eenduidig positief dan op het eerste gezicht lijkt. In november 2025[29] stelden ethische hackers 96 kwetsbaarheden vast bij overheidsdiensten, een stijging van 15% ten opzichte van 2024. Bovendien deden zich de afgelopen jaren meerdere cyberincidenten voor met verstrekkende gevolgen, wat aantoont dat ook een land met sterke institutionele fundamenten niet immuun is voor digitale ontwrichting. Ondanks de eerder beschreven structurele sterktes geven Vlaamse ondernemingen in de Voka Weerbaarheidsbevraging (zie hoofdstuk 4) aan dat zij zich nog steeds kwetsbaar voelen. Hoewel 54% van de bedrijven zichzelf voldoende weerbaar acht tegen cyberaanvallen of online misleiding, wil 66% bijkomende maatregelen nemen om hun cyberveiligheid te versterken. Ook andere dreigingen, zoals bedrijfsspionage, sabotage of uitval van digitale diensten, scoren laag in de zelfinschatting van weerbaarheid. Meer dan een derde van de ondernemingen beschouwt een uitval van telecomdiensten zelfs als een van de grootste bedreigingen voor hun operationele continuïteit.

Dit roept de vraag op hoe deze perceptie van kwetsbaarheid zich verhoudt tot het feit dat België internationaal bijzonder goed scoort op het vlak van cybersecurity. Een nadere blik op de bedrijven die aangeven extra maatregelen te willen nemen, biedt hiervoor een aanwijzing. Van deze groep zegt 58% nood te hebben aan begeleiding door experten, terwijl 40% aangeeft op zoek te zijn naar bijkomende informatie. Aangezien deze vormen van ondersteuning op overheidsniveau al bestaan, kan worden afgeleid dat zij ofwel onvoldoende hun weg vinden naar ondernemingen, ofwel niet als voldoende kwalitatief of toegankelijk worden ervaren. Het is daarbij belangrijk te benadrukken dat België het goed doet in vergelijking met andere landen, maar dat dit niet betekent dat de uitdagingen verdwenen zijn. Het wijst er vooral op dat België deze uitdagingen relatief beter beheerst, zonder ze volledig te kunnen uitsluiten.

De technologiestrategie kan ook een eerste stap vormen richting een duidelijker afbakening van de verantwoordelijkheden van ondernemingen en overheid op het vlak van cybersecurity.

Waar stopt de verantwoordelijkheid van het leger en start die van de onderneming?

In de fysieke wereld is de grens tussen publieke en private veiligheid doorgaans relatief duidelijk. De bescherming van het nationale grondgebied en de handhaving van de openbare orde behoren in de eerste plaats tot de

verantwoordelijkheid van publieke ordediensten, zoals het leger en de politie. Bedrijven huren bijvoorbeeld geen militairen in om hun fabrieksterreinen te beschermen. Ze plaatsen hekken, camera's en zetten privébewaking in om inbreuken door (niet-)statelijke actoren te voorkomen. Evenmin koopt een onderneming luchtafweersystemen om raketten neer te halen, dergelijke vormen van territoriale verdediging behoren tot de kerntaken van de overheid en haar veiligheidsdiensten.

Maar nieuwe technologieën vervagen die grens. De opkomst van drones roept bijvoorbeeld de vraag op of bedrijven, net als met hekken en sloten, ook eigen middelen moeten ontwikkelen om hun luchtruim te beschermen. Hoe ver moet private beveiliging gaan wanneer dreigingen niet meer alleen fysiek, maar ook technologisch of hybride zijn?

Die spanning wordt nog scherper in het cyberdomein. Bedrijven zijn dagelijks het doelwit van digitale aanvallen, soms door criminele netwerken, soms door statelijke actoren die economische of strategische schade willen berokkenen. Tot waar reikt hier de verantwoordelijkheid van de onderneming? Van bedrijven mag verwacht worden dat ze basisbescherming voorzien – denk aan firewalls, detectiesystemen, incidentrespons en opleiding van personeel – net zoals ze hekken plaatsen rond hun terrein. Maar wanneer een aanval duidelijk de schaal en intensiteit van een strategische operatie bereikt, gericht op het verstoren van vitale infrastructuur of meerdere sectoren tegelijk, verschuift de verantwoordelijkheid dan richting de overheid en het leger?

Het is precies in dat grijze gebied dat samenwerking noodzakelijk wordt. Defensie moet in staat zijn grootschalige of statelijke cyberdreigingen te herkennen en te neutraliseren, terwijl ondernemingen hun eigen digitale weerbaarheid op peil houden. Dat vraagt om een gezamenlijke strategie, met heldere afspraken over informatie-uitwisseling en verantwoordelijkheid. De grens tussen bedrijfsnetwerk en nationaal netwerk zal onvermijdelijk vervagen; de opdracht is die evolutie te organiseren en niet te laten ontsporen.

Artificial Intelligence

Artificiële intelligentie vormt een essentieel onderdeel van een technologiestrategie ter versterking van de weerbaarheid, aangezien AI gevaren inhoudt die zich over meerdere domeinen kunnen uitstrekken. In hybride oorlogsvoering zal AI-technologie een evolutie aandrijven waarbij dominantie in informatie en inzicht doorslaggevend kan blijken, door de snelheid, precisie en effectiviteit te vergroten waarmee informatie wordt ingezet en bruikbaar wordt gemaakt.[30] AI in asymmetrische oorlogsvoering kan bijzonder ontwrichtend zijn, omdat het kan leiden tot verregaande verstoring en overname van vrijwel alle domeinen van het maatschappelijk leven. Het heeft het potentieel om de economie, instellingen en het volledige sociale systeem van de doelstaat ernstig te verlammen.[31] AI kan ook in de positieve zin versterkend werken om weerbaarheid te verhogen. Zo speelt het nu al een belangrijke rol bij het voorspellen van verstoringen voordat ze zich voordoen. Door grote hoeveelheden data te analyseren kan AI vroegtijdige waarschuwingen geven over problemen in de toeleveringsketen, extreem weer of cyberdreigingen. Dit soort inzichten stelt organisaties in staat om maatregelen te nemen om deze risico's te beperken, in plaats van louter te reageren op crisissen terwijl ze zich ontvouwen.[32]

Zonder een robuuste en betrouwbare cloudinfrastructuur is grootschalige toepassing van artificiële intelligentie onmogelijk en voor een kennisintensieve economie als België betekent dit een structureel concurrentienadeel. Deze technologische soevereiniteit dient niet enkel een geopolitiek vraagstuk maar ook een economische noodzaak.[33] AI verandert de aard van kenniswerk fundamenteel: menselijke expertise wordt versterkt door technologie, waardoor werknemers in een 'superstate' belanden waarin productiviteit en innovatievermogen exponentieel toenemen. Wie toegang heeft tot veilige, soevereine digitale infrastructuur, kan deze transformatie benutten; wie afhankelijk blijft van externe spelers, neemt

Een cyber-trusted regio als exportproduct

De private cybersector groeit snel en telt zowel gevestigde spelers als innovatieve groeibedrijven die internationaal doorbreken, met sterke expertise in cybersecuritydiensten. Door dit duidelijker te positioneren binnen het bredere economische landschap ontstaan er kansen om technologie van eigen bodem verder te ontwikkelen, waardoor dienstverleners ook eigen producten kunnen commercialiseren en internationaal kunnen concurreren. Een gerichte technologiestrategie die good practices in kaart brengt en inzet op internationalisering kan deze groei versterken. In dat kader is de ambitie om België en Vlaanderen te profileren als een 'cyber-trusted regio' zowel geloofwaardig als strategisch waardevol: in een wereld waar grensoverschrijdend vertrouwen afneemt, kan aantoonbare cyberveiligheid uitgroeien tot een cruciale economische differentiator. Via een brede coalitie van federale en regionale overheden en private spelers kan zo een sterke internationale merkidentiteit worden opgebouwd, die niet alleen de weerbaarheid van het economisch weefsel versterkt, maar ook nieuwe welvaart creëert door exportgroei en internationale reputatie.

Best practice: de Nederlandse Agenda Digitale Open Strategisch Autonomie (DOSA)

1. Wat is DOSA (2023)?

De Nederlandse Agenda Digitale Open Strategische Autonomie (2023) beschrijft hoe Nederland minder afhankelijk wil worden van kwetsbare buitenlandse digitale technologieën, terwijl het open blijft voor internationale samenwerking. Het doel is meer controle over kritieke digitale systemen, data en technologische ketens.

2. Wat staat erin?

DOSA bevat een pakket maatregelen om strategische digitale afhankelijkheden te verkleinen, de veiligheid van vitale infrastructuren te verhogen en de Nederlandse en Europese technologische basis te versterken. De agenda zet in op veilige en soevereine cloudoplossingen, robuuste en beter beschermde data-infrastructuur, strengere cybersecuritynormen en scherpere monitoring van risico's in digitale waardeketens. Daarnaast stimuleert DOSA de ontwikkeling van innovatieve en betrouwbare technologische alternatieven, waaronder open-source-ecosystemen, en versterkt het de samenwerking tussen overheid, bedrijven en kennisinstellingen om digitale autonomie duurzaam op te bouwen.

3. Waarom versterkt dit de weerbaarheid?

De agenda maakt Nederland minder kwetsbaar voor geopolitieke druk, digitale sabotage en technologische ontwrichting. Door kritieke systemen veiliger en diverser te organiseren, wordt de continuïteit van overheid, economie en bedrijfsleven beter gewaarborgd in crisissituaties. Hierdoor wordt digitale en economische weerbaarheid structureel versterkt.

Het regeerakkoord-Jetten onderschrijft deze denkpiste en zegt dat de Nederlandse regering de digitale weerbaarheid wil versterken door te kiezen voor meer strategische autonomie, minder afhankelijkheid van buitenlandse technologie en de uitbouw van een sterke Nederlandse en Europese techsector, ondersteund door investeringen in sleuteltechnologieën zoals AI en cybersecurity, strengere beveiligingsnormen, centrale regie op het cyberbeleid en bijkomende maatregelen om vitale sectoren weerbaarder te maken via betere informatie-uitwisseling, stresstests en een actieve voorbereiding op grootschalige cyberaanvallen.

structurele risico's. Het loont dan ook om technologische soevereiniteit op te nemen in 'het Vlaams beleid voor Digitale Veiligheid'.

Quantumtechnologie

Quantumtechnologie vormt een opkomend strategisch risico doordat zij het potentieel heeft om bestaande fundamenten van digitale veiligheid en informatiebescherming te doorbreken.[32] Quantumtechnologie maakt gebruik van principes uit de kwantummechanica om informatie te verwerken, te communiceren en uiterst nauwkeurig te meten op manieren die met klassieke technologie niet mogelijk zijn. Dat maakt onder meer dat quantumcomputing de huidige cryptografische standaarden kunnen ondermijnen die cruciaal zijn voor overheidscommunicatie, financiële systemen en vitale infrastructuur.

Staten of actoren die als eerste over operationele quantumcapaciteiten beschikken, kunnen hierdoor een asymmetrisch voordeel verwerven, onder meer via het ontsleutelen van vertrouwelijke data en het creëren

Beleidsaanbevelingen

Ontwikkel een Vlaamse technologiestrategie die richting geeft aan het innovatie- en industriebeleid en expliciet inzet op het versterken van veiligheid, weerbaarheid en strategische autonomie.

- Maak keuzes door een beperkte set prioritaire sleuteltechnologieën te selecteren op basis van economisch potentieel, veiligheidsimpact en Vlaamse sterktes;
- Laat naast groei, innovatievermorgen en internationlisatiekansen, veiligheid en technologische soevereiniteit een voorwaarde zijn in de keuze voor prioritaire sleuteltechnologieën;
- Cybersecurity, artificiële intelligentie en quantumtechnologie zijn omwille van hun groeipotentie en weerbaarheidsbelang zeker prioritaire sleuteltechnologieën;
- Bepaal duidelijke ambities door per technologie een langetermijnvisie en concrete roadmap uit te werken.

van structurele afhankelijkheden.[35] In een context van hybride dreigingen en geopolitieke rivaliteit maakt dit quantumtechnologie tot een expliciet veiligheidsvraagstuk met verstrekkende maatschappelijke en economische gevolgen.

Tegelijk biedt quantumtechnologie belangrijke oplossingen en opportuniteiten om weerbaarheid en strategische autonomie te versterken. Quantumveilige cryptografie, quantumcommunicatie en geavanceerde sensortechnologieën maken een nieuwe generatie van beveiligde digitale infrastructuur mogelijk en verhogen het vermogen om risico's vroegtijdig te detecteren.[36] Voor een kennisintensieve regio als Vlaanderen biedt gerichte investering in quantumtechnologie bovendien aanzienlijke economische kansen, onder meer via hoogwaardige innovatie, talentontwikkeling en industriële valorisatie. Door quantumtechnologie expliciet op te nemen in een Vlaamse technologiestrategie kan Vlaanderen zijn digitale veiligheid versterken en actief bijdragen aan Europese technologische soevereiniteit. De Nederlandse Agenda Digitale Open Strategische Autonomie (DOSA) uit 2023 kan hier alvast als best practice gelden.

28. Wennink, 2025
29. Vrt, "Hack the government": 71 ethische hackers proberen Belgische overheidssystemen te kraken (2025)
30. Thiele, Artificial Intelligence – A key enabler of hybrid warfare (2020)
31. Sheikh, AI as a Tool of Hybrid Warfare (2022)
32. Arnold, The Practical Use of AI for Business Resiliency – Opportunities and Risks (2025)
33. FT, Europe has 'lost the internet', warns Belgium's cyber security chief (2025)
34. European Commission, Quantum as a disruptive technology in Hybrid Threats (2021)
35. Ali et al., Next-Generation Quantum Security: The Impact of Quantum Computing on Cybersecurity—Threats, Mitigations, and Solutions (2025)
36. Hanna, The Emerging Potential for Quantum Computing in Irregular Warfare (2025)

Hoofdstuk 4. Een vierstappenplan om weerbaarder te worden als onderneming

Dit hoofdstuk werkt een vierstappenplan uit dat ondernemingen helpt om hun weerbaarheid te versterken in een context van aanhoudende hybride dreigingen die zich situeren tussen oorlog en vrede. Het plan houdt rekening met internationale standaarden en best practices. Daarnaast toont het plan hoe weerbaarheid vandaag vaak nog louter en alleen op papier blijft staan, terwijl de uitvoering achterwege blijft. Door strategische, organisatorische en operationele keuzes te verbinden, biedt het hoofdstuk een concreet kader om bewustwording om te zetten in daadwerkelijke paraatheid en duurzaam concurrentieel voordeel.

Weerbaarheidsbevraging bij ondernemingen

Om beter te begrijpen hoe ondernemingen de toegenomen hybride dreiging ervaren, nam Voka een bevraging af bij zeventig ondernemers uit een geselecteerde groep bedrijven die actief zijn binnen het veiligheids- en defensiedomein. De resultaten tonen aan dat weerbaarheid steeds belangrijker wordt als strategisch thema, maar dat er nog duidelijke hiaten bestaan in kennis, voorbereiding en coördinatie. Vlaamse ondernemingen worden steeds vaker geconfronteerd met geopolitieke spanningen, cyberdreigingen, verstoringen in toeleveringsketens en uitval van vitale infrastructuur.

Alvorens een weerbaarheidsstrategie kan uitgewerkt worden, moet het concept ingang vinden bij ondernemingen. Meer dan de helft van de organisaties (56%) is goed vertrouwd met het begrip weerbaarheid en bespreekt dit ook op strategisch niveau. Tegelijk geeft 40% aan dat het thema slechts sporadisch of oppervlakkig aan bod komt, terwijl 4% het concept helemaal niet kent. Dit wijst erop dat weerbaarheid bij veel ondernemingen wel degelijk op de radar staat, maar dat ook bijna de helft er nog te weinig aandacht voor heeft.

Bijna de helft van de respondenten kreeg de voorbije drie jaar te maken met leveringsproblemen of cyberaanvallen, wat aansluit bij internationale analyses die geopolitieke instabiliteit en digitale dreigingen als structurele bedrijfsrisico's benoemen. Hoewel veel ondernemingen risico's in kaart brengen en kritieke processen identificeren, blijft de weerbaarheid vaak fragmentair: slechts een minderheid oefent crisissituaties of beschikt over geïntegreerde continuïteitsplannen. De eigen inschatting van paraatheid ligt daarbij niet altijd in lijn met de feitelijke kwetsbaarheid, vooral op het vlak van cyberdreigingen.

De bevraging toont daarnaast een duidelijke tweedeling in noden. Kmo's botsen vooral op hoge kosten (43%), een gebrek aan expertise (43%) en onvoldoende kennis over maatregelen (29%), terwijl grotere ondernemingen meer nood hebben aan duidelijke kaders, richtlijnen en sectorale afstemming (40%). Over alle ondernemingen heen vragen respondenten vooral meer informatie (45%), toegang tot expertenadvies (43%) en heldere beleids- en regelgevingskaders (40%), wat wijst op een breed en structureel ondersteuningsvraagstuk.

Kijkend naar de maatregelen die ondernemingen nemen om weerbaarder te worden, zijn volgende vier besluiten te vermelden:

Weerbaarheid wordt nog vooral als ‘analyse’ benaderd

De hoogste scores zijn: in kaart brengen (66%), inventariseren (59%), bespreken (50%). Dat zijn noodzakelijke stappen, maar ze blijven vaak in een fase waarbij weerbaarheid enkel op paper behandeld wordt.

De sprong naar ‘operational readiness’ is kleiner

Alles wat geld kost, weerstand oproept, of tijd vraagt (voorraad, oefenen, zelfredzaamheid) scoort lager (30% of 21%). Dat wijst op een gap tussen weten en doen.

Keten- en afhankelijkheidsdenken is nog onvoldoende ontwikkeld

Leveranciersafspraken (40%) en afhankelijkheden in kaart (36%) blijven achter op interne procesfocus. Terwijl veel hedendaagse crisissen net via ketens lopen (energie, componenten, IT, transport, geopolitiek).

Menselijke factor (training, routines) is onderbelicht

Zelfredzaamheid en oefenen (beiden 21%) tonen dat de ‘soft infrastructure’ van crisisbeheer (rolvastheid, communicatie, besluitvorming onder druk) vaak het laatste komt, terwijl het in de praktijk vaak de doorslag geeft.

Bedrijven bevinden zich vandaag in een fase waarin ze vooral inventariseren. Processen, risico’s en scenario’s worden opgelijst, maar die inzichten worden nog onvoldoende vertaald naar duidelijke keuzes. Echte weerbaarheid vraagt dat organisaties prioriteiten stellen en hun aandacht richten op een beperkt aantal cruciale kwetsbaarheden, gekoppeld aan duidelijke en concrete maatregelen om die risico’s te beperken. Daarnaast vormt het lage niveau van crisisoefeningen geen zwakte op zich, maar net een kans, omdat organisaties die bewust investeren in oefenen en simuleren relatief snel maturiteit opbouwen en ontdekken of plannen ook in de praktijk standhouden. Een derde aandachtspunt is het expliciet maken van afhankelijkheden, vooral in digitale systemen en toeleveringsketens, waar kwetsbaarheden vaak verborgen blijven tot ze zich in een crisis manifesteren. Tot slot moet weerbaarheid worden gezien als een volwaardige managementdiscipline en niet als een eenmalig project, maar als een vast ritme van evalueren, stress-testen en het regelmatig actualiseren van scenario’s, ingebed in de dagelijkse sturing van de organisatie.

Ondernemingen staan vandaag voor een fundamentele en structurele spanning in hun rol. Er wordt verwacht dat zij groei, innovatie en waardecreatie versnellen, terwijl zij tegelijk volledige verantwoordelijkheid dragen voor de continuïteit, betrouwbaarheid en weerbaarheid van hun organisatie. Besturen en investeerders accepteren geen groeistrategieën meer zonder aantoonbare bescherming van kritieke processen, data en reputatie, zeker nu grote cyberincidenten leiden tot operationele stilstand of financiële en reputatieschade. Tegelijk is het geen optie om strategische ambities af te zwakken om risico’s te vermijden, aangezien stilstand in veel sectoren onmiddellijk leidt tot concurrentieel verlies. Dit dwingt zaakvoerders om beslissingen te nemen die zowel groei mogelijk maken als structurele veerkracht inbouwen, vaak over silo’s en traditionele verantwoordelijkheden heen, zoals technologie, operations en aanvoerketens. Die gelijktijdige opdracht om groei en weerbaarheid samen te realiseren, zonder dat het ene het andere ondermijnt, is wat we vandaag de CEO-paradox[37] noemen.

Het versterken van de weerbaarheid van ondernemingen is in de eerste plaats een verantwoordelijkheid van de onderneming zelf. In de huidige verhoogde dreigingssituatie, die zich afspeelt in het spanningsveld tussen oorlog en vrede en wordt gekenmerkt door aanhoudende hybride dreigingen, volstaat een ad-hocbenadering niet langer. Ondernemingen worden gedwongen hun weerbaarheidsstrategie te herdenken of opnieuw op te bouwen, met een aanpak die afgestemd is op hun sector, schaal en internationale afhankelijkheden aan zowel vraag- als aanbodzijde. Het vierstappenplan dat hieronder wordt voorgesteld biedt daarvoor een gestructureerd kader en bouwt voort op de resultaten van de weerbaarheidsbevraging, aangevuld met inzichten uit de literatuur en bewezen praktijken uit het bedrijfsleven.

STAP 1

Veranker weerbaarheid strategisch via een bedrijfsbeleidsplan en scenariodenken

Weerbaarheid wordt het sterkst wanneer het bewust en expliciet op bestuursniveau wordt besproken. Organisaties merken dat ad-hocmaatregelen op de werkvloer weinig effect hebben als ze niet gedragen worden door duidelijke strategische keuzes. Benader weerbaarheid expliciet als een managementvraag: zorg voor een duidelijk kader dat bepaalt hoe de onderneming omgaat met onzekerheid en schokken.[38]

Het is daarbij belangrijk dat je aan de slag gaat met een formele beleidslijn waarin weerbaarheid expliciet wordt gedragen door de directie en de raad van bestuur. Dit schept duidelijkheid over rollen en verantwoordelijkheden en maakt zichtbaar hoe weerbaarheid doorwerkt in strategische keuzes, investeringen en groeitrajecten. Dat zorgt voor consistentie en houvast, zeker wanneer de druk toeneemt.

Concreet kunnen ondernemingen overwegen om:

- Weerbaarheid regelmatig te bespreken in strategische comités en bestuursvergaderingen, bijvoorbeeld als vast reflectiemoment naast de operationele agenda;
- Eén eindverantwoordelijke op directieniveau aan te duiden die het overzicht bewaart (een specifieke weerbaarheidsverantwoordelijke);
- Bij belangrijke beslissingen expliciet stil te staan bij weerbaarheid, door gerichte vragen te stellen bij overnames, IT-migraties of internationalisering.

Om deze gesprekken te structureren, kan scenariodenken een bijzonder nuttig hulpmiddel zijn. In plaats van te proberen de toekomst te voorspellen, helpt het om te werken met meerdere plausibele scenario's om het strategisch denkvermogen te vergroten. In scenarioworkshops met de directie en het bestuur kunnen organisaties zichzelf uitdagen met vragen zoals:

'Wat als dit scenario zich voordoet? Welke keuzes zouden we dan maken? Wat zouden we afbouwen, versnellen of net uitstellen?'

Scenario's kunnen volgende zaken behandelen:

- Trigger en tijdshorizon van het scenario
- Kritische aannames en belangrijkste onzekerheden
- Gevolgen voor strategie en groeikeuzes
- Concrete beslissingen: versnellen, pauzeren of stoppen

Een goede tip hierbij is om scenario's zo snel mogelijk te vertalen naar beslissingslogica. Dat kan bijvoorbeeld door:

- Per scenario eenvoudige beslissingsbomen uit te werken;
- De impact op strategie, investeringen en mogelijke exitbeslissingen te bespreken;
- Te toetsen wat elk scenario betekent voor de basisopstelling van een onderneming[39]: welke activiteiten moeten onder alle omstandigheden blijven functioneren?

STAP 2

Bouw systematische horizon scanning en vroegtijdige waarschuwing in

In deze stap analyseer je welke externe dreigingen een impact kunnen hebben op jouw onderneming. Strategische weerbaarheid vraagt continue alertheid. Wacht daarom niet tot risico's zich manifesteren, maar zet als onderneming een gestructureerd horizon-scanningproces op dat signalen, trends en spanningen detecteert vóór ze uitgroeien tot crisissen.[40] Dit sluit aan bij internationale richtlijnen rond risicomanagement, die expliciet benadrukken dat risico-identificatie en monitoring een doorlopend proces moeten zijn en geen eenmalige oefening.[41]

Organiseer dit proces niet in silo's, maar integreer het over functies en domeinen heen, waaronder technologie, geopolitiek, regelgeving, energie, arbeidsmarkt en klimaat. Organisaties die deze cross-functionele benadering hanteren kunnen sneller schakelen van bescherming naar aanpassingen en/ of groei.

Om van observatie naar actie te gaan, werkt een onderneming met vroege waarschuwingsindicatoren en duidelijke drempelwaarden. Het gebruik van vooraf vastgelegde signalen en triggers sluit aan bij best practices in risicomanagement en verhoogt de snelheid en kwaliteit van besluitvorming wanneer de onzekerheid toeneemt. Zodra deze drempelwaarden worden overschreden, moeten ze automatisch leiden tot escalatie, bijkomende analyse of gerichte besluitvorming.

Concreet wil dit zeggen dat

- Als onderneming voorzie je best een vast horizon-scanningproces dat analyses op vaste momenten evalueert, bijvoorbeeld op kwartaalbasis, zodat risico's systematisch worden opgevolgd en geactualiseerd;
- Organiseer je een multidisciplinaire input vanuit strategie, risicobeheer, informatietechnologie, juridische zaken en operationele werking, om versnippering te vermijden en samenhang te creëren;
- Koppel je inzichten uit horizon scanning rechtstreeks aan het enterprise risk management, zodat ze ook effectief doorwerken in beslissingen.

Met betrekking tot hybride aanvallen helpt een systematische horizon scanning om specifieke dreigingen als volgt in kaart te brengen. Onderstaande tabel biedt enkele illustratieve risicovectoren ter inspiratie; hybride dreigingen evolueren voortdurend en kunnen een veel breder en creatiever spectrum aan middelen en tactieken omvatten.

Risicovector	Typisch scenario	Doel van de aanvaller	Impact op de onderneming
Cyber- en operationeel	Ransomware legt productielijnen stil; malware blokkeert bedrijfssystemen	Economische dwang, creëren van onderhandelingshefboom	Omzetverlies, verstoringen in de supply chain, regelgevende boetes
Fysieke sabotage	Gemanipuleerde machines in magazijnen; brandstichting in logistieke knooppunten	Ontwrichting van vitale infrastructuur, machtsvertoon	Stilstand van faciliteiten, hoge nood- en herstelkosten, aansprakelijkheid rond werknemersveiligheid
Informatie en reputatie	Gelekte 'interne' nota's of gemanipuleerde berichten op sociale media die vertrouwen ondermijnen	Aantasten van vertrouwen, zaaien van wantrouwen, marktmanipulatie	Reputatieschade, volatiliteit van de aandelenkoers, klantenverlies
Economische dwang	Malware-gestuurde verstoring van de supply chain; gerichte marktgeruchten om aandelenkoers te drukken	Afdwingen van betalingen, verzwakken van onderhandelingspositie	Gedwongen betalingen, heronderhandeling van contracten, verlies aan onderhandelingsmacht

STAP 3

Identificeer afhankelijkheden en vitale functies

In deze fase onderzoek je waar je organisatie intern kwetsbaar is. Weerbaarheid vraagt scherpe keuzes: niet alles is even belangrijk. Via een impactanalyse van bedrijfsprocessen brengt de onderneming in kaart welke activiteiten, systemen en middelen cruciaal zijn voor continuïteit, veiligheid, compliance en vertrouwen. Dit leidt tot een duidelijke afbakening van de basisopstelling van een onderneming: het minimale geheel dat operationeel moet blijven bij ernstige verstoringen.[42]

Concreet omvat dit

- Identificatie van kritieke activiteiten die prioritair hersteld moeten worden;
- Bepaling van maximale aanvaardbare uitvaltijden;
- Koppeling aan herstelprioriteiten en continuïteitsstrategieën.

Daarnaast maakt de onderneming haar afhankelijkheden expliciet over de volledige waardeketen. Dat omvat leveranciers en single-source afhankelijkheden (afhankelijkheid van één enkele input), cloud- en SaaS-platformen, logistieke partners, energienetten en infrastructuur, evenals sleutelpersonen en geconcentreerde kennis. Door deze afhankelijkheden systematisch in kaart te brengen, worden kwetsbaarheden zichtbaar die de continuïteit en wendbaarheid van de organisatie kunnen beïnvloeden.[43]

Kennisveiligheid krijgt daarbij bijzondere aandacht. Kritieke knowhow, data en intellectuele eigendom worden beschermd via duidelijke toegangsniveaus, degelijke documentatie, back-ups en actieve kennisoverdracht. Concreet betekent dit onder meer het detecteren van afhankelijkheid van één IT- of cloudprovider en het identificeren van geografische concentratie en enkelvoudige faalpunten in de waardeketen. Deze stap vormt de basis voor gerichte bescherming en voor het creëren van flexibiliteit elders in de organisatie.

STAP 4

Test, organiseer en versterk weerbaarheid onder druk

Analyse alleen volstaat niet. Organisaties versterken hun weerbaarheid pas echt wanneer ze die actief testen onder realistische omstandigheden. Ondernemingen doen dit via geïntegreerde stressscenario's die meerdere vormen van externe druk combineren, zoals cyber-, operationele, financiële, juridische en reputatierisico's. Dergelijke hybride scenario's maken zichtbaar waar aannames fout lopen en waar besluitvorming onder druk tekortschiet.[44]

Concreet zet de onderneming in op het systematisch testen van haar weerbaarheid via

- Hybrid stress tests[45] die realistische crisissituaties simuleren over meerdere risicodomeinen heen;
- Tafeloefeningen[46] met directie en crisismanagementteam, om strategische en operationele besluitvorming onder tijdsdruk te testen;
- Dilemmasessies rond moeilijke strategische en operationele keuzes, die expliciet blootleggen waar trade-offs en escalaties nodig zijn.

Parallel aan deze testen richt de onderneming een multidisciplinair crisismanagementteam in. Best practices in crisisbeheer benadrukken dat een duidelijke rolverdeling, procedures en communicatielijnen essentieel zijn om verlamming te vermijden wanneer de druk[47] toeneemt.

Dit team beschikt over:

- Duidelijk afgebakende rollen en verantwoordelijkheden
- Vastgelegde interne en externe communicatiekanalen
- Objectieve escalatiecriteria en beslissingsdrempels, in lijn met goed risicomanagement

Daarbij verschuift de focus stap voor stap van enkel blijven functioneren naar echt wendbaar worden als organisatie. Organisaties die beslissingen waar mogelijk lager in de organisatie leggen, binnen duidelijke afspraken, middelen flexibel inzetten en bewust leren uit crisissen, kunnen zich sneller aanpassen en herstellen dan hun omgeving.[48]

Oefenen speelt hierin een sleutelrol. Door regelmatige crisisoefeningen, gerichte opleidingen en het jaarlijks verhogen van de ambitie en complexiteit van drills, verhogen ondernemingen hun maturiteit en verkorten ze hun responstijden.

Gebruik weerbaarheid als een opportuniteit

Met een Weerbaarheidsplan kunnen ondernemingen crisissen beheersen en er tegelijk kansen uit halen. Crisissen creëren niet alleen risico's, maar ook kansen. Dat geldt ook voor de huidige context van aanhoudende hybride dreigingen. Ondernemingen die in crisissituaties doordachte keuzes maken, kunnen vooruitgang boeken op het vlak van innovatie, cybersecurity, internationalisering en reputatie. Die effecten versterken rechtstreeks de bedrijfsweerbaarheid en vergroten het vertrouwen van klanten in de aangeboden producten en diensten.

Innovatie lijkt tijdens een crisis vaak beter mogelijk omdat een crisis een plots en onmiskenbaar gevoel van urgentie creëert, waardoor organisaties andere prioriteiten laten vallen en zich volledig kunnen richten op één concrete uitdaging, met een snelle reallocatie van middelen als gevolg. Die scherpe focus maakt het ieders verantwoordelijkheid om samen naar oplossingen te zoeken, wat nieuwe perspectieven en een grotere diversiteit aan ideeën samenbrengt. Tegelijk legitimeert diezelfde urgentie vormen van experimenteren en leren die in normale omstandigheden als verspilling zouden worden gezien. Omdat een crisis bovendien per definitie tijdelijk is, kunnen organisaties zich toestaan om gedurende een korte periode een uitzonderlijk hoge intensiteit en inzet aan te houden, wat samen een vruchtbare voedingsbodem vormt voor versnelde innovatie.[49]

Door cybersecuritytoepassingen binnen het bedrijf te versterken, verhoog je je weerbaarheid en verbeter je tegelijk je marktpositie. Goede cybersecurity levert niet automatisch meer klanten op, maar is wel essentieel om vertrouwen, servicekwaliteit en klantenloyaliteit te behouden in digitale en geautomatiseerde

dienstverlening.[50] Uit onderzoek blijkt ook dat voor 84% van de consumenten in het VK een bewezen staat van dienst in databeveiliging en bescherming van persoonsgegevens een cruciale rol speelt in hun aankoopbeslissing.[51] Eén studie vermeldt dat ondernemingen met een sterke cybersecurity het 7% beter doen dan de markt.[52] Verzekeraars vragen bij een grondige doorlichting steeds vaker om een duidelijk stappenplan voor cyberaanvallen en andere weerbaarheidsrisico's. Dankzij sterke cybersecurity neemt de operationele weerbaarheid toe, groeit het vertrouwen van verzekeraars en verstevigt de reputatie van de onderneming als betrouwbare en toekomstgerichte marktspeler.

In een context waarin hybride dreigingen structureel aanwezig zijn, vormt ondernemingsweerbaarheid een hefboom voor effectieve risicobeheersing en een versterking van de internationale competitiviteit. Wanneer een Vlaamse onderneming kan aantonen dat zij haar activiteiten ook tijdens hybride aanvallen zonder noemenswaardige verstoringen kan voortzetten, versterkt dit haar geloofwaardigheid en betrouwbaarheid op internationale markten. Die operationele robuustheid wordt zo een onderscheidende troef die de positie van Vlaamse ondernemingen op het internationale toneel structureel kan verbeteren.

37. World Economic Forum, CEO paradox: How to drive growth, ensure resilience during geopolitical turbulence (2025)
38. Asis International, Organisational Resilience Standard (2009)
39. Het minimale geheel van activiteiten, mensen en middelen dat onder alle omstandigheden moet blijven functioneren om de onderneming levensvatbaar te houden.
40. Siang, MIT Sloan: Ask Sanyin: How Do You Build for an Unpredictable Future? (2025)
41. ISO, Risk management — Guidelines (2018)
42. Thomson, What is the concept of a 'minimum viable company' and is it a useful approach? (2025)
43. De Tijd, Handleiding voor ondernemers in onzekere tijden (2025)
44. Cyber Risk GmbH (2026)
45. Hybrid Stress Testing is de methodologie waarmee de weerbaarheid van een organisatie wordt geëvalueerd onder gecombineerde financiële, operationele, cyber-, juridische, regelgevende, technologische en geopolitieke stressomstandigheden.
46. Gesimuleerde crisisscenario's waarbij directie en sleutelrollen rond de tafel beslissingen oefenen zonder operationele uitvoering.
47. Van Damme, Actieplan voor een weerbare supply chain (2022)
48. Uhlir, Decentralized Leadership: How It Drives Organizational Agility & Innovation
49. Johsnon & Murray, What a Crisis Teaches Us About Innovation (2020)
50. Panditharathna et al., How Cyber Security Enhances Trust and Commitment to Customer Retention: The Mediating Role of Robotic Service Quality (2024)
51. CBI (2018)
52. Bitsight (2020)

CONCLUSIE

Weerbaar worden is geen keuze meer, maar een absolute noodzaak

België bevindt zich in een veiligheidscontext waarin hybride dreigingen structureel en grensoverschrijdend zijn geworden en waarin economische, digitale en fysieke kwetsbaarheden elkaar versterken. Door zijn open economie, strategische infrastructuur en institutionele complexiteit is het land bijzonder gevoelig voor verstoringen die zich snel kunnen verspreiden over sectoren en bestuursniveaus heen. Weerbaarheid is daardoor geen louter defensief of militair vraagstuk meer, maar een kernvoorwaarde voor economische continuïteit, maatschappelijke stabiliteit en internationale geloofwaardigheid. Ondernemingen spelen hierin een sleutelrol, aangezien zij het merendeel van de kritieke infrastructuur, toeleveringsketens en digitale systemen beheren waarop veiligheid en welvaart steunen.

Deze paper toont dat weerbaarheid begint bij de onderneming zelf, maar niet kan slagen zonder een ondersteunend en samenhangend beleidskader. Het vierstappenplan biedt bedrijven een concreet handelingsperspectief om bewustwording te vertalen naar strategische keuzes, operationele paraatheid en competitief voordeel. Tegelijk maken internationale voorbeelden uit Finland, Duitsland en Nederland

duidelijk dat structurele publiek-private samenwerking onmisbaar is om risico's te delen, afhankelijkheden te beheren en gezamenlijke voorbereiding mogelijk te maken. Een robuust weerbaarheidsmodel, aangevuld met gerichte investeringen en gezamenlijke oefeningen, versterkt niet alleen crisisrespons maar ook het onderlinge vertrouwen tussen overheid en bedrijfsleven.

Tot slot onderstreept de paper dat technologische keuzes bepalend zijn voor de toekomstige weerbaarheid en autonomie van Vlaanderen en België. Een samenhangende technologiestrategie, met focus op sleuteltechnologieën zoals cybersecurity, artificiële intelligentie en quantumtechnologie, is essentieel om strategische afhankelijkheden te verkleinen en economische groeikansen te benutten. Door veiligheid, innovatie en soevereiniteit expliciet te verbinden, kan weerbaarheid uitgroeien tot een structurele hefboom voor duurzame welvaart. Zo wordt België niet alleen beter beschermd tegen hybride dreigingen, maar ook sterker gepositioneerd in een steeds competitievere en onzekerdere wereld.

Sterke instellingen en een stabiel veiligheidskader vormen de basis voor een weerbare samenleving en economie. In een wereld met toenemende hybride dreigingen, van cyberaanvallen tot sabotage en economische druk, is samenwerking tussen overheid en bedrijfsleven essentieel.

Deze Voka Paper draagt bij aan SDG 16 door het belang van goed bestuur en publiek-private samenwerking in het nationale weerbaarheidsbeleid te benadrukken. Ondernemingen zijn immers cruciale schakels in het beschermen van kritieke infrastructuur en economische continuïteit.

Voka pleit daarom voor een structurele verankering van ondernemingsweerbaarheid in beleidsplannen en voor een permanent partnerschap tussen overheid en bedrijven. Zo versterken we vertrouwen, stabiliteit en het vermogen om samen toekomstige dreigingen het hoofd te bieden.

Economische weerbaarheid vraagt sterke industrie, betrouwbare infrastructuur en voortdurende innovatie. In een context van hybride dreigingen, geopolitieke spanningen en verstoringen van kritieke infrastructuur worden robuuste economische structuren steeds belangrijker voor stabiliteit en groei. Deze Voka Paper draagt bij aan SDG 9 door het belang van innovatie, digitalisering en sterke infrastructuur te benadrukken voor een weerbare economie. Zo roept het onder meer op tot het uitwerken van een duidelijke technologische strategie die soevereiniteit en innovatie in bedrijven ondersteunt. Bedrijven moeten zich bovendien kunnen aanpassen aan schokken zoals cyberdreigingen, verstoringen in toeleveringsketens en geopolitieke spanningen.

Voka benadrukt daarbij het belang van samenwerking tussen overheid, bedrijven en kennisinstellingen om innovatie te versterken en strategische afhankelijkheden te verkleinen. Zo bouwen we aan een sterke, toekomstbestendige economie die beter bestand is tegen externe schokken.

Vlaams
netwerk van
ondernemingen

Samen ondernemen, samen groeien.