

Resilience-led Advantage: van compliance naar collectieve weerbaarheid

Een perspectief op geïntegreerde weerbaarheid
voor kritieke sectoren in Nederland



Inhoud

Wat is resilience en waarom nu?	03
Een terugblik in vogelvlucht op de juridische kaders	04
De CER-richtlijn	05
Tijdlijn CER en Wwke	06
De weg naar NIS2	07
De rol van de publieke sector	08
Een whole-of-society approach	09
De spanning in de oplossing	10
Concluderend	11
Neem contact op	12

Wat is resilience en waarom nu?

Het begrip resilience heeft in uiteenlopende vakgebieden zoals psychologie, organisatiekunde en defensie steeds dezelfde kern: het vermogen van een systeem om onder druk zijn functies te behouden en zich daarna te herstellen of opnieuw in te richten.

In 2022 publiceerden we al 'Brilliance in Resilience, A guide for European companies to survive and thrive in a sea of crises' samen met Critical Future. Daarin presenteerden we een eigen model voor organisatorische weerbaarheid waarmee bedrijven verstoringen niet alleen defensief opvangen, maar ook offensief in kansen omzetten.

In deze publicatie werd vanuit ecosysteem perspectief weerbaarheid al uitdrukkelijk in de bredere keten- en netwerkcontext geplaatst. Juist dat element nemen we hier als vertrekpunt. Waar Brilliance in Resilience de weerbaarheid binnen de organisatie centraal stelde, verschuift dit stuk de blik naar de weerbaarheid tussen organisaties.



Weerbaarheid is verschoven van een interne IT- en compliancevraag naar een collectieve sectoroverstijgende ontwerpopgave. Juist die verschuiving maakt de nieuwe wetgeving, de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke), tot een strategische hefboom in plaats van een afvinklijst. Het zou alleen niet enkel de wetgeving moeten zijn die als hefboom dient voor organisaties om de voorgeschreven maatregelen te nemen. Juist de overtuiging van de intrinsieke noodzaak die elke organisatie zou moeten voelen om deze maatregelen te willen implementeren als absolute noodzaak voor haar eigen operationele continuïteit, zou de boventoon moeten voeren. Want de juridische kaders schrijven in principe enkel het 'bare minimum' voor die een volwassen organisatie al lang zou moeten hebben geïmplementeerd, vanuit een eigen behoefte aan een wendbare, solide en toekomstbestendige bedrijfsvoering.

Dat is de kern van dit stuk.

In organisaties werd weerbaarheid lange tijd als IT-vraagstuk benaderd. Een robuust systeem, een goed beveiligd datacenter, een continuïteitsplan in de kast. Tegen een pandemie, een oorlog in Oekraïne, een beschadigde onderzeese kabel of een ransomware-aanval die tegelijk ziekenhuizen, havens en gemeenten raakt, houdt die aanpak geen stand meer. De wereld raakt steeds verder verbonden op alle vlakken en lagen.

De Europese regelgeving over kritieke infrastructuur is in de afgelopen jaren wezenlijk van karakter veranderd. Waar het oorspronkelijke kader zich beperkte tot het beschermen van fysieke infrastructuur in slechts de energiesector en de transportsector, is de focus verschoven naar het weerbaar maken van organisaties en processen over elf sectoren heen. Dat is de CER-richtlijn, die in Nederland is geïmplementeerd in de Wwke. Daarnaast staat een parallel en bewust gekoppeld kader voor digitale weerbaarheid: de NIS2-richtlijn, die in Nederland is geïmplementeerd in de Cbw. Tegelijkertijd heeft de publieke sector een nadrukkelijk actievere ondersteunende en coördinerende rol gekregen. Niet langer alleen toezicht, maar ook strategie, risicobeoordeling, informatie-uitwisseling en bijstand aan kritieke entiteiten.

Een terugblik in vogelvlucht op de juridische kaders



Het begon met de ECI-richtlijn, Richtlijn 2008/114/EG, het eerste EU-rechtsinstrument met een Unie-brede procedure voor het identificeren en aanmerken van Europese kritieke infrastructuren. Zij voorzag ook in een beoordeling of de bescherming daarvan tegen door de mens veroorzaakte dreigingen en natuurrampen verbeterd moest worden. Kenmerkend was de beperkte reikwijdte. De richtlijn was alleen gericht op de energiesector en de transportsector. Daarnaast was zij assetgericht in plaats van organisatiegericht. De nadruk lag op de bescherming van de infrastructuur zelf.

De richtlijn voorzag echter niet in bredere maatregelen om de weerbaarheid te vergroten van de entiteiten die deze infrastructuur exploiteren. Vanwege haar te smalle scope en de ruime ruimte voor nationale interpretatie is deze richtlijn ingetrokken en vervangen door de CER-richtlijn (EU) 2022/2557 over de weerbaarheid van kritieke entiteiten. Parallel daaraan heeft de NIS2-richtlijn (EU) 2022/2555 de NIS1-richtlijn vervangen. Samen beogen zij een omvattende aanpak van zowel de fysieke als de digitale weerbaarheid van kritieke entiteiten met een periodieke risicobeoordeling, een zorgplicht en een meldplicht.

De fysieke en operationele kant ligt in de CER, geïmplementeerd in Nederland in de Wwke; de digitale kant in de NIS2, geïmplementeerd in Nederland in de Cbw. De Eerste Kamer heeft op 7 juli 2026 met beide wetten ingestemd en zij zijn op 15 augustus 2026 in werking getreden. Vanaf dat moment gelden nieuwe verplichtingen voor ruim 8.000 organisaties in Nederland op het gebied van cyberbeveiliging.

De CER-richtlijn

De CER-richtlijn richt zich op de fysieke en operationele weerbaarheid van organisaties die essentiële diensten verlenen. Het oogmerk is het verhogen van de weerbaarheid van zogenoemde kritieke entiteiten. Qua scope bestrijkt zij elf sectoren: energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, overheid, ruimtevaart en levensmiddelen.

Het doel is de continuïteit van essentiële dienstverlening binnen de interne markt te borgen door de verschillen weg te nemen die tussen lidstaten bestonden in de eisen aan kritieke entiteiten. De strekking is dat entiteiten incidenten moeten kunnen voorkomen, beperken en beheersen en zich daaraan kunnen aanpassen. Dat is verankerd in een periodieke risicobeoordeling (artikel 14 Wwke als implementatie van artikel 12 CER), een zorgplicht (artikel 15 Wwke als implementatie van artikel 13 CER) en een meldplicht (artikel 17 Wwke als implementatie van artikel 15 CER).

Het geheel is ingebed in een stelsel van wederkerige verantwoordelijkheden tussen lidstaat en entiteit. De maatregelen onder de zorgplicht, zoals preventie, fysieke beveiliging, incidentbestrijding, herstel en personeelsbeveiliging, worden nader uitgewerkt in het Besluit weerbaarheid kritieke entiteiten oftewel het Bwke. Voor kritieke entiteiten in de sectoren bankwezen, infrastructuur voor de financiële markt en digitale infrastructuur gelden de risicobeoordeling, de zorgplicht en de meldplicht van de Wwke niet (artikel 23 Wwke); voor de financiële sectoren geldt DORA en voor digitale infrastructuur de Cbw.



Tijdslijn CER en Wwke

De Wwke is op 15 augustus 2026 in werking getreden. De eerste aanwijzingen van kritieke entiteiten in de sectoren uit de bijlage bij de wet moesten binnen één maand daarna plaatsvinden, dus uiterlijk op 15 september 2026 (artikel 43 Wwke). Na aanwijzing geldt: binnen negen maanden een eigen risicobeoordeling en binnen tien maanden volledige zorgplicht en meldplicht (artikel 14, derde lid, artikel 15, zesde lid, en artikel 17, zevende lid, Wwke). Voor wie in september 2026 wordt aangewezen, betekent dat een afgeronde risicobeoordeling uiterlijk in juni 2027 en volledige naleving van zorg- en meldplicht uiterlijk in juli 2027. Gegeven de scope is dat een krap jaar.

De verschuiving van twee naar elf sectoren is niet de enige belangrijke ontwikkeling. Ook de focus is verbreed. Waar deze eerst gericht was op de infrastructuur en op losse fysieke beschermingsmaatregelen, is een samenhangende aanpak ontstaan: fysieke beveiliging en operationele processen zijn geregeld in de CER en de Wwke, digitale beveiliging in NIS2 en de Cbw, en beide kaders zijn wettelijk aan elkaar gekoppeld. Entiteiten moeten incidenten kunnen voorkomen, bestrijden, beperken en beheersen en zich daartegen kunnen beschermen of eraan kunnen aanpassen. De gehele keten van preventie tot herstel wordt zo hun eigen weerbaarheidsverantwoordelijkheid.

De aanleiding voor de verbreding is de toegenomen onderlinge verwevenheid. Een incident dat beperkt is tot een entiteit of sector kan bredere cascade-effecten hebben met verstrekende en langdurige gevolgen voor de interne markt. Denk aan de Iberische stroomuitval op 28 april 2025: het Spaans-Portugese elektriciteitsnet stortte in minder dan negentig seconden volledig in. Zevenenveertig miljoen mensen kwamen zonder stroom te zitten. Het Expert Panel van ENTSO-E concludeerde in maart 2026 dat de directe oorzaken technisch waren, met name tekortkomingen in spanningsregeling en reactief vermogen die tot cascaderende afschakelingen leidden en beval sterkere coördinatie en data-uitwisseling tussen netbeheerders aan om herhaling te voorkomen.



De weg naar NIS2

NIS2 is het digitale spiegelbeeld van de CER-richtlijn.

De eerste cyberwetgeving was de NIS1-richtlijn die in Nederland is geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen oftewel de Wbni. NIS1 was de eerste omvattende EU-wetgeving gericht op het versterken van de cyberbeveiliging van netwerk- en informatiesystemen om vitale diensten voor de economie en samenleving van de Unie te beschermen. Zij zorgde voor de eerste nationale strategieën en capaciteiten voor de beveiliging van netwerk- en informatiesystemen en voor regelgeving gericht op essentiële infrastructuur en door de lidstaten geïdentificeerde entiteiten. Kenmerkend voor die eerste richtlijn was opnieuw de fragmentatie.

Op grond van Richtlijn (EU) 2016/1148 waren de lidstaten zelf verantwoordelijk voor het identificeren van de entiteiten die voldeden aan de criteria om als aanbieder van essentiële diensten te worden aangemerkt. Dat leidde tot grote verschillen tussen lidstaten voor wat betreft het soort eisen, de mate van detail en de wijze van toezicht. Het gevolg waren extra kosten en problemen voor grensoverschrijdend opererende entiteiten. Daarom is in december 2022 de NIS2-richtlijn aangenomen. De richtlijn trad in januari 2023 in werking. Lidstaten hadden tot 17 oktober 2024 de tijd om NIS2 om te zetten in nationaal recht.

De NIS2 streeft naar een hoog gezamenlijk niveau van cyberbeveiliging om de betrouwbaarheid en veiligheid van netwerk- en informatiesystemen te garanderen. Qua scope geldt zij voor essentiële en belangrijke entiteiten in zeer kritieke en kritieke sectoren. Dat zijn grotendeels dezelfde sectoren als bij de CER aangevuld met onder meer digitale dienstverleners, postdiensten, afvalbeheer, vervaardiging, chemie en onderzoek.

Het doel is het EU-brede cyberbeveiligingsniveau te verhogen via een ruimere reikwijdte, duidelijkere regels en sterkere toezichtinstrumenten. De strekking is een afdwingbare zorgplicht inclusief ketenbeveiliging, een meldplicht voor significante incidenten en geharmoniseerd toezicht met sancties.

De verschuivingen ten opzichte van NIS1 lopen opvallend parallel aan die van ECI naar CER. Een belangrijk verschil met de CER is echter de manier waarop entiteiten in beeld komen. Waar de Wwke werkt met expliciete aanwijzing per entiteit (artikel 6 Wwke), kent NIS2 grotendeels een automatische scope op basis van sector en omvang. Die zogenoemde size-cap betekent dat in beginsel middelgrote en grote organisaties binnen bereik vallen. Ook hier is de reikwijdte van sectoren uitgebreid omdat de Europese Commissie alle organisaties wil bestrijken die belangrijke functies in de samenleving vervullen.

NIS2 is daardoor ook van toepassing op sectoren als vervaardiging en afvalbeheer en raakt, via de eisen aan ketenbeveiliging, indirect ook de toeleveringsketen en is daarmee nog breder en bestrijkt achttien sectoren. Daarmee komen ook organisaties die zelf niet essentieel zijn maar wel toeleverancier van een kritieke partij met de verplichtingen in aanraking. Vergelijkbaar met de zorgplicht in de CER moeten entiteiten op grond van artikel 21 NIS2 (artikel 21 Cbw) passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor hun netwerk- en informatiesystemen te beheersen en incidenten te voorkomen of de gevolgen ervan te beperken. De minimumlijst omvat onder meer risicoanalyse, back-upbeheer, ketenbeveiliging, cyberhygiënetraining en multifactor-authenticatie. Daarnaast gelden een registratieplicht in het nationaal register van entiteiten (artikelen 43 en 44 Cbw) en een meldplicht voor significante incidenten (artikel 25 Cbw). De Cbw betreft bovendien het bestuur expliciet: het bestuur keurt de maatregelen goed en ieder bestuurslid moet aantoonbaar over de benodigde kennis en vaardigheden beschikken (artikel 24 Cbw).

De rol van de publieke sector

De publieke sector heeft in dit stelsel een dubbele positie. Enerzijds is zij regisseur: zij stelt de nationale strategie vast, beoordeelt risico's, houdt toezicht en biedt ondersteuning aan kritieke entiteiten. Anderzijds is zij zelf normadressaat. Onder de Cbw worden de centrale overheid (ministeries en hun dienstonderdelen) en de decentrale overheden (provincies, gemeenten en waterschappen) van rechtswege als essentiële entiteit aangemerkt, ongeacht hun omvang. Zelfstandige bestuursorganen (ZBO's) van de centrale overheid en de openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties van gemeenschappelijke regelingen zijn eveneens essentiële entiteit, voor zover zij voldoen aan de definitie van overheidsinstantie (artikel 8, eerste lid, onder g en h, en artikel 1 Cbw; artikel 6 punt 35 NIS2). Uitgezonderd zijn instanties die hoofdzakelijk actief zijn op het gebied van nationale veiligheid, defensie, openbare veiligheid of rechtshandhaving (artikel 5 Cbw).

Onder de Wwke ligt dat anders. Daar geldt geen automatische kwalificatie, maar een aanwijzing per entiteit. De vakminister wijst kritieke entiteiten aan na overleg met de minister van Justitie en Veiligheid (artikel 6 Wwke) en houdt daarbij rekening met de nationale strategie (artikel 13 Wwke) en de sectorale risicobeoordeling (artikel 9 Wwke). De minister van Justitie en Veiligheid is stelselverantwoordelijk: hij stelt de nationale strategie vast (artikel 13 Wwke), vervult de rol van centraal contactpunt (artikel 12 Wwke) en bewaakt de samenhang van het stelsel. De vakministers zijn de bevoegde autoriteit voor hun eigen sectoren (artikel 8 Wwke). Zo kunnen waterschappen worden aangewezen als kritieke entiteit in de sector kernen en beheren, een sector die Nederland op grond van artikel 7 Wwke aan de elf Europese sectoren heeft toegevoegd, en kunnen gemeenten via bijvoorbeeld afvalwater in beeld komen.

De twee stelsels zijn bewust op elkaar aangesloten. Elke entiteit die onder de Wwke als kritieke entiteit is aangewezen, is van rechtswege ook essentiële entiteit onder de Cbw (artikel 8, eerste lid, onder i, Cbw). Fysieke en operationele weerbaarheid en digitale weerbaarheid worden zo aan elkaar gekoppeld.



Een whole-of-society approach

Resilience wordt zo steeds meer gepositioneerd in een 'whole-of-society approach'. De kern is dat weerbaarheid geen eigenschap meer is van een enkele organisatie. Zij ontstaat of ontbreekt in de ruimte tussen organisaties.

Waarom dit nu urgent is: vier verstoringen, één patroon

Dat de wetgever ecosysteemdenken voorschrijft is geen academische keuze. Recente verstoringen laten zien hoe snel een incident in één knooppunt zich over sectoren en landsgrenzen verspreidt en hoe vaak governance en coördinatie daarbij de bottleneck blijken. Niet de techniek.

NotPetya 27 juni 2017. Een Oekraïens boekhoudsoftwarepakket cascadeerde binnen uren naar Maersk en legde zeventien APM-terminals wereldwijd plat, waaronder Rotterdam. Daar moest de havenmeester per telefoon worden gewaarschuwd omdat een gedeelde meldstructuur simpelweg niet bestond. Dit was de aanleiding voor de oprichting van het Haven Cyber Meldpunt Rotterdam in 2018.

CrowdStrike-uitval 19 juli 2024. Een foutieve update van een cyberbeveiligingsleverancier crashte binnen uren 8,5 miljoen Windows-systemen en ontwrichtte gelijktijdig luchtvaart, ziekenhuizen, banken, meldkamers en retail. De geschatte wereldwijde schade bedroeg tien miljard dollar zonder dat er een hacker aan te pas kwam.

Oostzee-infrastructuur 2022 tot 2025. Een reeks beschadigingen van, en deels aantoonbare sabotage aan, onderzeese kabels en pijpleidingen waaronder Nord Stream in 2022, Balticconnector in 2023 en BCS East-West en C-Lion1 in november 2024 en Estlink 2 op kerstdag 2024 maakte zichtbaar dat een kabelbreuk tegelijkertijd energiezekerheid, telecom, bankverkeer en militaire communicatie raakt. Beheersing is uitsluitend multinationalaal te beleggen waarop de NAVO in januari 2025 met Baltic Sentry reageerde.

Daarnaast laat de **Iberische stroomuitval van 28 april 2025**, die wij eerder noemden, eenzelfde patroon zien: zevenenveertig miljoen mensen zonder stroom binnen negentig seconden, met een technische trigger in de spanningsregeling en met coördinatie tussen netbeheerders als kwetsbaarheid in preventie en herstel.

Steeds dezelfde conclusie. Een verstoring in een knooppunt cascadeert binnen uren door meerdere sectoren en landsgrenzen. Werkelijke beheersing vraagt om governance en samenwerking die tussen organisaties en dimensies is belegd, en niet binnen één.

De spanning in de oplossing

Wie collectieve weerbaarheid bepleit, moet eerlijk zijn over de spanning die de oplossing zelf introduceert. Een gedeeld operationeel beeld, één betrouwbare bron en gegevensdeling over sectoren heen, maakt sterker. Maar juist doordat alles op één plek samenkomt, ontstaat er ook een nieuwe zwakke plek. De gedeelde data laag waarop alle partners in crisis sturen wordt zelf een knooppunt dat kan uitvallen, gemanipuleerd of gegijzeld worden.

Dat is precies het cascademechanisme dat collectieve weerbaarheid juist wil voorkomen. Hetzelfde geldt bestuurlijk. Het delen van afhankelijkheids- en kwetsbaarheidsinformatie tussen partijen die elkaars concurrent zijn, stuit op gerechtvaardigde terughoudendheid rond aansprakelijkheid, mededinging en vertrouwelijkheid.

En een 'whole-of-society approach' klinkt verbindend, maar verplaatst de kernvraag slechts: wie heeft in crisis het mandaat om over organisatiegrenzen heen te besluiten en wie draagt de gevolgen als dat besluit verkeerd uitpakt? Deze spanningen zijn geen reden om de ecosysteemaanpak los te laten. Zij laten zien dat weerbaarheid niet met een platform of een dashboard is opgelost, maar een ontwerp vraagstuk is van governance, vertrouwen en heldere besluitvormingsrechten. Juist daar ligt het verschil tussen technische integratie en een bestuurbaar model.

En juist daar ligt voor bestuurders het strategische werk dat de wet uiteindelijk vraagt; meer dan de wettekst zelf op het eerste gezicht laat zien.



Concluderend

De juridische, technologische en geopolitieke ontwikkelingen wijzen alle dezelfde kant op. Weerbaarheid is geen eigenschap meer van een afzonderlijke organisatie. Zij ontstaat of ontbreekt in de ruimte tussen organisaties.

De Wwke codificeert die werkelijkheid door kritieke entiteiten expliciet te verplichten hun afhankelijkheden van en voor andere sectoren mee te wegen (artikel 14, tweede lid, Wwke); de Cbw doet hetzelfde voor de toeleveringsketen (artikel 21, derde lid, onder d, Cbw). Wat de wet echter niet biedt, afgezien van de mogelijkheid voor kritieke entiteiten binnen een groep, gemeenschappelijke regeling of andere duurzame samenwerkingsstructuur om hun risicobeoordeling gezamenlijk uit te voeren en hun maatregelen gezamenlijk te beschrijven (artikel 14, vijfde lid, en artikel 15, vierde lid, Wwke), is een instrument waarmee partijen die onderlinge afhankelijkheid sectoroverstijgend gezamenlijk in beeld brengen, besturen en oefenen.

Dat is precies de plek waar sectorale risicobeoordelingen in de praktijk stuklopen. Voor bestuurders van kritieke entiteiten betekent dit een dubbele opgave. Aan de ene kant moet de eigen organisatie tijdig voldoen aan een afdwingbare zorgplicht, met krappe doorlooptijden tussen aanwijzing en volledige naleving.

Aan de andere kant levert die zorgplicht binnen de eigen muren onvoldoende weerbaarheid op zolang de afhankelijkheden in de keten en het bredere ecosysteem niet expliciet zijn geadresseerd.

Daarmee staan bestuurders voor een scherpere keuze dan de wettekst op het eerste gezicht suggereert. Niet de keuze om alles tegelijk te doen, dat kan geen enkele organisatie, maar de keuze hóé je begint. Wie elke maatregel als een losstaande verplichting afvinkt, met afzonderlijke risicobeoordelingen voor soevereiniteit, cyber en continuïteit, voldoet juridisch. Maar wie in de volgende cascade terechtkomt, staat alsnog stil, omdat de afhankelijkheden die de verstoring dragen nooit in samenhang in beeld zijn gebracht.

Het alternatief vraagt niet om alles ineens, maar om een andere blik op waar je start. Een organisatie kan haar weerbaarheid heel goed langs één dimensie beginnen te versterken, cybersecurity, soevereiniteit of operationele continuïteit, zolang die eerste stap wordt gezet als onderdeel van een samenhangend geheel en niet als eindpunt. Want geen van de dimensies levert op zichzelf werkelijke weerbaarheid op: een soevereine datalaag zonder cyberweerbaarheid is kwetsbaar, cyber zonder operationele continuïteit dekt de fysieke keten niet en alle drie samen missen hun waarde zonder de samenwerking die ze over organisatiegrenzen heen verbindt. De dimensies verstevigen elkaar of ze verzwakken elkaar; neutraal naast elkaar bestaan doen ze niet.

Contact:



Belle Webster
Associate Partner
Eraneos

belle.webster@eraneos.com

Daar ligt wat wij Resilience-led Advantage noemen.

Waar dit stuk het waarom en het wat schetst, ligt het hoe in de praktijk: langs welke dimensies een organisatie begint en welke eerste stappen verantwoord en haalbaar zijn. Eraneos begeleidt organisaties op die route langs vier samenhangende dimensies: soevereiniteit, operationele continuïteit, cybersecurity en samenwerking binnen en tussen ecosystemen. Wij beginnen niet met een plan maar met een positiebepaling. Onze ecosysteem-volwassenheidsmeting, die wij al in de praktijk toepassen, geeft bestuurders een objectief beeld van waar zij staan en van de stap die daarna het meeste oplevert. Dat is waar Resilience-led Advantage begint: niet bij een document, maar bij een gesprek over de eerste beweging.

Neem
contact op

Belle Webster
Associate Partner
Eraneos
belle.webster@eraneos.com

Eraneos Netherlands
De Passage 126-136
1101 AX Amsterdam

eraneos.com