



# Sterk in tijden van crisis:

Hoe de technieksector haar  
weerbaarheid vergroot

Resultaten van onderzoek naar impact van drie nationale scenario's  
en versterking van veerkracht van de technieksector

# Voorwoord



## Wie houdt Nederland draaiend als dreiging realiteit wordt?

Nederland draait op techniek. Dag in dag uit zorgen vakmensen en bedrijven in ons land voor energie, verbinding, mobiliteit en veiligheid. Juist daarom rust op onze schouders een grote verantwoordelijkheid.

De wereld om ons heen is ingrijpend veranderd. De geopolitieke spanningen lopen op. Cyberdreigingen, sabotage en uitval van vitale infrastructuur zijn geen abstracte risico's meer, maar reële scenario's waar ook techniekbedrijven direct mee te maken kunnen krijgen. De impact daarvan is groot – voor onze bedrijven, onze medewerkers, onze opdrachtgevers en voor de samenleving als geheel.

In tijden van ontregeling wordt zichtbaar hoe cruciaal onze rol is. Opdrachtgevers rekenen erop dat installaties blijven functioneren, dat noodvoorzieningen beschikbaar zijn en dat techniekbedrijven snel en adequaat kunnen handelen. Dat vraagt om voorbereiding. Niet pas als het misgaat, maar nu.

Dit weerbaarheidsrapport biedt concrete handvatten. Het laat zien hoe jij als ondernemer de regie kunt nemen: door risico's in kaart te brengen, noodplannen op te stellen (óók op papier!), noodcommunicatie te organiseren en samen te werken met collega-bedrijven en overheden. Ook schetst het rapport de rol die Techniek Nederland kan spelen als verbinder, kenniscentrum en coördinator binnen de sector.

Weerbaarheid is geen bijzaak, maar een voorwaarde voor continuïteit. Door vooruit te denken, afspraken te maken en scenario's te oefenen, vergroten we onze slagkracht en beperken we maatschappelijke schade wanneer het erop aankomt.

Ik nodig jou uit dit rapport te gebruiken als startpunt voor actie. Zo zorgen we er samen voor dat Nederland blijft draaien. Ook als het moeilijk wordt.

**Mark Harbers**

Voorzitter Techniek Nederland



# Inhoudsopgave

<b>Voorwoord</b>	<b>2</b>
<b>Managementsamenvatting</b>	<b>5</b>
<b>1. Inleiding</b>	<b>8</b>
1.1 Achtergrond	9
1.2 Scenario's	10
1.3 Leeswijzer	11
<b>2. Theoretische achtergrond</b>	<b>12</b>
2.1 Weerbaarheid	13
2.1.1 Weerbaarheidscyclus	14
2.1.2 De weerbaarheidsopgave van het kabinet	16
2.2 Vitale infrastructuur	17
2.3 Wetgeving	18
2.3.1 Wet weerbaarheid kritieke entiteiten (Wwke)	18
2.3.2 Cyberbeveiligingswet (Cbw)	20
2.3.3 Maatregelen om voorbereid te zijn op Wwke en Cbw	21
<b>3. Wat verwachten opdrachtgevers en andere partijen van techniekbedrijven in een crisis?</b>	<b>22</b>
3.1 Verwachtingen van opdrachtgevers en andere partijen	23
3.2 Wat betekent dit voor de technieksector?	24
<b>4. Weerbaarheid van de technieksector aan de hand van drie scenario's</b>	<b>26</b>
4.1 Uitval internet en telefonie of uitval elektriciteit	28
4.1.1 Korte beschrijving scenario uitval internet en telefonie door sabotage statelijke actor	28
4.1.2 Verdere toelichting scenario uitval internet en telefonie door sabotage statelijke actor	28
4.1.3 Korte beschrijving scenario uitval elektriciteit door sabotage statelijke actor	29
4.1.4 Verdere toelichting scenario uitval elektriciteit door sabotage statelijke actor	30
4.1.5 Gevolgen voor de technieksector bij uitval internet en telefonie of bij uitval elektriciteit	32
4.1.6 Maatregelen ter versterking weerbaarheid	35
4.1.7 Reflectie op hoe weerbaar de sector voor deze scenario's al is	39
4.2 Artikel 5 situatie / strategische bijstand	40
4.2.1 Korte beschrijving scenario Artikel 5 situatie	40
4.2.2 Verdere toelichting scenario Artikel 5 situatie	40
4.2.3 Gevolgen voor techniekbedrijven bij een Artikel 5 scenario	41
4.2.4 Maatregelen ter versterking weerbaarheid	43
4.2.5 Reflectie op hoe weerbaar de sector voor dit scenario al is	48
4.2.6 Reservisten	48



<b>5. Bijdrage technieksector wanneer scenario's zich voordoen</b>	<b>50</b>
<b>6. De rol van Techniek Nederland tijdens crises</b>	<b>54</b>
<b>6.1 Vooraf (koude fase): voorbereiden en versterken</b>	<b>55</b>
6.1.1 Duidelijkheid en kaders	55
6.1.2 Instrumenten en ondersteuning	55
6.1.3 Samenwerking en afspraken	56
<b>6.2 Tijdens (warme fase): mobiliseren en afstemmen</b>	<b>56</b>
6.2.1 Wat Techniek Nederland wél doet in de acute fase	56
6.2.2 Wat Techniek Nederland niet doet	57
<b>6.3 Na de crisis (herstel en evaluatie)</b>	<b>57</b>
<b>6.4 Overkoepelende rollen van Techniek Nederland</b>	<b>57</b>
<b>Verantwoording</b>	<b>58</b>
<b>Referenties</b>	<b>60</b>
<b>Bijlage 1 Verdere toelichting Artikel 5 scenario</b>	<b>62</b>
<b>Bijlage 2 Gestelde vragen interviewpartijen</b>	<b>64</b>



# Managementsamenvatting

De veiligheid in de wereld is afgenomen. Nederland krijgt vaker te maken met hybride aanvallen en kan betrokken raken bij grote conflicten. Daardoor is het belangrijk dat onze samenleving weerbaar is. Bedrijven, organisaties en burgers kunnen zich ook voorbereiden.

## Het onderzoek

Techniek Nederland wil met dit onderzoek graag antwoord op drie onderzoeksvragen:

1. Hoe weerbaar is de technieksector nu en hoe kan dat beter?
2. Hoe kunnen techniekbedrijven hun opdrachtgevers helpen tijdens crises?
3. Welke rol heeft Techniek Nederland als brancheorganisatie in crisistijd?

Deze vragen zijn onderzocht in de context van een drietal scenario's:

1. Uitval internet en telefonie door sabotage;
2. Uitval elektriciteit door sabotage;
3. Artikel 5 scenario<sup>1</sup>.

Dit hoofdstuk geeft beknopt antwoord op de drie onderzoeksvragen en sluit af met overkoepelende conclusies voor alle drie de scenario's.

## Onderzoeksvraag 1 Hoe weerbaar is de technieksector nu en hoe kan dat beter?

De weerbaarheid van de technieksector is onvoldoende. Techniekbedrijven zien veel kwetsbaarheden in communicatie, energievoorziening, logistiek en personele inzet. Continuïteitsplannen bestaan vooral bij grotere bedrijven; sectorbrede afstemming, scenario-oefeningen en zicht op ketenafhankelijkheden ontbreken vaak. Daardoor stopt dienstverlening bij uitval van internet/telefonie of elektriciteit en bij schaarste in een Artikel 5 situatie.

Aanbevelingen voor verbetering:

- Maak basis op orde: werk met een papieren crisishandboek (taken en verantwoordelijkheden, telefoonnummers/adressen van personeel, opdrachtgevers en leveranciers, noodprocedures, routekaarten) en houd kopieën offline beschikbaar.
- Ken je kritieke processen: breng vooraf in kaart wat door móet, welke opdrachtgevers vitaal zijn (zoals ziekenhuizen of waterbedrijven) en welke functies/medewerkers dan cruciaal zijn; leg prioritering vast.
- Zorg voor noodcommunicatie: denk aan portofoons voor interne communicatie, satelliettelefoons voor contact met vitale opdrachtgevers, en afspraken over fysieke verzamelpunten; oefen bereikbaarheid zonder ICT.
- Voorraad en alternatieven: bouw strategische voorraden (onderdelen zoals pompen, kabels en noodaggregaten op meerdere locaties) en organiseer collegiale inleen over regio's heen. Stel een bedrijfsnoodpakket samen met onder andere sleutels voor gebouwen, papieren werkbonden, accupakketten, noodradio en contant geld.

<sup>1</sup> Nederland is lid van de NAVO. Dit is een militaire samenwerking van 32 landen uit Noord-Amerika en Europa. De NAVO regelt de wederzijdse verdediging en samenwerking van de legers van de westerse landen. Artikel 5 uit het verdrag vormt de kern. Daarin staat dat een aanval op een van de landen wordt gezien als een aanval op allemaal.



- Train en oefen: train medewerkers in noodprocedures waarbij monteurs een installatie handmatig bedienen zonder digitale systemen. Voer (tabletop) scenario-oefeningen uit waarin, bijvoorbeeld, internet 72 uur uitvalt en het team moet werken met papieren administratie.
- Ketenafspraken: maak vooraf service level agreements waarin staat hoe toegang tot locaties geregeld is bij uitval van digitale toegangscontrole, en welke opdrachtgever als eerste geholpen wordt bij schaarste, maak schakelplannen, en denk aan contractclausules over betalingen bij uitval van internetbankieren.

## Onderzoeksvraag 2 **Hoe kunnen techniekbedrijven hun opdrachtgevers helpen tijdens crises?**

Veel van de voorgestelde maatregelen zijn relevant voor alle drie de onderzochte crises. Investing in deze maatregelen draagt dan ook bij aan de algehele weerbaarheid. Techniekbedrijven helpen opdrachtgevers zich voor te bereiden op crises. Tijdens crises leveren zij noodvoorzieningen, bedienen installaties handmatig als IT (Informatietechnologie) en/of OT (Operationele Technologie) uitvalt, en zetten extra capaciteit in voor vitale locaties (zoals zorg, water, energie, infrastructuur). Na afloop van een crisis leveren techniekbedrijven hersteldiensten. Bedrijven die vooraf afspraken maken over bereikbaarheid, strategische voorraden, toegang en prioriteiten reageren sneller en beperken de maatschappelijke schade.

Aanbevelingen voor verbetering:

- Vooraf: actualiseer informatie over installaties (schakelplannen), leg toegangsprocedures vast bij uitval van digitale toegang, maak afspraken over communicatie en prioriteiten met opdrachtgevers (wie eerst bij schaarste).
- Tijdens crisis: stuur monteurs proactief langs bij vitale opdrachtgevers; houd papieren administratie bij (uren, materialen, contant geld).
- Na afloop: werk papieren gegevens gestructureerd bij in digitale systemen en geef nazorg aan personeel.

## Onderzoeksvraag 3 **Welke rol heeft Techniek Nederland in crisistijd?**

Techniek Nederland vervult een verbindende en coördinerende rol. Niet als 24/7 crisisorganisatie, wel als knooppunt voor afspraken, informatie en mobilisatie: vóór, tijdens en na crises. De volgende aanbevelingen helpen de brancheorganisatie om haar rol sterker te maken.

In de voorbereidingsfase draait alles om het creëren van duidelijkheid en samenwerking, zodat bedrijven weten wat hun rol is en welke afspraken nodig zijn om in crisissituaties effectief te handelen.

- Duidelijke kaders: helpen bij duiding vitaal/niet-vitaal (bedrijven weten dan of zij onderdeel zijn van een vitale keten en welke verantwoordelijkheden daarbij horen), informeren over nieuwe wetten (Wwke/Cbw) en ketenverplichtingen, en stel templates (continuïteit, communicatie) beschikbaar.
- Samenwerking: opzetten van taskforces per vitale keten, organiseren van oefeningen, en coördineren strategische voorraden met groothandel en overheid, maak afspraken over prioritering.



Tijdens een crisis is snelheid en coördinatie cruciaal: de technieksector moet overzicht bieden, signalen bundelen en zorgen voor uniforme communicatie om chaos te voorkomen.

- Sectoroverzicht: zichtbaar maken wie kan wat, waar, wanneer;
- Bundelen sector-signalen;
- Stem af met overheid over wetgeving en verdeling van schaarse middelen;
- Ondersteunen uniforme crisiscommunicatie.

Na afloop van een crisis ligt de focus op leren en verbeteren: door evaluatie en innovatie kan de sector sterker terugkomen en beter voorbereid zijn op toekomstige verstoringen.

- Evaluatie en leren: verzamelen lessons learned en delen best practices.
- Aanjagen innovaties voor lokale energievoorziening en dubbel uitgevoerde (redundante) oplossingen voor de continuïteit.

### **Overkoepelende conclusies voor alle drie de scenario's**

De volgende punten vormen de kern van wat bedrijven nodig hebben om in alle drie de scenario's effectief te blijven functioneren en maatschappelijke schade te beperken

- Bereikbaarheid is bepalend. Zonder internet/telefonie of bij stroomuitval valt digitale communicatie weg. Bedrijven die alternatieve communicatie en fysieke verzamelpunten hebben, blijven inzetbaar. Dit geldt ook in Artikel 5 waar verstoringen en sabotage toenemen.
- Offline en met papier kunnen werken. Digitale besturing, toegang en planning vallen snel stil. Papieren werkbonden, routekaarten, offline schakelplannen en handmatige procedures zijn nodig om vitale installaties draaiend te houden.
- Prioriteren en capaciteit sturen. Schaarste aan mensen, middelen en onderdelen vraagt heldere prioriteiten: eerst vitale opdrachtgevers, vervolgens overige. Leg dit vooraf vast met opdrachtgevers en personeel; reken op personeelsuitval (reservisten, mantelzorg, angst).
- Strategische voorraden en ketenafspraken. Onderdeel- en brandstofschaarste kan werk platleggen. Gezamenlijke voorraden en collegiale inleen beperken stilstand; maak afspraken met groothandels en overheid over verdelen bij schaarste.
- Oefenen verhoogt slagkracht. Bedrijven die regelmatig oefenen op IT/OT-uitval en stroomuitval handelen sneller en veiliger; sectorbrede oefeningen via Techniek Nederland versnellen leren in de keten.
- Weerbaarheid is menswerk. Monteurs moeten handmatig kunnen werken, veilig kunnen opereren en mentaal weerbaar blijven. Investeren in training, duidelijk leiderschap en nazorg houdt teams inzetbaar.

### **Samenvattende eindconclusie**

De technieksector heeft grote impact op het functioneren van Nederland in crises, maar de huidige weerbaarheid schiet tekort. De weg vooruit is praktisch: leg basisafspraken vast, werk offline-bekwaam, organiseer noodvoorzieningen (communicatie, aggregaten), leg voorraden aan, oefen scenario's, en prioriteer vitale opdrachtgevers. Techniek Nederland versnelt dit door kaders, coördinatie en kennisdeling te bieden. Zo blijft de sector leveren bij uitval van internet en telefonie, bij stroomstoringen en in een Artikel 5 situatie, en verkleinen we samen de maatschappelijke schade.



# 1. Inleiding



## 1.1 Achtergrond

De veiligheid in de wereld is afgenomen. Nederland krijgt vaker te maken met hybride aanvallen en kan betrokken raken bij grote conflicten. Daardoor is het belangrijk dat onze samenleving weerbaar is [1]. De Rijksoverheid geeft aan dat we ons moeten kunnen beschermen tegen crises zoals oorlog, cyberaanvallen, pandemieën en natuurrampen. De overheid kan dit niet alleen. Bedrijven, organisaties en burgers kunnen zich ook voorbereiden. Dit komt tot uiting in de nationale weerbaarheidsopgave, dat bestaat uit het vergroten van zowel de maatschappelijke weerbaarheid als de militaire paraatheid.

Het ministerie van Economische Zaken (EZ), VNO-NCW en MKB-Nederland zijn in samenwerking met alle geïnteresseerde en aangesloten branches in 2025 aan de slag gegaan om de betekenis van die nationale weerbaarheidsopgave voor het bedrijfsleven in algemene zin verder uit te werken en er betekenis aan te geven. Techniek Nederland heeft daaraan volop bijgedragen.

VNO-NCW heeft een eigen handreiking gemaakt met praktische tips voor ondernemers, bedrijven en brancheorganisaties [2]. Ook andere landen, zoals Zweden, publiceren soortgelijke documenten om het bedrijfsleven voor te bereiden op crises [3].

Het onderwerp weerbaarheid is binnen diverse onderdelen van de brancheorganisatie Techniek Nederland besproken en de conclusie is getrokken dat het van groot belang is dat Techniek Nederland een eigen, specifieke aanpak en invulling gaat ontwikkelen, omdat de technieksector een grote en belangrijke rol speelt in het draaiend houden van vitale onderdelen zoals energie, telecom en infrastructuur c.q. in de reparatie daarvan bij uitval als gevolg van aanvallen of sabotage.

In maart 2025 is door Techniek Nederland en op basis van een vragenlijst van VNO-NCW een eerste aanzet gedaan om de weerbaarheid van de technieksector in kaart te brengen [4]. Daarbij is in grote lijnen gekeken naar de gevolgen van verschillende scenario's voor het doorgaan van werk bij en door techniekbedrijven. Kort samengevat: de inschatting was dat de technieksector nog te weinig weerbaar is. Technische installaties zijn sterk (wellicht volledig) afhankelijk van internet, telefonie en elektriciteit en van beschikbaarheid van reserveonderdelen of dienstverlening gericht op reparatie. Wanneer deze zaken uitvallen, komen vitale processen in gevaar. Bedrijven in de technieksector hebben dezelfde afhankelijkheid: zonder internet, telefonie en stroom kunnen zij hun diensten niet leveren.

Techniek Nederland heeft TNO daarom gevraagd om onderzoek te doen naar de weerbaarheid van de technieksector. Dit onderzoek kijkt naar drie onderzoeksvragen:

- Hoe weerbaar is de technieksector nu en hoe kan dat beter?
- Hoe kunnen techniekbedrijven hun opdrachtgevers helpen tijdens crises?
- Welke rol heeft Techniek Nederland als brancheorganisatie in crisistijd?

De resultaten laten zien hoe de sector sterker kan worden en hoe zij kan bijdragen aan een weerbare samenleving.

Dit rapport staat niet los van andere nationale en internationale publicaties over weerbaarheid, maar maakt concreet welke rol de technieksector speelt in de nationale weerbaarheid en wat nodig is om die rol te vervullen, voor zowel techniekbedrijven als de brancheorganisatie.

## 1.2 Scenario's

Voor het onderzoek zijn drie scenario's gekozen (zie figuur 1). Deze komen uit het Nationaal Programma Weerbaarheid en zijn afgestemd met het ministerie van EZ en Klimaat en Groene Groei (KGG). Elk scenario beschrijft een mogelijke crisis en de gevolgen voor bedrijven.

In dit onderzoek zijn de drie scenario's afzonderlijk bekeken, zoals gevraagd door EZ en KGG. Er is echter deels overlap, omdat gevolgen uit eerdere scenario's ook in latere scenario's kunnen optreden. Waar nodig, is dit in de tekst vermeld. In hoofdstuk 4 bespreken we deze scenario's uitvoerig.

### Uitwerking in drie voorstelbare scenario's\*



#### Uitval internet en telefonie door sabotage statelijke actor

- Duur: 72 uur
- Omvang: uitval één grote landelijke mobiele telefoonaanbieder; ga uit van 'jouw werkgebied'
- Gevolgen: uitval van mobiele netwerken, internetverbinding en vaste lijn; verstoring IoT, toonbankbetalingsverkeer en handel; uitval pinautomaten; treinverkeer belemmerd etc.



#### Uitval elektriciteit door sabotage statelijke actor

- Duur: 72 uur
- Omvang: 2 miljoen klanten; ga uit van 'jouw werkgebied'
- Gevolgen: uitval groot deel telecommunicatie; verstoring toonbankbetalingsverkeer en uitval pinautomaten; verkeer loopt vast; uitval van nuts na ong. 1 dag (verwarming, en drinkwater vanaf 2 hoog), ontregeling aanvoer diesel etc.



#### Artikel 5 situatie / strategische bijstand

- Duur: langdurig
- Focus op langdurige logistieke verstoringen
- Gevolgen: int. handel en toe-/doorvoer vallen stil, maximale druk op zorgsysteem, arbeidsmigranten uit oosten gaan terug, Defensie geen ruimte voor 3e hoofdtaak etc.

\*De inhoud van de drie scenario's is afkomstig van het ministerie van EZ en KGG, i.a.m. de sectoren telecom en elektriciteit. De parameters zijn in overleg met VNO-NCW en MKB-Nederland overeen gekomen en zijn in lijn met de aanpak van diverse Europese landen.

Figuur 1: De drie voorstelbare scenario's<sup>2</sup>

<sup>2</sup> Artikel 5 van het NAVO-verdrag zegt dat een aanval op één lidstaat geldt als een aanval op alle lidstaten

## 1.3 Leeswijzer

**Hoofdstuk 2** (Theoretische achtergrond) legt uit wat weerbaarheid betekent, inclusief de weerbaarheidscyclus en relevante wetgeving (Wet weerbaarheid kritieke entiteiten, Wwke; Cyberbeveiligingswet, Cbw). We leggen ook uit wat vitale infrastructuur is.

**Hoofdstuk 3** (Wat verwachten opdrachtgevers en andere partijen van techniekbedrijven in een crisis) vat samen wat opdrachtgevers van techniekbedrijven verwachten tijdens crises (zoals bereikbaarheid, noodvoorzieningen, gescreende medewerkers, crisismanagement) en wat dit betekent voor techniekbedrijven.

**Hoofdstuk 4** (Weerbaarheid van de technieksector aan de hand van drie scenario's) geeft per scenario een beschrijving, gevolgen voor techniekbedrijven, mogelijke maatregelen en reflectie op huidige weerbaarheid. We staan ook stil bij de rol van reservisten.

**Hoofdstuk 5** (Bijdrage technieksector wanneer scenario's zich voordoen) laat zien hoe de sector kan helpen om maatschappelijke impact te beperken.

**Hoofdstuk 6** (De rol van Techniek Nederland tijdens crises) beschrijft de mogelijke coördinerende en ondersteunende rol van de brancheorganisatie tijdens crises.

**Verantwoording** beschrijft op welke manier dit onderzoek is uitgevoerd.

## 2. Theoretische achtergrond



In dit hoofdstuk leggen we uit wat weerbaarheid betekent. We geven een korte uitleg van de theorie en laten zien wat de overheid verwacht van bedrijven en de samenleving. Ook bespreken we wetgeving die invloed heeft op de dienstverlening van de technieksector en benoemen we een aantal maatregelen die de technieksector kan nemen om hier mee om te gaan.

## 2.1 Weerbaarheid

Weerbaarheid (in het Engels resilience) krijgt de laatste jaren steeds meer aandacht in het Nederlandse veiligheidsbeleid. Weerbaarheid betekent dat een systeem of organisatie problemen kan voorkomen, opvangen en herstellen. Het gaat om veerkracht: het vermogen van een samenleving om schokken en verstoringen op te vangen, zich aan te passen en weer goed te functioneren.

Weerbaarheid vraagt om [5]:

- Sterke fysieke infrastructuur die tegen bedreigingen kan;
- Continuïteit van essentiële diensten;
- Samenwerking en sociale samenhang.

Daarnaast moet een organisatie flexibel kunnen reageren op nieuwe bedreigingen. Dat kan door te leren van ervaringen, snel te handelen en beleid en procedures aan te passen. Weerbaarheid heeft ook een preventieve kant: het verkleint de kans op schade en kan bedreigende acties afschrikken of ontmoedigen.

### Weerbaarheid versus toekomstbehendigheid

CONNECT 2030 [28] geeft inzicht in de vragen die op de technieksector afkomen, het geeft inzicht in relevante trends en ontwikkelingen en het duidt de impact hiervan voor de samenleving als geheel. Bedrijven in de sector staan voor keuzes om zich af te vragen op welke manier ze met deze sneller veranderende wereld om willen gaan. Willen bedrijven mee en toekomstbehendig worden? Kunnen ze dat ook, gelet op de prioriteiten van vandaag en morgen? Hebben we de vakkrachten, kennis en expertise om in deze nieuwe toekomst met andere opdrachten, middelen en partners te kunnen werken? Om de kansen te kunnen pakken zijn verschillende afwegingen van belang. Voor ieder bedrijf zullen die afwegingen anders zijn.

Binnen CONNECT 2030 wordt het thema 'toekomstbehendigheid' als overkoepelend thema geïntroduceerd, dat een centrale rol speelt binnen deze toekomstverkenning. Toekomstbehendigheid wordt hier als mindset gezien die overheden, organisaties en bedrijven helpt om zich voor te bereiden op de onzekerheid die complexe systemen – en met elkaar vervlochten uitdagingen – van nature hebben. Het gaat over een attitude die weergeeft dat de toekomst niet precies voorspeld kan worden, maar dat je je als organisatie wel op kan voorbereiden dát het anders is dan vandaag. Voorbeelden zijn: Code-rood-regen en overstromingen in Zuid-Limburg, de PFAS- en stikstof-lockdown, cyberaanvallen die bedrijven platleggen, binnen drie maanden een verlamme coronapandemie, de Russische inval in Oekraïne – met nog steeds voortdurende verstoring van de supplychain – en extreme droogte en branden.

'Weerbaarheid' en 'toekomstbehendigheid' liggen dicht bij elkaar, maar ze hebben verschillende accenten. Weerbaarheid is een voorwaarde voor toekomstbehendigheid. Als je niet weerbaar bent, kun je moeilijk toekomstgericht werken. Weerbaarheid zit vaak in de basis (veiligheid, stabiliteit), toekomstbehendigheid in de richting (visie, innovatie).



Een weerbaarheidsanalyse kijkt niet alleen naar bekende risico's, maar ook naar nieuwe ontwikkelingen. Het doel is om toekomstige bedreigingen inzichtelijk te maken en maatregelen te nemen om grote schade te voorkomen, in plaats van alleen te reageren op problemen uit het verleden.

De aandacht voor weerbaarheid groeit omdat systemen en infrastructuur beter beschermd moeten worden. Bijna alles is tegenwoordig digitaal en internationaal verbonden. Een storing in één onderdeel kan snel gevolgen hebben voor andere onderdelen. Daarom moeten bedrijven en organisaties nadenken over hoe zij zich voorbereiden op onverwachte problemen.

#### **Een weerbaar systeem:**

- Bereidt zich voor op risico's;
- Beperkt schade als er iets misgaat;
- Herstelt snel na een crisis;
- Past zich aan om sterker te worden.

Onderzoekers en beleidsmakers denken steeds meer na over wat weerbaarheid precies betekent. Het begrip wordt in veel verschillende situaties gebruikt, waardoor er veel definities bestaan. De overheid gebruikt in de Wet weerbaarheid kritieke entiteiten (Wwke, zie ook hoofdstuk 2.3) deze definitie: Het vermogen om een incident te voorkomen, te beperken of te beheersen, en om bescherming te bieden of bestand te zijn tegen, te reageren op of zich aan te passen aan en te herstellen van een incident.

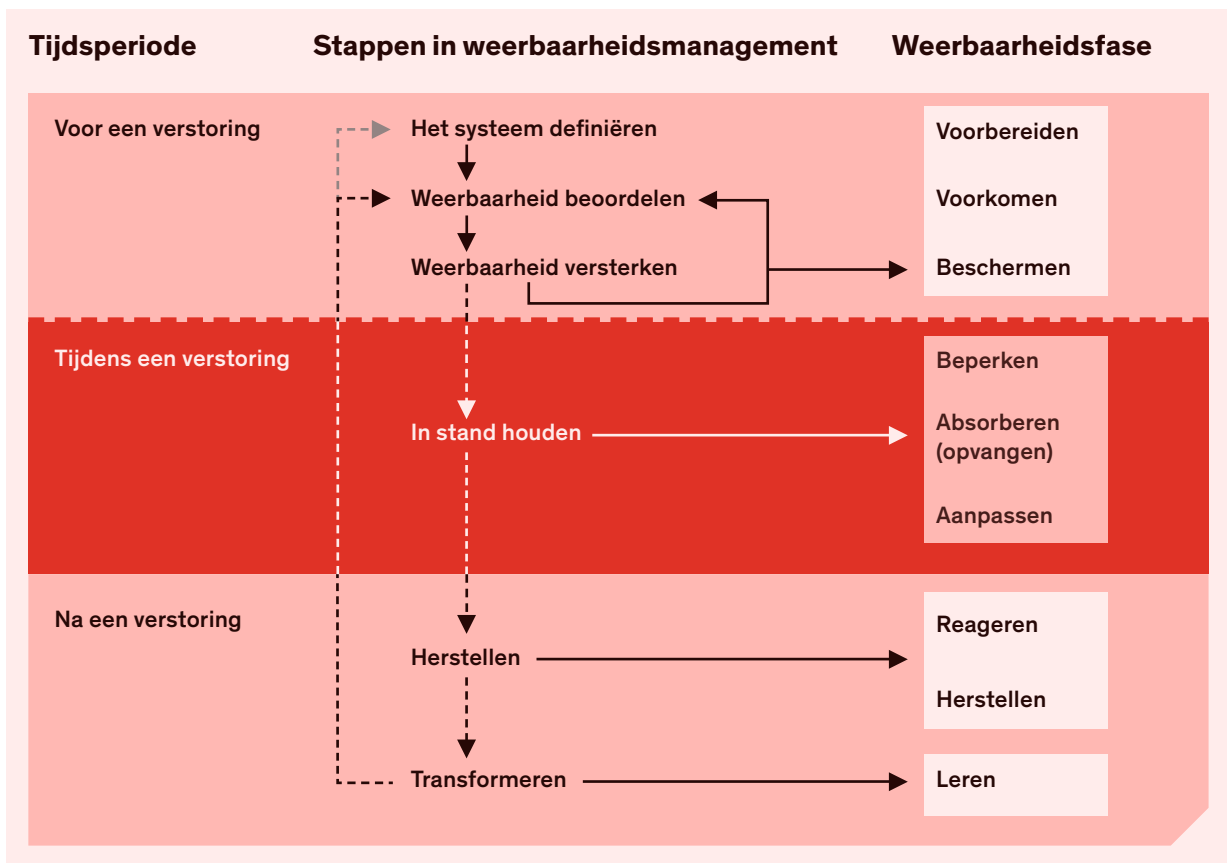
## 2.1.1 Weerbaarheidscyclus

Experts stellen één centrale vraag: Hoe zorg ik dat mijn systeem goed blijft werken tijdens een verstoring en snel herstelt daarna? Daarnaast willen ze voorkomen dat een probleem in één onderdeel een domino-effect veroorzaakt in andere onderdelen [6]. Figuur 2 laat dit zien.

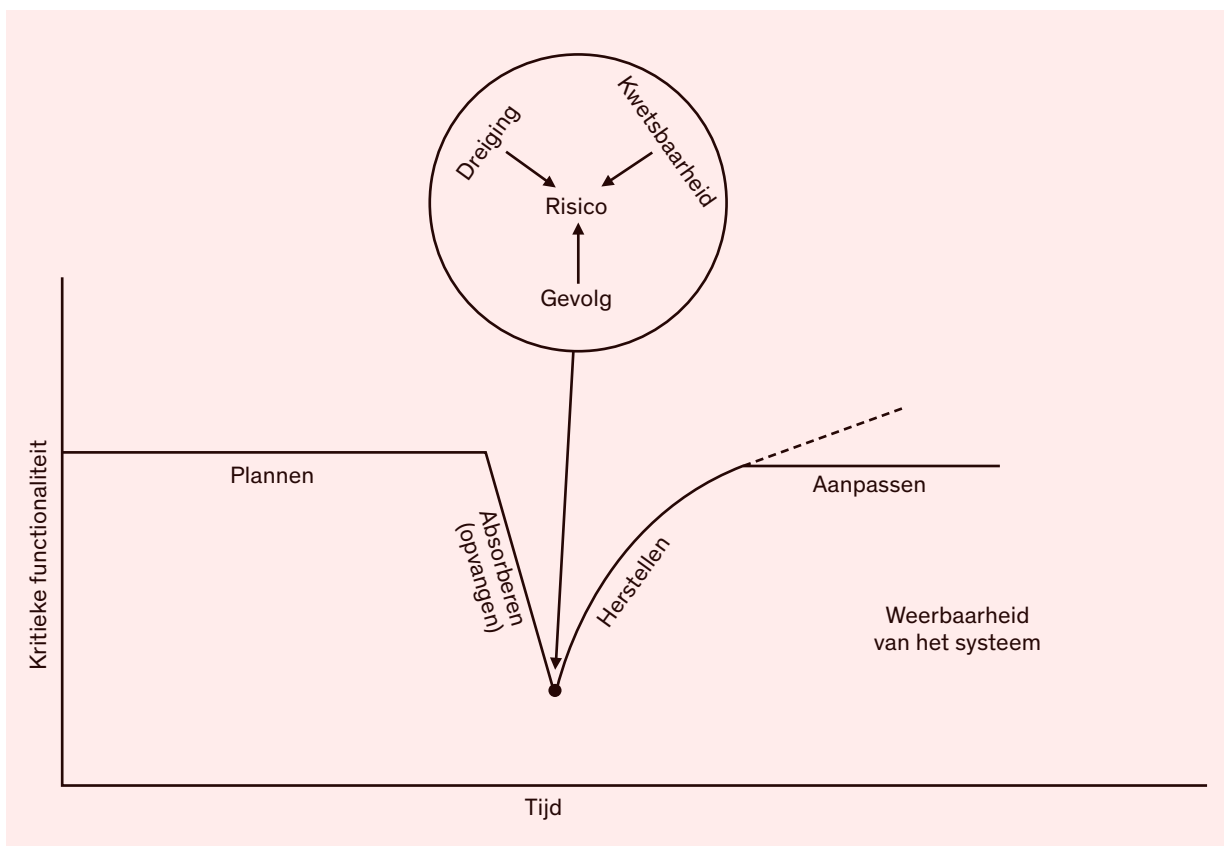
Deze vraag speelt vooral bij complexe systemen. Denk aan ziekenhuizen. Zij zijn afhankelijk van veel verbonden systemen, zoals:

- Het energienet;
- Informatiesystemen;
- Patiëntenregistratie;
- Medische toeleveringsketens.

Als één onderdeel uitvalt, kan dat grote gevolgen hebben. Soms gaat het om bedreigingen die weinig kans hebben, maar wel rampzalige gevolgen. Daar is vaak geen duidelijke strategie voor. Daarom moeten organisaties nadenken over hoe ze zulke risico's kunnen beperken en hoe ze hier van kunnen herstellen.



**Figuur 2:** De rol van weerbaarheid in systemen, waarbij het belang van het bestrijden van verstoringen wordt benadrukt [6]



**Figuur 3:** Een raamwerk voor weerbaarheid [7]

Igor Linkov hanteert in zijn weerbaarheidscyclus een aantal fasen die een systeem doorloopt bij schokken of verstoringen [7]:

1. Anticiperen / Plannen (voor een verstoring): het systeem bereidt zich voor op mogelijke dreigingen. Dit gebeurt via een risicoanalyse<sup>3</sup> en het opbouwen van buffers en het anticiperen op wat er mis kan gaan.
2. Absorberen (tijdens een verstoring): tijdens een verstoring beperkt het systeem de schade en blijft het zoveel mogelijk functioneren. Deze fase bepaalt hoe sterk het systeem intern is en hoeveel impact externe schokken hebben.
3. Herstellen (na een verstoring): na de verstoring herstelt het systeem zo snel mogelijk naar een normale of betere situatie.
4. Aanpassen (na een verstoring): het systeem leert van de gebeurtenis en wordt (mogelijk) sterker voor de toekomst.

### 2.1.2 De weerbaarheidsopgave van het kabinet

Het kabinet wil een weerbare maatschappij [1] [8]. Dat betekent dat overheid, bedrijven en burgers voorbereid zijn op crises en snel kunnen herstellen.

Denk aan:

- Hybride aanvallen (onder andere desinformatie, cyber, sabotage, spionage) of militaire conflicten;
- Overstromingen, pandemieën of langdurige uitval van vitale processen.

We moeten kunnen omgaan met een combinatie van langdurige uitval, schaarste en verstoring. De overheid geeft dit vorm door te werken aan zes pijlers, verdeeld over twee sporen:

<sup>3</sup> Risicoanalyse kijkt naar welke dreigingen kunnen ontstaan, hoe kwetsbaar een systeem is en wat de gevolgen zijn. Zo wordt duidelijk hoeveel belangrijke functies kunnen uitvallen.

Maatschappelijke weerbaarheid:

1. Het beschermen van vitale en andere belangrijke processen in de maatschappij;
2. Een parate en veerkrachtige samenleving;
3. Het overeind houden van de Nederlandse democratie, rechtstaat en overheid;
4. Een weerbare economie.

Militaire paraatheid:

5. Het beschermen en verdedigen van het eigen en bondgenootschappelijk grondgebied;
6. Het waarborgen van civiele ondersteuning aan de krijgsmacht bij de uitoefening van de militaire taak.

## 2.2 Vitale infrastructuur

Vitale infrastructuur zijn de essentiële processen, producten en diensten waar onze samenleving op draait, zoals elektriciteit, internet en drinkwater [9]. Als deze processen uitvallen of worden verstoord, heeft dat grote gevolgen voor de economie en de maatschappij. In het ergste geval kan het zelfs de nationale veiligheid bedreigen. Daarom werken overheid, bedrijven en veiligheidsdiensten samen om deze diensten te beschermen. Dit heet de 'Aanpak vitaal' [10].

De NCTV benadrukt dat bescherming steeds belangrijker wordt. Het dreigingsbeeld verandert en wordt complexer. Denk aan:

- Terroristische aanslagen;
- Cyberaanvallen;
- Natuurrampen;
- Spionage;
- Sabotage;
- Buitenlandse overnames van vitale bedrijven.

Omdat vitale processen steeds meer met elkaar verbonden zijn, kan een storing in één proces grote gevolgen hebben voor andere processen. Bijvoorbeeld: bij een overstroming kan stroom uitvallen, waardoor internet en ziekenhuizen ook problemen krijgen. Daarom moeten we de weerbaarheid van alle vitale diensten vergroten.

De overheid gebruikt de 'Aanpak vitaal' om vitale infrastructuur sterker te maken. Elke vier jaar wordt de cyclus vitaal doorlopen. Ministeries wijzen vitale aanbieders aan. Deze aanbieders moeten hun risico's kennen en maatregelen nemen om hun diensten te beschermen. Techniekbedrijven worden bijvoorbeeld gevraagd om zowel IT- als OT-systemen effectief te beveiligen bij vitale aanbieders.

Voor digitale veiligheid gelden nu de Wet Beveiliging Netwerk en Informatiesystemen (Wbni) en straks de Cyberbeveiligingswet (Cbw)<sup>4</sup>.

Voor sommige aanbieders geldt ook sectorale wetgeving, zoals de Drinkwaterwet of de Wet veiligheidstoets investeringen, fusies en overnames (Vifo).

<sup>4</sup> 23 maart 2026 staat het plenaire debat gepland in de Tweede Kamer over de Cbw.

De Europese Unie heeft de Critical Entities Directive (CER-richtlijn) gemaakt. Nederland voert deze in via de Wet weerbaarheid kritieke entiteiten (Wwke, zie ook hoofdstuk 2.3). Deze wet legt veel onderdelen van de Aanpak vitaal vast. Onder deze wet spreken we niet meer van vitale aanbieders, maar van kritieke entiteiten. Dat zijn organisaties die één of meer essentiële diensten leveren. Organisaties die nu al als vitale aanbieder zijn aangewezen, worden waarschijnlijk ook kritieke entiteit. Daarnaast komen er nieuwe sectoren bij, zoals gezondheidszorg en voedingsindustrie.

Binnen de Aanpak vitaal bekijkt de overheid alle risico's samen: fysiek, economisch en digitaal. Denk aan:

- Klimaatverandering;
- Ongewenste buitenlandse investeringen;
- Cyberaanvallen;
- Cascade-effecten (problemen die andere processen verstoren).

De overheid neemt maatregelen zoals:

- Beleidsplannen en wetgeving;
- Actieprogramma's samen met vitale aanbieders.

Vitale aanbieders nemen zelf ook maatregelen om hun dienstverlening veilig te houden. De overheid helpt hen daarbij, bijvoorbeeld met betere informatie-uitwisseling en aansluiting op crisisstructuren [10]. De technieksector draagt een cruciale verantwoordelijkheid voor het waarborgen van de continuïteit van de vitale infrastructuur.

## 2.3 Wetgeving

De Europese Unie heeft twee richtlijnen gemaakt om de weerbaarheid van landen en bedrijven te vergroten [11]:

- CER-richtlijn – Richt zich op bescherming van vitale processen;
- NIS2-richtlijn (Network and Information Security Directive) – Richt zich op digitale veiligheid.

Nederland voert deze richtlijnen in via:

- Wet weerbaarheid kritieke entiteiten (Wwke) – Voor organisaties die essentiële diensten leveren, zoals energie, drinkwater en gezondheidszorg;
- Cyberbeveiligingswet (Cbw) – Voor organisaties die digitale veiligheid moeten waarborgen.

Beide wetten gaan naar verwachting in het tweede kwartaal van 2026 in werking.<sup>5</sup>

Voor bedrijven in de technieksector – vooral als toeleverancier aan organisaties die onder de Wwke of Cbw vallen – zijn beide wetten belangrijk, omdat ze directe gevolgen hebben voor hun rol in de keten. Daarom worden deze hieronder verder toegelicht.

<sup>5</sup> 9 februari 2026 staat het plenaire debat gepland in de Tweede Kamer over de Wwke.

### 2.3.1 Wet weerbaarheid kritieke entiteiten (Wwke)

De Wwke wil organisaties sterker maken tegen dreigingen. Het gaat om organisaties die essentiële diensten leveren in Nederland. De wet richt zich op alle risico's die door mensen of door de natuur ontstaan en die deze diensten ernstig kunnen verstoren [12].

Organisaties kiezen niet zelf of ze onder de Wwke vallen. Dit is een taak voor alle ministeries in Nederland. Zij bepalen welke organisaties belangrijk zijn voor onze samenleving.

Deze organisaties horen bij sectoren die in de wet staan of later worden toegevoegd. Elk ministerie maakt een risicobeoordeling en wijst daarna kritieke organisaties aan. Daarbij kijken ze vooral naar hoe groot de invloed van een organisatie is op functies zoals economie, gezondheid, veiligheid en milieu [13]. De Wwke geldt in ieder geval voor deze sectoren:

- Energie;
- Vervoer;
- Banken;
- Financiële markten;
- Gezondheidszorg;
- Drinkwater;
- Afvalwater;
- Digitale infrastructuur;
- Overheid;
- Ruimtevaart;
- Productie, verwerking en distributie van voedsel.

#### *Risicobeoordeling*

Kritieke organisaties moeten zelf onderzoeken welke risico's hun dienstverlening kunnen verstoren. Ze brengen mogelijke dreigingen en kwetsbaarheden in kaart en schatten in wat de gevolgen zijn als er iets misgaat.

#### *Zorgplicht*

Kritieke organisaties zijn zelf verantwoordelijk voor hun weerbaarheid. Op basis van hun risicobeoordeling nemen ze maatregelen om incidenten te voorkomen, gevolgen te beperken en snel te herstellen als er toch iets gebeurt.

#### *Meldplicht*

Kritieke organisaties moeten incidenten die hun dienstverlening ernstig verstoren of kunnen verstoren zo snel mogelijk melden bij de bevoegde autoriteit. In de melding staat zoveel mogelijk informatie over de impact, oorzaak en gevolgen van het incident. Zo kan de autoriteit reageren en waar nodig helpen.

#### *Voor toeleveranciers in de technieksector*

Soms wijst een ministerie een organisatie aan als kritieke entiteit omdat een storing bij een leverancier grote gevolgen heeft. Leveranciers kunnen daarom onderdeel worden van risicobeoordelingen, zorgplichtmaatregelen (zoals beveiliging van machines) en meldplicht. Dit geldt als hun producten of diensten belangrijk zijn voor kritieke infrastructuur.

Techniekleveranciers moeten bereid zijn mee te werken aan risicomanagement en incidentenplannen van hun opdrachtgevers. Opdrachtgevers nemen maatregelen om continuïteit te garanderen. Dit kan betekenen dat techniekbedrijven eisen krijgen voor fysieke bescherming, onderhoud en communicatie bij storingen.

Alhoewel kritieke organisaties volgens de wet zelf verantwoordelijk zijn om het initiatief te nemen tot een risicobeoordeling, kunnen techniekbedrijven wel het gesprek aangaan over wat ze kunnen betekenen voor deze organisaties. De wet schrijft voor dat kritieke organisaties risicobeoordelingen uitvoeren, incidentprotocollen opstellen, fysieke beveiliging borgen en herstelplannen hebben. Techniekbedrijven leveren de instrumenten, expertise en implementatiekaders om deze maatregelen te realiseren (denk aan beveiligingssystemen, back-up, monitoring, toegangscontrole).

### 2.3.2 Cyberbeveiligingswet (Cbw)

De Cbw geldt voor essentiële en belangrijke organisaties in sectoren zoals energie, ruimtevaart, onderzoek, digitale infrastructuur en overheid. Ook grote bedrijven in andere sectoren vallen soms onder deze wet. Dit geldt bijvoorbeeld voor bedrijven met meer dan vijftig medewerkers of een jaaromzet en/of balanstotaal van meer dan tien miljoen euro. Toeleveranciers en dochterbedrijven van deze organisaties kunnen ook onder de wet vallen. Dit hangt af van hun rol in de keten [14]. Het is aan te raden dat techniekbedrijven controleren of hun bedrijf onder de Cyberbeveiligingswet valt op de website van het NCSC <sup>6</sup>.

Als een organisatie onder de Cbw valt, dan geldt er een aantal verplichtingen:

- Registratieplicht: de organisatie schrijft zich in bij het zogenaamde entiteitenregister.
- Zorgplicht: de organisatie neemt maatregelen om cyberproblemen te voorkomen.
- Meldplicht: de organisatie meldt cyberincidenten via een website van het NCSC [15] bij het betreffende sectorale CSIRT en de bevoegde toezicht-houder zodra de wet van kracht is.

Leveranciers die producten of diensten leveren aan organisaties die onder de NIS2-richtlijn vallen, vallen niet automatisch zelf onder deze richtlijn.

Maar organisaties die wél onder NIS2 vallen, moeten de beveiliging van hun toeleveringsketen controleren. Daarom kunnen zij informatie vragen over de maatregelen die de leverancier neemt ten aanzien van cyberrisico's van hun leveranciers. Soms stellen zij ook eisen aan die maatregelen [16].

Ook al vallen toeleveranciers in de technieksector vaak niet direct onder de wet, krijgen ze soms indirect verplichtingen. Dit komt doordat hun opdrachtgevers moeten voldoen aan de zorgplicht.

Op basis van risicoanalyses moeten leveranciers kunnen aantonen dat hun systemen voldoen aan technische, organisatorische en fysieke cybersecurity-maatregelen. Leveranciers zonder digitale koppeling vallen meestal buiten de wet. Toch kunnen er in de praktijk extra beveiligingseisen gelden als dit invloed heeft op de keten.

<sup>6</sup> <https://www.ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor>

### 2.3.3 Maatregelen om voorbereid te zijn op Wwke en Cbw<sup>7</sup>

Waarom zijn de Wwke en Cbw belangrijk voor techniekbedrijven?

- Risico's beperken en continuïteit waarborgen: leveranciers moeten laten zien dat hun producten of diensten geen zwakke plek vormen in essentiële infrastructuur. Dit geldt voor installatie, onderhoud én cybersecurity.
- Contractuele eisen: opdrachtgevers nemen vaak beveiligingsafspraken op in contracten. Leveranciers moeten zich daaraan houden. Het gaat niet alleen om kwaliteit, maar ook om informatiebeveiliging, fysieke toegang, probleemoplossing en het melden van incidenten.
- Strategisch voordeel: wie vroegtijdig aan deze wettelijke eisen voldoet, heeft een voorsprong op concurrenten. Het laat zien dat je een betrouwbare partner bent voor kritieke projecten. Zo voorkom je dat jouw bedrijf een risico vormt voor opdrachtgevers.

**Wat kun je nu al doen om klaar te zijn voor Wwke en Cbw? Als bedrijf in de technieksector kun je deze stappen nemen:**

#### 1. Governance en Risicomanagement

- Maak een risicoanalyse van je producten en diensten. Wat gebeurt er bij een storing of cyberaanval?
- Schrijf een continuïteitsplan. Zet daarin ook hoe je opschaaft bij problemen.
- Leg verantwoordelijkheden vast. Wie is contactpersoon bij incidenten? Wie beheert beveiligingsmaatregelen?

#### 2. Cybersecurity (Cbw/NIS2)

- Updates: Zorg dat software en firmware altijd op tijd worden bijgewerkt.
- Toegangsbeheer: Gebruik sterke inlogmethoden, zoals multifactorauthenticatie. Geef toegang op basis van rollen.
- Versleuteling: Versleutel gegevens tijdens verzending (bijvoorbeeld e-mails, webverkeer) én opslag (zoals harde schijven, USB-sticks, cloud).
- Controle: Houd systeemactiviteiten bij en stel meldingen in bij afwijkingen.
- Incidentplan: Beschrijf hoe je meldingen doet en communiceert bij een cyberincident.

#### 3. Fysieke en operationele weerbaarheid (Wwke)

- Beveilig installaties en onderdelen. Denk aan toegangscontrole, camera's en bescherming tegen sabotage.
- Zorg voor redundantie. Maak kritieke onderdelen dubbel waar mogelijk.
- Leg onderhoud vast. Beschrijf preventief onderhoud en hoe je storingen oplost.

#### 4. Afspraken in de keten

- Controleer je leveranciers. Vraag welke beveiligingsmaatregelen zij hebben.
- Maak een complianceverklaring. Beschrijf daarin jouw beveiligingsniveau en processen.
- Spreek meldtermijnen af. Leg vast hoe en wanneer je incidenten meldt aan opdrachtgevers.

#### 5. Bewustwording en training

- Train medewerkers in cybersecurity en fysieke beveiliging.
- Oefen incidenten met simulaties om je respons te testen.

Kijk op [Cybersecurity - Techniek Nederland](#) voor meer informatie over wat Techniek Nederland al beschikbaar heeft over dit onderwerp.

<sup>7</sup> Zie ook <https://www.nctv.nl/onderwerpen/w/wet-weerbaarheid-kritieke-entiteiten/hoe-kunnen-organisaties-zich-voorbereiden> en <https://www.nctv.nl/onderwerpen/c/cyberbeveiligingswet/aan-de-slag-waar-te-beginnen>

### 3. Wat verwachten opdrachtgevers en andere partijen van techniekbedrijven in een crisis?



**Als er een crisis is, willen opdrachtgevers dat techniekbedrijven snel en goed reageren. Ze rekenen erop dat techniekbedrijven helpen om vitale processen weerbaar te maken. Denk aan energie, water, infrastructuur en communicatie. Zonder techniekbedrijven komt veel stil te liggen.**

We hebben twaalf partijen bevroegd (zie ook Verantwoording en bijlage 2), die een goed beeld konden schetsen van hun verwachtingen aan techniekbedrijven, ook in relatie tot de vitale infrastructuur. We vroegen hen:

- Hoe afhankelijk bent u van techniekbedrijven tijdens een crisis?
- Wat verwacht u dan van deze bedrijven?
- Welke vaardigheden moeten experts uit de technieksector hebben?
- Welke stappen kan de sector nu al zetten om snel te handelen?
- Wat verwacht u van Techniek Nederland als brancheorganisatie?

### **3.1 Verwachtingen van opdrachtgevers en andere partijen**

De antwoorden laten zien dat opdrachtgevers veel waarde hechten aan voorbereiding en samenwerking. Hun verwachtingen zijn te bundelen in tien punten. Dat zijn in willekeurige volgorde:

1. *Snel bereikbaar zijn en blijven handelen*  
Opdrachtgevers willen direct contact kunnen maken, ook als omstandigheden moeilijk zijn. Bereikbaarheid en mobiliteit zijn cruciaal om storingen snel op te lossen.
2. *Beschikbaarheid van kritieke onderdelen*  
Onderdelen moeten op strategische plekken op voorraad zijn. Zonder onderdelen ligt herstel stil.
3. *Eigen crisismanagement op orde*  
Bedrijven moeten zelf voorbereid zijn, inclusief inzicht in afhankelijkheden. Zo kunnen ze opdrachtgevers beter helpen. Heldere afspraken vooraf (over samenwerking in crisissituaties) zorgen dat iedereen weet wat te doen als het misgaat.
4. *Noodvoorzieningen en terugvalopties*  
Bedrijven moeten tijdelijke oplossingen kunnen bieden, zodat processen doorgaan tot de storing is verholpen.
5. *Kennis van gebouw en installaties*  
Experts moeten weten hoe systemen werken, ook handmatig. Dit voorkomt stilstand als (digitale) systemen uitvallen.
6. *Medewerkers techniekbedrijven getraind in crisisscenario's*  
Oefening maakt het verschil. Wie weet wat te doen, werkt sneller en voorkomt fouten.

7. *Opschaling van personeel*  
Bij grote schade is soms veel handkracht nodig. Bij een crisis moet de storingsdienst op volle kracht kunnen draaien. Bedrijven moeten meedenken over hoe snel extra mensen kunnen worden ingezet. Dat vraagt om flexibiliteit en planning. Techniekbedrijven moeten weten wie beschikbaar is, ook bij ziekte, thuissituaties of inzet van reservisten en arbeidsmigranten.
8. *Proactief meedenken over kwetsbaarheden*  
Opdrachtgevers waarderen bedrijven die vooraf meedenken over risico's en robuuste oplossingen.
9. *Signaleer (wettelijke) beperkingen*  
Techniekbedrijven kunnen bij Techniek Nederland en/of de overheid aangeven waar wet- en regelgeving de dienstverlening van techniekbedrijven belemmert (vb: elektrificatie wagenpark versus zelfredzaam zijn wanneer elektriciteit uitvalt).
10. *Veilige en betrouwbare werkomgeving voor vertrouwelijke informatie*  
Door strengere wetgeving (zoals Wwke, Cbw, ABDO/ABRO<sup>8</sup>) moeten medewerkers vooraf gecontroleerd zijn. Dit geeft opdrachtgevers zekerheid. Sommige werkzaamheden vragen om een omgeving waar gerubriceerde informatie veilig blijft.

### 3.2 Wat betekent dit voor de technieksector?

Deze verwachtingen van opdrachtgevers vragen om actie van techniekbedrijven. Bedrijven moeten investeren in kennis, voorraadbeheer, training en crisismanagement. Ook samenwerking en duidelijke afspraken zijn belangrijk. Ga zo vroeg mogelijk het gesprek aan met je opdrachtgever. Ook over bijvoorbeeld ethische dilemma's (zoals veiligheid van inzet eigen medewerkers versus maatschappelijke noodzaak tijdens crises) en schaarste.

Techniekbedrijven kunnen zelf een prioritering maken welke opdrachtgever ze eerst willen helpen. Echter, bij de verdeling van schaarse middelen tijdens crisisbeheersing ligt de primaire verantwoordelijkheid bij de overheid om inzet te prioriteren, in samenwerking met publieke en private partners.

Techniek Nederland speelt hier als brancheorganisatie een cruciale rol door de achterban te ondersteunen en als spreekbuis van de sector te fungeren richting overheid. Hoofdstuk 6 gaat verder in op de rol van Techniek Nederland tijdens crises.

<sup>8</sup> Vanaf 1 januari 2026 gelden er nieuwe beveiligingseisen voor bedrijven die voor de overheid een opdracht uitvoeren met risico's voor de nationale veiligheid. Dat zijn de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO).

Per punt wordt in de tabel hieronder aangegeven wat techniekbedrijven kunnen doen om aan de verwachtingen van opdrachtgevers te voldoen.

Punt	Waarom belangrijk	Wat betekent dit voor techniekbedrijven
1. Snel bereikbaar zijn en blijven handelen	Opdrachtgevers moeten direct hulp krijgen om stilstand te voorkomen.	Zorg voor 24/7 storingsdienst, noodplannen voor mobiliteit en duidelijke contactkanalen.
2. Beschikbaarheid van kritieke onderdelen	Zonder onderdelen ligt herstel stil en loopt schade op.	Richt strategische voorraadpunten in en maak afspraken met leveranciers.
3. Eigen crisismanagement op orde	Bedrijven moeten zelf voorbereid zijn om opdrachtgevers te helpen. Helderheid voorkomt chaos tijdens een crisis.	Stel een crishandboek <sup>9</sup> op en test dit regelmatig. Leg afspraken vast in contracten of Service Level Agreements (SLA').
4. Noodvoorzieningen en terugval-opties	Processen moeten doorgaan tot de storing is opgelost.	Investeer in mobiele noodinstallaties en standaard noodscenario's.
5. Kennis van gebouw en installaties	Bij uitval van digitale systemen moet handmatige bediening mogelijk zijn.	Bouw een actuele database (bij uitval systemen handig deze op papier te hebben) van installaties en train medewerkers in noodprocedures.
6. Medewerkers techniekbedrijven getraind in crisisscenario's	Oefening voorkomt fouten en versnelt herstel.	Organiseer crisistrainingen en scenario-oefeningen.
7. Opschaling van personeel	Bij een crisis is extra capaciteit nodig. Beschikbaarheid van personeel bepaalt continuïteit.	Ontwikkel een opschalingsplan en flexibele contracten. Monitor inzetbaarheid, inclusief reservisten en externe krachten. Werk samen met brancheorganisaties en opleiders voor snelle inzet.
8. Proactief meedenken over kwetsbaarheden	Voorkomt problemen en versterkt klantrelatie.	Voer risicoanalyses uit op de systemen van je opdrachtgevers en adviseer over robuuste oplossingen en technische mogelijkheden.
9. Signaleer (wettelijke) beperkingen	Opdrachtgevers moeten weten wat kan en wat niet.	Bespreek (wettelijke) beperkingen met Techniek Nederland/de overheid.
10. Veilige en betrouwbare werkomgeving voor vertrouwelijke informatie	Sommige projecten bevatten gerubriceerde gegevens. Wetgeving vereist voorafgaande controles voor veiligheid.	Creëer beveiligde werkplekken en duidelijke procedures. Voer screenings uit en houd certificeringen actueel.

**Tabel 1:** Verwachtingen van opdrachtgevers en gevolgen voor techniekbedrijven

<sup>9</sup> In hoofdstuk 4.1.6 vind je een lijst met wat er minimaal in een crishandboek moet staan. Kijk in het kader met maatregelen voor bedrijven.

## 4. Weerbaarheid van de technieksector aan de hand van drie scenario's



**In dit onderzoek is per scenario uit hoofdstuk 1.2 gekeken hoe weerbaar en zelfstandig techniekbedrijven zijn. In drie workshops met leden van Techniek Nederland bespraken we welke gevolgen elk scenario heeft voor bedrijven en hoe groot de gevolgen zijn (impact hoog/middel/laag). Daarna onderzochten we welke maatregelen deze gevolgen kunnen verkleinen.**

Er zijn drie soorten maatregelen: maatregelen die je vooraf neemt om schade te voorkomen, maatregelen die helpen om tijdens een scenario goed om te gaan met verstoringen, en maatregelen die zorgen dat een bedrijf na afloop snel herstelt. Sommige maatregelen zijn geschikt voor één bedrijf, andere voor de hele technieksector. Er zijn ook maatregelen die medewerkers persoonlijk sterker maken. Hoe weerbaar een bedrijf is, hangt af van een goede mix van deze drie soorten maatregelen. Dit is vaak maatwerk en afhankelijk van hoe een bedrijf is georganiseerd, welke processen belangrijk zijn en welke (financiële) middelen beschikbaar zijn.

In de volgende paragrafen lees je meer over de scenario's, de gevolgen voor techniekbedrijven, de maatregelen om de weerbaarheid te vergroten en een reflectie op de vraag hoe weerbaar de sector nu is. We beschrijven de gevolgen en maatregelen van de eerste twee scenario's samen. Veel gevolgen en maatregelen bij uitval van internet en telefonie gelden namelijk ook wanneer de elektriciteit uitvalt. Bij een stroomstoring kunnen de gevolgen nog groter en ingewikkelder zijn. Om te laten zien hoe de maatschappelijke gevolgen tijdens een stroomuitval toenemen, tonen we in de toelichting op het scenario 'uitval elektriciteit' de gevolgen in verschillende tijdsfasen.

In de kaders met gevolgen en maatregelen in hoofdstuk 4.1.5 en 4.1.6 zie je duidelijk:

- welke gevolgen en maatregelen bij uitval van internet en telefonie horen, en
- welke gelden als de elektriciteit uitvalt.

## 4.1 Uitval internet en telefonie of uitval elektriciteit

### 4.1.1 Korte beschrijving scenario uitval internet en telefonie door sabotage statelijke actor

#### SCENARIO

In verschillende landen in Europa zijn teams actief die namens een statelijke actor<sup>10</sup> digitale infrastructuur aan het saboteren zijn. Doelwitten zijn strategische locaties, zoals glasvezelkabels bij datacenters, internetknooppunten en telecomaانبieders. In Nederland wordt door een dergelijk team een landelijke mobiele telecomaانبieder getroffen.

De uitval heeft onmiddellijk grote gevolgen op het dagelijks leven. Mobiele netwerken, en het vaste netwerk vallen in delen van het land stil, waardoor bellen en internetgebruik niet mogelijk is. Doordat steeds meer apparaten verbonden zijn met internet ('Internet of Things'), zoals verlichting, zonnepanelen en de thermostaat, zullen deze ook niet beschikbaar zijn. Het toonbankbetalingsverkeer raakt verstoord, waardoor men niet meer kan afrekenen in onder andere supermarkten en apotheken. Contant geld opnemen is niet meer mogelijk door de verstoring van pinautomaten.

Ook de handel met het buitenland wordt geraakt. Reizigers kunnen de weg op, maar dit zal ook belemmerd worden omdat Rijkswaterstaat geen digitaal zicht meer heeft op de weg, en het treinverkeer is regionaal belemmerd door uitval van interne netwerken. De telecomaانبieder geeft aan dat het onduidelijk is hoe lang het zal duren voordat de telefonie- en datavoorziening weer is hersteld. Herstelwerkzaamheden worden bemoeilijkt doordat monteurs ook geen toegang tot interne digitale systemen hebben die noodzakelijk zijn voor onderhoudswerkzaamheden.

In dit scenario gaan we ervan uit dat het 72 uur duurt om het grootste deel van de netwerk- en telecomvoorzieningen in het getroffen gebied weer op gang te brengen met behulp van noodoplossingen en provisorische oplossingen.

Bron: Voorstelbare scenario's t.b.v. de uitvraag weerbaarheid van VNO-NCW en MKB-Nederland, d.d. 16 januari 2026

### 4.1.2 Verdere toelichting scenario uitval internet en telefonie door sabotage statelijke actor

#### Voorbeeld van SCENARIO

Grootschalig uitval van internet en telefonie en de gevolgen daarvan is geen onrealistisch scenario meer. Onze maatschappij geniet veel voordelen van de voortschrijdende digitalisering, maar het maakt ons ook kwetsbaar. Een voorbeeld van 19-20 oktober 2025 liet zien hoeveel invloed een storing bij een internet-cloudprovider kan hebben [17] [18] [19] [20]: op die dag vond een grote storing plaats bij de clouddienst AWS in de regio Noord-Virginia in de Verenigde Staten. Door een fout in het systeem dat domeinnamen omzet naar adressen konden belangrijke diensten niet goed werken. De storing begon in de nacht en duurde tot de volgende middag.

<sup>10</sup> De Nederlandse overheid definieert een statelijke actor als een buitenlandse regering, of groepen die voor die regering werken. Zij doen soms in het geheim dingen die Nederland kunnen schaden. Dat kan gevaarlijk zijn voor de veiligheid van ons land en voor onze democratie.

Dit had grote gevolgen voor bedrijven en gebruikers wereldwijd:

- Apps zoals Snapchat, Netflix of Adobe werkten niet of waren traag.
- Klanten van banken konden niet bij hun rekeningen.
- Reizigers konden niet inchecken.
- Slimme apparaten thuis (zoals de spraakassistent Alexa) functioneerden niet goed.
- E-commerceplatforms, financiële transacties en interne bedrijfsapplicaties lagen stil.

Wereldwijd werden er meer dan 17 miljoen incidenten gemeld, wat de schaal en impact van de storing laat zien.

Wanneer in Nederland internet en telefonie gedurende 72 uur uitvallen, verandert het dagelijkse functioneren van organisaties en de samenleving ingrijpend:

1. Mensen kunnen elkaar niet meer bereiken en geen informatie krijgen.
2. Bedrijven kunnen niet goed werken. Transport en handel raken verstoord.
3. Mensen weten niet wat er gebeurt en maken zich zorgen.
4. Het kan gevaarlijk worden voor mensen en hun gezondheid.
5. Energiesystemen en betalingen werken niet goed meer.
6. Reizen en verkeer wordt lastig.

#### 4.1.3 Korte beschrijving scenario uitval elektriciteit door sabotage statelijke actor

## SCENARIO

In een regio van Nederland valt de stroom uit, waardoor de 2 miljoen klanten van een netbeheerder zonder stroom komen te zitten. Al snel wordt duidelijk dat het om een aanval van een statelijke actor gaat. Bij de aanslag zijn op meerdere plekken verdeelstations kapot gemaakt. De netbeheerders werken aan herstel. Het is onduidelijk hoe lang het zal duren voor de elektriciteitsvoorziening weer is hersteld.

De uitval heeft onmiddellijk grote gevolgen op het dagelijks leven. Elektrische apparaten met een accu, zoals mobiele telefoons en laptops, maar ook medische thuisapparatuur en elektrische auto's kunnen enkele uren functioneren, maar vallen vervolgens ook uit. De telecommunicatie valt binnen enkele uren ook grotendeels uit. Het toonbankbetalingsverkeer raakt verstoord, waardoor men niet meer kan afrekenen in onder andere supermarkten en apotheken.

Ook contant geld opnemen is niet meer mogelijk door de uitval van pinautomaten. Het treinverkeer valt uit, wat voor grote drukte op de stations zorgt. Het verkeer op wegen loopt vast vanwege het uitvallen van matrixborden, verkeerslichten en op afstand bestuurbare infrastructuur als bruggen. Schiphol ligt buiten het gebied waar de stroom is uitgevallen, maar raakt wel ontgeld door het vastlopen van snelwegen en treinen.

Ongeveer een dag na de uitval vallen meer nutsvoorzieningen uit. De verwarming doet het niet meer en bij woningen boven de tweede verdieping komt er geen water meer uit de kraan. Er ontstaan problemen met de noodstroomvoorzieningen bij vitale objecten, omdat brandstofvoorraden niet overal aanwezig zijn.

Het duurt 72 uur om het grootste deel van de stroomvoorziening in het getroffen gebied weer op gang te brengen met behulp van noodoplossingen, hulp uit het buitenland en provisorische oplossingen.

Bron: Voorstelbare scenario's t.b.v. de uitvraag weerbaarheid van VNO-NCW en MKB-Nederland, d.d. 16 januari 2026

#### 4.1.4 Verdere toelichting scenario uitval elektriciteit door sabotage statelijke actor

In het voorjaar 2025 keek Europa ongelovig naar Spanje en Portugal. Deze landen werden op maandag 28 april 2025 getroffen door een enorme, grootschalige stroomstoring die vrijwel het hele Iberisch Schiereiland lamlegde, inclusief delen van Zuid-Frankrijk. De impact was aanzienlijk:

- Miljoenen huishoudens zaten urenlang zonder elektriciteit;
- Mobiele netwerken vielen uit;
- Het verkeer raakte ontregeld door uitgevallen verkeerslichten;
- Treinen kwamen tot stilstand;
- Hulpdiensten konden nauwelijks met elkaar communiceren.

De totale hersteltijd van de stroomuitval betrof ongeveer 18 uur [21].

In januari 2026 kreeg Berlijn in Duitsland te maken met de langste stroomuitval sinds de Tweede Wereldoorlog. In het zuidwesten van de stad kwamen zo'n 45.000 tot 50.000 huishoudens én ruim 2.000 bedrijven zonder elektriciteit te zitten door brandstichting op een elektriciteitskabelbrug.

De storing begon in het weekend van 3 januari en duurde zeker tot 7 januari, toen het elektriciteitsnet pas volledig was hersteld.

De gevolgen waren groot:

- De mensen in de getroffen wijken hadden geen verwarming, lampen of warm water.
- Wegen, treinen en mobiele telefoons hadden last van storingen.
- Monteurs moesten in bevroren grond en kabels werken: daardoor duurde het herstel enkele dagen [22].

Ook in Nederland was in november 2025 een storing. In Roosendaal en Nispen zaten duizenden huishoudens een paar uur zonder stroom door een probleem in een verdeelstation [23]. Deze uitval was overzichtelijk en beperkt tot twee gemeentes, maar wanneer de stroom plotseling in grote delen van Nederland uitvalt verandert het leven in de getroffen regio's in korte tijd aanzienlijk. De situatie wordt dan steeds ernstiger naarmate de stroom langer uitvalt<sup>11</sup>.

<sup>11</sup> Tijdsfasering gebaseerd op informatie van de Nationale Coalitie Weerbaarheid. In de Nationale Coalitie Weerbaarheid werken zo'n 50 bestuurders uit het bedrijfsleven, overheid en kennisinstellingen (waaronder VNO-NCW en TNO) aan oplossingen voor een veilig en weerbaar Nederland [29].

## Gevolgen uitval internet en telefonie of uitval elektriciteit

### 0-2 uur na uitval

- Mensen proberen massaal thuis te komen en elkaar te bereiken
- Winkels en scholen sluiten
- OV ligt stil, bruggen en spoorbomen staan vast, stoplichten gaan uit, tunnels gaan dicht
- Honderden mensen vast in liften
- Apparaten werken door op accu's
- Betalingsverkeer valt uit

### 2-8 uur na uitval

- Telecom valt uit
- Digitale communicatie niet meer mogelijk (zonder noodnetwerk)
- Planbare niet kritieke zorg uitgesteld
- Waterdruk daalt, geen water boven 3e verdieping, eerste problemen met riolering
- Evacuatie en opvang gestrande reizigers
- Havenindustrie en logistiek ligt stil, uitval kranen en installaties

### 8-24 uur na uitval

- Tankstations werken niet meer
- Transport en logistiek ernstig beperkt, vrachtwagens staan vast
- Informatievoorziening richting maatschappij fragmentarisch via noodradio's
- Riolerpompen vallen uit, overstort
- Geruchten en nepnieuws verspreiden zich
- Brandstofaanvoer stopt, aanvulling noodaggregaten in de knel. De overheid bepaalt hoe diesel in Nederland wordt verdeeld in geval van schaarste (NCP-E) [25], (LCP-O), [30].
- Eerste meldingen onrust openbare orde
- Pluimvee sterfte als gevolg van uitval airconditioning of verwarming

### 24-48 uur na uitval

- Verlies van vertrouwen en onzekerheid over herstel
- Tekort aan medicijnen
- Tekort aan drinkwater
- Tekort aan voedsel
- Hulpdiensten massaal ingezet en overbelast
- Op verschillende plekken plunderingen en agressie
- Hygiëne problemen door uitval water en overstromingen riolering
- Toenemend gevoel van onveiligheid

### 48-72 uur na uitval

- Hoge druk op kwetsbare groepen door uitval medische hulpmiddelen, thuiszorg en overbelasting mantelzorgers
- Zorg verschuift volledig naar crisisgeneeskunde
- Openbare orde sterk onder druk, onrust door toenemende schaarste
- Vermoeidheid en overbelasting hulpdiensten
- Reserves raken op, distributie levensmiddelen via nooduitgifte
- Noodstroomvoorziening valt om door tekort aan brandstof
- Beperkte capaciteit bij gemalen, lokale overstromingen tijdens aanhoudende regenval



#### 4.1.5 Gevolgen voor de technieksector bij uitval internet en telefonie of bij uitval elektriciteit

We hebben onderzocht wat een grote uitval van internet en telefonie of een langdurige stroomstoring betekent voor de technieksector.

Dat deden we aan de hand van zes domeinen:

1. Gevolgen door verstoring van communicatie en informatievoorziening;
2. Gevolgen door verstoring van operationele processen, logistiek en handel;
3. Gevolgen door verstoring van de maatschappij;
4. Gevolgen door impact op veiligheid en gezondheid;
5. Gevolgen door verstoring van energievoorzieningen en betalingsverkeer;
6. Gevolgen door beperkingen in mobiliteit en verkeer.

De onderstaande kaders tonen de gevolgen per domein. Een kruisje ('X') in de kolom 'uitval internet en telefonie' en/of 'uitval elektriciteit' betekent dat dit gevolg hoort bij die vorm van uitval.

1. Communicatie & Informatievoorziening		Uitval internet en telefonie	Uitval elektriciteit
<b>Impact hoog</b>	▶ Je bedrijf (servicedesk) is telefonisch niet bereikbaar.	X	X
	▶ Je weet niet waar personeel/monteurs zich bevinden.	X	X
	▶ Je kan collega's, opdrachtgevers, de overheid en je leden/achterban niet meer bereiken, omdat e-mail, berichten-apps (zoals Whatsapp, Signal, etc.) en (mobiele) telefoons niet werken.	X	X
	▶ Je medewerkers kunnen elkaar niet goed bereiken.	X	X
	▶ Je kan geen informatie via digitale systemen verkrijgen (mobiele telefoon, laptop/computer, tv, digitale radio).	X	X
<b>Impact middel</b>	▶ Je weet niet hoe je je partners in de keten of opdrachtgevers kan laten weten welke dienstverlening je wel/niet kan bieden.	X	X
<b>Impact laag</b>	▶ Je hebt back-up systemen, maar je weet niet hoe lang de uitval gaat duren en of de back-up systemen lang genoeg mee zullen gaan.	X	X

## 2. Operationele processen, Logistiek & Handel

		Uitval internet en telefonie	Uitval elektriciteit
<b>Impact hoog</b>	▶ Je opdrachtgevers kunnen geen operationele storingen bij je melden.	X	X
	▶ Er is geen planning meer mogelijk, omdat je hiervoor software gebruikt die in een online cloud-omgeving draait en door de uitval niet meer bereikbaar is.	X	X
	▶ Je moet overschakelen naar de manier van werken die je in een crisishandboek hebt beschreven, indien je dit vooraf hebt vastgelegd.	X	X
	▶ Je kan geen materieel/onderdelen bij je leverancier inkopen, omdat hun online-portaal niet werkt en je ze telefonisch niet kan bereiken. Ook fysiek bij hun langsrijden helpt alleen maar voor een beperkt aantal onderdelen, omdat hun geautomatiseerd magazijnproces niet werkt door de internetuitval.	X	X
	▶ Bij gedeeltelijk uitval van systemen ervaar je achteraf problemen omdat de bewijslast waarom iets niet/wel gedaan is (storing verholpen, facturen betaald, etc.) beperkt is.	X	X
<b>Impact middel</b>	▶ Je monteurs kunnen gebouwbeheersystemen niet uitlezen.	X	X
	▶ Je kan je voorraden/materiaal niet aanvullen.	X	X
	▶ Jij en je personeel kunnen bepaalde (opdrachtgever-)locaties niet goed bereiken omdat toegangscontrolesystemen niet werken (poorten, slagbomen, gebouwauthenticatie).	X	X
	▶ Je bedrijfslocatie is niet langer beveiligd door uitval van het alarmsysteem.	(X)	X
<b>Impact laag</b>	▶ Je weet niet zeker welke van je bedrijfslocaties kritiek zijn voor je bedrijfsvoering, indien je dit niet vooraf in kaart hebt gebracht.	X	X

## 3. Maatschappij

		Uitval internet en telefonie	Uitval elektriciteit
<b>Impact hoog</b>	▶ Er ontstaat onrust bij medewerkers en hun familieleden door gebrek aan informatie en omdat onduidelijk is hoelang de uitval nog zal duren.	X	X
	▶ Er ontstaat paniek bij collega's, zeker bij collega's met een specifieke zorgsituatie thuis omdat medische thuiszorg-apparatuur uitvalt.		X
	▶ Je kan/wil medewerkers 's nachts niet meer naar bepaalde opdrachtgeverlocaties toe sturen, omdat deze zich in een maatschappelijk onrustig gebied bevinden. Hierdoor kom je afspraken met opdrachtgevers niet meer na.		X
	▶ Je dreigt een personeelstekort te krijgen (terwijl je opdrachtgevers opschaling verwachten) omdat medewerkers door onzekerheid thuis blijven.		X
	▶ Medewerkers raken sneller overbelast door zorgen, overbelasting, piekgedrag verdere uitval of schaarste.		X



## 4. Veiligheid & Gezondheid

		Uitval internet en telefonie	Uitval elektriciteit
<b>Impact hoog</b>	▶ Je bedrijfslocatie (kantoor, opslag) functioneert minder goed omdat algemene, vitale voorzieningen in de omgeving verstoord raken. Zo ontstaat wateroverlast door uitvallende pompen, en is er geen water meer voor keukens en toilet.		X
<b>Impact middel</b>	▶ Je kan/wil medewerkers bepaalde activiteiten niet meer uit laten voeren, omdat hun persoonlijke veiligheid niet meer geborgd kan worden (als bepaalde geautomatiseerde processen niet meer veilig werken).	X	X
	▶ Jij en je medewerkers lopen een hoger risico op ongevallen (op locatie, de werkplaats, in het verkeer), waardoor persoonlijk mogelijk (tijdelijk) uitvalt.		X

## 5. Energie & Betalingsverkeer

		Uitval internet en telefonie	Uitval elektriciteit
<b>Impact hoog</b>	▶ Je kan salarissen niet uitbetalen, waardoor onrust bij je medewerkers ontstaat.	X	X
	▶ Jij en je medewerkers hebben niet voldoende contant geld en kunnen dingen zoals koffie, lunch etc. niet betalen.	X	X
	▶ Je kan je leveranciers niet betalen waardoor leveringen onzeker zijn.	X	X
	▶ Je kan geen contant geld meer ophalen, waardoor je lopende verplichtingen niet meer contant kan betalen.	X	X
	▶ Op je bedrijfslocaties, maar ook bij opdrachtgevers valt verwarming, koeling en verlichting uit.		X
<b>Impact middel</b>	▶ Je financiële controle is beperkt, omdat je online geen inzicht hebt in je financiën.	X	X
	▶ Je kan geen facturen betalen.	X	X
	▶ Jouw opdrachtgevers kunnen je facturen niet betalen.	X	X

## 6. Mobiliteit & Verkeer

		Uitval internet en telefonie	Uitval elektriciteit
<b>Impact hoog</b>	▶ Je kan je opdrachtgevers minder goed/niet bereiken omdat tanken/laden van je bedrijfsvoertuigen niet mogelijk is.	X	X
	▶ Je bedrijfslocatie (kantoor, opslag) is niet goed bereikbaar door verkeerschaos.		X
	▶ Jij en je medewerkers zijn minder mobiel en kunnen opdrachtgevers en leveranciers niet goed bereiken door verkeerschaos.		X
<b>Impact middel</b>	▶ Jij en je medewerkers lopen vertraging op bij het bereiken van locaties (opdrachtgevers, groothandel, eigen opslaglocaties etc.) door beperkingen in het verkeer.	X	



#### 4.1.6 Maatregelen ter versterking weerbaarheid

In dit hoofdstuk lees je welke maatregelen de gevolgen kunnen verkleinen. Sommige maatregelen kan Techniek Nederland uitvoeren voor de hele technieksector. Andere maatregelen zijn voor bedrijven. Er zijn ook maatregelen die medewerkers persoonlijk sterker maken.

Een kruisje ('X') in de kolom 'uitval internet en telefonie' en/of 'uitval elektriciteit' betekent dat deze maatregel hoort bij die vorm van uitval.

Maatregelen sector/brancheorganisatie		Uitval internet en telefonie	Uitval elektriciteit
Vooraf	▶ Door middel van dit rapport inzichten bieden in de gevolgen van deze scenario's, en met welke maatregelen techniekbedrijven hun weerbaarheid kunnen verhogen.	X	X
	▶ Coördinatie van strategische voorraden: bepalen wat kritische reservedelen zijn en afspraken maken voor wat betreft noodvoorraden en verdeling bij schaarste.	X	X
	▶ Met overheid afspraken maken over financiering noodvoorraad en noodmaatregelen in relatie met de nieuwe wetgeving.		X
	▶ Ondersteunen door kennisdeling, trainingen, gezamenlijke oefeningen en het ontwikkelen van sectorale draaiboeken.	X	X
	▶ Weerbaarheid, de risico's van deze scenario's en de maatschappelijke opgave onder de aandacht brengen bij (het management van) bedrijven, zodat de operationele werkvloer meer kan denken over maatregelen en oplossingen.	X	
	▶ Met de overheid afspraken maken voor brandstofvoorziening voor noodaggregaten in de technieksector.		X
	▶ Regionale kringen opzetten, inclusief een actueel overzicht met voorraad van essentiële onderdelen.		X
Tijdens	▶ Regionale kringen opzetten, inclusief een actueel overzicht met voorraad van essentiële onderdelen.		X
Erna	▶ Evalueren hoe de crisis is verlopen en wat ervan geleerd kan worden.	X	X

Maatregelen bedrijven		Uitval internet en telefonie	Uitval elektriciteit
Vooraf	▶ Ga met je bank in gesprek over hoe betalingsverkeer door kan gaan in geval van een crisissituatie, zoals groot-schalige uitval van internet en telefonie of elektriciteit.	X	X
	▶ Breng vooraf je kritieke processen in kaart om te bepalen hoe kwetsbaar je bent tijdens dit scenario. Wat werkt allemaal niet meer als internet en telefonie of elektriciteit uitvalt, en hoe belangrijk zijn deze processen? Vervolgens kan je specifieke maatregelen of alternatieven bedenken.	X	X

		Uitval internet en telefonie	Uitval elektriciteit
Vooraf	<ul style="list-style-type: none"> <li>▶ Bepaal:               <ul style="list-style-type: none"> <li>- Welke opdrachtgevers aangemerkt zijn als vitale organisaties (of wat je kritieke opdrachtgevers zijn) die in geval van crisis door moeten blijven werken, en vervolgens:</li> <li>- Welke functies binnen je organisatie cruciaal zijn tijdens crisis (voor het werk bij kritieke opdrachtgevers en voor je eigen bedrijfsvoering). Houd er rekening mee dat sommige medewerkers met een cruciale functie extra taken doen, zoals werk als mantelzorger. Hierdoor kunnen zij in een noodsituatie langere tijd afwezig zijn. Leg dit vast in een plan voor personele continuïteit;</li> <li>- Welke middelen heb je in dit soort scenario's beschikbaar (vervoersmiddelen, materieel).</li> </ul> </li> </ul> <p>Prioriteer vervolgens op deze punten en bedenk hoe je schaarse middelen (medewerkers, vervoersmiddelen, materieel) tussen hun wil toedelen.</p>	X	X
	<ul style="list-style-type: none"> <li>▶ Zorg voor permanent actuele lokale en papieren back-up voor alle essentiële informatie, inclusief commerciële en financiële informatie, navigatie informatie (kaarten), voorraad informatie.</li> </ul>	X	X
	<ul style="list-style-type: none"> <li>▶ Zorg voor communicatiemiddelen die bij uitval van (één of meerdere) telecomdiensten blijven functioneren en test deze regelmatig.</li> </ul>	X	
	<ul style="list-style-type: none"> <li>▶ Maak afspraken met je opdrachtgevers hoe je dienstverlening in geval van grootschalige telecomverstoring door kan gaan.</li> </ul>	X	
	<ul style="list-style-type: none"> <li>▶ Maak afspraken (met je medewerkers, maar ook richting je opdrachtgevers) met welke prioritering je je opdrachtgevers in geval van schaarste of crisis zal helpen.</li> </ul>	X	X
	<ul style="list-style-type: none"> <li>▶ Maak afspraken met toeleveranciers/groothandel hoe je materieel je kan krijgen als hun systemen door uitval internet en telefonie of elektriciteit verstoord raken.</li> </ul>	X	X
	<ul style="list-style-type: none"> <li>▶ Maak afspraken met opdrachtgevers over strategische voorraden (wat, hoeveel, waar).</li> </ul>		X
	<ul style="list-style-type: none"> <li>▶ Maak afspraken met (collega-)bedrijven (over regio's heen) over collegiale inleen en gebruik van elkaars schaarse resources, zodat je onderling hulp kan bieden. Bijvoorbeeld als je buurbedrijf zonne-energie accu-laadcapaciteit heeft, maar zelf tijdens crisis geen belangrijke taken moet uitvoeren, kun jij dan zijn laadcapaciteit gebruiken om je busjes op te laden?</li> </ul>	X	X
	<ul style="list-style-type: none"> <li>▶ Schrijf een crisishandboek met daarin minimaal de volgende informatie:               <ul style="list-style-type: none"> <li>- Wat is een crisis? Leg kort uit wat jullie organisatie een crisis noemt.</li> <li>- Wie doet wat? Zet duidelijk wie verantwoordelijk is voor welke taak.</li> <li>- Belangrijke telefoonnummers: noem interne en externe nummers, zoals hulpdiensten, opdrachtgevers, leveranciers.</li> </ul> </li> </ul>	X	X

		Uitval internet en telefonie	Uitval elektriciteit
<b>Vooraf</b>	<ul style="list-style-type: none"> <li>▶ - Stappenplan bij crisis en middelen: beschrijf duidelijk de stappen en werkprocedures die in verschillende noodsituaties genomen moeten worden, welke back-up plannen je hebt om door te kunnen blijven werken en wat/wie je daarvoor nodig hebt.</li> <li>- Communicatie: wie praat met medewerkers, opdrachtgevers en pers? Hoe en via welk kanaal?</li> <li>- Locaties: waar zijn nooduitgangen, EHBO-koffers? Maak afspraken over verzamelplaatsen (bijvoorbeeld dat medewerkers bij geen bereik/in geval van een uitval of crisissituatie fysiek naar kantoor komen.</li> <li>- Risico's en maatregelen: welke risico's zijn er en wat doe je om ze te beperken?</li> <li>- Contactpersonen: namen en functies van het crisisteam.</li> <li>- Checklist: een korte lijst om te controleren of alles gedaan is.</li> <li>- Evaluatie: hoe en wanneer bespreek je na afloop wat goed en fout ging?</li> </ul>	X	X
	▶ Zorg dat je kopieën van het crisishandboek op papier beschikbaar hebt.	X	X
	▶ Deel de informatie uit het crisishandboek met je medewerkers, zodat iedereen weet wat in geval van een noodsituatie te doen is.	X	X
	▶ Oefen deze scenario's samen met je medewerkers (en eventueel ook dienstverleners die voor jouw werken, zoals beveiligingsbedrijven of de portier en ketenpartners zoals leveranciers) om te testen of afspraken bekend zijn en of crisisprotocollen werken.	X	X
	▶ Zorg dat je eigen noodstroomvoorzieningen hebt. Bepaal voor welke processen je stroom nodig hebt, en welke noodstroomvoorziening daarbij past. Denk hierbij ook aan (een combinatie van) PV-oplossingen, slimme lokale buffers en opslagcapaciteit die je als noodstroomvoorziening kan inzetten.		X
	▶ Breng in kaart of er in jouw gebied radioamateurs zijn die je in geval van een crisis kan gebruiken om aan informatie te komen, of informatie te delen <sup>12</sup> .	X	
	▶ Organiseer een vervoersservice waarmee alle medewerker van en naar hun werk kunnen komen.		X
	▶ Stel een bedrijfsnoodpakket samen dat belangrijke middelen bevat die je medewerkers bij uitval elektriciteit (of een ander crisisscenario) nodig hebben (bijvoorbeeld: sleutels voor gebouwen, papieren routekaarten, accupakketten, papieren werkbonnen, etc.) en beschrijf de aanwezigheid van het bedrijfsnoodpakket in het crisishandboek.	X	X
	▶ Organiseer satelliettelefoons en oplaadmogelijkheden via bijvoorbeeld PV-cellen, zodat je met belangrijke opdrachtgevers en medewerkers in contact kan blijven.	X	

<sup>12</sup> Je vindt meer informatie over radiozendamateurs op deze websites: VERON - Vereniging voor Experimenteel Radio Onderzoek in Nederland (<https://veron.nl/>) en VRZA – de officiële website van de Vereniging van Radio Zend Amateurs (<https://www.vrza.nl/wp/>).

		Uitval internet en telefonie	Uitval elektriciteit
<b>Vooraf</b>	▶ Zorg dat je weet waar je betrouwbare informatie van de overheid (over de situatie) kan krijgen en dat je de middelen daarvoor hebt (bijvoorbeeld: opwindbare radio, frequentie van rampenzender van je regio).	X	X
	▶ Bereid je voor op de hoeveelheden storingsmeldingen die binnen zullen komen op het moment dat elektriciteit weer beschikbaar is.		X
	▶ Bereid je voor op de hoeveelheid reserveonderdelen die vaak na stroomuitval nodig zijn en waar je die kan krijgen.		X
<b>Tijdens</b>	▶ Verzamel informatie (over de situatie, maar ook over de behoeften van je opdrachtgevers) lokaal en fysiek ter plaatse (bij je gemeente, bij je opdrachtgevers) door iemand ernaar toe te sturen.	X	X
	▶ Laat medewerkers bij geen bereik/in geval van een uitval of crisissituatie fysiek naar kantoor of een andere centrale locatie komen, om daar informatie en opdrachten in ontvangst te nemen. Maak hiervoor vooraf afspraken met je medewerkers en leg dit vast in een crishandboek. Houdt hierbij rekening met de bereikbaarheid van de locatie bij mogelijke chaos op de weg en openbaar vervoer.	X	X
	▶ Zorg dat jij en medewerkers hun batterijen/accu's (voor materieel, communicatie- en vervoersmiddelen) elke nacht opladen.	X	X
	▶ Maak gebruik van betrouwbare bronnen om informatie te verkrijgen, bijvoorbeeld de Rijksoverheid, je gemeente of de veiligheidsregio via de frequentie van de rampenzender in jouw regio. Als je toegang of contacten met radioamateurs hebt, maak gebruik van informatie die zij kunnen delen.	X	X
	▶ Zorg dat jij en je medewerkers een papieren back-up administratie bijhouden (voor urenregistratie, materiaalgebruik bij opdrachtgevers en cashbetalingen bij leveranciers als de tablet niet meer werkt).	X	X
	▶ Verplaats belangrijke activiteiten naar een andere regio, die door de uitval niet is getroffen. Maak hiervoor vooraf afspraken met de verschillende vestigingen en leg dit vast in het crishandboek.	X	X
	▶ Zorg dat je een herstelplan hebt, waarin vastgelegd is welke handelingen nodig zijn, door wie en in welke volgorde, om van een verstoring in je bedrijfsvoering zo snel mogelijk te herstellen (bijvoorbeeld: Beschrijf de stappen die nodig zijn om terug te schakelen van papieren naar digitale administratie; Procedures/werkwijzen herstart van voorzieningen.)	X	X
<b>Erna</b>	▶ Evalueer hoe de crisis is verlopen en wat je bedrijf ervan kan leren.	X	X

Maatregelen medewerker		Uitval internet en telefonie	Uitval elektriciteit
Vooraf	▶ Zorg dat je gegevens over de laatste betaling aan medewerkers opgeslagen hebt en koppel dit los van het internet, zodat je weet welke salarissen je door moet betalen. Dit geeft medewerkers rust.	X	X
	▶ Biedt voor je medewerkers thuis laadpalen aan, zodat ze elektrische voertuigen over nacht kunnen opladen.	X	X
	▶ Oefen scenario's samen met je medewerkers zodat ze zich in een noodsituatie voorbereid voelen.		X
	▶ Stel samen met je medewerkers een 'bel-/of bezoekboom' op, zodat duidelijk is wie bij welke collega (fysiek) langs gaat om informatie te verstrekken.	X	X
	▶ Geef je medewerkers een (deel van) het burgernoodpakket, met bijvoorbeeld een noodradio en informatie over waar betrouwbare informatie tijdens een crisis te verkrijgen is.	X	X
	▶ Laat onderhoudsmonteurs door trainingen vaardigheden ontwikkelen zodat er altijd aandacht wordt besteed aan het 'what-if uitval scenario'. Hierdoor versterk je een cultuur waarin serieus naar dit soort incidenten gekeken wordt.	X	X
	▶ Zorg dat je medewerkers diepgaande kennis hebben van de systemen van je vitale opdrachtgevers, zodat ze snel en creatief (met beperkte middelen) kunnen repareren.	X	X
	▶ Geef alle medewerkers een basistraining in eerste hulp, brandveiligheid en evacuatieprocedures.	X	X
Tijdens	▶ Zorg voor goed werkgeverschap en houd contact met je werknemers.	X	X
Erna	▶ Biedt nazorg op menselijk niveau voor medewerkers.	X	X

#### 4.1.7 Reflectie op hoe weerbaar de sector voor deze scenario's al is

De technieksector is nu nog niet goed voorbereid op deze scenario's. De maatregelen hierboven worden nog niet vaak toegepast. Bedrijven denken vooral na over wat ze moeten doen als hun eigen bedrijf wordt getroffen door een cyberaanval, zoals ransomware. Ze denken minder aan een situatie waarin internet, telefonie of elektriciteit in een groot deel van Nederland uitvalt en wat dat betekent voor hun werk. Dit geldt niet alleen voor techniekbedrijven. Uit de Nederlandse Innovatie Monitor 2025 [24], blijkt dat het bedrijfsleven slechts beperkt bestand is tegen uitval van essentiële voorzieningen. Het merendeel van de bedrijven kan binnen een halve dag niet meer functioneren zonder elektriciteit, telecom of andere ICT-diensten. Belangrijke conclusie in de Nederlandse Innovatie Monitor is dat organisaties die meer maatregelen nemen gemiddeld weerbaarder blijken.

## 4.2 Artikel 5 situatie / strategische bijstand

### 4.2.1 Korte beschrijving scenario Artikel 5 situatie

#### SCENARIO

Nederland raakt betrokken bij een militair conflict in Oost-Europa en zal moeten voldoen aan haar bondgenootschappelijke verplichtingen onder de NAVO. Het betreft een langdurige situatie met daarin de volgende gebeurtenissen:

- Doorvoer van grote hoeveelheden militair materiaal en personeel zorgt ervoor dat transport van andere goederen wordt verstoord.
- Door dreiging ten aanzien van zeehavens en transportverbindingen worden handel en economie breed en langdurig verstoord.
- Europese landen aan de oostgrens hebben een mobilisatie afgekondigd waar veel arbeidsmigranten gehoor aan geven.
- Defensie heeft beperkt capaciteit om zich te richten op haar derde hoofdtaak: ondersteuning van de civiele maatschappij bij rampen of crisis, of voor de beveiliging van objecten.
- Er is sprake van een vluchtelingstroom naar Nederland.
- Ziekenhuizen liggen vol, gewonde militairen en vluchtelingen belasten het Nederlands zorgsysteem maximaal.

Bron: Voorstelbare scenario's t.b.v. de uitvraag weerbaarheid van VNO-NCW en MKB-Nederland, d.d. 16 januari 2026

### 4.2.2 Verdere toelichting scenario Artikel 5 situatie

#### Voorbeeld van SCENARIO

Sinds het einde van de Koude Oorlog is de Nederlandse krijgsmacht alleen betrokken geweest bij conflicten die ver buiten ons eigen grondgebied plaats vonden. Echter met de oorlog in Oekraïne is de geopolitieke situatie veranderd en is het risico op een conflict met een militaire grootmacht veel dichterbij gekomen. In de kamerbrief over Weerbaarheid tegen militaire en hybride dreigingen van december 2024 [1] stelt het Ministerie van Justitie en Veiligheid dat: Voor het eerst in lange tijd is het reëel dat Nederland via de collectieve verdedigingsclausule in het NAVO-verdrag ("artikel 5") direct betrokken raakt bij een grootschalig gewapend conflict. Verschillende partijen, waaronder Defensie en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), zijn bezig om in kaart te brengen wat de Artikel 5 clausule voor Nederland betekent. Veel van deze scenario's, plannen en analyses zijn vanwege het vertrouwelijke karakter niet publiekelijk beschikbaar. Algemeen bekend is dat:

- Nederland een belangrijke rol heeft als doorvoerland voor militaire transporten van bondgenoten richting Oost-Europa.
- Nederland net als andere NAVO-lidstaten gevechtseenheden moet leveren voor gezamenlijke verdediging. Een deel staat bij buitengrenzen van NAVO. Een ander deel wordt ingezet bij oplopende spanningen.
- Militaire eenheden beschermen ook Nederlands grondgebied (land, zee, lucht, cyber).
- Defensie helpt bij rampen en crises in Nederland, maar bij oorlog zijn er minder eenheden beschikbaar voor deze hulp.

In Bijlage 1 Verdere toelichting Artikel 5 scenario staat een mogelijk scenario dat stap voor stap is uitgewerkt.



### 4.2.3 Gevolgen voor techniekbedrijven bij een Artikel 5 scenario

We hebben onderzocht wat een Artikel 5 scenario betekent voor de technieksector. Dat deden we aan de hand van zeven domeinen:

1. Gevolgen door mobiliteits- en verkeersbeperkingen;
2. Gevolgen door oproep militairen en reservisten;
3. Gevolgen door desinformatie, angst en onzekerheid in de maatschappij, en omdat het vertrouwen in de overheid onder druk komt te staan;
4. Gevolgen door cyberaanvallen en uitval van (vitale) processen;
5. Gevolgen door verstoring van de (internationale) handelsketen;
6. Gevolgen door verschuiving van productie en andere prioritering van de Nederlandse overheid;
7. Gevolgen door grootschalig opvang van mensenmassa's.

De onderstaande kaders tonen de gevolgen per domein. Op het moment dat Nederland in een Artikel 5 scenario terecht komt zullen cyberaanvallen en sabotage van (vitale) organisaties en objecten naar verwachting toenemen. Hierdoor kunnen ook problemen met internet en telefonieverbindingen ontstaan en de elektriciteit (regionaal) uitvallen. In principe gelden daarom in dit scenario (deels) ook de gevolgen die in de eerste twee scenario's in hoofdstuk 4.1 geïdentificeerd zijn, waardoor overlap ontstaat. Kijk voor een compleet overzicht van de gevolgen door cyberaanvallen en uitval van (vitale) processen ook in hoofdstuk 4.1.5.

## 1. Mobiliteits- en verkeersbeperkingen

- |                    |  |
|--------------------|--|
| <b>Impact hoog</b> | <ul style="list-style-type: none"><li>▶ Je bedrijfslocatie (kantoor, opslag) is niet goed bereikbaar door verkeersbeperking/afsluiting van routes.</li></ul>   |
|                    | <ul style="list-style-type: none"><li>▶ Jij en je medewerkers zijn minder mobiel en kunnen opdrachtgevers en leveranciers niet goed bereiken door verkeersbeperking/afsluiting van routes, waardoor je reguliere bedrijfsvoering minder effectief is met mogelijk financiële gevolgen.</li></ul> |

## 2. Oproep militairen en reservisten

- |                      |  |
|----------------------|--|
| <b>Impact hoog</b>   | <ul style="list-style-type: none"><li>▶ Je verliest personeel en daarmee capaciteit, kennis en ervaring (personeelstekort) door:<ul style="list-style-type: none"><li>- Medewerkers uit het buitenland die in hun eigen land worden opgeroepen of op eigen initiatief naar hun eigen land gaan;</li><li>- Medewerkers die als reservist worden opgeroepen.</li><li>- Medewerkers die zich aanmelden bij het leger, of van baan wisselen om elders van betekenis te zijn.</li></ul></li></ul> |
| <b>Impact middel</b> | <ul style="list-style-type: none"><li>▶ Je kan niet/onvoldoende aan de Service Level Agreements en afspraken met je opdrachtgevers voldoen, omdat je een tekort aan mensen en middelen hebt.</li></ul>   |
|                      | <ul style="list-style-type: none"><li>▶ Jij en je medewerkers ervaren dat de werkdruk toeneemt.</li></ul>  |

### 3. Maatschappelijk onrust door desinformatie, angst, onzekerheid en dalend vertrouwen in de overheid

<b>Impact hoog</b>	<ul style="list-style-type: none"><li>▶ De effectiviteit in je eigen bedrijf wordt negatief beïnvloed door:<ul style="list-style-type: none"><li>- Medewerkers die onrustig zijn en veel met de geopolitieke situatie bezig zijn in plaats van met hun werk;</li><li>- Medewerkers die werk om verschillende redenen weigeren (bijvoorbeeld omdat ze zich niet veilig voelen, of niet meer willen werken voor bepaalde opdrachtgevers);</li></ul></li></ul>
<b>Impact middel</b>	<ul style="list-style-type: none"><li>▶ De effectiviteit in je eigen bedrijf wordt negatief beïnvloed door medewerkers die zich uit angst of zorgen ziek melden (verhoogd ziekteverzuim).</li><li>▶ Goed werkgeverschap vraagt van jou extra inspanning op sociaal vlak om voor rust en vertrouwen te zorgen.</li></ul>
<b>Impact laag</b>	<ul style="list-style-type: none"><li>▶ In jouw bedrijf wordt cruciale bedrijfsinformatie niet/onvoldoende geborgd omdat medewerkers afgeleid zijn door de geopolitieke situatie.</li></ul>

### 4. Cyberaanvallen, uitval (vitale) processen

<b>Impact hoog</b>	<ul style="list-style-type: none"><li>▶ Je bedrijf krijgt vaker te maken met de gevolgen van verstoringen of (tijdelijke) uitval van internet, telefonie of elektriciteit. Kijk hiervoor naar de gevolgen die in de eerdere scenario's beschreven zijn in hoofdstuk 4.1.5. Daarnaast kunnen ook andere vitale processen verstoord raken, zoals vliegverkeer, scheepvaart, drinkwater, gas/warmte, navigatiesystemen, digitale overheidsdiensten, etc.</li><li>▶ Door de toename van cyberaanvallen vragen je opdrachtgevers om storingsdienst op veel verschillende locaties om besturingssystemen van vitale objecten handmatig te bedienen. Je hebt hier extra mensen voor nodig en krijgt een personeelstekort.</li></ul>
--------------------	--

### 5. Verstoringen (internationale) handel

<b>Impact middel</b>	<ul style="list-style-type: none"><li>▶ Je kan bij je leveranciers geen cruciale onderdelen en materialen (bijvoorbeeld kabels, leidingen) meer krijgen, en je eigen voorraad raakt op.</li></ul>
----------------------	---

### 6. Verschuiving productie en prioritering overheid

<b>Impact hoog</b>	<ul style="list-style-type: none"><li>▶ Je verliest flexibiliteit om je eigen bedrijf te leiden omdat de overheid bepaalt:<ul style="list-style-type: none"><li>- Hoe schaarse goederen (bijvoorbeeld diesel, elektriciteit) verdeeld worden;</li><li>- Welke van jouw opdrachtgevers (bijvoorbeeld vitale organisaties) voorrang krijgen bij reparaties en onderhoud.</li></ul></li><li>▶ Aan de andere kant moet je bedrijf juist flexibel zijn om met de verschuivingen in type werk om te kunnen gaan wat in het begin wellicht minder effectief is.</li><li>▶ Je moet zelf bepaalde keuzes kunnen maken, omdat de overheid niet alles kan aansturen. Dit vraagt extra tijd en ervaring.</li></ul>
<b>Impact middel</b>	<ul style="list-style-type: none"><li>▶ Je bedrijf moet ander soort werk uitvoeren wat (deels) om andere competenties van je medewerkers vraagt (bijvoorbeeld meer revisie, herstelwerk en meer tijdelijke infrastructuur zoals ziekenhuizen, mobiele waterzuiveringsinstallaties, locaties voor opvang mensen in plaats van nieuwbouw).</li><li>▶ Je medewerkers moeten, meer dan nu, zelfstandig hun werk uitvoeren, omdat in tijden van crisis de focus mogelijk minder ligt op (veiligheids) procedures en meer op snelle dienstverlening.</li><li>▶ Je medewerkers (of delen daarvan) zijn minder inzetbaar, omdat ze bepaalde certificering of security clearance niet hebben en bepaalde activiteiten niet mogen uitvoeren. Dat kan bepaalde deelgroepen personeel zeer schaars maken en vraagt om extra planning.</li></ul>



## 7. Opvang mensenmassa's

**Niet van toepassing** De opvangen van grote groepen mensen heeft niet direct nadelige gevolgen voor het werk van techniekbedrijven. Het is juist een kans om extra opvanglocaties of tijdelijke nutsvoorzieningen te bouwen. Dit punt is daarom opgenomen in hoofdstuk 5 als bijdrage die de technieksector kan leveren.

### 4.2.4 Maatregelen ter versterking weerbaarheid

In dit hoofdstuk is beschreven welke maatregelen de gevolgen kunnen verkleinen. Sommige maatregelen kan de brancheorganisatie uitvoeren voor de hele technieksector. Andere maatregelen zijn voor bedrijven. Er zijn ook maatregelen die medewerkers persoonlijk sterker maken. Een kruisje ('X') in de kolom 'Basismaatregel' betekent dat deze maatregel ook geldt in de andere twee scenario's of in een algemene crisissituatie. Een kruisje ('X') in de kolom 'Maatregel bij Artikel 5' laat zien dat deze maatregel speciaal belangrijk is in een Artikel 5-situatie.

## Maatregelen sector/brancheorganisatie

		Basis- maatregel	Maatregel bij Artikel 5
<b>Vooraf</b>	▶ Door middel van dit rapport inzichten bieden in de gevolgen van deze scenario's, en met welke maatregelen techniekbedrijven hun weerbaarheid kunnen verhogen.	X	
	▶ Coördinatie van strategische voorraden: bepalen wat kritische reservedelen zijn en afspraken maken voor wat betreft noodvoorraden en verdeling bij schaarste (met overheid, groothandel, techniekbedrijven).	X	
	▶ Met overheid afspraken maken over financiering noodvoorraad en noodmaatregelen in relatie met de nieuwe wetgeving.	X	
	▶ Ondersteunen door kennisdeling, trainingen, gezamenlijke oefeningen en het ontwikkelen van sectorale draaiboeken.	X	
	▶ Weerbaarheid, de risico's van deze scenario's en de maatschappelijke opgave onder de aandacht brengen bij (het management van) bedrijven, zodat de operationele werkvloer meer kan denken over maatregelen en oplossingen.	X	
	▶ Met de overheid afspraken maken voor brandstofvoorziening voor noodaggregaten in de technieksector.	X	
	▶ Vooraf met de overheid in gesprek gaan, zodat wetgeving in geval van crisis versoepeld wordt.		X
	▶ Communiceren welke belangrijke diensten de sector levert in een Artikel 5 situatie.		X
	▶ Initiatief nemen om een taskforce per vitale sector op te zetten met vertegenwoordigers van Rijkswaterstaat, provincies, veiligheidsregio's, vitale aanbieders, techniekbedrijven (vergelijkbaar met huidige taskforce voor bruggen en sluisen). Doel is om werkzaamheden beter af te stemmen, te prioriteren en te bepalen waar robuustere oplossingen nodig zijn (bijvoorbeeld: versterking van bruggen).		X

		Basis- maatregel	Maatregel bij Artikel 5
	▶ Kansen verkennen om personeel gezamenlijk met Defensie op te leiden voor technische functies, met als doel dat deze daarna instromen bij techniekbedrijven en mogelijk als reservist actief blijven.		X
	▶ Samen met Defensie een praktische handreiking voor de technieksector maken voor de inzet van reservisten.		X
<b>Tijdens</b>	▶ Regionale kringen opzetten, inclusief een actueel overzicht met voorraad van essentiële onderdelen.	X	
	▶ Tijdens de crisissituatie met de overheid afspraken bevestigen zodat wetgeving versoepeld wordt en dat handelingskaders duidelijk zijn (wat mag wel, wat mag niet).		X
	▶ Afstemming en coördinatie binnen de sector en over regio's heen: Informatie verstrekken over transportroutes en wegafzettingen door Defensie.		X
	▶ In afstemming met de veiligheidsregio's inzicht verkrijgen en binnen de sector delen over bijzondere behoeften en benodigde opschaling (bijvoorbeeld aanleg van noodopvang).		X
<b>Erna</b>	▶ Evalueren hoe de crisis is verlopen en wat ervan geleerd kan worden.	X	

## Maatregelen bedrijven

		Basis- maatregel	Maatregel bij Artikel 5
<b>Vooraf</b>	▶ Breng vooraf je kritieke processen in kaart om te bepalen hoe kwetsbaar je bent als belangrijke nutsvoorzieningen (internet, telefonie, elektriciteit, gas, water) uitvallen. Wat werkt dan allemaal niet meer, en hoe belangrijk zijn deze processen? Vervolgens kan je specifieke maatregelen of alternatieven bedenken.	X	
	▶ Bepaal: <ul style="list-style-type: none"> <li>- Welke opdrachtgevers aangemerkt zijn als vitale organisaties (of wat je kritieke opdrachtgevers zijn) die in geval van crisis door moeten blijven werken, en vervolgens:</li> <li>- Welke functies binnen je organisatie cruciaal zijn tijdens crisis (voor het werk bij kritieke opdrachtgevers en voor je eigen bedrijfsvoering). Houd er rekening mee dat sommige medewerkers met een cruciale functie extra taken doen, zoals werk als reservist of mantelzorg. Ook kunnen zij worden opgeroepen voor de dienstplicht (in een ander land). Hierdoor kunnen zij in een noodsituatie langere tijd afwezig zijn. Leg dit vast in een plan voor personele continuïteit;</li> <li>- Welke middelen heb je in dit soort scenario's beschikbaar (vervoersmiddelen, materieel).</li> </ul> Prioriteer vervolgens op deze punten en bedenk hoe je schaarse middelen (medewerkers, vervoersmiddelen, materieel) tussen hun wil toedelen.	X	



	Basis- maatregel	Maatregel bij Artikel 5
▶ Zorg voor permanent actuele lokale en papieren back-up voor alle essentiële informatie, inclusief commerciële en financiële informatie, navigatie informatie (kaarten), voorraad informatie.	X	
▶ Maak afspraken (met je medewerkers, maar ook richting je opdrachtgevers) met welke prioritering je je opdrachtgevers in geval van schaarste of crisis zal helpen.	X	
▶ Maak afspraken met toeleveranciers/groothandel hoe je materieel je kan krijgen als hun systemen (door uitval internet en telefonie of elektriciteit) verstoord raken.	X	
▶ Maak afspraken met opdrachtgevers over strategische voorraden (wat, hoeveel, waar).	X	
▶ Maak afspraken met (collega-)bedrijven (over regio's heen) over collegiale inleen en gebruik van elkaars schaarse resources, zodat je onderling hulp kan bieden.	X	
▶ Schrijf een crisishandboek met daarin minimaal de volgende informatie: - Wat is een crisis? Leg kort uit wat jullie organisatie een crisis noemt. - Wie doet wat? Zet duidelijk wie verantwoordelijk is voor welke taak. - Belangrijke telefoonnummers: noem interne en externe nummers, zoals hulpdiensten, opdrachtgevers, leveranciers. - Stappenplan bij crisis en middelen: beschrijf duidelijk de stappen en werkprocedures die in verschillende nood-situaties genomen moeten worden, welke back-up plannen je hebt om door te kunnen blijven werken en wat/wie je daarvoor nodig hebt. - Communicatie: wie praat met medewerkers, opdrachtgevers en pers? Hoe en via welk kanaal? - Locaties: waar zijn nooduitgangen, EHBO-koffers? Maak afspraken over verzamelplaatsen (bijvoorbeeld dat medewerkers bij geen bereik/in geval van een uitval of crisissituatie fysiek naar kantoor komen. - Risico's en maatregelen: welke risico's zijn er en wat doe je om ze te beperken? - Contactpersonen: namen en functies van het crisisteam. - Checklist: een korte lijst om te controleren of alles gedaan is. - Evaluatie: hoe en wanneer bespreek je na afloop wat goed en fout ging?	X	
▶ Zorg dat je kopieën van het crisishandboek op papier beschikbaar hebt.	X	
▶ Deel de informatie uit het crisishandboek met je medewerkers, zodat iedereen weet wat in geval van een noodsituatie te doen is.	X	
▶ Oefen deze scenario's samen met je medewerkers (en eventueel ook dienstverleners die voor jouw werken, zoals beveiligingsbedrijven of de portier en ketenpartners zoals leveranciers) om te testen of afspraken bekend zijn en of crisisprotocollen werken.	X	

		Basis- maatregel	Maatregel bij Artikel 5
	▶ Stel een bedrijfsnoodpakket samen dat belangrijke middelen bevat die je medewerkers bij uitval elektriciteit (of een ander crisisscenario) nodig hebben (bijvoorbeeld: sleutels voor gebouwen, papieren routekaarten, accupakketten, papieren werkbonnen, etc.) en beschrijf de aanwezigheid van het bedrijfsnoodpakket in het crisishandboek.	X	
	▶ Zorg dat je weet waar je betrouwbare informatie van de overheid (over de situatie) kan krijgen en dat je de middelen daarvoor hebt (bijvoorbeeld: opwindbare radio, frequentie van rampenzender van je regio).	X	
	▶ Breng in kaart welke medewerker welke expertise, kennis en rol heeft, zodat je bij een langdurige crisis snel kunt schakelen als je functies anders moet plannen.		X
	▶ Breng in kaart voor welke werkzaamheden bij opdrachtgevers veiligheidsscreenings van medewerkers noodzakelijk zijn. Zorg voor een soepel proces om screenings uit te voeren, en houd certificeringen actueel.		X
	▶ Breng in kaart hoe afhankelijk je bent van je toeleveranciers, en probeer het risico dat je van één partij afhankelijk bent te verminderen door alternatieven te zoeken.		X
	▶ Inventariseer de mogelijkheid om snel kennis te delen (binnen je bedrijf en extern met partners of collega-bedrijven).		X
	▶ Maak een plan hoe je je werk bij een langdurige crisis wil/ moet prioriteren (wat moet wel, wat niet).		X
	▶ Maak afspraken met opdrachtgevers over wat nodig is aan (financiële) garanties in geval van een langdurige crisis.		X
<b>Tijdens</b>	▶ Laat medewerkers bij geen bereik/in geval van een uitval of crisissituatie fysiek naar kantoor of een andere centrale locatie komen, om daar informatie en opdrachten in ontvangst te nemen. Maak hiervoor vooraf afspraken met je medewerkers en leg dit vast in een crisishandboek. Houdt hierbij rekening met de bereikbaarheid van de locatie bij mogelijke chaos op de weg en openbaar vervoer.	X	
	▶ Maak gebruik van betrouwbare bronnen om informatie te verkrijgen, bijvoorbeeld de Rijksoverheid, je gemeente of de veiligheidsregio via de frequentie van de rampenzender in jouw regio. Als je toegang of contacten met radioamateurs hebt, maak gebruik van informatie die zij kunnen delen.	X	
	▶ Zorg dat jij en je medewerkers een papieren back-up administratie bijhouden (voor urenregistratie, materiaalgebruik bij opdrachtgevers en cashbetalingen bij leveranciers als de tablet niet meer werkt).	X	
	▶ Maak duidelijke afspraken tot welk opleverniveau je werkt, indien dit anders is dan tijdens je reguliere dienstverlening.		X
	▶ Stimuleer je medewerkers om innovatieve en creatieve oplossingen te bedenken, zodat (kritieke) onderdelen niet meer nodig zijn.		X

		Basis- maatregel	Maatregel bij Artikel 5
Erna	▶ Zorg dat je een herstelplan hebt, waarin vastgelegd is welke handelingen nodig zijn, door wie en in welke volgorde, om van een verstoring in je bedrijfsvoering zo snel mogelijk te herstellen.	X	
	▶ Evalueer hoe de crisis is verlopen en wat je bedrijf ervan kan leren.	X	

## Maatregelen medewerker

		Basis- maatregel	Maatregel bij Artikel 5
Vooraf	▶ Oefen scenario's samen met je medewerkers zodat ze zich in een noodsituatie voorbereid voelen.	X	
	▶ Stel samen met je medewerkers een 'bel-/of bezoekboom' op, zodat duidelijk is wie bij welke collega (fysiek) langs gaat om informatie te verstrekken.	X	
	▶ Geef je medewerkers een (deel van) het burgersnoodpakket, met bijvoorbeeld een noodradio en informatie over waar betrouwbare informatie tijdens een crisis te verkrijgen is.	X	
	▶ Laat onderhoudsmonteurs door trainingen vaardigheden ontwikkelen zodat er altijd aandacht wordt besteed aan het 'what-if uitval scenario'. Hierdoor versterk je een cultuur waarin serieus naar dit soort incidenten gekeken wordt.	X	
	▶ Zorg dat je medewerkers diepgaande kennis hebben van de systemen van je vitale opdrachtgevers, zodat ze snel en creatief (met beperkte middelen) kunnen repareren.	X	
	▶ Laat je medewerkers nieuwe/alternatieve handelingen leren, zodat ze voorbereid zijn op het anders werken tijdens een langdurige crisis.		X
	▶ Geef alle medewerkers een basistraining in eerste hulp, brandveiligheid en evacuatieprocedures.	X	
	Tijdens	▶ Zorg voor goed werkgeverschap en houd contact met je werknemers.	X
▶ Stuur medewerkers aan zodat ze met vrijwilligers, tijdelijke krachten, militairen of (internationale) partners kunnen samenwerken als dat nodig is.			X
▶ Zorg dat je medewerkers volgens veiligheidsprotocollen kunnen werken, ook onder zware omstandigheden.			X
▶ Moedig medewerkers aan om alert te zijn op berichten die sterke emoties oproepen. Vraag hen om informatie altijd bij meerdere bronnen te controleren en alleen berichten te delen die van betrouwbare bronnen komen.		(X)	X
Erna	▶ Bied nazorg op menselijk niveau voor medewerkers.	X	



#### 4.2.5 Reflectie op hoe weerbaar de sector voor dit scenario al is

Veel mensen en bedrijven weten nog niet goed wat een Artikel 5 scenario betekent en wat de gevolgen zijn voor Nederland, en hun eigen bedrijf. Dat geldt ook voor de technieksector. Er zijn nog bijna geen maatregelen genomen. Een duidelijke gezamenlijke aanpak en maatregelen geven wel zekerheid. Dit schrikt tegenstanders af, omdat zij zien dat er een sterke en goed georganiseerde verdediging klaarstaat. Dat maakt de technieksector en Nederland sterker.

#### 4.2.6 Reservisten

Reservisten zijn militairen die naast hun gewone baan parttime werken bij Defensie. Zij vormen de flexibele schil van de krijgsmacht. Dankzij reservisten kan Defensie snel extra mensen inzetten als dat nodig is. Zo blijft Nederland beter voorbereid op rampen, crises en zelfs oorlog. Defensie wil het aantal reservisten de komende jaren flink vergroten. Daarmee speelt Defensie in op de krappe arbeidsmarkt zonder deze mensen permanent uit de civiele maatschappij te onttrekken, en werkt zij nauwer samen met de maatschappij om de weerbaarheid te vergroten.

Reservisten worden ingezet waar, wanneer en waarvoor zij nodig zijn. Sommige reservisten voeren vooral militaire taken uit, zoals bewaken en beveiligen van belangrijke objecten. Zij werken vaak bij het Korps Nationale Reserve van de landmacht, maar ook bij de marine, luchtmacht en marechaussee. Hun inzet is meestal in Nederland, bijvoorbeeld bij rampenbestrijding. Wie dat wil, kan ook worden uitgezonden naar het buitenland.

Andere reservisten brengen specifieke kennis mee. Denk aan weg- en waterbouwkundigen, cyberspecialisten, juristen of tolken. Zij ondersteunen Defensie bij complexe projecten en internationale missies. Deze kennis is onmisbaar, zeker in een wereld waarin techniek en digitale veiligheid steeds belangrijker worden.

##### **Wat betekent dit voor werkgevers?**

Voor werkgevers biedt het werken met reservisten een aantal mogelijke voordelen en nadelen. Genoemde voordelen zijn de ontwikkelingen op het vlak van leiderschap, samenwerken en stressbestendigheid, het flexibeler omgaan met onverwachte situaties, het krijgen van een “can-do”-mentaliteit en een betere fysieke en mentale fitheid. Genoemde nadelen zijn de mogelijk grotere kans op arbeidsongeschiktheid waarbij de normale regels voor werkgevers daarvoor wel blijven gelden en mogelijke spanningen bij de werkgever in relatie tot plannings en projecten.

Werkgevers doen er goed aan om afspraken te maken over verlof of werktijd, om de inzet bij Defensie goed te combineren. Bij langdurige inzet kan de werkgever een financiële tegemoetkoming krijgen. Defensie betaalt een salaris tijdens inzet en zorgt voor pensioenopbouw. Zo blijft het voor beide partijen aantrekkelijk.

### **Reservisten en de technieksector**

Voor Defensie zijn reservisten uit de Technieksector extra waardevol. Veel reservisten hebben een technische achtergrond, bijvoorbeeld in bouw, infrastructuur of IT. Zij brengen hun kennis mee naar Defensie, waar die hard nodig is voor het onderhoud van wegen, bruggen, energievoorzieningen en digitale netwerken. Andersom nemen zij militaire ervaring mee terug naar hun werk. Denk aan projectplanning onder druk, teamwork en probleemoplossend denken. Dat maakt hen tot sterke en veelzijdige medewerkers. In een tijd waarin techniek steeds complexer wordt, is deze kruisbestuiving een groot voordeel.

In de Technieksector heerst een structurele arbeidsmarktkrapte. Een substantieel deel van de medewerkers in de techniek vervult een cruciale functie in sector en de bijhorende dienstverlening, zoals onder meer op energievoorzieningen, telecominstallaties of andere infrastructuur. Hun inzet als reservist zet die dienstverlening mogelijk onder druk. Het is van belang dat de sector hierover evenwichtige afspraken maakt met Defensie.

### **Reservisten in een Artikel 5 scenario**

Wanneer een Artikel 5 scenario zich voordoet, moet Nederland snel opschalen. Reservisten spelen dan een cruciale rol. Toch is niet iedereen beschikbaar. Sommige reservisten werken in vitale sectoren, zoals energie. Die mensen blijven nodig in hun gewone baan om Nederland draaiend te houden. Daarom maakt Defensie afspraken met bedrijven en houdt rekening met deze dubbelfuncties. Het doel: een weerbare samenleving waarin Defensie en bedrijfsleven samenwerken.

### **Samen sterker**

Defensie wil het voor reservisten én werkgevers makkelijker maken om samen te werken. Er komen meer opleidingen, duidelijke afspraken en speciale functies voor reservisten. Ook krijgen reservisten voorrang bij sollicitaties voor vaste functies bij Defensie. Voor werkgevers betekent dit dat zij medewerkers duurzaam inzetbaar houden en bijdragen aan de veiligheid van Nederland. Voor reservisten betekent het een kans om iets terug te doen voor de maatschappij én zich persoonlijk te ontwikkelen.

## **Aanbeveling voor werkgevers en Techniek Nederland**

De inzet van reservisten heeft gevolgen voor alle bedrijven, defensie en de werknemer zelf. Het is daarom verstandig om hier onderling afspraken over te maken. Steeds meer bedrijven en organisaties nemen hierover afspraken op in de arbeidsvoorwaarden en geven leidinggevendenden, HR-adviseurs en werknemers praktische hulpmiddelen en handreikingen. In de handreikingen staat onder andere:

- wat het betekent om reservist te zijn;
- welke gevolgen dit heeft voor pensioen en verzekeringen;
- hoe verlof voor reservisten wordt geregeld;
- welke afspraken er zijn over de beschikbaarheid van reservisten.

Techniek Nederland treedt in overleg met het ministerie van Defensie om regelingen op te stellen of te actualiseren en beleid voor de hele sector af te spreken.

# 5. Bijdrage technieksector wanneer scenario's zich voordoen



**De drie scenario's in dit rapport hebben gevolgen voor techniekbedrijven. Maar techniekbedrijven zijn essentieel om de maatschappelijke impact van deze scenario's kleiner te maken. Zo zijn zij belangrijk bij het repareren van vitale infrastructuur. Vaak hebben zij de kennis en ervaring om storingen op te lossen of tijdelijke noodvoorzieningen te plaatsen.**

**Naast hun gewone werk kunnen techniekbedrijven in geval van een crisis het volgende doen:**

1. Bij uitval van internet en telefonie: monteurs proactief langs sturen naar belangrijke opdrachtgevers om te vragen of en waar hulp nodig is.
2. Kwetsbare systemen in kaart brengen en versterken: een overzicht maken van systemen die afhankelijk zijn van internet, telefonie of elektriciteit en robuustere en toekomstbestendige oplossingen en/of configuraties voorstellen.
3. Schakelplannen<sup>13</sup> opstellen en bijwerken: voor belangrijke installaties plannen maken en actueel houden, zodat storingen snel verholpen kunnen worden.
4. Bij stroomuitval in één of meerdere regio's: tijdelijke installaties en overbruggingsoplossingen opzetten vanuit gebieden waar nog stroom is.
5. Samenwerken met Defensie: samen met Defensie leerwerktrajecten opzetten.
6. Personeel inzetten bij vitale objecten: medewerkers tijdelijk afstaan om installaties handmatig op locatie te bedienen als systemen uitvallen.
7. In een Artikel 5 scenario: technische installaties leveren aan Defensie, extra middelen zoals personeel en materieel beschikbaar stellen, of extra opvanglocaties en nutsvoorzieningen opzetten. Een flexibele, "can-do" mentaliteit kan eraan bijdragen dat de civiele maatschappij zoveel mogelijk door functioneert.

De leden van Techniek Nederland zijn in specifieke delen van de technieksector actief: Utiliteitsbouw (ziekenhuizen, stations, winkelcentra); Infra (wegen/ bruggen, elektriciteits- en telecomnetten); Industrie (industriële productieprocessen en/of de bijbehorende infrastructuur voor energie- en watervoorziening); Woningbouw (nieuwbouw, onderhoud, renovatie van gebouwen). Wanneer de behandelde scenario's in dit rapport zich voordoen zal het onderdeel "Infra" een belangrijke rol spelen bij het herstellen van vitale infrastructuur en installaties die verstoord raken. Ook als er weinig militaire hulp beschikbaar is in een Artikel 5 scenario, kan "Infra" snel bijspringen. Bij het bouwen van nooddijken tijdens overstromingen heeft "Infra" bijvoorbeeld meer kennis en capaciteit dan Defensie.

Het onderdeel "Utiliteitsbouw" is vooral belangrijk bij storingen in nutsvoorzieningen bij vitale locaties, zoals ziekenhuizen, supermarkten en distributiecentra. Zij zorgen dan voor reparaties of tijdelijke noodoplossingen. Het onderdeel "Industrie" helpt vooral bij het opnieuw opstarten en herstellen van industriële en voedselproductieprocessen na een grote stroomuitval.

<sup>13</sup> Een schakelplan (ook wel schakelschema genoemd) is een technisch document dat de elektrische verbindingen en schakelingen binnen een installatie of machine weergeeft. Het wordt veel gebruikt in techniekbedrijven, vooral in elektrotechniek, machinebouw en industriële automatisering.

In een Artikel 5 scenario verdwijnen deze scheidingen waarschijnlijk. Dan is het slim om personeel en middelen over de hele sector flexibel in te zetten en uit te lenen. Dat levert de meeste waarde op, zeker als deze middelen schaars zijn. Toch kan de technieksector haar werk alleen maar doen als aan bepaalde randvoorwaarden voldaan wordt. Belangrijkste randvoorwaarde is dat techniekbedrijven zelf weerbaar genoeg zijn en hun eigen dienst ook tijdens een crisissituatie kunnen verlenen. Met een geschikte combinatie van de maatregelen uit hoofdstuk 4 is dat mogelijk.

Daarnaast zijn er randvoorwaarden die afhangen van overheid en opdrachtgevers. Deze randvoorwaarden zijn als volgt:

#### **Randvoorwaarden vitale aanbieders/opdrachtgevers:**

1. Bereid zijn om afspraken te maken over:
  - a. bereikbaarheid tijdens verstoring communicatiemiddelen, of alternatieve communicatiemiddelen;
  - b. toegang tot opdrachtgeverlocaties tijdens uitval toegangscontrolesystemen;
  - c. actualisatie van schakelplannen en andere installatie informatie;
  - d. strategische voorraden;
  - e. verwachte dienstverlening tijdens een crisis;
  - f. garanties en/of financiële compensatie in geval van een crisis.
2. Meer aandacht voor redundantie: Vitale aanbieders moeten meer aandacht hebben voor redundantie en bereid zijn om met techniekbedrijven te kijken, hoe installaties robuuster gemaakt kunnen worden.
3. Oefenen met crisisscenario's: Opdrachtgevers moeten bereid zijn om samen met techniekbedrijven te oefenen.

#### **Randvoorwaarden overheid:**

1. Meer bewustzijn creëren over de dreigingen van deze scenario's.
2. Met Techniek Nederland afspraken maken over strategische voorraden (welke materialen, met welke garanties, beveiliging en financiering van voorraden).
3. Onderzoeken welke regels aangepast kunnen worden:
  - a. zodat techniekbedrijven in een crisis snel kunnen werken (zoals uitzonderingen op avondklok tijdens COVID-19). Bijvoorbeeld door de werkzaamheden van techniekbedrijven als vitaal aan te merken.
  - b. hoe een goede balans tussen weerbaarheid en duurzaamheid gemaakt kan worden (bijvoorbeeld elektrificatie wagenpark).
4. Duidelijkheid geven over prioritering en coördinatie van schaarse middelen.

# 6. De rol van Techniek Nederland tijdens crises



**Tijdens een crisis is snelheid, duidelijkheid en samenwerking belangrijk. Techniek Nederland kan hierbij een coördinerende en verbindende rol spelen. Techniek Nederland is geen 24/7 crisisorganisatie, maar kan wél veel betekenen in voorbereiding, afstemming en herstel. Dit hoofdstuk beschrijft wat Techniek Nederland kan doen vooraf, tijdens en na een crisis, en welke overkoepelende taken daarbij horen.**

Techniek Nederland is het logische knooppunt voor de technieksector om samen te werken, kennis te delen en afspraken te maken. Zo kan de sector sneller en effectiever handelen wanneer het echt nodig is, zónder de bestaande crisisstructuur te hinderen.

## **6.1 Vooraf (koude fase): voorbereiden en versterken**

In de koude fase draait alles om weerbaarheid, afspraken en kennisdeling. Techniek Nederland helpt leden en vitale opdrachtgevers om klaar te zijn voor verschillende scenario's.

### **6.1.1 Duidelijkheid en kaders**

- **Vitaal / niet-vitaal:** Techniek Nederland werkt met overheid en vitale organisaties aan duidelijkheid vooraf. Bedrijven weten dan of zij onderdeel zijn van een vitale keten en welke verantwoordelijkheden daarbij horen.
- **Wet- en regelgeving:** Techniek Nederland informeert tijdig over aankomende wetten en regels, over plichten en rechten bij noodwetgeving, en signaleert knelpunten waar techniekoplossingen vastlopen. Dit helpt bedrijven zich aan te passen en stimuleert praktische oplossingen.
- **Competenties en belangen:** Techniek Nederland maakt richting overheid duidelijk hoe belangrijk de technieksector is en welke competenties de sector brengt.
- **Reservisten:** Techniek Nederland kan met Defensie samenwerken om een praktische handreiking voor de hele technieksector op te stellen.

### **6.1.2 Instrumenten en ondersteuning**

- **Crisishandboek:** Techniek Nederland stelt voorbeelden en templates beschikbaar voor bedrijfscontinuïteit, inclusief rollen, communicatie, IT/OT-veiligheid, alternatieve energie, prioritering van opdrachtgevers, en afspraken over toegang tot locaties.
- **Best practices:** Techniek Nederland deelt praktische tips over voorbereiding richting opdrachtgevers en medewerkers (bijvoorbeeld alternatieve energievoorziening, data-veiligheid, noodprocedures, analoge bedrijfsvoering).
- **Oefenen:** Techniek Nederland organiseert oefeningen (inclusief periodieke herhaling ten behoeve van borging) met vitale opdrachtgevers (bijvoorbeeld serious games) om ketensamenwerking te testen.
- **Crisiscafé's:** Techniek Nederland faciliteert crisiscafé's voor leden om ervaringen te delen, vragen te stellen en kennis te vergroten.
- **Crisisopleidingen voor leden.** Wij Techniek, het ontwikkelingsfonds voor de technische installatiebranche, kan hierbij ondersteunen.
- **Praktische handreikingen,** zoals richtlijnen noodcommunicatie (portofoons, papieren werkbonden).

### 6.1.3 Samenwerking en afspraken

- Taskforce Weerbaarheid: Techniek Nederland initieert een taskforce met sectorpartners (bijvoorbeeld bouw) en vitale partijen om samen scenario's en protocollen te ontwikkelen.
- Weerbaarheidsclausules (contractuele bepalingen die expliciet regelen hoe partijen handelen bij een crisis of verstoring, zodat continuïteit van vitale processen gewaarborgd blijft): Techniek Nederland helpt bij het opstellen van weerbaarheidsclausules voor vitale infrastructuur en stemt de inhoud af met leden. Te denken valt aan Bereikbaarheid en communicatie (welke alternatieve middelen worden gebruikt als internet of telefonie uitvalt); Prioritering van dienstverlening (welke opdrachtgevers of installaties krijgen voorrang bij schaarste); Toegang tot locaties (afspraken over fysieke toegang als digitale toegangscontrole niet werkt); Strategische voorraden (wie zorgt voor welke onderdelen en hoe verdeling bij schaarste plaatsvindt); Financiële afspraken (hoe betalingen en garanties geregeld zijn bij langdurige uitval van systemen); Compliance en veiligheid (eisen rond screening van personeel en beveiliging van systemen).
- Koppeling vraag-aanbod: Techniek Nederland brengt vraag en aanbod van kennis, mensen en middelen in kaart en verbindt bedrijven, overheid en andere branches.
- Competenties en screening: Techniek Nederland werkt mee aan afspraken over competenties, screening van medewerkers, systeembeveiliging, en (versnelling) certificering (bijvoorbeeld normen Baseline Informatiebeveiliging Overheid).
- Belangenbehartiging: lobby voor toegang tot brandstof en transportcorridors.
- Reservisten: Techniek Nederland maakt samen met Defensie een handreiking voor inzet reservisten.
- Duurzaamheidsdoel en weerbaarheid: Techniek Nederland overlegt met de overheid hoe ze duurzaamheid kunnen combineren met meer weerbaarheid en welke regels daarvoor nodig zijn.
- Verdeling schaarse middelen: Techniek Nederland denkt mee over verdeling van schaarse middelen (zoals diesel of personeel of coördinatie van inzet bij vitale sectoren) op basis van maatschappelijk belang.

## 6.2 Tijdens (warme fase): mobiliseren en afstemmen

In de acute fase ligt de primaire verantwoordelijkheid bij Rijksoverheid, veiligheidsregio's, LOCC/ KCR2 en vitale organisaties. Techniek Nederland is geen operationele crisisorganisatie, maar kan wel mobiliseren, coördineren en communiceren op generieke thema's.

### 6.2.1 Wat Techniek Nederland wél doet in de acute fase

- Centraal aanspreekpunt: Techniek Nederland fungeert als centraal punt voor leden en overheid op generieke vragen en bundelt signalen uit de sector.
- Sectoroverzicht: Techniek Nederland geeft overzicht van expertise en capaciteit (wie kan wat, waar, wanneer), zodat de juiste bedrijven snel gevonden worden.
- Mobiliseren: Techniek Nederland helpt bij het mobiliseren van bedrijven, installateurs en materieel en het samenbrengen van partijen, zonder de crisisstructuur te verstoren.

- **Crisiscommunicatie:** Techniek Nederland ondersteunt bij duidelijke sectorcommunicatie en uniforme boodschappen over bijvoorbeeld strategische voorraden, militaire transportcorridors, benodigde opschaling (bijvoorbeeld aanleg van noodopvang). Techniek Nederland kan een centrale informatiehub vormen via alternatieve kanalen, en deze kanalen mogelijk ook helpen opzetten.
- **Samenwerking met overheid:** afstemming met overheid over acute inzet sector.

### 6.2.2 Wat Techniek Nederland niet doet

- Techniek Nederland is niet de primaire lijn voor operationele aansturing tijdens de crisis. Die rol ligt bij de bestaande crisisstructuren.
- Techniek Nederland treedt niet onverwacht toe tot crissoverleg waar dat communicatie en besluitvorming zou verstoren.

## 6.3 Na de crisis (herstel en evaluatie)

In de herstelfase draait het om coördinatie, leren en verbeteren.

- **Herstelafspraken:** Techniek Nederland maakt samen met techniekbedrijven afspraken over herstel, prioritering en communicatie, zodat niet iedereen tegelijk aanklopt en ketens niet vastlopen.
- **Eén aanspreekpunt:** Techniek Nederland streeft naar een duidelijk contactpunt voor sectorbrede afstemming (realistisch: tijdens kantooruren).
- **Evaluatie en kennisdeling:** Techniek Nederland verzamelt ervaringslessen, organiseert workshops, en vertaalt inzichten naar best practices en standaarden.
- **Innovatie en weerbaarheid:** Techniek Nederland stimuleert innovaties die de sector weerbaarder maken (bijvoorbeeld AI-bewaking van kritische installaties, lokale energievoorzieningen bij netuitval, redundante pompvoorzieningen in hoogbouw).

## 6.4 Overkoepelende rollen van Techniek Nederland

- **Verbinder tussen sector en overheid**  
Techniek Nederland spreekt namens bedrijven met ministeries en vitale organisaties, deelt situatierapportages, en versterkt de positie van de sector door heldere signalen te geven.
- **Regisseur van kennis en afspraken**  
Techniek Nederland zorgt voor bewustwording, handreikingen, templates, en branchebrede protocollen. Techniek Nederland helpt bij standaardisatie en certificering, en bouwt een overzicht van expertises en capaciteiten.
- **Aanjager van publiek-private samenwerking**  
Techniek Nederland faciliteert samenwerking tussen bedrijven, overheid en andere branches (bijvoorbeeld via een Infra Capacity Alliance of taskforces), zodat gezamenlijke oplossingen rendabel en opschaalbaar worden.
- **Talent en opleiding**  
Techniek Nederland (samen met Wij Techniek) stimuleert leer-werkplekken en opleidingen (bijvoorbeeld in defensietechniek). Medewerkers kunnen na diensttijd doorstromen naar techniekbedrijven, wat de beschikbaarheid van vakmensen vergroot.
- **Ondersteuning bedrijven en medewerkers**  
Praktisch en psychosociaal.



# Verantwoording

Het onderzoek is uitgevoerd op basis van deskresearch, interviews en workshops, in nauwe samenwerking en afstemming met de begeleidingsgroep van Techniek Nederland en Wij Techniek.

Het onderzoek bestaat uit de volgende stappen:

1. Verkenning
2. Interviews
3. Consultatie achterban door middel van workshops
4. Opstellen rapportage

## Verkenning

Als eerste stap in dit onderzoek hebben we informatie verzameld. We hebben gekeken naar weerbaarheid, naar belangrijke wetten en regels, en naar recente gebeurtenissen in Europa die lijken op de scenario's in dit onderzoek. Samen met de begeleidingsgroep van Techniek Nederland en Wij Techniek hebben we bepaald:

- met welke opdrachtgevers en andere partijen we interviews zouden houden;
- welke techniekbedrijven en medewerkers zouden meedoen aan de workshops.

## Interviews

Er zijn twaalf partijen geïnterviewd, waaronder opdrachtgevers van techniekbedrijven, een gemeente, en een andere branchevereniging. De opdrachtgevers zijn actief in infra, industrie of utiliteit. De resultaten van deze interviews komen terug in hoofdstuk 3 van dit rapport.

De geïnterviewde partijen zijn:

1. Bravis Ziekenhuis
2. Bouwend Nederland
3. Stedin Group
4. Rijkswaterstaat
5. Vertegenwoordiger levensmiddelenindustrie <sup>14</sup>
6. ProRail
7. Vitens
8. Dunea
9. Sint Franciscus Ziekenhuis
10. Telecombedrijf <sup>15</sup>
11. Veiligheidsregio Utrecht
12. Rijksvastgoedbedrijf

De gestelde vragen aan de interviewpartijen zijn terug te vinden in bijlage 2.

<sup>14</sup> Geïnterviewde partij heeft aangegeven mee te willen werken aan het interview, maar zonder gebruik van de organisatiernaam.

<sup>15</sup> Zie voetnoot hierboven.

## Consultatie achterban Techniek Nederland

Er zijn drie workshops met leden en medewerkers van Techniek Nederland en Wij Techniek geweest, onder begeleiding van de experts van TNO. In die workshops zijn de drie scenario's besproken en de gevolgen en mogelijke maatregelen besproken en vastgelegd.

## Conceptrapportage

De resultaten van de verkenning, interviews en workshops hebben we in een conceptrapportage verwerkt. In hoofdstuk 4 staan kaders met lijsten van gevolgen voor techniekbedrijven per scenario. Deze lijsten laat alleen de gevolgen zien die workshopdeelnemers hebben genoemd. De kaders met maatregelen in hoofdstuk 4 bevatten maatregelen die de workshopdeelnemers hebben genoemd en die TNO op sommige punten heeft aangevuld. Hiervoor heeft TNO onder andere gekeken naar maatregelen die in het Landelijk Crisisplan Elektriciteit [25] en de Zweedse handreiking voor het bedrijfsleven [3] zijn beschreven, en naar analyses van de oorlog in Oekraïne [26] [27]. Daaruit blijkt welke kennis en vaardigheden personeel nodig heeft om belangrijke onderdelen van vitale infrastructuur tijdens een crisis te laten werken. Om te zien hoe weerbaar de sector nu is, hebben we in de workshops samen met leden van de technieksector gekeken welke maatregelen al worden gebruikt. Op één maatregel na zeiden de deelnemers dat zij nog geen maatregelen hebben genomen. Omdat maar een kleine groep bedrijven meedeed aan de workshops, geeft dit geen volledig beeld van de hele technieksector. Het is alleen een indicatie. Deze indicatie past wel bij de conclusie uit de Nederlandse Innovatie Monitor 2025 [24]. Daaruit blijkt dat veel bedrijven nog niet goed kunnen omgaan met uitval van belangrijke voorzieningen.

Bij het opstellen van delen van dit rapport is Microsoft Copilot gebruikt om teksten te herformuleren naar B1-taalniveau en een actieve schrijfstijl.

Techniek Nederland heeft de conceptrapportage voorgelegd aan de volgende commissies en gevraagd om de tekst te beoordelen en, indien nodig, aan te vullen met concrete suggesties: Ondernemerschap, Infra, Industrie, Innovatie, Groot, MKB, en P&O.

Na deze stap en verwerking van de input is de eindrapportage opgeleverd.

# Referenties

- [1] Ministerie van Justitie en Veiligheid, „Kamerbrief over weerbaarheid tegen militaire en hybride dreigingen,” Ministerie van Justitie en Veiligheid, 06 12 2024. [Online]. Available: <https://www.rijksoverheid.nl/documenten/kamerstukken/2024/12/06/tk-weerbaarheid-tegen-militaire-en-hybride-dreigingen>
- [2] VNO-NCW, MKB Nederland, „Handreiking Weerbaarheid ‘Ondernemen Is Vooruit Denken,’” 2026. [Online]. Available: [https://www.vno-ncw.nl/documenten/handreiking-weerbaarheid-ondernemen-is-vooruitdenken?gad\\_source=1&gad\\_campaignid=21174149653&gclid=CjwKCAiAncvMBh-BEEiwA9GU\\_fpVP9kEQFbYrgt1ejc4nOk5BxWAr\\_3dZOoeZ2Lvfet6djgFm-kwnLzhoCMYcQAvD\\_BwE](https://www.vno-ncw.nl/documenten/handreiking-weerbaarheid-ondernemen-is-vooruitdenken?gad_source=1&gad_campaignid=21174149653&gclid=CjwKCAiAncvMBh-BEEiwA9GU_fpVP9kEQFbYrgt1ejc4nOk5BxWAr_3dZOoeZ2Lvfet6djgFm-kwnLzhoCMYcQAvD_BwE)
- [3] Swedisch Civil Defence and Resilience Agency, „In case of crisis or war. Preparedness for businesses,” 01 2026. [Online]. Available: <https://rib.msb.se/filer/pdf/31178.pdf>
- [4] Techniek Nederland, Uitvoeriger antwoorden op de vragenlijst VNO-NCW en MKB Nederland, Techniek Nederland, 28-03-2025.
- [5] F. Nederveen, S. Hoorens, E. Frinking en H. van Soest, „Weerbaarheid becijferd,” RAND Europe, 01 02 2024. [Online]. Available: [https://www.rand.org/pubs/research\\_reports/RRA2357-1.html](https://www.rand.org/pubs/research_reports/RRA2357-1.html)
- [6] I. Linkov, „Resilience-based Strategies and Policies to Address Systemic Risks,” Organisation for Economic Co-operation and Development (OECD), 17-18 09 2019. [Online]. Available: [https://one.oecd.org/document/SG/NAEC\(2019\)5/en/pdf](https://one.oecd.org/document/SG/NAEC(2019)5/en/pdf)
- [7] I. Linkov, „Changing the resilience paradigm,” Nature Climate Change, 04 06 2014. [Online]. Available: [https://www.pik-potsdam.de/~anders/publications/linkov\\_bridges14.pdf](https://www.pik-potsdam.de/~anders/publications/linkov_bridges14.pdf)
- [8] Ministerie van Justitie en Veiligheid, „Weerbaarheidsopgave,” Rijksoverheid, 12 2024. [Online]. Available: <https://www.nctv.nl/site/binaries/site-content/collections/documents/2024/12/06/weerbaarheidsopgave/TK+Bijlage+2+weerbaarheidsopgave.pdf>
- [9] Ministerie van Justitie en Veiligheid, „Vitale infrastructuur,” Nationaal Coördinator Terrorismebestrijding en Veiligheid, [Online]. Available: <https://www.nctv.nl/onderwerpen/v/vitale-infrastructuur>
- [10] Ministerie van Justitie en Veiligheid, „Aanpak vitaal,” Nationaal Coördinator Terrorismebestrijding en Veiligheid, [Online]. Available: <https://www.nctv.nl/onderwerpen/v/vitale-infrastructuur/aanpak-vitaal>
- [11] Ministerie van Justitie en Veiligheid, „NIS2- en CER-richtlijnen,” Nationaal Coördinator Terrorismebestrijding en Veiligheid, [Online]. Available: <https://www.nctv.nl/onderwerpen/c/cer--en-nis2-richtlijnen>
- [12] Ministerie van Justitie en Veiligheid, „Wet weerbaarheid kritieke entiteiten,” Nationaal Coördinator Terrorismebestrijding en Veiligheid, [Online]. Available: <https://www.nctv.nl/onderwerpen/w/wet-weerbaarheid-kritieke-entiteiten>
- [13] P. Damen, „Wet weerbaarheid kritieke entiteiten,” WWKE implementatie., [Online]. Available: <https://wwke-implementatie.nl/wat-is-de-wwke>
- [14] Rijksinspectie Digitale Infrastructuur, „Cyberbeveiligingswet,” Ministerie van Economische Zaken, [Online]. Available: <https://www.rdi.nl/onderwerpen/cyberveiligheid/cyberbeveiligingswet>
- [15] Nationaal Cyber Security Centrum, „Meldplicht,” [Online]. Available: <https://www.ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor/meldplicht>



- [16] Digitale Overheid, „Veelgestelde vragen Cyberbeveiligingswet,” Rijksoverheid, [Online]. Available: <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/cyberbeveiligingswet/#v7>
- [17] K. Jaiswal, „Complete Case Study On The AWS and Azure Outages Of October 2025,” Opstree, 4 November 2025. [Online]. Available: <https://opstree.com/blog/2025/11/04/aws-and-azure-outages/>
- [18] S. B. Thiel, „AWS Went Down — and Took the Internet With It,” Built In, 22 Oktober 2025. [Online]. Available: <https://builtin.com/articles/aws-outage-what-happened>
- [19] J. Taylor, „Amazon reveals cause of AWS outage that took everything from banks to smart beds offline,” The Guardian, 24 Oktober 2025. [Online]. Available: <https://www.theguardian.com/technology/2025/oct/24/amazon-reveals-cause-of-aws-outage>
- [20] Y. Spinner, „Amazon: bug geautomatiseerd DNS-database zorgde voor kettingreactie AWS-storing,” Tweakers, 24 Oktober 2025. [Online]. Available: <https://tweakers.net/nieuws/240718/amazon-bug-geautomatiseerd-dns-database-zorgde-voor-kettingreactie-aws-storing.html>
- [21] NIPV, „Grootschalige stroomuitval: ervaringen uit Spanje en Portugal 2025,” 5 11 2025. [Online]. Available: <https://nipv.nl/wp-content/uploads/2025/11/20251104-NIPV-VRK-Grootschalige-stroomuitval-ervaringen-uit-Spanje-en-Portugal-2025.pdf>
- [22] Tagesschau, „Stromversorgung in Berlin läuft laut Betreiber an,” [Online]. Available: <https://www.tagesschau.de/inland/berlin-stromversorgung-100.html>
- [23] H. Verbeem, „Grote stroomstoring treft Roosendaal en Nispen,” Zuidwest TV, 2 November 2025. [Online]. Available: <https://www.zuidwestupdate.nl/nieuws/grote-stroomstoring-treft-roosendaal-en-nispen/>
- [24] Henk Volberda & Rick Hollen (Amsterdam Centre for Business Innovation), Gerben de Jong & Stef Konijn (SEO Economisch Onderzoek), „Nederlandse Innovatie Monitor 2025,” 11 2025. [Online]. Available: <https://www.seo.nl/wp-content/uploads/2025/11/2025-178-Nederlandse-Innovatie-Monitor-2025.pdf>
- [25] Ministerie van Economische Zaken en Klimaat, „Nationaal Crisisplan Elektriciteit,” 16 03 2022. [Online]. Available: <https://www.nctv.nl/documenten/2022/03/15/nationaal-crisisplan-elektriciteit-2021>
- [26] Simon Aebi, Andrin Hauri, Jurgena Kamberaj, „Risk and Resilience Report. Critical Infrastructure Resilience in Ukraine: Energy, Transportation, and Communication,” 03 2024. [Online]. Available: <https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-security-studies/pdfs/RR-Report-2024-Critical-Infrastructure-Resilience.pdf>
- [27] Neil Walker, „Building Ukraine’s Shield: The bold new effort to train critical infrastructure security professionals,” 19 09 2025. [Online]. Available: <https://www.cip-association.org/building-ukraines-shield-the-bold-new-effort-to-train-critical-infrastructure-security-professionals/>
- [28] Techniek Nederland, „Overkoepelend thema: toekomstbehendigheid,” 2025. [Online]. Available: <https://www.startmetconnect.nl/connect2030/overkoepelend-thema-toekomstbehendigheid>
- [29] Deloitte, „Een veilig en weerbaar Nederland: tijd voor concrete stappen,” Deloitte, 20 11 2024. [Online]. Available: <https://www.deloitte.com/nl/nl/Industries/defense-security-justice/perspectives/een-veilig-en-weerbaar-nederland-hoogste-tijd-voor-concrete-stappen.html>
- [30] Ministerie van Economische Zaken en Klimaat, „Landelijk Crisisplan Olie,” 03 02 2023. [Online]. Available: <https://www.rijksoverheid.nl/documenten/rapporten/2023/02/03/bijlage-landelijk-crisisplan-olie>



# Bijlage 1

## Verdere toelichting

### Artikel 5 scenario

Bij dit scenario is als uitgangspositie gekozen dat er reeds enige tijd een staakt-het-vuren is in Oekraïne. Nadat er in Oekraïne een staakt-het-vuren is bereikt gaat de militaire opbouw van Rusland door. Doordat er niet meer gevochten wordt in Oekraïne is Rusland in staat haar militair arsenaal op te bouwen en haar gevechtservaring om te zetten in een sterk leger met goed getrainde capabele militaire eenheden. Rusland blijft een bedreiging voor Europa, en met name de Oost-Europese buurlanden voelen die dreiging dagelijks.

De NAVO bevindt zich in fase 0, er is geen oorlog, maar ook geen vrede. Rusland blijft actief met hybride activiteiten onder de grens van een openlijk conflict. Met onder meer desinformatiecampagnes, cyberaanvallen, politieke beïnvloeding en sabotageacties probeert Rusland het bondgenootschap te verzwakken en uit elkaar te spelen. NAVO-lidstaten blijven investeren in Defensie, maar niet in alle Europese hoofdsteden wordt de noodzaak even zwaar gevoeld. In Nederland gaat de versterking van de krijgsmacht door. Nederlandse troepen zijn in deze fase permanent aanwezig in Oost-Europa voor bescherming en afschrikking tegen Russische agressie. Op enig moment voert Rusland echter toch een gerichte aanval uit op een van de NAVO-lidstaten. Grenstroepen raken in gevecht en er vallen vele doden en gewonden.

Er breekt nu een nieuwe fase aan: NAVO activeert Artikel 5. Nederlandse troepen worden onder NAVO-commando gesteld en versterkingen worden in verschillende fases naar het oosten gestuurd. NAVO-troepen bevinden zich over het algemeen op verschillende niveaus van gereedheid. Er zijn eenheden die binnen tien dagen gereed moeten zijn voor inzet, andere eenheden moeten binnen dertig dagen, of 180 dagen gereed zijn. Nederland maakt alle aan NAVO toegezegde eenheden gereed voor inzet en verplaatst de eenheden naar de door NAVO aangewezen inzetgebieden in Noordoost Europa. Tegelijkertijd loopt er in Nederland een grootschalige doorvoeroperatie via havens en logistieke corridors richting Oost-Europa. De beveiliging van vitale objecten in eigen land wordt opgevoerd. In deze fase nemen cyberaanvallen op vitale processen verder toe, worden er sabotageacties op vitale infrastructuur (op land en zee) uitgevoerd en proberen desinformatiecampagnes de steun van de bevolking te ondermijnen. Allemaal activiteiten die tegenwoordig al in Europa gebeuren, maar die in een Artikel 5 scenario duidelijk in intensiteit zullen toenemen.

Hopelijk is deze eerste reactie voldoende om de Russische eenheden terug te dwingen naar hun eigen grondgebied. Anders zal het conflict zich verder verheven. De logistieke doorvoeroperaties voor militaire versterkingen worden dan steeds crucialer, maar ook steeds vaker verstoord door steeds agressievere vijandelijke acties. Periodieke uitval van vitale infrastructuur,

gewelddadige sabotage en druk op mondiale aanvoerroutes zorgen voor een instabiele situatie. Vluchtelingenstromen en gewonden uit Oost-Europa bereiken Nederland en moeten hier worden opgevangen en verzorgd.

Uiteindelijk stapelen de crises zich op: de economie, arbeidsmarkt en samenleving raken langdurig en breed verstoord, de capaciteit van vitale infrastructuur degradeert door aanhoudende aanvallen, en het zorgsysteem staat continu onder druk. In deze fase kunnen extra crises zoals een natuurramp de situatie verder verergeren terwijl de militaire bijstandscapaciteit beperkt is. Een deel van de bevolking keert zich tegen de deelname aan het conflict en vormt daardoor een extra uitdaging voor de samenhang van de maatschappij.

De directe impact op de maatschappij is veelzijdig, ingrijpend en langdurig. Op militair vlak worden troepen en materieel in gereedheid gebracht en reservisten geactiveerd. Militaire objecten en kritieke infrastructuur worden extra beschermd en de militaire doorvoeroperaties beperken het reguliere verkeer, vooral op belangrijke transportcorridors. Voor de bevolking betekent het scenario een toename van desinformatiecampagnes, extremisme en polarisatie, wat het vertrouwen in elkaar en de overheid ondermijnt. De samenleving wordt beïnvloed door digitale en fysieke aanvallen, zoals brandstichting, drone-aanvallen of aanslagen, wat leidt tot angst en onzekerheid. Vitale processen, zoals elektriciteit, telecom en dataverbindingen en transportsystemen, worden bedreigd door cyberaanvallen en sabotageacties waardoor burgers en bedrijven (tijdelijk) zonder nutsvoorziening komen te zitten. Ook de economie wordt geraakt: internationale handelsketens raken verstoord door blokkades, aanvallen en sancties en het wordt lastig voor organisaties en bedrijven om cruciale voorraden aan te vullen. De overheid moet productiebehoeften en prioriteiten bijstellen, zoals bijvoorbeeld de verdeling van diesel voor noodaggregaten. Criminaliteit en het zwarte circuit nemen toe en worden soms ook door de tegenstander ingezet als middel om de maatschappij verder te ondermijnen. Ten slotte wordt Nederland geconfronteerd met de opvang van grote groepen buitenlandse vluchtelingen en gewonden, wat een enorme druk legt op zorgvoorzieningen. Lokale ontruiming kunnen noodzakelijk zijn bij incidenten zoals chemische ongevallen, uitval van voorzieningen of ernstige milieuschade.

# Bijlage 2

## Gestelde vragen interviewpartijen

Wij willen een beeld krijgen van de verwachtingen die uw organisatie heeft ten aanzien van de technieksector, in het geval uw organisatie geraakt wordt door een van deze drie crisisscenario's:

1. Uitval internet en telefonie door sabotage statelijke actor (72 uur);
2. Uitval elektriciteit door sabotage statelijke actor (72 uur);
3. Artikel 5 situatie / strategische bijstand.

In geval van (één van) deze crisisscenario's maakt uw organisatie mogelijk gebruik van de dienstverlening die bedrijven in de technieksector aanbieden. Denk hierbij o.a. aan het onderhouden, repareren en veilig houden van technische installaties.

Door beter te begrijpen welke verwachtingen en behoeften uw organisatie heeft kunnen bedrijven in de technieksector zich beter hierop voorbereiden, zodat ze uiteindelijk kunnen helpen de impact van de crisisscenario's te verzachten.

### Interviewvragen:

1. Naam, organisatie, functie
2. Wat gaat er bij jullie mis wanneer deze scenario's gaan spelen?
  - a. Heeft uw zelf al inzicht in de omvang van de impact van deze scenario's op uw organisatie?
  - b. Welke keteneffecten ziet u ontstaan bij elk van de drie scenario's?
    - i. Uitval internet en telefonie door sabotage statelijke actor (72 uur);
    - ii. Uitval elektriciteit door sabotage statelijke actor (72 uur);
    - iii. Artikel 5 situatie / strategische bijstand.
3. In hoeverre is uw organisatie afhankelijk van de dienstverlening van bedrijven uit de technieksector om de impact van deze scenario's te verminderen/ te verhelpen?
4. Heeft u in dat geval bepaalde verwachtingen van, of eisen aan deze bedrijven?  
Denk bijvoorbeeld aan:
  - a. Bereikbaarheid
  - b. Inzetsnelheid
  - c. Wat voor type hulp (kortdurend - monteur die langskomt om iets te repareren; langdurend - monteur voor langere tijd ter plaatse handmatig taken laten uitvoeren om installatie in noodstand te laten draaien)
  - d. Individuele competenties van personeel (van een techniekbedrijf)

5. Heeft u deze verwachtingen/ eisen vastgelegd in bijvoorbeeld contracten?
  - a. Zijn hier generieke contractbeschrijvingen voor beschikbaar waarin die eisen zijn vermeld?
    - i. Indien er generieke contracten zijn, zijn de eisen daarin voldoende doorgedacht voor de 3 scenario's die we beschouwen?
  - b. Zo nee, overweegt u hierover afspraken te maken?
6. De technieksector heeft ook een brancheorganisatie: Techniek Nederland.
  - a. Bent u hier mee bekend?
  - b. Welke rol kan de brancheorganisatie tijdens crisis nemen (die voor uw organisatie relevant is)?
7. Welke tips heeft u voor de technieksector die zij nu kunnen nemen om tijdens crisis aan uw verwachtingen te kunnen voldoen?

## Colofon

### Opdrachtgever

Dit onderzoek is uitgevoerd in opdracht van Techniek Nederland door TNO. Het onderzoek is mede mogelijk gemaakt door Wij Techniek.

### Fotografie

cover: GettyImages/Jasper Bussemaker

pagina 8: Ed Buying

pagina 12: GettyImages/Doctor\_bass

pagina 22: Ed Buying

pagina 26: GettyImages/posteriori

pagina 50: GettyImages/hxdyl

### © Techniek Nederland, februari 2026

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, film, elektronisch, op geluidsband of op welke andere wijze ook en evenmin in een retrieval systeem worden opgeslagen zonder voorafgaande schriftelijke toestemming van Techniek Nederland. De inhoud van deze publicatie is met de grootst mogelijke zorgvuldigheid samengesteld. Toch kan het risico van onduidelijkheden of onjuistheden niet geheel worden vermeden. Techniek Nederland sluit iedere aansprakelijkheid uit voor zowel de schade die mocht voortvloeien uit het gebruik van deze gegevens, als schade die zou kunnen ontstaan als gevolg van onvolledigheden, onjuistheden of onvolkomenheden in deze publicatie.

