OFL-Rapport

VERSNELLINGSNETWERK WEERBAARHEID FYSIEKE LEEFOMGEVING

Thema's Drones en PNT

Aangeboden aan de minister van Infrastructuur en Waterstaat

Met afschrift aan:

de minister van Defensie

de minister van Economische Zaken en Klimaat

de minister van Justitie en Veiligheid

Overlegorgaan Fysieke Leefomgeving · Juni 2026

Status: Definitief, maar nog vertrouwelijk tot 25 juni (NB: opmaak wordt nog gewijzigd)

Inhoudsopgave

Voorwoord

1. Inleiding en aanleiding
   - *1.1 Een veranderde wereld vraagt een andere aanpak*
   - *1.2 Twee kwetsbaarheden, één aanpak*
   - *1.3 Waarom dit netwerk, waarom nu*
   - *1.4 Wat dit document is en wat niet*

Weerbaarheid: Een generiek kader

Thema I: Drones

2. Analyse: hoe het netwerk naar het drone-vraagstuk kijkt
   - *2.1 Waarom dit vraagstuk anders is*
   - *2.2 Drie typen vitale infrastructuur*
   - *2.3 Eerste reflectie: wat het netwerk heeft opgehaald*

3. Opbrengst
   - *3.1 De matrix als denkkader*
   - *3.2 Dilemma's*
   - *3.3 Doorbraakadviezen*
   - *3.4 Actievoorstellen: wat nu al kan*
   - *3.5 Best practices: leren van wat werkt*

Thema II: Plaats-, navigatie en tijdsbepaling (PNT)

4. Analyse: hoe het netwerk naar het PNT-vraagstuk kijkt
   - *4.1 De kern: een onzichtbare fundering waarop bijna alles leunt*
   - *4.2 Wat dit vraagstuk wezenlijk anders maakt*
   - *4.3 Drie functies, één onderlaag: plaats, navigatie en tijd*
   - *4.4 Wat het netwerk heeft opgehaald: zeven patronen*

5. Opbrengst
   - *5.1 De aard van de opbrengst*
   - *5.2 Dilemma's: waar keuzes onvermijdelijk zijn*
   - *5.3 Doorbraakadviezen*
   - *5.4 Actievoorstellen: wat nu al kan*
   - *5.5 Best practices: leren van wat werkt*

6. Advies: hoe nu verder

Woord vooraf

Het Overlegorgaan Fysieke Leefomgeving (OFL) brengt al meer dan dertig jaar publieke en private partijen bij elkaar rond de grote opgaven in onze fysieke leefomgeving. Op verzoek van de minister en staatssecretaris van Infrastructuur en Waterstaat (IenW) hebben wij het afgelopen half jaar een Versnellingsnetwerk ingericht rond een vraagstuk dat niet langer kan wachten: het meer weerbaar maken van de infrastructuur van Nederland tegen hybride en militaire dreigingen. Gezien het open concept van 'kritieke entiteiten' in de Wwke (entiteiten kunnen door ministers worden aangewezen als kritiek) en de plicht die ministers in deze wet krijgen om een strategie vast te stellen om de weerbaarheid van kritieke entiteiten te verbeteren (artikel 13 van de Wwke), heeft het OFL ervoor gekozen het veld te verkennen en aanbevelingen te doen voor verbetering van de weerbaarheid.

Het Versnellingsnetwerk richt zich in principe op de meest belangrijke infrastructuur in Nederland. Hoewel we afwisselend schrijven over "vitaal" en "kritiek" bedoelen wij dat niet in de juridische zin, maar duiden wij de positie aan van die infrastructuur die direct impact heeft op het (door)draaien van de Nederlandse maatschappij en economie.

Samen met de deelnemers is ervoor gekozen om de huidige, hybride situatie als uitgangspunt te kiezen voor de sessies van het Versnellingsnetwerk. Hoewel het "inroepen van artikel 5" zeker aan de orde is gekomen, constateerde de deelnemers dat juist de huidige hybride-situatie de nodige uitdagingen kent en dat hierop de eerste focus moest liggen. Dit laat uiteraard onverlet dat de mogelijke consequenties van een daadwerkelijk artikel 5-scenario ook op tafel ligt en de impact daarvan voor organisaties die de vitale infrastructuur van Nederland dragen doordacht dient te worden. Het opzetten van een actierepertoire om weerbaarheid te versterken in de hybride situatie heeft bovendien het voordeel dat het ingeval van een 'artikel 5' situatie sowieso een 'no regret'-optie is.

Het vraagstuk is groot. Om het hanteerbaar te maken, heeft het netwerk zich in dit halfjaar gericht op twee concrete en urgente kwetsbaarheden: de dreiging van drones voor vitale objecten en netwerken en de afhankelijkheid van vitale processen van satellietsystemen voor plaats-, navigatie en tijdsbepaling (PNT). Twee verschillende thema's, maar met dezelfde onderliggende logica: kwetsbaarheden die reëel zijn, die snel groter worden, en die vragen om samenwerking tussen publieke en private partijen die nu nog onvoldoende van de grond komt.

Met drie werksessies per thema hebben vertegenwoordigers van meer dan 50 organisaties uit de energie-, haven-, luchtvaart-, spoor-, drinkwater-, chemie-, telecom- en veiligheidssector gezamenlijk deze vraagstukken doordacht. Niet om compleet te zijn, maar om vanuit een gedeelde analyse de dilemma's te duiden en handelingsopties in beeld te brengen: herkend en gedragen door de mensen die er dagelijks mee te maken hebben.

Het doel van deze exercitie was van meet af aan helder: netwerkvorming, agendering, een gezamenlijke taal ontwikkelen en bestaande kennis en ervaring uit het veld ophalen, om dit vraagstuk in positie te brengen voor verdere versnelling. Dat is wat hier ligt.

Wat dit netwerk heeft opgeleverd, is meer dan een rapport. Er is kennis gedeeld die voorheen versnipperd was. Er zijn stappen geïdentificeerd die partijen nu al (kunnen) zetten, binnen bestaande kaders en zonder te wachten op nieuw beleid. En er zijn dilemma's en fundamentele vragen benoemd

“

die het landschap voor de komende jaren moeten vormen: vragen die niet ambtelijk opgelost kunnen worden, maar die politieke keuzes vereisen. En bovenal: er is een scherper bewustzijn van weerbaarheid als netwerkvraagstuk, voorbij de eigen ‘business continuity’ van de afzonderlijke ‘schakels’.

Daarmee bied ik u twee dingen aan: een aanbod en een advies. Een aanbod van het netwerk om zelf stappen te zetten en de samenwerking die hier tot stand is gekomen voort te zetten. En een advies aan u als bewindspersonen over wat aanvullend nodig is in beleid, in regelgeving, in bevoegdheden en in structuur, om de weerbaarheid van onze vitale infrastructuur daadwerkelijk te versterken.

Tot slot. Dit document gaat over inhoud, maar de werkwijze die eraan ten grondslag ligt verdient ook aandacht. Door het relevante netwerk bij elkaar te brengen, samen het vraagstuk te doordenken en in een beperkt aantal gerichte sessies tot een gedragen eerste opbrengst te komen, hebben we een aanpak gevonden die snel resultaat oplevert zonder de diepgang te verliezen. Ik hoop dat deze methode, werken met de partijen die het betreft, vanuit gezamenlijkheid en met gerichte tijdsinvesteringen, navolging krijgt. In een tijd waarin geopolitieke ontwikkelingen snel gaan en de druk op vitale sectoren toeneemt, is dit precies de manier waarop de rijksoverheid en het Versnellingsnetwerk samen versnelling kunnen aanbrengen op de thema's die er het meest toe doen. Een dergelijk netwerk is complementair aan wat de (rijks)overheid zelf al doet en bedenkt vanuit de eigen verantwoordelijkheid voor weerbaarheid. ‘Van binnen naar buiten’ werken kan met het netwerk worden aangevuld met ‘van buiten naar binnen’ werken. Voor weerbaarheid zijn beide nodig.

Het is nu aan het netwerk én aan u om hierop verder te gaan.

Christophe van der Maat

Voorzitter Versnellingsnetwerk Weerbaarheid Fysieke Leefomgeving

Overlegorgaan Fysieke Leefomgeving

1. Inleiding en aanleiding

1.1 Een veranderde wereld vraagt een andere aanpak

De wereldorde is in korte tijd veranderd en de veranderingen raken direct de veiligheid van de fysieke leefomgeving in Nederland. Statelijke en niet-statelijke actoren zetten steeds vaker middelen in die zich bevinden in het grijze gebied tussen vrede en oorlog: desinformatie, cyberaanvallen, economische druk en fysieke sabotage. Het heldere onderscheid tussen binnenlandse en buitenlandse dreigingen, tussen militaire en civiele doelen, tussen vrede en conflict is vervaagd. Digitalisering heeft die vervaging versterkt en tegelijk nieuwe kwetsbaarheden gecreëerd. Wie software beheerst, beheerst steeds vaker ook het fysieke systeem dat erop draait.

De dreigingen zijn niet nieuw van aard, maar wel nieuw van schaal, nabijheid en intensiteit. Het AIVD-jaarrapport en het WRR-onderzoek over Nederland in een fragmenterende wereldorde (2024) schetsen eenzelfde beeld: de kans op een serieus incident met ontwrichtende impact is reëel. Sabotage van kabels en buisleidingen, verkenningsvluchten boven kritieke infrastructuur in Scandinavië, de stroomstoring in Spanje en Portugal van april 2025 die de verwevenheid van (digitale) ketens pijnlijk zichtbaar maakte: het zijn geen verre waarschuwingen meer. De MIVD rapporteerde in 2024 concrete pogingen tot sabotage van Nederlandse vitale infrastructuur.

Nederland heeft zijn vitale infrastructuur decennialang opgebouwd in een context van relatieve veiligheid en geopolitieke stabiliteit. Die stabiele omgeving maakte optimalisatie op efficiëntie mogelijk: systemen werden ingericht op just-in-time logica, processen werden ‘lean’, geoptimaliseerd en sterk verweven. Dat leverde veel op, maar het is ook een vredesdividend dat zijn keerzijde laat zien nu de context fundamenteel is veranderd. Energie, water, havens, luchtvaart, spoor, telecom, financiën en chemie zijn kwetsbaar op manieren die niet zo lang geleden nog theoretisch leken. Die kwetsbaarheid neemt toe naarmate systemen verder digitaliseren en meer afhankelijk worden van technologieën buiten onze directe invloedsfeer.

Het vraagstuk past in het bredere landschap van moedwillige dreigingen waarvoor Nederland kaders heeft ontwikkeld op het gebied van alertering, crisisbeheersing en nationale veiligheid. De Wet weerbaarheid kritieke entiteiten (Wwke) verplicht kritieke entiteiten om sabotage- en terrorismescenario's structureel te verankeren in hun risicobeheer en bedrijfscontinuïteit. Het versnellingsnetwerk biedt de infrastructuur om dergelijke scenario’s in de context van publiek-private samenwerking te verkennen.

1.2 Twee kwetsbaarheden, één aanpak

Het OFL concludeerde eerder in de impactanalyse spoor “*Tijd om te handelen*”, op verzoek van staatssecretaris Aartsen, dat afwachten geen optie is. Die conclusie geldt breder. Daarom heeft het ministerie van IenW het Versnellingsnetwerk gevraagd om komend jaar enkele thema's verder uit te diepen. In overleg met de vitale sectoren is de keuze gemaakt om als eerst twee concrete en urgente kwetsbaarheden op te pakken: drones en PNT. Daar gaat het voorliggende aanbod en advies over.

De eerste kwetsbaarheid is de dreiging van ongewenste drones: ongeautoriseerde vluchten die een bedreiging kunnen vormen voor belangrijke infrastructuur. Drones zijn vaak goedkoop, wendbaar, moeilijk te traceren en in hoog tempo geavanceerder geworden. Tegelijkertijd brengen ze veel goeds: ze worden in toenemende mate ingezet voor inspectie, monitoring, logistiek en tal van andere maatschappelijke en economische toepassingen. Nederland beweegt naar een samenleving waarin drones een vanzelfsprekend onderdeel zijn van het dagelijks verkeer. Juist die groei maakt

voorspelbaarheid, heldere regelgeving en robuuste kaders des te noodzakelijker. De combinatie van lage drempel, hoge potentiële impact en razendsnelle technologische ontwikkeling maakt drones tot een vraagstuk dat vanuit beide perspectieven moet worden bekeken: als kans én als risico. De weerbaarheid van onze vitale systemen is op dit moment voor geen van beide voldoende ingericht.

De tweede kwetsbaarheid is de afhankelijkheid van plaats-, navigatie- en tijdsbepaling via satelliet, kortweg PNT. Systemen als GPS en Galileo vormen een essentiële, maar veelal onzichtbare laag onder vrijwel alle vitale processen: de continuïteit van de energievoorziening, financiële transacties, scheepvaart, luchtvaart, spoor, telecom en waterbeheer zijn er stuk voor stuk van afhankelijk. Die afhankelijkheid groeit verder door digitalisering en is in veel gevallen nog niet voorzien van adequate back-up of noodprocedures. Sterker nog, door de vanzelfsprekende beschikbaarheid van PNT in Nederland kan het bewustzijn eroderen van de afhankelijkheid ervan. Verstoring of manipulatie van PNT, door ruimteweer, technisch falen of een statelijke actor, kan cascade-effecten veroorzaken dwars door meerdere vitale sectoren heen.

Beide thema's zijn anders van karakter: drones zijn zichtbaar en fysiek, PNT-uitval is onzichtbaar en systemisch. Maar ze delen dezelfde urgentie. Het gaat erom dat wij niet de planning bepalen van actoren die moedwillig onze bedrijfsvoering en/of samenleving (ernstig) willen verstoren. De kwetsbaarheid is reëel, het bewustzijn blijft achter en de benodigde samenwerking tussen overheid, vitale sectoren en bedrijven komt nog onvoldoende van de grond.

1.3 Waarom dit netwerk, waarom nu

Op verzoek van de minister en staatssecretaris van IenW heeft het OFL het Versnellingsnetwerk Weerbaarheid Fysieke Leefomgeving ingericht. Het OFL, onafhankelijk, onpartijdig en met meer dan dertig jaar ervaring in het organiseren van samenwerking tussen overheid, bedrijfsleven en maatschappelijke organisaties, is gevraagd dit vraagstuk op te pakken met een breed netwerk van vitale sectoren.

De inrichting van dit Versnellingsnetwerk volgde op een verkenning waarin tientallen gesprekken zijn gevoerd, zowel binnen IenW als met C-level van private partijen, over nut en noodzaak van een Versnellingsnetwerk, de afbakening en de voorwaarden, zoals scherpe afbakening van de thema’s, commitment vanuit IenW en private partijen en betrokkenheid van in ieder geval de bewindspersoon van IenW.

Tijdens de verkenning is een duidelijke behoefte geuit aan een actie gedreven netwerk dat gericht werkt aan een beperkt aantal weerbaarheidsvraagstukken. Partijen willen van praten naar doen via een werkwijze waar de betrokken partijen richting geven, keuzes maken en daadwerkelijk tot resultaten komen. Concreet had men behoefte aan handelingsperspectief en doorzettingsmacht. Voor dat laatste is per thema een stevige kopgroep ingericht, ingevuld door de betrokken directeur-generaal van IenW en een bestuurder uit het netwerk. Deze kopgroep heeft het proces bewaakt, de inhoudelijke lijn aangestuurd en gezorgd dat men daadwerkelijk aan de slag kan met de opbrengst.

Voor beide thema's zijn vertegenwoordigers van tientallen organisaties bijeengekomen: energiebedrijven, havens, luchthavens, spoorwegbedrijven, waterschappen, drinkwaterbedrijven, chemische industrie, telecombedrijven, defensie, justitie en kennisinstellingen. Dit traject is uitgevoerd in overleg met de interdepartementale werkgroep versnelde aanpak tegen ongewenste drones (ook wel taskforce genoemd) en het programmateam Maatschappelijke Weerbaarheid tegen Militaire Dreigingen (MWMD) van IenW. Hiermee sluit het advies en aanbod zoveel mogelijk aan op bestaande initiatieven en structuren.

1.4 Wat dit document is en wat niet

Dit rapport is de eerste opbrengst van het Versnellingsnetwerk. Het is geen uitputtende inventarisatie, maar een stevige basis om samen met de overheid verdere stappen te zetten in het weerbaar maken van de vitale infrastructuur. Het is tegelijkertijd een aanbod en een advies: een aanbod, omdat het netwerk bereid is zelf stappen te zetten, een advies, omdat een deel van wat nodig is buiten het bereik van individuele organisaties ligt en politieke keuzes vereist.

Het netwerk is bewust samengesteld uit organisaties die verantwoordelijk zijn voor vitale infrastructuur. Deze organisaties denken al lang na over bedrijfscontinuïteit bij verstoringen en hebben doorgaans (op basis van de ervaring en verplichtingen uit wet- en regelgeving) veel maatregelen getroffen om de continuïteit te borgen. Op organisatieniveau is de basis voor weerbaarheid veelal aanwezig. Wat ontbreekt, is het collectieve beeld en een gerichte sturing op de onderlinge afhankelijkheden. Partijen realiseren zich niet altijd welke afhankelijkheden zij hebben van anderen of gaan ervan uit dat een verstoring buiten de eigen organisatie ook buiten hun verantwoordelijkheid valt. Het netwerk doorbreekt die aanname. Het vergroot het bewustzijn van gedeelde kwetsbaarheden én vergroot de opties van maatregelen die individuele organisaties alleen niet overwegen of kunnen realiseren, maar vanuit het geheel wél te overwegen zijn. Dat zien we zowel bij de verdieping op drones als PNT terug.

Uit de verdieping op drones en PNT is een aantal gemeenschappelijke noties over weerbaarheid te destilleren. Deze treft u aan in het generiek kader over weerbaarheid. De hoofdstukken die volgen werken de twee thema's afzonderlijk uit: eerst drones, dan PNT. Elk thema kent dezelfde opbouw: analyse, dilemma’s, doorbraken en actiepunten, toegesneden op de eigen aard en dynamiek van het vraagstuk. We sluiten dit rapport af met het perspectief over de wijze waarop het Versnellingsnetwerk verdergaat.

Weerbaarheid: Een generiek kader

Weerbaarheid staat voor het bestand zijn tegen een dreiging. Over weerbaarheid en strategieën om weerbaarheid te versterken wordt in verschillende disciplines al jaren nagedacht (de 'safety sciences', de organisatiewetenschappen, de bestuurswetenschappen en de '(software-)engineering' bijvoorbeeld). De opbrengst uit bestaand onderzoek kan worden gebruikt om een generiek kader op te spannen voor concrete maatregelen. Ten minste drie lessen zijn uit de bestaande literatuur te destilleren:

1. Weerbaarheid gaat niet alleen om het bouwen van een robuuste 'vesting' om de te beschermen belangen (infrastructuur, maar binnen het ICT-domein moet om cruciale informatie een 'vesting' worden gebouwd), maar ook om het herstel na een aanval ('bouncing back' of zelfs 'bouncing forward'). Het toevoegen van herstel, reparatie en 'redundantie' of alternatieven aan het actierepertoire is een belangrijke les uit het onderzoek naar 'resilience' en zorgt ervoor dat de infrastructuur ook weerbaar blijft als alle voorbereiding en beveiliging toch onverhoopt tekortschiet.
2. Weerbaarheid gaat niet alleen om het moment van de dreiging, aanval of ramp, maar begint met het 'upstream' nemen van maatregelen om ofwel de dreiging te voorkomen, tijdig beschermende maatregelen te nemen of de aanval of ramp op het moment dat die zich voordoet beheersbaar(der) te maken (mitigerende maatregelen). Voor het versterken van de weerbaarheid volstaat 'end point protection' niet. Door 'stroomopwaarts', zowel in de tijd als in de 'dreigingsketen', maatregelen te nemen, wordt 'endpoint protection' wel beter beheersbaar.
3. Weerbaarheid kan niet los van de context worden gezien. Dat begint al met wat zijn de wederzijdse verwachtingen van de overheid en betrokken (private) organisatie en ketenpartners binnen de meest belangrijke infrastructuur van wat eigenlijk als weerbaar wordt beschouwd. Is weerbaarheid hetzelfde als 'onaantastbaarheid' of 100 procent veiligheid, of mag het ook minder zijn? Omdat weerbaarheid ook kosten met zich meebrengt, zal het doorgaans neerkomen op een afweging of 'trade off' tussen de kosten (bijvoorbeeld door redundantie in processen te bouwen, of extra veiligheidsmaatregelen te versterken) en de veiligheidswinst die wordt geboekt. Dit zijn geen geïsoleerde afwegingen en keuzes van individuele 'schakels' in ketens en netwerken, maar moeten ten minste ook op het niveau van de keten of het netwerk worden doordacht.

Weerbaarheid vereist dus een netwerkaanpak, omdat in het domein van fysieke en digitale infrastructuur processen en organisaties soms onbewust onderling afhankelijk zijn van elkaar.

In generieke zin leveren deze lessen de volgende stappen op om infrastructuur in brede zin weerbaar(der) te maken; Voordat we de stappen doorlopen, is er één onderscheid dat alles kleurt: het dreigingsniveau. Uit de werksessies kwam een driedeling naar voren die bepaalt wie wat doet, welke informatie nodig is en welke bevoegdheden van toepassing zijn.

- **Koude fase** — geen actuele dreiging. De focus ligt op voorbereiding: risico-afwegingen maken, plannen opstellen, beschermingsmaatregelen treffen (zoals afschermen van infrastructuur), oefenen, standaarden vaststellen en kennis opbouwen en delen. Denk aan het aanbrengen van fysieke beveiligingen (van simpele maatregelen als netten tot 'jammers' en extra wanden), maar ook aan de voorbereiding van alternatieven in het geval van een

drone-aanval). Dit is primair het domein van de eigenaar, maar die is hierbij ten minste deels afhankelijk van informatie vanuit de overheid (risicoanalyses) en sectorale samenwerking.

- **Lauwe fase** — verhoogde alertheid. Er zijn signalen of aanwijzingen die vragen om opschaling van bewustzijn en detectie. Dynamische dreigingsinformatie wordt relevant: wat speelt er op dit moment, in welke regio, voor welk type object? Ook hier speelt informatie-uitwisseling tussen publieke en private partijen een grote rol.
- **Warme fase** — actuele dreiging. Er is een concrete waarneming of incident. De vraag is niet meer of er gehandeld moet worden, maar wie dat doet, op basis van welk mandaat en binnen welke tijd.

Dit koud-lauw-warm onderscheid loopt als een rode draad door onderstaande zeven stappen. Het bepaalt welke informatie nodig is, welke actor aan zet is en welke bevoegdheden van toepassing zijn. In de warme fase is de reactietijd leidend, zowel qua duiding als qua interventie, en juist daar zit de grootste spanning tussen wat nodig is en wat het huidige systeem toelaat.

Elke stap heeft een eigen karakter, vraagt andere capaciteiten en kent andere verantwoordelijkheden. Door de stappen afzonderlijk te bekijken wordt zichtbaar waar de belangrijkste vraagstukken en dilemma's liggen, maar ook waar de meeste ruimte voor actie zit. De operationalisering volgt in de hoofdstukken over drones en PNT-uitval.

1. Bewustwording en dreigingsbeeld

De meest basale stap: begrijpen wat de dreiging is en hoe reëel die is voor de eigen organisatie en omgeving. Bij veel partijen is dit bewustzijn nog onvoldoende ontwikkeld, niet omdat de wil ontbreekt, maar omdat er geen gemeenschappelijk risicobeeld bestaat, geen gedeelde norm voor wat een adequate basisuitrusting voor weerbaarheid is of omdat er geen direct voorhanden handelingsperspectief is (wat handelingsverlegenheid kan opleveren). Bewustwording vraagt om inzicht in relevante incidenten, in de typen actoren die dreiging veroorzaken en in de specifieke kwetsbaarheden van de eigen infrastructuur. De overheid speelt hierin een onmisbare rol: zonder toegang tot dreigingsinformatie kunnen vitale aanbieders geen gefundeerd beeld opbouwen. De verschillen tussen sectoren, objecten, clusters en netwerken zijn groot, en dat vraagt om een gedifferentieerde aanpak.

2. Risicoanalyse

Op basis van de analyse van te beschermen ‘assets’, kwetsbaarheden in de infrastructuur en het dreigingsbeeld bepaalt een organisatie welke risico's relevant zijn, welke scenario's de meeste aandacht verdienen en welke risico's acceptabel zijn. Pas als die afweging is gemaakt, is duidelijk welke maatregelen proportioneel en noodzakelijk zijn. Dit is primair het domein van de eigenaar van de infrastructuur, maar die is hierbij afhankelijk van informatie vanuit de overheid en van sectorale kennisdeling. Een gedeeld risicoanalysekader, met gemeenschappelijke scenario's en normen, voorkomt dat elke organisatie het wiel opnieuw uitvindt en bevordert onderlinge vergelijking en samenwerking. tot het uitvoeren van een risicobeoordeling. Hierin moeten zij alle relevante door de natuur en door de mens veroorzaakte risico's meenemen. Hierin moet in ieder geval gekeken worden naar risico's van sectoroverschrijdende of grensoverschrijdende aard, ongevallen, natuurrampen, noodsituaties op het gebied van volksgezondheid en hybride en andere antagonistische dreigingen. De partijen ervaren hierbij weinig houvast; Hoe ver en diep reikt de verplichting of, anders benaderd, wanneer is het voor wat betreft de wettelijke verplichting genoeg?

3. Maatregelen treffen

Als de risicoanalyse uitwijst dat een organisatie kwetsbaar is, treft zij structurele maatregelen: fysieke en digitale bescherming van kritieke plekken, maar ook back-upvoorzieningen, protocollen en het oefenen daarvan. Elke organisatie bepaalt op basis van haar eigen risicoprofiel welke maatregelen passend zijn. Voor oplossingen valt niet alleen te denken aan sectorale samenwerking,

maar ook aan partijen stroomopwaarts en stroomafwaarts in de keten. Voorbereiding is geen eenmalige activiteit maar een continu proces, gevoed door wat er in de laatste stap, herstel en leren, wordt opgedaan.

4. Detectie en data-analyse
Wanneer de organisatorische en fysieke maatregelen zijn getroffen, is de volgende stap het technisch herkennen en registreren van dreigingen. Centrale vragen zijn: wie doet wat, hoe wordt data uitgewisseld en hoe vindt besluitvorming op basis van die data plaats?

5. Besluitvorming
Detectie levert waarnemingen op, maar vaak geen antwoorden, en verlaagt de kwetsbaarheid niet. Zonder opvolging in duiding en interventie verandert het risico feitelijk niet. De cruciale vraag is dus: wat betekent een waarneming en wat doen we ermee? Elke waarneming vraagt triage, en dat stelt hoge eisen aan de beschikbaarheid van dreigingsinformatie en aan de capaciteit om die snel te interpreteren. Bij drones draait dit om de vraag of een toestel kwaadwillend is, met een reactietijd van soms enkele minuten; bij PNT om de vraag of een signaal nog te vertrouwen is en wanneer wordt overgeschakeld op een onafhankelijke back-up. Is de dreiging geduid, dan volgt de beslissing: wat doen we, wie doet het en hoe snel? Juist die snelheid maakt besluitvorming tot een van de meest urgente knelpunten in de keten.

6. Interventie
De daadwerkelijke ingreep om de dreiging af te wenden. Dit is doorgaans de escalatieladder waar juridische kaders, technische middelen en operationele capaciteit samenkomen, en waar de spanning tussen wat nodig is en wat nu mogelijk is het scherpst voelbaar is. Bij drones gaat het om een (fysieke) ingreep, met bevoegdheden die nogal eens uitsluitend bij de overheid liggen; de rol van private partijen is daar beperkt, wat snelle en betrouwbare samenwerking met de bevoegde instanties des te belangrijker maakt. Bij PNT ligt de interventie juist meer bij de partijen zelf: overschakelen op een onafhankelijke back-up en herstellen binnen de eigen systemen. In sommige gevallen kan het ook gaan om een meer ‘offensieve’ actie om bijvoorbeeld verstorende apparatuur uit te schakelen of cyberaanvallers uit te schakelen (door een ‘tegenaanval’ waarmee het systeem van de aanvallers wordt uitgeschakeld). Voor drones én PNG geldt dat interventie alleen werkt als de stappen ervoor, detectie en duiding, op orde zijn.

7. Herstel en leren
Na een incident of oefening volgt herstel en reflectie. Wat is er gebeurd? Wat werkte wel en wat niet? Welke lacunes zijn zichtbaar geworden in het dreigingsbeeld, de risicoanalyse, de detectie of de besluitvorming? De lessen uit deze stap voeden direct de volgende ronde van bewustwording en maatregelen. Zo sluit de cyclus zich: herstel en leren is niet het eindpunt, maar het beginpunt van een volgende, betere voorbereiding. Publiek-private uitwisseling van lessons learned is daarbij essentieel en komt nu nog onvoldoende van de grond.

Dit generieke kader passen we in de volgende hoofdstukken toe op drones en PNT-uitval. Daarbij onderscheiden we ook nog verschillende ‘niveaus’ waarop deze stappen kunnen worden toegepast: de eigenaar of beheerder van infrastructuur, het netwerk van eigenaren en beheerders (sectoraal of in de ‘supply chain’) en de overheid (en in het bijzonder welke overheidsinstantie).

Thema I

Drones

2. Analyse: Hoe het netwerk naar het drone-vraagstuk kijkt

Drones brengen niet alleen uitdagingen maar ook grote kansen. Inspectie, monitoring, logistiek, hulpverlening: de toepassingen nemen toe en de technologie ontwikkelt zich in hoog tempo. Nederland beweegt naar een samenleving waarin drones een vanzelfsprekend onderdeel zijn van het maatschappelijk en economisch verkeer. De verdieping in dit thema is dan ook een no-regret aanpak: wat nodig is om vitale infrastructuur te beschermen tegen ongewenste drones, is tegelijkertijd nodig om het verantwoord en veilig opschalen van dronegebruik mogelijk te maken.
Het Versnellingsnetwerk benadert het vraagstuk vanuit het perspectief "van buiten naar binnen". Hierbij redeneert het Versnellingsnetwerk vanuit de logica van de vitale sectoren zelf: hoe ervaren zij de dreiging, wat kunnen zij zelf doen en waar stuiten zij op grenzen? Het 'buitenperspectief' is de meerwaarde van dit netwerk in aanvulling op het overheidsperspectief, want juist de verbinding tussen beide perspectieven is nodig om tot werkbare oplossingen te komen.

2.1 Waarom dit vraagstuk anders is

Wie het vraagstuk van ongewenste drones nader bekijkt, ziet al snel dat drones zich op een aantal punten wezenlijk onderscheiden van eerdere veiligheidsopgaven voor vitale infrastructuur. Dat begint al bij de dimensie van de dreiging zelf. Decennialang was fysieke beveiliging een tweedimensionaal probleem: terreinbeveiliging, hekken en toegangscontrole. Die aanpak is niet verdwenen, maar deze is onvoldoende geworden. De dreiging kan – naast cyber - ook van boven en, zoals recente waarnemingen aantonen, van het wateroppervlak en eronder komen. Een haven die zijn terrein uitstekend beveiligd heeft, heeft nog geen antwoord op een drone die op grote hoogte overvliegt of onder water de haven binnenkomt.

Daar komt bij dat de noodzakelijke reactietijd onverenigbaar is met bestaande procedures. Wanneer een ongeautoriseerde drone wordt gedetecteerd boven een vitaal object, is de beschikbare tijd voor interventie in de orde van grootte van enkele minuten. Bestaande escalatieprocedures, van melding bij politie tot beoordeling en inzet, zijn daar niet op ingericht. De keten is te lang voor de tijdshorizon.

Ook de snelheid van technologische ontwikkeling stelt bestaande kaders onder druk. Nieuwe dronetypen, groter, sneller, autonomer en moeilijker te detecteren, worden in hoog tempo beschikbaar. Regelgeving die vandaag adequaat is, kan binnen twee maanden al achterhaald zijn. Alleen al vanwege de snelheid van de technologische ontwikkeling volstaat het niet om nu een weerbaarheidsaanpak te ontwikkelen maar er moet ook een continu proces van monitoring en bijstelling met bijbehorende 'infrastructuur' aan worden toegevoegd.

Ten slotte is er het kernprobleem van classificatie. Er is niet één type drone-dreiging. De schaal loopt van geautoriseerd gebruik naar een hobbyist die onbewust te dicht bij een luchthaven vliegt, via een crimineel die een bedrijfsterrein verkent, tot een statelijke actor die vitale infrastructuur systematisch in kaart brengt als voorbereiding op sabotage (compliant, clueless, careless en criminal). Op het moment van waarnemen is vaak niet duidelijk met welk type dreiging men te maken heeft. Detectie en duiding zijn fundamenteel verschillende stappen en juist die duiding is momenteel de zwakste schakel.

2.2 Drie typen vitale infrastructuur

Om grip te krijgen op het drone-vraagstuk helpt het om onderscheid te maken tussen drie typen vitale infrastructuur. Dit onderscheid is geen doel op zich, maar een denkkader: het maakt zichtbaar waar de kwetsbaarheden verschillen van aard en het vormt de basis voor het gestructureerd in beeld brengen van handelingsopties;

Een **object** is een afgebakende, op zichzelf staande locatie: zoals een datacenter, een gemaal, een energiecentrale of een waterzuiveringsinstallatie. De kwetsbaarheid is geconcentreerd op één plek, wat het tegelijkertijd een herkenbaar doelwit maakt.

Een **cluster** is een geografisch gebied met meerdere vitale partijen in elkaars nabijheid, zoals de Rotterdamse haven, een industrieel bedrijventerrein, zoals de chemieclusters in Zeeland, Brabant en Limburg, of een luchthaven met zijn directe omgeving. De uitdaging hier is coördinatie tussen partijen die individueel kwetsbaar zijn, maar gezamenlijk meer kunnen organiseren.

Een open **netwerk**, spoorwegen, hoogspanningsnetten, buisleidingen en (vaar)wegen, kent geen begrensd terrein en is kwetsbaar over de volle lengte. Prioritering is hier onvermijdelijk: niet alles kan tegelijk worden beschermd.

Bij toepassing van het generieke kader voor weerbaarheid(sversterking) uit het vorige hoofdstuk blijkt dat bij uitstek op het terrein van drones ‘end point protection’ niet volstaat; de tijd die dan voor actie beschikbaar is (enkele minuten) is te weinig om weerbaarheid te borgen. Door ‘stroomopwaarts’, zowel in de tijd als in de ‘dreigingsketen’, maatregelen te nemen, wordt ‘endpoint protection’ wel beter beheersbaar.

2.3 Eerste reflectie: wat het netwerk heeft opgehaald

Uit de werksessies met meer dan 50 deelnemende organisaties kwam een aantal patronen en gedeelde ervaringen naar voren. Ze kleuren niet alleen de analyse; Ze bieden het vertrekpunt voor de opbrengst in hoofdstuk 3.

Kansen en dreiging zijn twee kanten van dezelfde medaille

Deelnemers benadrukten expliciet dat drones niet alleen een veiligheidsvraagstuk zijn. Een goede aanpak van ongeautoriseerde drones is tegelijkertijd een voorwaarde voor het benutten van de kansen die drones bieden voor inspectie, logistiek en monitoring. Bovendien bieden initiatieven voor geautoriseerd droneverkeer ook mogelijkheden om ongeautoriseerd droneverkeer aan te pakken. Die verbinding moet bewust worden gemaakt in de aanpak, in beleid en in regelgeving. Wie alleen naar de dreiging kijkt, mist een belangrijk deel van het verhaal.

Goede voorbeelden zijn er, maar blijven geïsoleerd

Er zijn waardevolle initiatieven: het U-space initiatief van het Havenbedrijf Rotterdam, de publiek-private cameranetwerken bij haven en luchthaven, de meldtools van Stedin en Shell en de samenwerking in landelijke en regionale branches. Deze voorbeelden laten zien dat samenwerking werkt en dat partijen bereid zijn te investeren. Maar ze staan vooralsnog op zichzelf. Systematische kennisdeling en opschaling komen nog onvoldoende van de grond.

Publiek-private samenwerking als fundament

Publiek-private samenwerking wordt breed gezien als de onmisbare basis voor een werkende aanpak. Noch de overheid, noch de private sector kan dit vraagstuk alleen oplossen. De vitale aanbieders hebben de sensoren, de lokale kennis en de operationele aanwezigheid. De overheid heeft het dreigingsbeeld, de interventiebevoegdheden en het wettelijk kader. Alleen in combinatie ontstaat een keten die functioneert. Die samenwerking vraagt om structurele inbedding, niet om ad-hocverbanden die afhankelijk zijn van persoonlijke relaties of lokale initiatieven.

“

Bereidheid tot investeren vraagt wederkerigheid

Veel partijen zijn bereid te investeren in weerbaarheid, ook buiten de eigen hekken. Maar die bereidheid is niet onvoorwaardelijk. Ze is afhankelijk van de zekerheid dat ook elders in de keten wordt geïnvesteerd en geleverd. Wie investeert in detectie, wil weten dat er opvolging is. Wie meldt, wil terugkoppeling. Deze investeringslogica en de onderlinge afhankelijkheden die daaraan ten grondslag liggen, zijn een cruciaal gegeven voor de opbrengst in hoofdstuk 3.

Fundamentele keuzes liggen op tafel

De werksessies brachten ook een aantal spanningsvelden naar voren dat niet ambtelijk opgelost kan worden. Over de verdeling van verantwoordelijkheden en bevoegdheden, over wie bepaalt wanneer een organisatie weerbaar genoeg is, over de voorwaarden voor informatiedeling en over de vraag of de huidige interventiebevoegdheden houdbaar zijn. Deze dilemma's worden uitgewerkt in paragraaf 3.4, omdat ze de kern vormen van wat politieke en bestuurlijke keuzes vraagt.

3. Opbrengst

3.1 De matrix als denkkader

Het drone-vraagstuk is complex, niet omdat de afzonderlijke onderdelen onbegrijpelijk zijn, maar omdat ze samenhangen. Om die samenhang inzichtelijk te maken en de handelingsopties gestructureerd in beeld te brengen, werkt dit hoofdstuk met een matrix.

De horizontale as volgt de zeven stappen: van bewustwording en dreigingsbeeld via risicoanalyse, maatregelen treffen, detectie en data-analyse en besluitvorming naar interventie, en terug via herstel en leren. De verticale as beschrijft wie een rol speelt: de eigenaar van het object of netwerk, sectorale en regionale samenwerkingsverbanden, private dienstverleners, en de overheid, inclusief IenW, JenV (politie, NCTV), Defensie en KMAR.

De matrix is geen blauwdruk, maar het hulpmiddel dat in de werksessies is gebruikt om het gesprek te structureren en witte vlekken te achterhalen. De opbrengst laat zich langs drie lijnen ordenen: dilemma's (3.2), doorbraakadviezen (3.3) en actievoorstellen (3.4).

Actor / Fase	1. Bewust-wording & Dreigings-beeld	2. Risico-Analyse	3. Maat-regelen treffen	4. Detectie & data-analyse	5. Besluit-vorming	6. Inter-ventie	7. Herstel & leren
Eigenaar object / netwerk	Risicoanalyse uitvoeren; dreiging in kaart brengen; afhankelijkheden kennen	Eigen kwetsbaarheden bepalen; scenario's doordenken; norm vaststellen	Fysieke bescherming; netten, afstand, back-up; protocollen opstellen en oefenen	Eigen sensoren inzetten; waarnemingen registreren; data delen met keten	Intern escalatieprotocol; beslissen over zelfverdediging/opschaling; contact overheid activeren	Passieve maatregelen activeren; operatie aanpassen; bevoegd gezag ondersteunen	Eigen schade herstellen; incident documenteren; lessen intern verankeren
Sectoraal & veiligheids-regio	Gezamenlijk dreigingsbeeld opbouwen; sectorale incidenten delen; regionaal risicobeeld opstellen	Gedeeld risicoanalysekader; gemeenschappelijke scenario's; onderlinge afhankelijkheden inzichtelijk	Gezamenlijke standaarden; gedeelde inkoop detectie; sectorale oefeningen	Gedeelde detectieinfrastructuur; publiek-private cameranetwerken; gezamenlijk meldprotocol	Regionaal coördinatiepunt; veiligheidsregio als schakel; gedeeld beeld voor overheid	Veiligheidsregio coördineert; private partijen ondersteunen; operationele terugkoppeling	Collectieve lessons learned; best practices delen; opschaling van wat werkt
Private dienst-verlener	Dreigingsintelligentie leveren; risicotools aanbieden; standaarden ontwikkelen	Assessmenttools aanbieden; sectorspecifieke expertise; onafhankelijk advies	Detectieapparatuur leveren; certificering; installatie en onderhoud	Data-analyse als dienst; AI-gestuurde duiding; platforms voor informatie-uitwisseling	Beslissingsondersteuning; realtimeinformatie; situational awareness tools	Countermeasure-technologie; drone-overname of -verstoring; onder gecertificeerde voorwaarden	Technisch herstel; forensische analyse; productontwikkeling op basis van lessen
Overheid (JenV (politie / NCTV) / defensie / KMAR)	Dreigingsbeelden delen; JenV en Defensie-informatie ontsluiten; normen en kaders stellen (Wwke)	Risicoanalysemethodiek beschikbaar stellen; toezicht op uitvoering; no-fly zones actualiseren	Programma van eisen detectie; vliegverbodenlijst coherent maken; regelgeving actueel houden	Centraal meldpunt operationaliseren; feedback aan melders; data uit publiek domein delen	Duiding op basis van inlichtingen; mandaat voor opschaling; coördinatie interventie	Geweldsmonopolie uitoefenen; politie / KMAR intervenieert; interventieladder toepassen	Incident analyseren; beleid aanpassen; lessen leren publiek-privaat borgen

Figuur 1: Matrix stappen en actoren drone-aanpak

3.2 Dilemma's: waar keuzes onvermijdelijk zijn

De matrix laat niet alleen zien welk breed scala aan handelingsopties denkbaar is, deze laat ook zien waar het systeem vastloopt. De volgende dilemma's zijn geen technische of organisatorische problemen die met een protocol op te lossen zijn. Ze raken aan fundamentele keuzes over bevoegdheden, verantwoordelijkheden en normen, keuzes die bestuurlijk en politiek gemaakt moeten worden. Het netwerk benoemt ze expliciet, omdat ze zonder deze explicitering blijven hangen als olifanten in de kamer.

De volgorde is bewust: de dilemma's bouwen op elkaar voort. De discussie over informatiedeling, over regie en over interventie kan pas goed worden gevoerd als het eerste dilemma, wanneer ben je weerbaar genoeg en wie bepaalt dat, is geadresseerd. Wie begint bij interventie, loopt vast op weerstand zonder feitelijke onderbouwing.

1. Wanneer ben je weerbaar genoeg? Verantwoordelijkheid, bevoegdheid en investeringen

De Wwke stelt open normen aan de hand van een zorgplicht om passende en evenredige maatregelen te nemen. Dat biedt organisaties ruimte, maar ook onzekerheid. De fundamentele vraag blijft onbeantwoord: wanneer heeft een organisatie genoeg gedaan en het goed gedaan? Welk niveau van beveiliging ‘upstream’ volstaat? Hoe lang moet een organisatie, of beter nog het netwerk, kunnen blijven functioneren in geval van een verstoring door drones of PNT-uitval? Volgens de Wwke bepaalt de toezichthouder dat achteraf, maar partijen zouden graag op voorhand meer duidelijkheid hebben. En wie accepteert het restrisico als een incident toch plaatsvindt?

Dit dilemma is breder dan het dronestuk alleen: het speelt in de gehele Wwke-implementatie en verdient een plek in de geplande evaluatie. De EU CER-richtlijn, waarop de Wwke is gebaseerd, hanteert een all-hazard benadering en benadrukt daarin ook een Europees gelijk speelveld. Wat van Nederlandse vitale partijen wordt gevraagd, moet in lijn zijn met wat van hun Europese concurrenten wordt verwacht.

Die onzekerheid over de invulling van de norm heeft directe financiële consequenties. Investeren in weerbaarheid kost geld, maar een organisatie wil weten of ook op andere plekken in de keten de juiste dingen gebeuren. Dit maakt de investeringsafweging niet alleen een interne bedrijfsbeslissing; het is een ketenafweging waarbij zichtbaarheid over wat anderen doen een voorwaarde is voor eigen actie.

Voor veel vitale sectoren heeft deze afweging bovendien een bestuurlijke complicatie. Waterbedrijven, netbeheerders en havenbedrijven zijn vaak deelnemingen van de overheid. De tafel waaraan de investeringsbeslissing wordt gemaakt, is daarmee ook de tafel waaraan de overheid zit: als aandeelhouder, als toezichthouder én als normsteller. Die driedubbele rol vraagt expliciete erkenning. Het kan niet zo zijn dat de overheid via de Wwke weerbaarheid eist, via de eigenaarsrol investeringen afremt en via het tariefbeleid kostenverhoging blokkeert. Die drie rollen moeten met elkaar in verbinding staan.

2. Informatiedeling: wat mag, wie valideert, wie is eigenaar?

Dreigingsinformatie is de smeerolie van de keten. Zonder gedeeld beeld geen goede risico-afwegingen, geen gerichte investeringen en geen effectieve besluitvorming. De bereidheid om informatie te delen is in het netwerk aanwezig. Maar die bereidheid stuit op reële belemmeringen: juridische, waarbij privacywetgeving en classificatieniveaus onduidelijkheid scheppen over wat wel en niet vergaard en gedeeld mag worden; Organisatorische belemmeringen, waarbij de vraag speelt wie verantwoordelijk is voor de juistheid van gedeelde informatie en concurrentiegevoelige belemmeringen, waarbij informatie over kwetsbaarheden raakt aan bedrijfsvertrouwelijke gegevens.

“

Informatiedeling is ook een voorwaarde voor proportionaliteit: je kunt alleen een goede risicoafweging maken als je weet wat de dreiging is en wat anderen in de keten doen. Dat maakt dit niet alleen een juridisch vraagstuk, maar een bestuurlijk.

De aanpak van drugscriminaliteit laat zien dat informeel informatiedelen zonder formeel MoU of wetgeving aantoonbaar resultaat kan opleveren. Dat precedent verdient een plek in de aanpak van het drone-vraagstuk. Daarnaast is in de werksessies breed de behoefte uitgesproken om elementen van het voormalige Alerteringssysteem Terrorismebestrijding opnieuw te activeren als onderdeel van de oplossing, in de lijn van ATB 2.0; Een publiek-privaat informatie- en alerteringssysteem voor overheid en vitale aanbieders, onder regie en beheer van de NCTV, gericht op fysieke en hybride dreigingen. Het systeem faciliteert het veilig delen van dreigingsinformatie, het veilig delen van *good practices* (*trusted community*), het tijdig waarschuwen van vitale aanbieders, het vooraf afspreken van overheids- en sectormaatregelen bij dreiging, het gecoördineerd opschalen en handelen tijdens perioden van verhoogde dreiging, en het structureel en sectoroverstijgend oefenen.

Het dilemma zit niet in de vraag of informatie gedeeld moet worden; daarover bestaat consensus. Het zit in de voorwaarden. Wie valideert de informatie? Is de technische operabiliteit aanwezig om de informatie te delen? Wie is eigenaar van het gedeelde beeld? En hoe bereikt die informatie de mensen in de organisatie die er daadwerkelijk iets mee kunnen doen? Het Versnellingsnetwerk vraagt de rijksoverheid een juridisch en organisatorisch kader te ontwikkelen dat partijen de zekerheid geeft die zij nodig hebben om daadwerkelijk te delen, en dat wederkerigheid als principe verankert: wie detectiedata aanlevert, mag ook informatie terugverwachten.

3. Centrale regie en regionale diversiteit

Nationale standaarden zijn nodig om versnippering te voorkomen. Maar de uitvoering van weerbaarheid is per definitie lokaal en contextueel. Een energiecentrale in Zeeland heeft andere kwetsbaarheden dan een spoorknooppunt in Utrecht. Het organisatieprincipe dat uit de werksessies naar voren komt is helder: nationaal protocolleren, regionaal operationaliseren. Maar dat principe vraagt uitwerking op concrete vragen die nu onbeantwoord blijven: wie heeft de nationale regie, en is die regie belegd met voldoende mandaat en middelen? En hoe wordt geborgd dat regionale uitvoering aansluit op de nationale standaard?

Het netwerk onderschrijft het principe en is bereid op regionaal niveau actief aan te sluiten, maar vraagt de rijksoverheid om de bijbehorende verantwoordelijkheden expliciet te beleggen en de veiligheidsregio's te mandateren en toe te rusten.

4. Operationele autonomie van private beheerders

Een vraagstuk dat in de werksessies naar voren kwam maar nog niet volledig is uitgewerkt, verdient eveneens een expliciete positie: de vrijheid van private organisaties om bij een aanhoudende dreiging zelf te besluiten de operatie te staken. Hier staat de continuïteit van vitale processen als publiek belang op gespannen voet met de autonomie van private beheerders. Wie draait de haven dicht als er drones cirkelen? Wie beslist dat een spoortraject wordt stilgelegd? En op basis van wiens oordeel? Zolang dit vraagstuk niet is geadresseerd, blijft de beslissing liggen bij de individuele operator, zonder helder kader en zonder politieke dekking.

5. De interventiebevoegdheden en de reactietijd

De kern van dit dilemma is simpel en schrijnend: degene die wettelijk mag ingrijpen, is er in de warme fase nooit op tijd. De politie heeft het mandaat, maar niet de capaciteit en de reactiesnelheid die het drone-vraagstuk vereist. Private beheerders zijn ter plaatse, maar mogen niet ingrijpen. Het resultaat is een systeem dat op papier sluitend is, maar in de praktijk een gat laat precies op het moment dat het er het meest toe doet.

“

Dit dilemma hangt als een deken over het gehele vraagstuk. Het ondermijnt het vertrouwen in de zinvolheid van investeringen in alle andere fasen. Waarom investeren in detectie als er toch geen adequate opvolging mogelijk is? In de werksessies werd dit gevoel breed gedeeld: investeringsbereidheid wordt aangehouden, zolang op dit fundamentele punt geen stappen worden gezet.

Het netwerk stelt niet dat het geweldsmonopolie moet worden afgeschaft. Het stelt wel de vraag of de huidige invulling ervan houdbaar is in een hybride tijdperk waarin de reactietijd enkele minuten bedraagt. Met digitalisering is bovendien een heel nieuw palet aan ‘digitale’ (offensieve) interventies mogelijk geworden waarvan het nog te vraag is in hoeverre deze tot het ‘geweldsmonopolie’ mogen worden gerekend (denk aan het ‘hacken’ van ‘gijzelaars’ om te voorkomen dat losgeld moet worden betaald). De interventieladder verdient uitwerking langs drie assen: welk type interventie (van fysieke afscherming tot neerhalen), wie voert die uit (van gecertificeerde private partij tot politie en defensie), en waar vindt die plaats (boven eigen terrein zonder risico voor derden, tot in de openbare ruimte). In België wordt nagedacht over een wetsvoorstel om specifieke partijen te mandateren om onder strikte voorwaarden ongewenste drones te kunnen verstoren. Vooruitgang op dit punt is een voorwaarde voor vooruitgang op vele andere punten. Dit vraagt een expliciete politieke keuze.

3.3 Doorbraakadviezen

Hier zijn de drie doorbraakadviezen die er bovenuit springen. Ze zijn niet de enige aanbevelingen in dit advies, maar ze zijn de voorwaarde waaronder de overige actievoorstellen tot hun recht komen. Ze hangen ook onderling samen: duidelijkheid verschaffen maakt gericht investeren mogelijk, maar geloofwaardige interventiecapaciteit is tegelijkertijd een voorwaarde voor die investeringsbereidheid. Wie investeert in detectie, wil weten dat er ook daadwerkelijk opvolging mogelijk is. Alle drie de doorbraken moeten daarom gelijktijdig worden opgepakt.

Doorbraak 1: Bied organisaties informatie en handvatten voor effectieve weerbaarheidsafwegingen

Aan: Kabinet

Weerbaarheid tegen dreigingen als ongewenste drones is op de eerste plaats een strategisch vraagstuk dat thuishoort in de boardroom en bij toezichthoudende organen. Niet alleen bij organisaties die onder de Wwke vallen, maar ook bij partijen die een wezenlijke rol spelen in een vitale keten zonder als kritieke entiteit te zijn aangewezen. Die bewustwording is de eerste stap, en die moet hoger op de agenda.

Investeren in weerbaarheid is in de kern een proportionaliteitsafweging. Het lijkt op een verzekering: je legt nu geld in voor maatregelen waarvan je achteraf hoopt dat ze overbodig waren. De vraag is dus niet óf je investeert, maar hoe groot je die premie wilt maken. En dat kun je alleen goed wegen als je weet waartegen je je verzekert.

Daarvoor zijn informatie en handvatten nodig: statische dreigingsinformatie voor structurele voorbereiding en dynamische informatie om te weten wanneer op te schalen. Beide moeten vanuit de rijksoverheid worden ontsloten aan de partijen die de proportionele premie moeten bepalen. Zonder dat beeld blijven afweging en investeringsbeslissingen hangen, ook bij partijen die niet verplicht zijn tot een formele risicoanalyse.

Die afweging reikt verder dan de eigen organisatie. Wie alleen naar het eigen risicoprofiel kijkt, mist de afhankelijkheden in de keten en de regio. Juist op dat gezamenlijke niveau horen de risicoafwegingen en de investeringsvraagstukken thuis.
Het netwerk stelt voor in één of twee regio's nu concreet te starten: organisaties uit dezelfde keten en regio oefenen samen hoe de afweging is te maken en wat dat vraagt aan informatie-uitwisseling. Dat levert een schaalbaar model op voor de rest van Nederland. De private partijen vragen de

“

rijksoverheid dit te faciliteren en daarbij de eigen driedubbele rol te erkennen: wie als normsteller weerbaarheid eist, mag die niet via de aandeelhoudersrol of het tariefbeleid tegelijk onmogelijk maken.

Doorbraak 2: Investeer samen in detectie en beeldopbouw

Aan: Kabinet en vitale partijen

De bereidheid om te investeren is aanwezig, maar heeft een voorwaarde: partijen willen weten dat ook anderen in de keten investeren en dat hun bijdrage aansluit op een groter geheel.

De doorbraak zit in gezamenlijke detectie en beeldopbouw. Organisaties investeren nu al in sensoren en detectiesystemen, maar zonder gemeenschappelijke standaarden en zonder gedeelde infrastructuur. De meerwaarde zit juist in de verbinding: als systemen van partijen in dezelfde sector en/of regio op elkaar aansluiten en data uitwisselen, ontstaat een dekkend regionaal beeld dat elk van de partijen afzonderlijk nooit zou kunnen opbouwen.

Dit is ook een no-regret keuze. De infrastructuur voor beeldopbouw en datadeling die nu wordt opgebouwd om ongewenste drones te duiden, is dezelfde infrastructuur die nodig is voor bijvoorbeeld de ‘use case’ om het snel groeiende geautoriseerde droneverkeer veilig mogelijk te maken of de luchtvaartveiligheid te waarborgen. Investeren in detectie dient die doelen tegelijk.

Drie stappen zijn nodig: standaardisering van detectieapparatuur en data-uitwisseling, gedeelde publiek-private detectienetwerken per regio met heldere afspraken over beheer en terugkoppeling, en wederkerigheid als principe: wie data aanlevert, krijgt informatie terug middels eenvoudige ontsluiting. Daarvoor moeten ook eventuele juridische randvoorwaarden (ten aanzien van informatiedeling) worden gecreëerd. Het netwerk stelt voor om in de twee regio's waarmee doorbraak één wordt opgestart ook hierop direct een concrete stap te zetten. Koplopers uit de sector zijn bereid als actieve partners te fungeren en vragen een kader waarbinnen de samenwerking juridisch en organisatorisch is geborgd.

Doorbraak 3: Maak interventiecapaciteit schaalbaar

Aan: Kabinet en vitale partijen

"Waarom zouden wij investeren in detectie als er toch geen adequate opvolging mogelijk is?" Dit was een van de meest gestelde vragen tijdens de werksessies en het raakt direct aan de kern van dit dilemma. Zolang er geen verandering komt in de huidige situatie zet dat een slot op de vervolgstappen en investeringen die nodig zijn. Het geweldsmonopolie-dilemma is daarmee niet alleen een juridisch vraagstuk: het is het fundament onder de investeringsbereidheid van het gehele netwerk.

De politie heeft het mandaat, maar niet de capaciteit en reactiesnelheid die het drone-vraagstuk vereist. Private beheerders zijn ter plaatse, maar mogen niet ingrijpen. Dit is de status quo, en die is onhoudbaar.

Het netwerk vraagt om het geweldsmonopolie niet als een ondeelbaar geheel te behandelen, maar het te ontleden: wie mag wat, waar en onder welke voorwaarden? Dit heeft te maken met mandaat, regelgeving, robuustheid en redundantie voor de keten en een benodigd coördinatiemechanisme. De ontleding vraagt een concrete verkenning langs drie assen: welk type interventie is aan de orde, variërend van fysieke afscherming tot verstoring of het neerhalen van een drone; wie kan die interventie uitvoeren, variërend van een gecertificeerde private partij op eigen terrein tot politie en defensie; en onder welke voorwaarden, met bijzondere aandacht voor situaties waarbij geen risico voor derden bestaat en voor de mogelijke schadelijke neveneffecten door het optreden van interferentie ten gevolge van de inzet van radio-interventie door private partijen.

“

Het netwerk roept de minister van Justitie en Veiligheid op om nu opdracht te geven dit te onderzoeken: hoe kan de interventiecapaciteit worden uitgebreid en onder welke voorwaarden? We adviseren tevens gerichte pilots mogelijk te maken. België bereidt wetgeving voor die specifieke partijen onder strikte voorwaarden mandateert om ongewenste drones te verstoren. Bovendien kent België het fenomeen van de Havenkapitein (in plaats van de Havenmeester) en die gaat ook over het luchtruim. Nederland kan van die ontwikkeling leren en hoeft het wiel niet opnieuw uit te vinden.

3.4 Actievoorstellen: wat nu al kan

De volgende actiepunten vragen geen nieuwe wetgeving, geen grote budgetten en geen politieke doorbraken. Ze liggen binnen bereik, mits de juiste partij ze oppakt. Per punt is aangegeven wie de actiehouder is en wat er concreet van wordt verwacht. Hierbij sluit het Versnellingsnetwerk zoveel mogelijk aan bij bestaande structuren (in willekeurige volgorde).

a. Standaard meldprotocol drone-incidenten vaststellen en invoeren

[bewustzijn en detectie / alle typen] Actiehouder: IenW, Defensie en JenV

Er is geen gemeenschappelijke standaard voor het melden van drone-incidenten. Partijen melden nu op verschillende manieren (diversiteit in registratie), bij verschillende loketten (zoals politie, eigen bedrijf, etc.) en met verschillende informatie (type, hoogte, snelheid, etc.). Een generiek meldprotocol, wie meldt wat, aan wie, op welk moment en wat gebeurt er vervolgens met die melding, is een basisvoorwaarde voor een werkende keten. Het netwerk vraagt de rijksoverheid dit protocol op te stellen en te implementeren. Vitale sectoren committeren zich aan gebruik zodra het protocol er ligt.

b. Vliegverbodenlijst coherent maken met de lijst vitale objecten

[voorbereiding en besluitvorming / object en cluster] Actiehouder: IenW

De huidige lijst van vliegverboden, luchtruimsluitingen, oftewel no-fly zones, sluit niet aan op de lijst van vitale objecten. Deels komt dat doordat bepaalde no-fly zones niet openbaar staan geregistreerd omwille van het te beschermen belang. Evenwel mag boven sommige kritieke locaties legaal worden gevlogen. Dit is een administratieve inconsistentie die relatief eenvoudig te corrigeren is, maar die nu een serieus gat laat in de bescherming. Het netwerk vraagt de rijksoverheid deze twee lijsten op elkaar af te stemmen en te waarborgen dat alle vitale objecten en clusters op de vliegverbodenlijst staan waar dat voor de hand ligt.

c. Programma van eisen voor detectieapparatuur vaststellen

[detectie / alle typen] Actiehouder: IenW, Defensie en JenV, in samenwerking met vitale partijen

Partijen die willen investeren in detectiecapaciteit, weten niet aan welke eisen hun apparatuur moet voldoen. Er is geen nationale standaard. Het gevolg is een lappendeken van incompatibele systemen die onderling geen informatie kunnen uitwisselen. Een nationaal programma van eisen, opgesteld door de rijksoverheid in samenwerking met vitale sectoren en kennisinstellingen, voorkomt versnippering en maakt gedeelde informatie-uitwisseling mogelijk. De ambtelijke taskforce werkt momenteel aan een programma van eisen voor detectieapparatuur. Het netwerk is bereid hieraan inhoudelijk bij te dragen.

Hierbij dient te worden opgemerkt dat detectie onlosmakelijk verbonden is met de behoefte van partijen aan duiding van de dreiging, om een inschatting te kunnen maken van proportionele maatregelen, en in geval van een ongewenste drone de behoefte aan het perspectief op interventie.

d. Proactieve sturingsinformatie structureel beschikbaar stellen: statisch én dynamisch

[duiding / alle typen] Actiehouder: Defensie en JenV

Partijen hebben behoefte aan een gesprek over twee soorten informatie: statische informatie voor de koude fase enerzijds, wat is het algemene dreigingsbeeld voor mijn type object of sector, en dynamische alerteringsinformatie voor de lauwe en warme fase anderzijds, wat speelt er op dit

“

moment, is er verhoogde dreiging voor mijn regio of sector? Partijen geven aan deze informatie nodig te hebben om af te kunnen wegen of en welke proportionele maatregelen zij kunnen en willen treffen. Veel partijen verwijzen in dit verband naar de oorspronkelijke werkwijze “Alerteringssysteem Terrorismebestrijding” van de NCTV. Die informatie en maatregelen is nu onvoldoende beschikbaar en dat raakt direct aan de investeringsbereidheid: van vitale partijen wordt redelijkerwijs verwacht dat zij investeren in weerbaarheid, maar zonder informatieonderbouwing is die investering een slag in de lucht en disproportioneel.

Daar komt een tweede vraag bij. Als er geen dreigingsinformatie beschikbaar is, wat betekent dat dan? Betekent de afwezigheid van informatie dat er geen verhoogde dreiging is of is er simpelweg niets gedeeld? Het netwerk vraagt de rijksoverheid hier helderheid over te geven: er moet een minimale basiswaarde worden afgesproken die geldt als er geen actuele dreigingsinformatie beschikbaar is. Zo weten vitale partijen altijd op welk basisniveau ze moeten zijn voorbereid. De rijksoverheid wordt gevraagd een structureel informatiekanaal in te richten, afgestemd op de specifieke kwetsbaarheid en verantwoordelijkheid van vitale sectoren.

Concreet: De politie en KMAR verzamelen, delen en verrijken onderling al data die zij verzamelen over droneverkeer in Nederland. Voeg hier bijvoorbeeld stapsgewijs vertrouwde partijen aan toe. Maak bovendien juridisch mogelijk dat publieke en private partijen op regionaal niveau relevante data kunnen uitwisselen.

e. Risicoanalyse specifiek op drones verplichten op basis van de Wwke

[voorbereiding / object en cluster] Actiehouder: Vitale partijen in samenwerking met vakdepartementen en IenW, Defensie en JenV

De Wet weerbaarheid kritieke entiteiten (Wwke) verplicht partijen een risicobeoordeling uit te voeren en waar nodig passende en evenredige maatregelen te treffen, maar de invulling daarvan is open. De verplichting om in de risicoanalyse specifiek ook te kijken naar de mogelijke drone-dreiging, uitgevoerd door iedere kritieke entiteit op basis van een gestandaardiseerde methodiek, is een logische eerste stap. Het netwerk vraagt de rijksoverheid hiertoe een heldere methodiek beschikbaar te stellen. Bij de uitvoering van de risicoanalyse hebben bedrijven informatie en handvatten nodig vanuit de inlichtingendiensten als het bijvoorbeeld gaat om statelijke dreigingen. Vitale sectoren committeren zich aan het uitvoeren van de analyse en het delen van geaggregeerde uitkomsten ten behoeve van een gezamenlijk dreigingsbeeld.
Het verdient bovendien aanbeveling om ook partijen die niet zijn aangewezen als kritieke entiteit te verzoeken een risicoanalyse uit te voeren op mogelijke dronedreiging, als die partijen nauw samenwerken met partijen met belangrijke infrastructuur.

Hierbij is het Europese gelijke speelveld een belangrijk aandachtspunt. De stappen die Nederland zet op het gebied van verplichtingen en investeringen kunnen op gespannen voet staan met wat van Europese concurrenten wordt gevraagd. Het is van belang die balans te bewaken: ambitieus waar het kan, in lijn met het Europese kader waar het moet.

Aanvullend adviseert het netwerk om in één of twee (regionale) clusters een gezamenlijke stresstest uit te voeren, een instrument dat ook het Europese actieplan uitdrukkelijk aanbeveelt. Een stresstest maakt de vraag wanneer ben je weerbaar genoeg concreet en toetsbaar: wat gebeurt er als een drone boven dit cluster vliegt, wie reageert, hoe snel, en wat valt er in de keten weg? Mogelijk kan hierbij worden gedacht aan de inzet van een zogeheten “red team” (net zoiets als *white hat hackers*). De uitkomsten leveren het gedeelde feitelijke beeld op dat nu ontbreekt en dat investeringsbeslissingen kan onderbouwen. Het netwerk is bereid om de organisatie van een eerste pilot-stresstest actief te ondersteunen.

“

f. Nationaal protocol, regionale invoering

[besluitvorming en interventie / alle typen] Actiehouder: Rijk (IenW / JenV) voor de kaders; en vitale partijen voor de uitvoering

Uit de werksessies komt een helder organisatieprincipe naar voren: protocollen, standaarden en afspraken over data-analyse en data-uitwisseling, waaronder het bundelen van detectiedata uit verschillende bronnen, moeten nationaal worden vastgesteld, maar de operationalisering moet regionaal plaatsvinden. Vitale sectoren zijn bereid op regionaal niveau actief aan te sluiten. Bestaande lokale initiatieven kunnen relatief snel worden ingezet op andere locaties als helder is aan welke voorwaarden dit moet voldoen. Landelijk is het einddoel, regionaal is het beginpunt.

g. Expertisecentrum inrichten en kennisdeling structureel organiseren

[voorbereiding en bewustzijn / alle typen] Actiehouder: IenW, Defensie en JenV, vitale partijen en veiligheidsregio's gezamenlijk

De goede (Europese) voorbeelden zijn er, maar ze blijven geïsoleerd. Het netwerk committeert zich aan het actief delen van kennis, ervaringen en werkende oplossingen. Daarvoor is een structuur nodig die dat op duurzame wijze organiseert: een expertisecentrum, gedragen door vitale sectoren, de rijksoverheid, veiligheidsregio’s en kennisinstellingen gezamenlijk.
Het netwerk is expliciet over wat dit centrum moet zijn en wat niet. Een lichte netwerkorganisatie uitsluitend met overheidspartijen, zonder inhoudelijke verantwoordelijkheid en zonder betrokkenheid van vitale sectoren, is onvoldoende. Het centrum moet ambitieus worden opgezet, met vitale partijen als actieve deelnemers en medefinanciers, met een duidelijke inhoudelijke opdracht en met koplopers uit de sector in een expliciete rol. Zij beschikken over kennis die nu niet systematisch wordt benut.

Het Nationaal Cyber Security Center biedt een goed referentiemodel: dat doet op het gebied van cybersecurity precies wat het expertisecentrum op drones zou moeten doen. Het bundelt kennis, stelt die beschikbaar via een herkenbaar loket en helpt organisaties zich voor te bereiden op basis van hun specifieke situatie. Daarnaast is zeer recent het samenwerkingsverband GOPIN (Gezamenlijke Ontwikkelings- en Productiesamenwerking voor Integrated Air Missile Defence (IAMD) in Nederland) opgericht, waarin overheid, kennisinstellingen, academia en het bedrijfsleven samenwerken aan onderzoek en kennisontwikkeling voor een geïntegreerde lucht- en raketverdediging.

De scope van het beoogde expertisecentrum omvat nadrukkelijk ook de voorkant: best practices uitwisselen, kennis beschikbaar stellen, organisaties helpen bij risicoanalyses en hen wegwijs maken in het aanbod van gecertificeerde oplossingen. Het centrum fungeert als trechterpunt voor commerciële aanbieders en zorgt dat vitale entiteiten toegang hebben tot onafhankelijk advies over detectieapparatuur, countermeasures, fysieke weerbaarheidsmaatregelen en juridische kaders. Voor veiligheidsregio's biedt het een directe verbinding tussen nationale kennis en regionale uitvoering.
Het voorkomen van een nieuwe lappendeken is het expliciete doel. De NCTV is gelijktijdig met de start van het Versnellingsnetwerk begonnen met de coördinatie van een expertisecentrum CUAS. Het Versnellingsnetwerk adviseert hierbij; Neem het initiatief, zet het centrum stevig neer en betrek vitale sectoren en veiligheidsregio's actief bij inhoud en governance.

NB: Voor PNT bestaat een soortgelijke behoefte aan een expertisecentrum. We laten ter overweging van IenW hoe dit het best kan worden georganiseerd.

h. Pilotstrategie voor gecertificeerde private interventie: eerste cases identificeren

[interventie / object en cluster] Actiehouder: Rijk (JenV / IenW) samen met twee à drie koplopers uit het netwerk

Volgend uit doorbraakadvies 3 stelt het netwerk voor de verkenning van schaalbare interventiecapaciteit te starten met een gerichte pilot. Twee à drie vitale entiteiten, bij voorkeur in

“

de regio's waar ook de stresstesten worden uitgevoerd, passen onder gecontroleerde omstandigheden een eerste trede van gecertificeerde zelfbescherming toe. Daarbij wordt meegelift op de kennis van Defensie en wordt het concept van weerbaarheid als dienst verkend: gecertificeerde private partijen die onder strikte voorwaarden specifieke interventiestappen uitvoeren op eigen terrein.

De behoefte en volwassenheid verschillen per regio, dus de pilot begint waar de condities het meest gunstig zijn. Het netwerk vraagt de rijksoverheid geschikte pilotlocaties te identificeren en het bijbehorende juridische en governance-kader te ontwikkelen. De uitkomsten vormen de basis voor de bredere politieke discussie over de inrichting van het interventiestelsel.

3.5 Best practices: leren van wat werkt

De volgende voorbeelden uit het netwerk laten zien dat reeds een aantal initiatieven is ontplooid waarmee de andere leden uit het netwerk hun voordeel kunnen doen. Deze initiatieven tonen aan dat samenwerking werkt en dat partijen bereid zijn te investeren. Ze zijn nog niet systematisch gedeeld of opgeschaald, maar ze bieden concrete aanknopingspunten.

1. U-space Airspace Havenbedrijf Rotterdam

[cluster / detectie en duiding]

Waar Luchtverkeersleiding Nederland een groot deel van het bemande vliegverkeer beheert, ontbreekt voor het groeiende droneverkeer nog een vergelijkbaar landelijk stelsel voor het lage luchtruim. Het U-space Airspace Prototype van het Havenbedrijf Rotterdam laat zien hoe een havenbeheerder in een complex en veiligheidsgevoelig gebied meer grip kan krijgen op dit nieuwe domein. Door het lage luchtruim boven de haven te monitoren, ontstaat beter inzicht in wie of wat er vliegt, welke vluchten zijn toegestaan en waar sprake kan zijn van afwijkend of ongeautoriseerd gebruik. Daarmee draagt het systeem direct bij aan de beveiliging van de haven: Geautoriseerd droneverkeer wordt herkenbaar en beheersbaar, terwijl onbekend of verdacht vliegverkeer sneller kan worden geduid en opgevolgd door de daartoe bevoegde partijen. De waarde van het prototype ligt daarmee niet alleen in het faciliteren van nieuwe drone-toepassingen, maar juist ook in het versterken van toezicht, veiligheid en weerbaarheid in een vitale infrastructuur.

2. Publiek-private cameranetwerken haven en Schiphol

[cluster / bewustzijn en detectie]

Zowel bij het Havenbedrijf Rotterdam als bij Schiphol zijn publiek-private cameranetwerken operationeel die drone-activiteit in beeld brengen. De samenwerking tussen private beheerders en publieke partijen in de opzet en het beheer van deze netwerken is een voorbeeld van hoe gedeelde infrastructuur versnippering voorkomt. Een generiek meldprotocol en registratieprotocol is een voorwaarde om de informatie uit deze netwerken ook buiten de eigen organisatie bruikbaar te maken.

3. Samenwerking in Zeeland

In Zeeland heeft de Veiligheidsregio Zeeland een regierol gepakt door het beeld op te halen bij meerdere publieke en private partijen. Hierdoor konden waarnemingen vanuit verschillende partijen bij elkaar worden gelegd, werd het fenomeen duidelijk en kon het potentiële (en bedrijfsoverstijgende) risico worden geagendeerd.

4. Meldtools Stedin en Shell

[object / bewustzijn en detectie]

Stedin en Shell hebben eigen meldtools ontwikkeld waarmee medewerkers drone-waarnemingen kunnen registreren en doorgeven. Een eenvoudig, maar effectief instrument dat bewustzijn en detectie verbindt, en dat als basis kan dienen voor een breder gestandaardiseerd meldprotocol.

5. Pilot Dienst Justitiële Inrichtingen drone-overname

[object en cluster / interventie]

Dienst Justitiële Inrichtingen gaat een pilot uitvoeren, waarbij ongeautoriseerde drones kunnen worden verstoord. Dit is een voorbeeld van een technische interventieoptie waarbij vraagstukken rondom fysieke veiligheid (zoals het mogelijk neerkomen van de drone) en governance (welke bevoegdheden zijn nodig om een drone over te nemen) worden afgepeld. Dit is zeer relevant voor de discussie over wat private partijen zelf kunnen en mogen doen. De herijking van de vrijstellingsregeling voor afwijkend frequentiegebruik is een directe voorwaarde voor het legaal kunnen inzetten van dit soort technieken.

6. Pilot ANWB medisch transport Meppel-Zwolle

[netwerk / voorbereiding]

De ANWB-pilot, in samenwerking met een aantal publieke en private partijen, waaronder IenW, voor het transporteren van medisch weefsel via drones op de route Meppel-Zwolle laat zien dat geautoriseerde drone-inzet ook in open netwerken mogelijk is. In de pilot wordt onder meer geëxperimenteerd met het (juridisch) beheer van het luchtruim tot 150 meter, door de ANWB, terwijl tegelijk afstemming plaatsvindt voor uitzonderingen zoals de hulpdiensten. Alle haken en ogen die hierbij aan bod komen bieden voeding voor toekomstige pilots en mogelijke wet- en regelgeving. Dit voorbeeld illustreert bovendien de verbinding tussen kansen en dreiging: infrastructuur die voor geautoriseerde drones wordt ingericht, draagt ook bij aan het zichtbaar maken van ongeautoriseerde activiteit. Het netwerk vraagt om een landelijke visie op geautoriseerde drone-inzet als voorwaarde voor een coherente aanpak van ongeautoriseerde drones.

7. Pilot Rabobank

[object / bewustzijn en detectie]

Rabobank ziet dat drones voor de maatschappij en de eigen operationele veiligheid een groeiend risico zijn; Ongewenste observatie, in kaart brengen van kritieke processen, verstoring van bedrijfsvoering en processen, bedrijfsspionage, fysieke bedreiging van veiligheid en aantasting van privacy. Deze risico’s leiden tot schade aan de continuïteit, betrouwbaarheid en veiligheid van aangewezen kritieke infrastructuur van Rabobank.

Om huidige risico’s van drones rondom de kritieke locaties van Rabobank inzichtelijk te maken en om te bepalen of een real-time detectiesysteem van toegevoegde waarde is, is Rabobank in Q1 2026 gestart met de pilot real-time drone detectie. Met de pilot wordt in de praktijk onderzocht hoe vaak, op welke manier en met welk doel drones rondom de campus worden ingezet. Het drone-detectiesysteem maakt het namelijk mogelijk om drone-activiteiten real-time te detecteren en te beoordelen. Bovendien biedt het de mogelijkheid om snel diverse acties op te ondernemen.

Op basis van deze informatie kan Rabobank een weloverwogen keuze maken in beleid en praktijk met betrekking tot systematische, effectieve inzet van drone-detectie. En het levert ook data om beperkende maatregelen, zoals een no-fly zone aanvragen, te nemen. De pilot draagt daarmee bij aan een proactieve aanpak van veiligheid, digitale weerbaarheid en continuïteit van Rabobank, passend bij de huidige maatschappelijke verwachtingen en het internationale dreigingsbeeld.

Thema II

Plaats-, navigatie en tijdsbepaling (PNT)

4. Analyse: Hoe het netwerk naar het PNT-vraagstuk kijkt

4.1 De kern: een onzichtbare fundering waarop bijna alles leunt

PNT (Plaats-, Navigatie- en Tijdsbepaling) is in dertig jaar tijd de onzichtbare fundering geworden waarop vrijwel alle vitale processen in Nederland leunen: energievoorziening, telecom, mobiliteit, waterbeheer, chemische processen, financiële transacties en overheidsdiensten. De oorzaak hiervan is digitalisering: soms zijn de primaire processen gedigitaliseerd (bijvoorbeeld het geldverkeer), maar bij veel fysieke processen is de besturing ervan gedigitaliseerd (zoals energie, transport en logistiek, luchtverkeer en communicatie door nooddiensten). Dat heeft de afgelopen decennia de efficiëntie en de productiviteit enorm vergroot tegen relatief lage kosten. Het signaal van satellietsystemen als Galileo en GPS is gratis, eenvoudig te ontvangen en wordt in het algemeen als betrouwbaar ervaren. Het gemak en de vanzelfsprekende beschikbaarheid van bijvoorbeeld navigatie-informatie heeft ongemerkt de afhankelijkheid ervan grotendeels onzichtbaar vergroot. Vanwege deze afhankelijkheid is PNT in 2017 aangewezen als vitaal proces en bij de wettelijke herijking in 2025 opnieuw bevestigd. De Inventarisaties Kwetsbaarheden Uitval Satellietnavigatie (IKUS I in 2016, IKUS II in 2022) brachten de kwetsbaarheden in kaart en concludeerden steeds dat het besef en de kennis bij gebruikers moeten verbeteren. Dit Versnellingsnetwerk bouwt daarop voort en richt zich op het bestuurlijk adresseren ervan.

De opdracht aan het netwerk laat zich samenvatten in één vraag:

"Hoe borgen partijen de continuïteit van vitale processen in Nederland bij verstoring, uitval of manipulatie van plaats-, navigatie- en tijdsbepaling?"

Omdat dit vraagstuk meerdere vitale processen tegelijkertijd raakt, heeft PNT-uitval het karakter van een systeemvraag. Het meest sprekende historische precedent is de millenniumproblematiek (Y2K). Ook daar werd een technisch ogenschijnlijk probleem omgezet in een gezamenlijke verantwoordelijkheid van vitale sectoren en overheid en mede daardoor zijn de gevreesde verstoringen uitgebleven. De lessen uit die periode zijn relevant: heldere nationale regie en bestuurlijke urgentie, sterke publiek-private samenwerking door gezamenlijke verantwoordelijkheid, concrete inventarisaties en ketenanalyses, oefenen en scenariodenken, zodat de inhoud tastbaar wordt en bewustwording met handelingsperspectief zijn onmisbaar. Net als bij Y2K gaat het bij het PNT-vraagstuk om een verstoring die potentieel de hele samenleving kan ontwrichten. Als telecom- en internetverbindingen uitvallen vallen economische processen stil doordat betalingssystemen niet werken, hulpdiensten zijn onbereikbaar en cruciale logistieke infrastructuur wordt ernstig beperkt doordat bijvoorbeeld bruggen en sluizen niet meer te bedienen zijn. Een serieuze PNT-verstoring heeft door de verknoping van ICT enorme keteneffecten en kan de besturing van hele ketens platleggen.

Door de 'hybride' wereld tussen oorlog en vrede waarin we terecht zijn gekomen en de technologische verknoping is het opzettelijk verstoren van GNSS-signalen (Global Navigation Satellite System), zoals die van Galileo en GPS, steeds laagdrempeliger geworden. Soms gebeurt dat 'lokaal', zoals verstoringen rondom het vliegverkeer laten zien. In conflictgebieden is verstoring van GNSS routinematig; Nederland en zeven andere EU-landen hebben in 2025 een gezamenlijke VN-klacht ingediend over Russische satellietinterferentie. Het GNSS-monitoringonderzoek op vier

“

Nederlandse vitale locaties (Schiphol, Havenbedrijf Rotterdam, Stedin en het Nationaal Metrologisch Instituut (VSL)) heeft in een korte meetperiode 77 verstoringen geregistreerd die als waarschuwing of alarm zijn geclassificeerd. De Europese Commissie heeft Galileo expliciet als kritieke ruimtevaartinfrastructuur benoemd. Versnelling van de weerbaarheid van PNT is dus dringend nodig.

4.2 Wat dit vraagstuk wezenlijk anders maakt

Het PNT-vraagstuk vertoont de typische kenmerken van ‘cyberveiligheid’. In ten minste vier opzichten is dit vraagstuk wezenlijk anders dan veel andere veiligheidsopgaven en dan het drone-vraagstuk uit Thema I.

Onzichtbare systeemafhankelijkheid

Anders dan bij drones is er niet één fysiek object om naar te wijzen, zowel voor wat betreft de dreiging als voor wat betreft het te beschermen ‘asset’. Er zijn zeker ‘fysieke’ plekken waar informatie over tijd, positie en navigatie wordt geproduceerd, zoals satellieten, grondstations (Nederland huisvest een op Bonaire en een in Noordwijk) en ontvangers. Omdat voor het gebruik van satelliet-informatie voor gebruikers niet meer nodig is dan een ontvanger en de informatie vrijelijk beschikbaar is, is dit een hedendaags voorbeeld van een “nutsvoorziening”, onmisbare infrastructuur; Het moet altijd beschikbaar zijn en is maatschappelijk cruciaal. Niet voor niets is bij nutsvoorzieningen de rol van de overheid altijd sterk geweest: continuïteit is dan niet afhankelijk van een kosten-opbrengstencalculatie, maar van een betrouwbare beschikbaarheid zodat de voorziening voor iedereen beschikbaar is (‘universal access’).

Aan continuïteit, redundantie en toezicht worden dan ook terecht hoge eisen gesteld, zoals we dat ook zagen bij het bankverkeer tijdens en na de financieel-economische crisis in 2007/2008. Bij dit type ‘onzichtbare vanzelfsprekendheden’ wordt de noodzaak pas zichtbaar wanneer een PNT-verstoring optreedt. Een sprekend voorbeeld is de NAFIN-storing bij Defensie, waarbij een ogenschijnlijk zelfstandig tijdsynchronisatieprobleem ernstige netwerkstoringen veroorzaakte. Hulpdiensten waren beperkt bereikbaar, Eindhoven Airport lag urenlang stil, DigiD werkte niet goed en een aantal gemeenten kon burgers niet helpen, omdat inlog- en registratiesystemen uitvielen. Zo zal een PNT-uitval ook doorwerken via daaropvolgende uitval of compromittering van andere systeemdiensten; het is bij uitstek een voorbeeld van een cascade-effect. De Onderzoeksraad voor Veiligheid heeft eerder de complexiteit en de impact laten zien van ICT-uitval in ziekenhuizen, waarbij de raad vooral aanbeveelt veelvuldig te oefenen met dit scenario.

PNT kan daarmee worden beschouwd als een ‘supra-infrastructuur’ waarvan vrijwel alle vitale voorzieningen in meer of mindere mate afhankelijk zijn. Daarmee is bewustwording in dit dossier geen begeleidende activiteit, maar de eerste opgave. Die onzichtbaarheid geldt ook voor de afhankelijkheden zelf: zelfs goed geïnformeerde organisaties weten vaak niet hoe hun systemen en processen precies op satellietsignalen leunen.

Universele afhankelijkheid

PNT-verstoring raakt vrijwel alle vitale sectoren tegelijk: energie, financiën, telecom, transport, water, voedsel. Een verstoring is overal op hetzelfde moment een feit en merkbaar, en heeft andere consequenties dan een sectorale dreiging. Dat verandert de operationele dynamiek fundamenteel: niet sectoraal opvangen, maar in samenhang doordenken.

Integriteit weegt zwaarder dan beschikbaarheid

Voor PNT-toepassingen is zowel de beschikbaarheid van het signaal als de integriteit ervan kritisch. Een systeem dat geen signaal heeft, schakelt over op back-up of werkt volgens de ontworpen noodprocedure. Een systeem dat een ‘gespoofd’ signaal vertrouwt, kan zonder waarschuwing verkeerde beslissingen nemen. Verkeerde informatie is in de meeste gevallen erger dan geen informatie. Daarin ligt ook een rol voor ‘legacy’-systemen: een ‘instrument landing system’ of een

“

atoomklok die al decennia bestaat en niet op satelliet leunt, kan precies dat referentiepunt zijn waartegen een ontvanger controleert of het signaal klopt. Het is de aanwezigheid van zo’n onafhankelijk referentiepunt dat ‘spoofing’ detecteerbaar maakt. Dat heeft directe consequenties voor mitigatie: authenticatie (zoals via Galileo PRS), redundantie, kruisvalidatie tussen meerdere bronnen en monitoring zijn belangrijker dan enkel ruwe beschikbaarheid. Celeste is hierbij een voorbeeld van een satelliet die als aanvulling op Galileo in een lage aardbaan wordt ontwikkeld door de European Space Agency (ESA), waarbij de Nederlandse Space Agency de Nederlandse belangen voor ogen houdt. Celeste zal sterkere signalen geven en hierdoor minder vatbaar zijn voor ‘spoofen’ en ‘jammen’.

Voor de component tijd geldt vaak dat de back-up afwezig of zeer beperkt is; Zonder referentie ontbreekt de tijdsynchronisatie en zal in geval van noodzakelijke communicatie met systemen/servers/software buiten het eigen tijdnetwerk per direct verstoring en/of uitval plaatsvinden. Op serverniveau is dat zeker binnen 5 uur en bij gevoeliger datacommunicatie eerder.

Cascade-tempo in uren en dagen, niet seconden

Waar het drone-vraagstuk een reactietijd in seconden vraagt, ontvouwt de impact van PNT-verstoring zich voor plaatsbepaling en navigatie exponentieel in tijd. Maatschappijbreed is in het eerste uur de schade beperkt; tussen zes en tweeënzeventig uur verschuift het probleem van technisch naar organisatorisch, en worden de problemen meer systemisch; daarna stapelen de cascade-effecten zich. Daarmee verschuift de operationele opgave van detectie en interventie naar redundantie, *business continuity*, triage en herstel. Omdat de besturing van processen en ketens helemaal gedigitaliseerd is, kunnen processen en ketens korte tijd nog gebruik maken van ‘bypasses’, maar naarmate de verstoring langer duurt neemt de ontwrichting exponentieel toe. De effecten van uitval van tijd zijn vrijwel direct zichtbaar.

4.3 Drie functies, één onderlaag: plaats, navigatie en tijd

PNT werkt omdat satellieten extreem nauwkeurige tijdsignalen uitzenden. Door te meten hoe lang zo'n signaal onderweg is, weet een ontvanger waar hij zich bevindt en in welke richting hij beweegt. Tijd is daarmee niet één van de drie functies, maar de fundering onder alle drie.

Plaatsbepaling is kritisch voor wie precies moet weten waar iets of iemand zich bevindt: treindienstleiders, kustwacht, loodswezen, hulpdiensten op afgelegen locaties. Navigatie raakt aan het bewegen door de fysieke ruimte: havens, luchthavens, wegverkeer en defensie. Tijd is het meest fundamentele en tegelijk het meest verborgen onderdeel. Het ligt niet alleen onder positie en navigatie, maar ook onder vrijwel alle digitale ketens: tijdstempels in financiële transacties, synchronisatie van 5G-netwerken en servers, herkenning tussen systemen en netcongestiebesturing in het elektriciteitsnet. Zonder gedeelde tijd vallen systemen binnen minuten stil.

Wat de werksessies duidelijk maakten: de T(ijd) was voor veel aanwezigen een echte openbaring. Sectoren als luchtvaart, telecom en energie herkenden hun kwetsbaarheid op tijdsynchronisatie veel directer dan op plaatsbepaling of navigatie. Dat maakt tijd tot de gemeenschappelijke noemer die alle sectoren verbindt, en daarmee tot het meest logische startpunt voor bewustwording en actie.

Een belangrijk onderscheid daarbij is dat systemen die vóór de brede introductie van GPS zijn gebouwd, grofweg vóór 2000, door hun ouderdom vaak robuuster zijn: ze draaien bij uitval gemakkelijker terug op methoden die niet van satelliet afhangen. In de luchtvaart is dat zichtbaar: het ILS-systeem, een grondgebonden radiobaken dat vliegtuigen begeleidt bij de nadering en landing en al meer dan veertig jaar in gebruik is, functioneert als cruciaal terugvalsysteem juist omdat het nooit is uitgeschakeld. Die les is breed toepasbaar. Bestaande (back-up-) systemen die niet op GNSS leunen verdienen bescherming. Waar ze zijn afgeschakeld, verdient heractivering serieus onderzoek.

“

Daarnaast verdienen elektriciteit en telecom daarbinnen een aparte vermelding. Voor beide sectoren is de infrastructuur sterk afhankelijk van nauwkeurige tijdsynchronisatie. Bij elektriciteit wordt tijd gebruikt voor balansbesturing en de coördinatie van het netwerk. Bij verstoring van PNT valt eerst de optimalisatie weg, wat kan leiden tot capaciteitsreductie en uiteindelijk instabiliteit van delen van het net. Ook telecomnetwerken zijn afhankelijk van uiterst nauwkeurige tijdsynchronisatie voor het functioneren van mobiele netwerken, dataverkeer en de afhandeling van communicatie tussen zendmasten en netwerken. Zonder betrouwbare tijdsinformatie kunnen delen van mobiele communicatie en internetverbindingen ontregeld raken of uitvallen. Daarmee worden niet alleen burgers en bedrijven direct getroffen, maar ook vitale processen zoals betalingsverkeer, hulpdiensten en logistieke aansturing. Tegelijkertijd is vrijwel alles in dit dossier op zijn beurt afhankelijk van elektriciteit en telecom. Die dubbele rol, zowel slachtoffer als doorgeefluik, maakt elektriciteit en telecom tot de meest kritieke knooppunten in de cascadeketen.

4.4 Wat het netwerk heeft opgehaald: zeven patronen

Over de drie functies heen ziet het netwerk een aantal terugkerende patronen die richting geven aan de dilemma’s en de opbrengst hierna.

Bewustwording is de eerste opgave en het grootste laaghangende fruit

In tegenstelling tot drones, waar de dreiging zichtbaar en tastbaar is, vraagt PNT eerst om het zichtbaar maken van de eigen afhankelijkheid. In beide werksessies bleek dat ook ervaren vitale partijen niet altijd weten hoe lang hun kritieke systemen zonder tijdsynchronisatie kunnen doordraaien en welke processen in hun eigen organisatie precies op satellietsignalen leunen. Organisaties geven aan begeleiding en advisering op dit vlak te verwelkomen. Het PNT-portaal van het Centre of Excellence PNT (pntportal.eu), dat in opdracht van IenW is ontwikkeld in samenwerking met ESA en de Netherlands Space Agency (NLSA), biedt voor die basislaag masterclasses, een *Resilience Assessment Tool* langs zeven categorieën en gestructureerde mitigatiestrategieën. Daarmee is het een waardevolle vervolgstap voor organisaties die hun bewustwording willen omzetten in gestructureerde actie.

Just-in-time was rationeel in vredestijd, just-in-case is nodig ten tijde van hybride oorlogsvoering

Onze ketens zijn decennialang verfijnd op efficiëntie. Voorraden zijn afgebouwd, redundantie is uit kostenoverwegingen weggesneden. Dat is rationeel zolang de onderlaag betrouwbaar is, maar het maakt de keten kwetsbaar zodra die onderlaag wegvalt. De omslag naar bewuste redundantie, in de woorden van het netwerk: van just-in-time naar just-in-case, is daarmee een strategische opgave en geen technische afweging. Daarmee komt direct de vraag: aan wie is het om die redundantie aan te leggen, en wie betaalt?

Integriteit boven beschikbaarheid

‘Spoofing’ (overnemen van het signaal, inclusief de mogelijkheid om het signaal te veranderen en daarmee onjuiste informatie door te geven) is een grotere dreiging dan ‘jamming’ (verstoren van het signaal), omdat een ontvanger een vals signaal voor waar aanneemt en de gebruiker zich daardoor niet bewust is van de verstoring. Dat maakt authenticatie van het signaal (onder andere door gebruik van Galileo PRS, het beveiligde Galileo signaal voor het gebruik bij overheids-, vitale en crisisgevoelige diensten), kruisvalidatie tussen meerdere bronnen als onderdeel van een ‘system of systems’-benadering, en monitoring van het radiospectrum belangrijker dan enkel ruwe beschikbaarheid. Het is een belangrijk uitgangspunt voor mitigatie. Voor de component tijd is zowel de beschikbaarheid als de integriteit zeer belangrijk in dit vraagstuk.

Wanneer ben je weerbaar genoeg blijft een open vraag onder Wwke en Cbw

De Wet weerbaarheid kritieke entiteiten (Wwke) en de Cyberbeveiligingswet (Cbw, implementatie NIS2) stellen open normen. PNT valt niet onder de Wwke, omdat er geen sprake is van Nederlandse

“

entiteiten; EUSPA is beheerder, eigenaar en exploitant van de grondsystemen. Entiteiten die wel onder de Wwke en Cbw vallen weten echter niet wat er van hen wordt verwacht op PNT-vlak. Hetzelfde geldt voor toezichthouders en ketenpartners, zij missen een gedeelde maat. Maar de vraag is ook: aan wie is het eigenlijk om dat te beoordelen? Aan de entiteit zelf, aan de toezichthouder, aan de sector, of aan de keten gezamenlijk?
Die onduidelijkheid is geen detail: wie kiest voor een lager weerbaarheidsniveau brengt door de onderlinge afhankelijkheid via het cascade-effect onbedoeld de continuïteit van anderen in het geding en daarmee het nationale belang. Weerbaarheid is daardoor per definitie een gezamenlijke opgave, niet een individuele afweging. Kaderstelling op het niveau van de entiteit, de keten en minimale continuïteitseisen bij aanbestedingen is nodig om die gedeelde verantwoordelijkheid hanteerbaar te maken.

Binnen de implementatie van de Wwke moet uitval en manipulatie van PNT expliciet als dreiging meegenomen worden als onderdeel van de zorgplicht. Zo wordt het een verplicht onderdeel van de beoordeling van relevante risico’s binnen vitale sectoren. Op deze wijze is de bewustwording beter verankerd en ontstaat een beter gedeeld kader voor organisaties, toezichthouders en ketenpartners wanneer de weerbaarheid tegen PNT verstoringen voldoende is. Dit zal dan leiden tot kaderstelling op het niveau van de entiteit, de keten en minimale continuïteitseisen bij aanbestedingen die nodig is om de gedeelde verantwoordelijkheid hanteerbaar te maken.

Versnipperde regie staat versnelling in de weg

Het PNT-dossier raakt minimaal vier ministeries en bevindt zich daardoor zonder helder loket. Voor het bedrijfsleven kan dat verlammend zijn: er is geen langetermijnvisie waar partijen op kunnen aansluiten, geen duidelijke trekker, geen integraal investeringsplan. Één interdepartementale trekker met mandaat is een voorwaarde voor beweging.

Crisismindset is verwaterd; the best we can get vraagt om mentale en juridische voorbereiding nu

We zijn comfortabel geworden met PNT die altijd werkt. Afgeleid daarvan zijn we gewend aan hyperefficiënte en altijd beschikbare systemen, waardoor we geen rekening meer houden met uitval of verrassingen en wat we dan moeten doen. Calamiteitenplannen besteden weinig aandacht aan deze afhankelijkheid en onzekerheid en de bereidheid om echt te oefenen - te durven afschalen of de stekker er eens uit te trekken - is verwaterd. Waar veel organisaties wel oefenen met stroomstoringen en daarvoor (nood)voorzieningen hebben ontwikkeld, is dat voor ICT-uitval nog veel minder het geval. Tegelijk is duidelijk dat in een verstoringssituatie het maximaal haalbare leveren beter is dan niet leveren, ook als dat betekent dat bestaande regels naar beste vermogen moeten worden gehanteerd. Dat principe en de daaraan gekoppelde triage vragen om kaderstelling en oefening voordat de crisis er is. Het concept triage impliceert hier niet zozeer schaarste aan het GNSS-signaal zelf, maar aan de redundantie die nodig is om zonder dat signaal te functioneren: reserveklokken, noodgeneratoren, alternatieve tijdsdistributie en terugvalprocedures zijn schaarse middelen die een verdringingsreeks rechtvaardigen.

Effectieve weerbaarheid vraagt meer dan compliance

Een terugkerend inzicht in de gesprekken is dat wettelijke naleving niet per definitie hetzelfde is als effectieve weerbaarheid. Diverse cases laten dat zien: volledig compliant met alle wetgeving, en toch waren er fouten die de samenleving raakten. Normen en afvinklijsten geven houvast, maar de werkelijke weerbaarheid wordt bepaald door de vraag of bestuurders en anderen het thema persoonlijk doorleven en erdoor gestuurd handelen. Dat vraagt iets van de bedrijfscultuur en van bestuurlijke verantwoordelijkheid: PNT moet als thema op de agenda van de raad van bestuur komen, niet als compliancepost, maar als strategische afweging. Bewustwording leidt pas tot investering als het de boardroom bereikt.

5. Opbrengst

5.1 De aard van de opbrengst

De opbrengst van het PNT-traject heeft een ander karakter dan die van drones. Bij drones laat het vraagstuk zich operationeel ordenen langs een matrix met diverse concrete handelingen. Bij PNT staat de systemische afhankelijkheid centraal: de dilemma's, doorbraakadviezen en actievoorstellen draaien niet om operationeel ingrijpen, maar om de vraag hoe verantwoordelijkheid, regie en investering bestuurlijk belegd moeten worden om een onzichtbare kwetsbaarheid hanteerbaar te maken.

Hieronder volgen achtereenvolgens de dilemma's die uit de analyse direct voortvloeien (paragraaf 5.2), de doorbraakadviezen die het netwerk aan de bewindspersonen voorlegt (paragraaf 5.3), de actievoorstellen die binnen bestaande kaders al in gang gezet kunnen worden (paragraaf 5.4) en de best practices waar Nederland nu al op kan voortbouwen (paragraaf 5.5).

5.2 Dilemma's: waar keuzes onvermijdelijk zijn

De volgende dilemma's zijn geen technische of organisatorische problemen die met een protocol op te lossen zijn. Ze raken aan fundamentele keuzes over verantwoordelijkheid, regie en risicoacceptatie, en moeten bestuurlijk en politiek gewogen worden. Het netwerk benoemt ze expliciet, omdat ze zonder die explicitering blijven hangen.

Dilemma 1: Wanneer ben je weerbaar genoeg? Open norm, investeringsplicht en ketenafhankelijkheid

Volgt uit: bewustwording, open normering, just-in-case

De Wwke en de Cbw stellen open normen. Zoals eerder vermeld valt PNT formeel niet onder de Wwke, maar wordt van entiteiten die als "kritiek" zijn bestempeld wel verwacht dat zij uitval en verstoring van PNT als dreiging meenemen in hun zorgplicht. Dit leidt tot fundamentele vragen: Waar investeer je op, wat moet kunnen doordraaien en hoe? Wanneer ben je weervaar genoeg en wie bepaalt dat eigenlijk? De entiteit zelf, de toezichthouder, of de keten? Want weerbaarheid is geen individuele opgave. Een luchthaven, een luchtvaartmaatschappij en de luchtverkeersleiding moeten tegelijk weerbaar zijn; als één schakel wegvalt, heeft het geheel geen zin. Wie individueel een lager weerbaarheidsniveau kiest, raakt via het cascade-effect de continuïteit van anderen.

Voor PNT komt daar een extra spanning bij. De overheid vraagt om weerbaarheid, maar een groot deel van de benodigde oplossingen vraagt om publieke investering die nog niet is belegd. Deelnemers omschrijven dat treffend als een verzekeringspremie: hoog, onzeker van nut, maar te laat te betalen op het moment dat het misgaat. Hoe hoog die premie mag zijn verschilt per entiteit en per maatschappelijke functie, en vraagt daarom een antwoord op drie niveaus: het bestuur van de entiteit, de toezichthouder per sector en de politiek voor wat collectief wordt gedragen. Zonder die gelaagde governance blijft de open norm een loze verplichting.

Dilemma 2: Centralisatie als oplossing en als kwetsbaarheid

Volgt uit: universele afhankelijkheid, tijd als onderlaag

PNT-weerbaarheid vraagt om gecoördineerde oplossingen, maar elke poging tot centralisatie roept het risico op dat de gecreëerde infrastructuur zelf een kritiek doelwit wordt. Dit dilemma speelt niet alleen bij een nationaal tijdnetwerk, maar bij elke PNT-voorziening die op centrale knooppunten leunt. Vanuit het denken in termen van een nutsvoorziening is centrale coördinatie logisch en legitiem, maar de uitvoering vraagt om een federatief model met voldoende redundantie, geografische spreiding en robuuste knooppunten. Tegelijkertijd centraliseren van de coördinatie en decentraal aanbieden van PNT-voorzieningen is hier het devies. De belangrijkste keuze die voorligt,

“

ligt op dit moment bij de overheid: in hoeverre beschouwt de overheid PNT daadwerkelijk als een nutsvoorziening waarvan de continuïteit moet worden geborgd en waarvoor de overheid zelf de verantwoordelijkheid wil nemen? Vanuit het nemen van verantwoordelijkheid voor de continuïteit kan in de uitvoering dan vervolgens gebruik worden gemaakt van private oplossingen voor redundantie. Een tweede laag is dat de (rijks)overheid bij centrale infrastructuur normsteller, eigenaar en toezichthouder tegelijk dreigt te worden: die drie rollen moeten expliciet worden onderscheiden en op elkaar afgestemd. Het netwerk vraagt het kabinet om dit dilemma bij de uitwerking van publieke PNT-voorzieningen expliciet bestuurlijk te adresseren.

Dilemma 3: Marktordening en aanbestedingsregels versus publiek belang

Volgt uit: just-in-case, versnipperde regie

De geopolitieke urgentie van dit moment rechtvaardigt een fundamentele vraag: in hoeverre kunnen markt en overheid, binnen de huidige kaders van aanbestedingsrecht en level playing field, op het benodigde tempo samen optrekken om Nederland weerbaar te maken? Partijen uit het netwerk geven aan dat de gezamenlijke aanleg van publieke PNT-infrastructuur nu stuit op aanbestedings- en mededingingsregels die samenwerking eerder belemmeren dan bevorderen. Dat knelpunt is niet uniek voor PNT, maar hier raakt het direct aan nationale veiligheid. Het netwerk vraagt het kabinet om na te gaan of vraagstukken van vitaal nationaal belang rechtvaardigen dat de balans tussen markt en overheid opnieuw wordt gewogen, en of gerichte intensivering van publiek-private samenwerking, ook als dat scherper aan de wind zeilen betekent op het punt van aanbestedingsrecht, hier geboden is.

Dilemma 4: Triage en risicoacceptatie: durven kiezen wat we niet doen

Volgt uit: cascade-tempo, the best we can get, crisismindset

Een terugkerend punt in beide werksessies was de vraag: wat ga je als overheid niet doen en welke risico’s accepteer je expliciet? Niet elk proces kan worden gered, niet ieder incident kan worden voorkomen. Een verdringingsreeks tussen en binnen vitale sectoren, vergelijkbaar met de prioritering die in andere crisisdomeinen wel bestaat, ontbreekt voor PNT. Het meebewegen van wetgeving onder het principe ‘the best we can get’ is daarvan een onlosmakelijk onderdeel: in welke situatie kunnen welke normen tijdelijk opzij worden gezet, op welk gezag en met welke verantwoording? Het netwerk vraagt het kabinet om deze keuzes niet te ontwijken. Het benoemen van geaccepteerde restrisico’s versterkt de geloofwaardigheid van de wel gekozen weerbaarheidsmaatregelen.

Dilemma 5: Wat communiceer je en wat niet

Volgt uit: integriteit boven beschikbaarheid, bewustwording

Voor PNT geldt scherper nog dan voor drones dat transparantie en terughoudendheid bij het delen van informatie op gespannen voet staan. Openheid over kwetsbaarheden helpt bij bewustwording en bij het mobiliseren van investeringen. Dezelfde openheid geeft echter potentiële tegenstanders inzicht in zwakke schakels. Deelnemers wezen erop dat absolute terughoudendheid leidt tot een illusie van veiligheid en de urgentie bij bestuurders onvoldoende zichtbaar maakt. Het netwerk vraagt het kabinet om een afgewogen communicatielijn te ontwikkelen, waarbij actieve duiding van risico’s in algemene zin samengaat met meer gerichte en vertrouwelijke informatiedeling met vitale sectoren.

Dilemma 6: Nederland als eiland of als Europese speler

Volgt uit: universele afhankelijkheid, geopolitieke urgentie

PNT kent geen landsgrenzen. Schepen, vliegtuigen, pijpleidingen en elektriciteitsnetwerken werken over grenzen heen en een Nederlandse aanpak die niet aansluit op Europese ontwikkelingen mist effect. Galileo is een Europees systeem, GPS is Amerikaans. De relatie met, en invloed op, ESA en de EU Agency for the Space Programme (EUSPA) door de NLSA en Ministerie van IenW op de doorontwikkeling van Europese PNT in de vorm van Celeste en PRS vraagt daarom hoge prioriteit.

“

Tegelijkertijd is snelle Europese consensus moeilijk, en is niet elke maatregel die PNT-weerbaarheid versterkt per definitie een Europese aangelegenheid. Concrete voorbeelden laten zien hoe nabuurlanden verder zijn: het Verenigd Koninkrijk heeft een PNT Office met Defensie als co-eigenaar; Duitsland werkt via zijn nieuwe ruimteministerie aan alternatieven voor GNSS; de luchthaven Brussel heeft via het gezamenlijke bedrijf Skeyes al een geïntegreerd drone- en luchtruimbeheerssysteem operationeel. Nederland kan en moet op bepaalde bouwstenen nationaal voortvarend doorpakken, maar heeft er ook baat bij van deze ervaringen te leren. Het netwerk vraagt het kabinet om een dubbel spoor te kiezen: nationaal doorpakken op bouwstenen die geen Europese coördinatie vragen en parallel actief de Europese agenda mede vormgeven.

5.3 Doorbraakadviezen

Uit de dilemma’s en de patronen die in de analyse zijn benoemd, destilleert het netwerk een beperkt aantal doorbraakadviezen. De doorbraken zijn nodig om juist andere acties mogelijk te maken en daarmee verdere stilstand te voorkomen. Ze vragen om politieke besluitvorming en zijn niet op te lossen binnen bestaande kaders. Het netwerk legt ze voor aan u als bewindspersonen als de kern van dit advies.

Het PNT-vraagstuk heeft een fundamenteel agendasettingprobleem. De kwetsbaarheid is onzichtbaar, de verantwoordelijkheid is versnipperd over ministeries, en bestuurders in vitale sectoren worden niet gedwongen positie te nemen. Zolang deze drie condities bestaan, bewegen organisaties en overheid onvoldoende.

Doorbraakadvies 1: Kwalificeer PNT als nutsvoorziening

Aan: Kabinet

PNT is de onzichtbare fundering onder vrijwel alle vitale processen. Dit kwalificeert PNT tot een onmisbare basisvoorziening van algemeen nut, vergelijkbaar met gas, water, elektriciteit en telecommunicatie. Hoe groot dit punt is wordt geïllustreerd door het feit dat niemand de uitval van PNT in de praktijk durft te testen, de gevolgen zijn simpelweg te groot. Dit legitimeert dat de rijksoverheid niet alleen eisen stelt, maar ook verantwoordelijkheid neemt voor de infrastructuur die de markt niet zelf aanlegt. Dat vraagt één coördinerend ministerie met mandaat, middelen en een langetermijnvisie. Zolang meerdere ministeries dit dossier delen zonder helder eigenaarschap, weet het bedrijfsleven niet waar het moet aankloppen en kan het de eigen investeringsbeslissingen niet afstemmen op wat de rijksoverheid gaat doen.

Doorbraakadvies 2: Breng PNT in de boardroom en bescherm de basis

Aan: Vitale partijen

Bewustwording werkt pas als bestuurders het thema persoonlijk doorleven, er intern verantwoordelijkheid voor nemen en PNT expliciet opnemen in het plan voor de bedrijfscontinuïteit. Dat is een opgave voor de organisaties zelf: een bestuursbesluit over weerbaarheidsambities, een intern aanspreekpunt en een moment van zelfevaluatie. Het netwerk vraagt het kabinet om die stap te ondersteunen met een verplicht bestuurlijk bewustwordingsmoment voor kritieke entiteiten, analoog aan de verplichte cyberbewustwordingsopleiding die in de financiële sector al bestaat.

Doorbraakadvies 3: Organiseer ‘backup-opties’ die niet afhankelijk zijn van satelliet-informatie

Aan: Kabinet en vitale partijen

Uitvoering van de eerste twee doorbraakadviezen levert een robuust netwerk op dat PNT-informatie borgt en bij uitval bijdraagt aan snel herstel. Toch moet er gezien de dreiging van worden uitgegaan dat PNT-uitval in de (nabije) toekomst een reëel scenario is, hoe robuust het (digitaal) netwerk ook is. Er ligt daarom een eigen investeringsopgave: systemen die niet op satellietsignalen leunen zijn de meest directe route naar redundantie. Bestaande systemen verdienen bescherming. Systemen die zijn afgeschakeld, zoals cesiumklokken bij energiebedrijven of grondgebonden navigatie-

infrastructuur, verdienen heroverweging. Die keuzes en de bijbehorende investeringen zijn aan de organisaties zelf. Zoals ook oefeningen en onderzoek naar cyberuitval in brede zin leren, moet dan kunnen worden teruggevallen op een werkelijkheid waarin vitale processen min of meer 'ongestoord' doorgang kunnen vinden ook zonder de beschikbaarheid van digitale hulpmiddelen.

Soms zijn daarvoor vertrouwde, maar technologisch geavanceerde middelen nodig als atoomklokken, de systemen die in de luchtvaart gebruikelijk zijn of die in havens voor verkeersgeleiding worden gebruikt. In andere situaties volstaat een 'protocol' of een stelsel van afspraken over hoe te handelen, waarbij de afhankelijkheid van digitale precisiehulpmiddelen niet nodig is. Zo houdt de NS rekening met 'speling' van enkele minuten; bij uitval kan dan een blik op het horloge van de machinisten volstaan, omdat het niet op seconden aankomt en horloges doorgaans niet binnen enkele dagen minuten achter of voor lopen.

Oefenen in netwerkverband, vastleggen van de lessen en kwetsbaarheden en op basis daarvan 'backup-opties' organiseren die niet afhankelijk zijn van satelliet-informatie is niet alleen dringend nodig, maar in veel organisaties en sectoren al gebruikelijk. Door deze oefenpraktijken en protocollen 'op te tillen' naar het niveau van netwerken worden vitale processen veel minder kwetsbaar voor PNT-uitval.

Doorbraakadvies 4: Investeer in een nationaal tijdnetwerk

Aan: Kabinet

Van alle kwetsbaarheden in het PNT-dossier is tijdsynchronisatie de meest urgente, omdat vrijwel alle vitale sectoren er direct van afhankelijk zijn en er nu geen alternatief is als het GNSS-signaal wegvalt. Dat maakt dit de meest kwetsbare schakel in de keten: één verstoring raakt alles tegelijk. In feite zijn twee functies nodig voor de tijd; Een redundantiepunt voor de beschikbaarheid van tijd in het geval van 'jamming' en een referentiepunt voor de continue controle op betrouwbaarheid van de tijd in het geval van 'spoofing'. Nederland heeft met VSL een nationaal metrologisch instituut dat voor het ministerie van Economische Zaken de Nederlandse tijd beheert en de basis kan vormen voor een GNSS-onafhankelijk tijdnetwerk waarop vitale partijen in theorie zouden kunnen inprikken. Die basis is er dus al. Bovendien valt te leren van buurlanden die hier al mee bezig zijn, zoals het Verenigd Koninkrijk dat bouwt aan een nationaal tijdnetwerk. Nu is het nodig te beslissen het tijdnetwerk meer robuust uit te bouwen, geografisch gespreid en bestand tegen uitval van individuele onderdelen, en (regionaal) beschikbaar te maken voor vitale gebruikers. Het netwerk vraagt het kabinet die beslissing te nemen.

5.4 Actievoorstellen: wat nu al kan

De volgende actievoorstellen liggen binnen bereik van de partijen die als actiehouder staan vermeld. Per voorstel is aangegeven wie aan zet is en wat er concreet van wordt verwacht (in willekeurige volgorde).

Actievoorstel a: PNT-specifieke risicoanalyse uitvoeren

Actiehouder: Vitale sectoren zelf, gestimuleerd door vakdepartementen en toezichthouders

Veel organisaties weten niet precies hoe en waar hun processen afhangen van satellietnavigatie. Die blinde vlek is het vertrekpunt van alle andere kwetsbaarheden. Het netwerk vraagt vitale sectoren om een PNT-specifieke risicoanalyse uit te voeren, met gebruikmaking van de Resilience Assessment Tool van het Centre of Excellence PNT als gestandaardiseerde methodiek. Vitale sectoren committeren zich aan het uitvoeren van die analyse en aan het delen van de geaggregeerde uitkomsten, zodat een gezamenlijk beeld van kwetsbaarheden ontstaat en organisaties van elkaar kunnen leren.

“

Actievoorstel b: Minimumeisen voor zelfstandige weerbaarheid per sector vaststellen

Actiehouder: Vakdepartementen samen met vitale sectoren

Zonder gedeelde norm investeert niemand genoeg. Het netwerk vraagt vakdepartementen om per vitale sector een minimale termijn vast te stellen waarvoor zelfstandige weerbaarheid bij GNSS-uitval geldt, met 72 uur als algemene basislijn en ruimte voor sectorspecifieke nuance. Daarbij moet netwerkdenken leidend zijn: ketenpartners die van elkaar afhangen bepalen hun weerbaarheidsambities gezamenlijk, want een keten is zo sterk als de zwakste schakel.

Actievoorstel c: Aansluiting op Galileo PRS en andere authenticatiemodellen actief stimuleren

Actiehouder: Ministerie van IenW, in samenwerking met vitale sectoren

Galileo, de Europese satellietnavigatieconstellatie, biedt een beveiligd navigatie- en tijdsignaal voor overheidsgebruikers en vitale sectoren: de Public Regulated Service. Dit signaal is aanzienlijk beter beschermd tegen verstoringen en manipulatie dan het gewone, ‘open’ Galileo of GPS-signaal. De Competente PRS Autoriteit (CPA), onderdeel van het ministerie van IenW, beheert in Nederland de toegang tot deze dual-use dienst.

Het netwerk vraagt vitale sectoren om proactief te beoordelen of inzet van Galileo PRS een goede oplossing zal zijn ter bescherming van hun processen. Voorts vraagt het netwerk IenW en de CPA om de vitale sectoren actief te ondersteunen bij het maken van een gezamenlijk actieplan voor de inzet van PRS. Waar PRS een te zwaar middel is, wordt IenW gevraagd om mee te denken bij het inzetten van andere beschikbare authenticatiemethoden onder het Galileo-systeem, zoals OSNMA en SAS.

Actievoorstel d: Nationale interferentiemonitoring opzetten

Actiehouder: Rijksinspectie Digitale Infrastructuur, in samenwerking met VSL en vitale sectoren

Je kunt pas handelen bij een verstoring als je weet dat die er is. Nu ontbreekt een nationaal beeld van de kwaliteit van het GNSS-signaal. Het Versnellingsnetwerk vraagt om een nationaal netwerk van monitoringsystemen dat de overheid een continu beeld geeft en de vitale gebruikers waarschuwt bij verstoringen. Daarbij hoort een meldroute waarbij de Rijksinspectie Digitale Infrastructuur ook buiten kantooruren bereikbaar is en een meldplicht bij vermoede verstoring.

Actievoorstel e: Stresstesten uitvoeren: durf de stekker eruit te trekken

Actiehouder: Vitale sectoren zelf, ondersteund door vakdepartementen en veiligheidsregio’s

Weerbaar zijn op papier is iets anders dan weerbaar zijn in de praktijk. Het netwerk stelt voor om in één of twee sectoren een gerichte PNT-stresstest uit te voeren waarbij onder gecontroleerde omstandigheden de afhankelijkheid van tijd en navigatie zichtbaar wordt gemaakt. Op het niveau van sectoren en wellicht in ‘ketens’ is het uitvoeren van stresstests en vooral het oefenen met uitval veruit de beste manier om tot eenvoudige afspraken en ‘protocollen’ te komen. De uitkomsten leveren niet alleen technische lessen op, maar ook inzicht in hoe ketens uitvallen en in welke volgorde herstel mogelijk is. Vitale sectoren zijn bereid hieraan deel te nemen.

Actievoorstel f: PNT-eisen standaard opnemen in aanbestedingen

Actiehouder: Vitale entiteiten zelf, VSL en gefaciliteerd door vakdepartementen

Een groot deel van de huidige PNT-afhankelijkheid is onbedoeld opgebouwd doordat tijdsynchronisatie en signaalintegriteit nooit als eis in aanbestedingen stonden. Door eisen op het gebied van redundantie, integriteit en terugvalopties voortaan standaard op te nemen in programma’s van eisen, ontstaat over meerdere contractcycli een geleidelijke versterking. Het netwerk vraagt vakdepartementen om hiervoor een praktische handreiking te ontwikkelen.

“

Actievoorstel g: Nationaal kennispunt voor PNT-weerbaarheid inrichten en kennisopbouw borgen

Actiehouder: IenW, Defensie, Centre of Excellence PNT, VSL, TNO en NLR gezamenlijk

Het Centre of Excellence PNT vormt een bestaande, herkenbare basis voor kennis over GNSS-weerbaarheid. Het netwerk pleit ervoor om dit centrum door te ontwikkelen tot het nationale aanspreekpunt, naar voorbeeld van het PNT Office in het Verenigd Koninkrijk: voor masterclasses, de Resilience Assessment, sectorale best practices en onafhankelijk advies. Daarbij past een verbinding met dit Versnellingsnetwerk en nadrukkelijk ook met het ministerie van Defensie, zodat de opgebouwde dialoog na oplevering niet doodbloedt. Tegelijk vraagt het netwerk om de kennis uit de IKUS-rapportages en het TNO-onderzoek actief te benutten: niet door een nieuwe inventarisatie, maar door de bestaande aanbevelingen nu daadwerkelijk uit te voeren en de voortgang periodiek te meten.

Actievoorstel h: Actief aansluiten op en investeren in Europese en internationale ontwikkelingen

Actiehouder: Rijk, in samenwerking met Europese partners en buurlandse kennisinstituten

PNT kent geen landsgrenzen. Landen als het Verenigd Koninkrijk en Duitsland zijn verder in het organiseren van hun PNT-weerbaarheid; rondom Brussel Airport is er al een geïntegreerd systeem voor luchtruimbeheer en dronedetectie operationeel waarvan Nederland kan leren. Het netwerk vraagt het kabinet om de Nederlandse aanpak actief te verbinden aan Europese initiatieven rond Galileo en de richtlijn voor kritieke entiteiten en om ervaringen met vooroplopende landen actief op te halen en te benutten.

5.5 Best practices: leren van wat werkt

De volgende voorbeelden laten zien dat op het PNT-vraagstuk al stevig wordt gewerkt, maar dat de initiatieven nog niet systematisch worden gedeeld of opgeschaald. Ze bieden concrete aanknopingspunten voor de actievoorstellen in paragraaf 5.4. Ook internationaal zijn er, zoals eerder genoemd voorbeelden om van te leren: het Verenigd Koninkrijk heeft een PNT Office met Defensie als mede-eigenaar; Duitsland werkt via zijn nieuwe ruimteministerie aan alternatieven voor GNSS; en rondom Brussel Airport is via Skeyes een geïntegreerd luchtruimbeheersysteem operationeel met uitgewerkte zones en interventieprotocollen. Nederland hoeft niet alles zelf te bedenken.

1. PNT-portaal en Resilience Assessment Tool

[kennis / alle sectoren]

Het Centre of Excellence PNT, opgericht in opdracht van IenW in samenwerking met ESA en de Netherlands Space Agency, beheert het publiek toegankelijke portaal pntportal.eu. Daarop staan masterclasses over GNSS, een Resilience Assessment Tool waarmee organisaties hun eigen kwetsbaarheden in beeld brengen en een gestructureerd overzicht van mitigatiestrategieën. Het is een praktisch vertrekpunt voor organisaties die hun bewustwording willen omzetten in concrete stappen, al vraagt de tool om voldoende technische kennis van de eigen systemen.

2. Tijdsdistributie op nationale en regionale schaal: VSL en Havenbedrijf Rotterdam

[infrastructuur / nationaal en cluster]

Op nationaal niveau beheert VSL, door de rijksoverheid aangewezen als Nationaal Metrologisch Instituut van Nederland, de Nederlandse tijdreferentie op basis van atoomklokken in Delft, met koppelingen naar onderzoeksinstituten en commerciële partijen. VSL beheert de Nederlandse Tijdschaal en maakt deze beschikbaar. VSL vormt daarmee de natuurlijke ruggengraat voor een GNSS-onafhankelijk nationaal tijdnetwerk. Op clusterniveau laat het Havenbedrijf Rotterdam zien hoe het regionaal kan werken: als beheerder van de gemeenschappelijke haveninfrastructuur onderzoekt het actief hoe een tijdsignaal vanaf de Nederlandse Tijdschaal kan worden gedistribueerd naar bedrijven in het havengebied die onvoldoende eigen redundantie hebben. Vergelijkbare

initiatieven lopen in de regio Westerschelde. Samen illustreren deze voorbeelden dat tijdsdistributie schaalniveaus te organiseren is en dat de bouwstenen er al liggen.

3. GNSS-monitoringonderzoek op vitale locaties

[kennis / cluster]

In 2024 en 2025 zijn onder regie van IenW monitoringcampagnes uitgevoerd op vier vitale locaties: Schiphol, Havenbedrijf Rotterdam, Stedin en VSL. De uitkomst was helder: verstoringen van het GNSS-signaal komen ook in Nederland voor, en zijn meetbaar. Dat maakt dit onderzoek tot het feitelijke bewijs van urgentie. De volgende stap is dit uit te bouwen naar een permanent, landsdekkend monitoringsysteem.

4. Wat sectoren al doen: waardevolle voorbeelden die gedeeld moeten worden

[kennis en governance / alle sectoren]

Verschillende sectoren hebben al concrete stappen gezet die als voorbeeld kunnen dienen. De luchtvaart heeft het ILS-systeem, een grondgebonden radiobaken voor nadering en landing, nooit uitgeschakeld en beschikt daarmee over een bewezen terugvaloptie die niet van satelliet afhankelijk is. Schiphol heeft een eigen tijdorganisatie binnen het hekwerk en een 24-uurs terugvalprocedure. Drinkwaterbedrijven hebben strategische dieselvoorraden voor noodaggregaten. Defensie beschikt over alternatieve tijdvoorzieningen met synchronisatie naar VSL en kennis over grondgebonden navigatie. Deze voorbeelden bewijzen dat weerbaarheid haalbaar is. De opgave is ze zichtbaar te maken en op te schalen.

6. Advies: hoe nu verder

Tijdens de doorbraaksessie van 4 juni is de inhoud van dit rapport aangescherpt en getoetst bij zowel de deelnemers aan de themasessies als bij C-level. Hiermee is duidelijk geworden wat de private partijen aanbieden en welke verwachtingen zij hebben van de (rijks)overheid.
Met de aanbieding van dit rapport aan de minister van Infrastructuur en Waterstaat wordt vooralsnog de behandeling van de thema's drones respectievelijk PNT door het Versnellingsnetwerk afgerond.

De urgentie, de onderlinge afhankelijkheden en het handelingsperspectief is in beeld gebracht. Het kabinet en de private partijen staan nu samen aan de lat en aan de start om de doorbraakadviezen en actievoorstellen van het Versnellingsnetwerk concreet in praktijk te brengen. Het échte werk begint nú.

Daarom adviseren wij de rijkspartners en de vitale bedrijven om samen een slimme en sterke netwerkschakel te organiseren, zodat de vitale infrastructuur van Nederland weerbaarder wordt. Dit verlangt dat alle betrokkenen actief tijd en capaciteit vrijmaken om hiermee aan de slag te gaan. Startend met de opbrengsten vanuit de thema's drones en PNT, in de wetenschap dat andere thema's kunnen volgen.

Uiteraard is een deel van de uitvoering ook afhankelijk van de beschikking over voldoende financiële middelen, maar het Versnellingsnetwerk roept dringend op om dit niet als opschortende voorwaarde te stellen en juist alvast in werking te zetten wat nu al kan.

Dit vraagt van de overheid één voorkant, één single point of contact, zodat de vitale partijen niet voortdurend alle departementen langs hoeven en bovendien dat het Rijk daarachter zijn eigen organisatie op orde heeft.

En van alle partijen samen, dus ook van de vitale partijen, wordt verwacht dat zij hun kennis en expertise inbrengen en hun werkpraktijk ter beschikking stellen om zaken te testen en te oefenen. Zo bundelen we in één schakel het contact én de kennis, en sluiten we aan op de behoefte aan een expertisecentrum die in onze sessies is uitgesproken. Want de vitale partijen zijn zelf óók aan zet: zij willen dit netwerk gebruiken om de actievoorstellen uit het advies te realiseren, zijn bereid pilots te draaien en goede voorbeelden te delen. Zo gaat het netwerk verder, en pakken we samen met het Rijk op wat hier is begonnen.

Het advies is gedragen en de mensen zijn gemobiliseerd. Het netwerk is bereid zijn rol te blijven spelen en de zelfbindende uitspraken uit dit advies waar te maken. Wij hopen dat u, samen met uw collega's in het kabinet, dit oppakt en er met het netwerk een echt vervolg aan geeft. Met dit in gedachten verzoek ik u als betrokken ministers vanuit uw eigen beleidsterrein gezamenlijk met een gecoördineerde reactie te komen op dit rapport. Gelet op het vervolg van het Versnellingsnetwerk vanaf september, en gelet op de urgentie, zouden wij het zeer op prijs stellen als wij binnen afzienbare tijd van u vernemen.

Het netwerk staat klaar. Nu is het moment om samen door te pakken.

Christophe van der Maat

Voorzitter Versnellingsnetwerk Weerbaarheid Fysieke Leefomgeving

Overlegorgaan Fysieke Leefomgeving

Deelnemende organisaties

De volgende organisaties hebben bijgedragen aan de werksessies van het Versnellingsnetwerk Weerbaarheid Fysieke Leefomgeving, thema Drones en thema PNT.

Alliander/Liander
CBL
Chemelot
CGI
Dienst Justitiële Inrichtingen
Dares
Defensie
Defensie Pijpleidingeorganisatie
Dow Terneuzen
Dunea
Eindhoven Airport
Energie Nederland
Enexis
EPZ
EZK
FNLI
Gasunie
Gemeente Haarlemmermeer
Groningen Seaports
Havenbedrijf Amsterdam
Havenbedrijf Rotterdam
Hoogheemraadschap de Stichtse Rijnlanden
Hutchison Ports ECT Rotterdam
IenW
KNMI
Luchtverkeersleiding Nederland
MUAC/Eurocontrol
Nationaal Metrologisch Instituut – VSL
NCTV
Nederlandse Spoorwegen
Nederlandse Vereniging voor de Bakkerij
NLR
North Sea Port
Oasen
Port of Moerdijk
ProRail
Rabobank
Rijkswaterstaat
Rotterdam the Hague Airport
RWE
Sabic
S[&]T
Schiphol
Shell
Stichting Dutch Data Center Association
Stedin

“

TUI fly
TenneT
Transavia
Urenco
VELIN
VEWIN
VNCI
VNO-NCW
VOTOB
Veiligheidsregio Rotterdam-Rijnmond
Veiligheidsregio Zeeland
Vitens
Waterschap Drents Overijsselse Delta