Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

30 821 Nationale Veiligheid

Nr. 182 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 30 mei 2023

De processen en diensten die samen de vitale infrastructuur vormen, zijn het fundament waarop de Nederlandse samenleving draait. Elektriciteit, toegang tot internet, drinkwater en betalingsverkeer zijn hier voorbeelden van. Uitval, verstoring of manipulatie van dergelijke processen en diensten kan grote gevolgen hebben voor het functioneren van de Nederlandse economie en maatschappij en in het uiterste geval een bedreiging vormen voor de nationale veiligheid. Daarom werken overheden, bedrijven, organisaties en inlichtingen- en veiligheidsdiensten voortdurend nauw samen aan het beschermen van de weerbaarheid van onze vitale infrastructuur.

Deze opgave wordt steeds complexer: de toenemende dreiging van statelijke actoren en cybercriminelen, de groeiende digitale verwevenheid en complexe ketenafhankelijkheden vragen om nieuwe oplossingen en aanvullende maatregelen. Het kabinet werkt daarom aan de doorontwikkeling van de bescherming van de vitale infrastructuur, om te komen tot een aanpak die robuuster en meer adaptief is. Er wordt gewerkt aan een versterking van de huidige nationale aanpak door de wet- en regelgeving, het huidige beleidsinstrumentarium en de governance te actualiseren en toekomstbestendiger te maken.[1]

Dit past binnen de bredere inzet op het veilig en weerbaar maken van onze samenleving. Zo wordt bijvoorbeeld gewerkt aan een versterking van de open strategische autonomie van de Europese Unie, zal de Wet veiligheidstoets investeringen, fusies en overnames spoedig in werking treden, werd uw Kamer geïnformeerd over de kabinetsaanpak van strategische afhankelijkheden, is er een nationale grondstoffenstrategie

[1] Conform de motie van het lid Van den Berg c.s. over een versterkte aanpak van de bescherming van de vitale processen en diensten (Kamerstuk 24 095, nr. 487).

kst-30821-182
ISSN 0921 - 7371
's-Gravenhage 2023

opgesteld en wordt ingezet op een betere bescherming van de Noordzee-infrastructuur.[2]

Zoals eerder toegezegd[3] informeer ik uw Kamer met deze brief namens het kabinet over de versterkte aanpak bescherming vitale infrastructuur (hierna: Aanpak vitaal). Hieronder zal ik achtereenvolgens ingaan op de dreigingen voor de vitale infrastructuur en de hoofdlijnen van de inzet voor de komende jaren.

Een veranderend dreigingslandschap

De vitale infrastructuur kan door een veelheid aan dreigingen worden aangetast: zowel moedwillige als niet-moedwillige en zowel interne als externe. Deze dreigingen staan vaak niet op zichzelf, maar kennen een onderlinge verwevenheid en verbondenheid, die onder andere door technologische ontwikkelingen sterk toeneemt.[4] Bovendien zijn dreigingen, maar ook de te beschermen belangen, niet statisch van aard, maar continu onderhevig aan maatschappelijke, internationale en technologische ontwikkelingen. In de Veiligheidsstrategie van het Koninkrijk der Nederlanden 2023–2029 en recente risico- en dreigingsbeelden, zoals het Cybersecuritybeeld Nederland, het Dreigingsbeeld Statelijke Actoren en de Rijksbrede Risicoanalyse Nationale Veiligheid, is een aantal ontwikkelingen en dreigingen geïdentificeerd waar ook de vitale infrastructuur tegen beschermd zal moeten worden.[5]

Allereerst is het geopolitieke klimaat instabieler geworden en staat de internationale rechtsorde onder druk. Steeds vaker zijn vitale processen in Nederland en de Europese Unie doelwit van handelingen van statelijke actoren die onze veiligheidsbelangen kunnen schaden, zoals spionage en sabotage. Verstoringen en beperkingen van vitale processen of diensten kunnen worden nagestreefd om maatschappelijke onrust te zaaien of het vertrouwen in de overheid aan te tasten.[6] De meest opvallende en zorgelijke ontwikkeling is de illegale Russische oorlog in Oekraïne, die de relatie tussen het Westen en Rusland onder hoge spanning zet. Het is bekend dat Russische entiteiten interesse tonen in de Nederlandse vitale infrastructuur. Daarnaast kan Nederland ook gevolgen ondervinden van sabotage van vitale infrastructuur elders in Europa.[7]

Ten tweede wordt Nederland steeds vaker geconfronteerd met dreigingen op het snijvlak van economie en veiligheid. De verwevenheid van de mondiale economie biedt Nederland veel welvaart en kansen, maar zorgt ook voor risico's en kwetsbaarheden. Binnen de vitale infrastructuur is de continuïteit van bepaalde processen afhankelijk van buitenlandse partijen. Wanneer er beperkte alternatieve aanbieders van producten en diensten beschikbaar zijn en deze niet op de korte termijn substitueerbaar zijn, kunnen risicovolle strategische afhankelijkheden ontstaan. Deze afhankelijkheden kunnen door statelijke actoren worden ingezet als drukmiddel

---

[2] Kamerstuk 35 982, nr. 9; Kamerstukken 35 880 en 32 637, nr. 19; Kamerstuk 32 852, nr. 224; Kamerstuk 33 450, nr. 118.

[3] Aanhangsel Handelingen II 2022/23, nr. 970.

[4] Zie ook: Veiligheidsstrategie Koninkrijk der Nederlanden 2023–2029 (Kamerstuk 30 821, nr. 178).

[5] «Cybersecuritybeeld Nederland 2022» (Kamerstuk 26 643, nr. 891), NCTV, 2022; «Dreigingsbeeld Statelijke Actoren 2», AIVD, MIVD, NCTV, 2022; «Rijksbrede Risicoanalyse Nationale Veiligheid», ANV, 2022 (Kamerstuk 30 821, nr. 165); Veiligheidsstrategie Koninkrijk der Nederlanden 2023–2029, 2023.

[6] Dit beeld wordt onder meer bevestigd door het rapport «De Russische invasie in Oekraïne: Implicaties voor Nederland» van het Hague Centre for Strategic Studies (HCSS) en de «Verdiepende analyse bij Rijksbrede risicoanalyse nationale veiligheid» van het Analysenetwerk Nationale Veiligheid (ANV).

[7] «Dreigingsbeeld Statelijke Actoren 2», AIVD, MIVD, NCTV, 2022 (Bijlage bij Kamerstuk 30 821, nr. 175).

voor geopolitieke doeleinden. In bepaalde gevallen kunnen strategische afhankelijkheden ook het risico op ongewenste kennisoverdracht, waaronder diefstal van hoogwaardige kennis binnen de vitale infrastructuur, vergroten.

Ten derde is de digitale dreiging onverminderd hoog. Digitalisering zorgt voor een verbondenheid van systemen en een grote afhankelijkheid van digitale processen. Dit maakt vitale infrastructuur kwetsbaar voor uitval als gevolg van cyberincidenten. De digitale ruimte is een speelveld voor statelijke en niet-statelijke actoren. Er zijn landen die op structurele basis proberen zich digitaal toegang te verschaffen tot de vitale infrastructuur, om daar voorbereidingshandelingen voor digitale sabotage of spionage te treffen. Maar ook cybercriminelen spelen in op afhankelijkheid van digitale processen. Zij handelen vanuit financieel motief en hebben niet de intentie om de maatschappij te ontwrichten, maar hun aanvallen kunnen desalniettemin omvangrijke schade toebrengen aan de vitale infrastructuur.[8]

Tot slot vormen de gevolgen van klimaatverandering een toenemende dreiging voor de vitale infrastructuur. Een stijgende frequentie en intensiviteit van natuurrampen en extreem weer kunnen de continuïteit van vitale processen als de elektriciteits-, drinkwater- en gasvoorziening en telecommunicatie verstoren, met mogelijke cascade-effecten tot gevolg.[9] Dit vraagt om een Aanpak vitaal waarin het toenemende risico op klimaat- en natuurrampen wordt meegenomen en rekening wordt gehouden met ruimtelijk beleid, zoals het principe van water en bodem sturend en een klimaatbestendige inrichting van Nederland.[10]

Hoofdlijnenschets Aanpak vitaal 2023–2028

De bescherming van de vitale infrastructuur is al langere tijd onderdeel van het kabinetsbeleid. Zoals hierboven geschetst zien we echter dat het dreigingslandschap als gevolg van actuele ontwikkelingen verandert en veelzijdiger wordt. Dit noodzaakt tot een versterkte aanpak. Hieronder zal ik de hoofdlijnen van de Aanpak vitaal aan de hand van drie overkoepelende speerpunten toelichten.

I. Een integrale benadering: meer samenhang

Om de grote verscheidenheid aan dreigingen en risico's doeltreffend te kunnen mitigeren is een brede, meer integrale aanpak voor de bescherming van de vitale infrastructuur nodig. Fysieke, economische en digitale risico's zullen zoveel mogelijk in samenhang worden beoordeeld. De nationale veiligheid kan namelijk niet alleen in het geding komen wanneer de territoriale of fysieke veiligheid geschaad wordt, ook risicovolle strategische afhankelijkheden of verstoringen in digitale systemen kunnen de nationale veiligheid raken, ook wanneer de vitale infrastructuur hier zelf niet direct schade van ondervindt.[11, 12]

---

[8] «Cybersecuritybeeld Nederland 2022», NCTV, 2022.

[9] «Themarapportage Klimaat- en Natuurrampen», ANV, 2022 (Bijlage bij Kamerstuk 30 821, nr. 165).

[10] Zie ook de brief over Water en Bodem sturend van de Minister van Infrastructuur en Waterstaat: Kamerstukken 27 625 en 30 015, nr. 592.

[11] Kamerstuk 30 821, nr. 178.

[12] Verstoring van vitale infrastructuur kan op zichzelf een dreiging voor de nationale veiligheid vormen, maar andersom kan een gebeurtenis als een overstroming, ongeval, of cyberaanval ook een verstoring van de vitale infrastructuur teweeg brengen. Daarnaast is mogelijk dat een dreiging gericht op de vitale infrastructuur niet direct een verstoring van de vitale processen tot gevolg heeft, maar wel de nationale veiligheid raakt, zoals bijvoorbeeld in het geval van spionage.

Ten tweede zal niet uitsluitend gekeken worden naar de mate van impact van uitval, verstoring of manipulatie van een proces of dienst op de veiligheid van Nederland, maar zal er aandacht zijn voor de bredere EU-belangen. Dit omdat de vitale infrastructuur een sterke internationale verwevenheid kent en de verschillende nationale en internationale processen in grote mate van elkaar afhankelijk zijn. Ook wordt verkend hoe de NAVO-belangen bij een weerbare infrastructuur in de aanpak meegenomen kunnen worden. Het kabinet vindt het van belang dat de EU en NAVO ten aanzien van dit onderwerp waar mogelijk kennis delen en samenwerken. Het kabinet verwelkomt dan ook de recente oprichting van de EU-NAVO taskforce met een focus op het verbeteren van de samenwerking op het gebied van versterking van de weerbaarheid van kritieke infrastructuur.

Ten derde zal er meer aandacht zijn voor sectoroverstijgende risico's, doordat het verkrijgen van zicht op risicovolle strategische afhankelijkheden en mogelijke cascade-effecten een meer integraal onderdeel van de Aanpak vitaal wordt. Hoe dit in de aanpak bestendigd is wordt hieronder nader toegelicht.

II. Versterken van de weerbaarheid: meer zicht op risico's en een adaptief en toekomstbestendig instrumentarium voor het nemen van maatregelen

De constante ontwikkelingen in het dreigingslandschap vragen om een actueel en aanhoudend zicht op de weerbaarheid van de vitale infrastructuur. De afgelopen jaren is door de NCTV samen met de vakdepartementen een beleidsaanpak ontwikkeld, de cyclus vitaal. Met de cyclus vitaal kunnen de vakdepartementen en vitale aanbieders dreigingen en risico's identificeren en maatregelen nemen om de weerbaarheid te verhogen en te borgen. De cyclus vitaal bestaat uit verschillende stappen die periodiek worden doorlopen: (1) het identificeren van vitale processen en de aanbieders daarbinnen; (2) het analyseren van de risico's en de weerbaarheid; (3) het opstellen van een actieprogramma met te treffen weerbaarheidsverhogende maatregelen; en (4) het toetsen van de effectiviteit en het waar nodig bijstellen van deze maatregelen. De vakdepartementen voeren deze cyclus in samenwerking met de vitale aanbieders minimaal vierjaarlijks uit, of vaker wanneer de actualiteit daarom vraagt.

De cyclus vitaal is onlangs herzien en aangescherpt, met het doel uitgebreider en blijvend inzicht te verkrijgen in de weerbaarheid van vitale processen tegen de toegenomen dreigingen. Een belangrijke ontwikkeling is dat het veilig inkopen van producten en diensten steviger is opgenomen in de cyclus en er expliciet aandacht is voor risicovolle strategische afhankelijkheden, sectoroverstijgende risico's en cascade-effecten. Het is van belang dat wordt gewogen of de inkoop en het gebruik van specifieke producten of diensten niet leidt tot strategische afhankelijkheden met een onaanvaardbaar risico.[13]

Hiermee wordt tegemoetgekomen aan de motie van het lid Rajkowski c.s, waarin wordt verzocht een scan uit te voeren naar de aanwezigheid van apparatuur of programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda in de kern van de vitale infrastructuur.[14] Een dergelijk verzoek is complex en omvangrijk om uit te voeren en vraagt medewerking van de vitale aanbieders. De motie wordt langs twee lijnen opgevolgd. Ten eerste wordt door TNO een *case study* uitgevoerd naar de aanwezigheid van dergelijke apparatuur en program-

[13] Kamerstuk 35 982, nr. 9.
[14] Kamerstuk 26 643, nr. 830.

matuur bij een geselecteerd aantal vitale sectoren. Op basis van de resultaten en inzichten die deze *case study* (zowel op inhoud als methodiek) oplevert wordt bezien welke vervolgstappen kunnen worden uitgevoerd binnen andere vitale sectoren, vanuit het doel meer zicht te krijgen op kwetsbaarheden in de vitale infrastructuur.

Ten tweede maken risico's bij inkoop- en aanbestedingen en strategische afhankelijkheden van producten en diensten – en de mogelijke invloed van buitenlandse partijen op een vitaal proces die daaruit kan voortvloeien – integraal onderdeel uit van de weerbaarheidsanalyse. Alle vitale processen zullen deze weerbaarheidsanalyse doorlopen. Daarmee wordt zowel bovengenoemde motie als de toezegging in de appreciatie van de motie van het lid Rajkowski c.s. om nationale veiligheid als zwaarwegend criterium op te nemen in de beoordeling van inkoopopdrachten en aanbestedingen van vitale aanbieders, structureel opgevolgd.[15, 16] Daarnaast vormt het verminderen van risicovolle strategische afhankelijkheden binnen de vitale infrastructuur ook onderdeel van de bredere Kabinetsaanpak Strategische Afhankelijkheden.[17, 18]

Daarnaast hecht het kabinet aan een goede ondersteuning van vitale aanbieders bij het toepassen van economische veiligheidsinstrumenten en het verhogen van de bewustwording en weerbaarheid, zoals de Wet veiligheidstoets investeringen, fusies en overnames (Wet Vifo) en de inkoop- en aanbestedingstoolboxen. Voor inkoop en aanbesteding is in 2018 en 2019 instrumentarium ontwikkeld dat organisaties handvatten biedt om bij de inkoop van producten en diensten een risicoanalyse uit te voeren en maatregelen te treffen op nationale veiligheidsrisico's. Op dit moment wordt gewerkt aan een actualisatie en aanscherping van het instrumentarium. Toepassing hiervan wordt vervolgens verplicht gesteld voor relevante inkoopopdrachten binnen de Rijksoverheid. Voor meer informatie verwijs ik u naar de Kamerbrief over de uitvoering van de moties Rajkowski vanuit de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties.[19] De geactualiseerde instrumenten worden beschikbaar gesteld voor en actief verspreid onder vitale aanbieders. Tevens wordt doorlopend ingezet op bewustwording bij vitale aanbieders over het signaleren van risico's in het inkoopproces.

Voorbeeld nieuwe cyclus vitaal:

Het Ministerie van Infrastructuur en Waterstaat voert minimaal vierjaarlijks de cyclus vitaal uit voor het vitale proces «keren en beheren waterkwantiteit». Als daaruit blijkt dat uitval, manipulatie of verstoring van dit vitale proces leidt tot gevolgen voor de nationale veiligheid, worden vervolgstappen ondernomen. Ten eerste worden de vitale aanbieders (de partijen die essentieel zijn voor het vitale proces) geïdentificeerd (stap 1). Vervolgens voert IenW samen met deze vitale aanbieders een weerbaarheidsanalyse uit (stap 2). Hiermee worden relevante dreigingen voor het vitale proces en de weerbaarheid daartegen uiteengezet. Hierbij wordt getoetst op de volgende indicatoren: fysieke weerbaarheid, digitale weerbaarheid, economische weerbaarheid, weerbaarheid tegen grote ketenafhankelijkheden en crisisbeheersing. Op basis van deze weerbaarheids-

[15] Kamerstuk 26 643, nr. 830.
[16] Kamerstuk 36 200, nrs. 62 en 150.
[17] Kamerstuk 30 821, nr. 181.
[18] Daarnaast verwelkomt het kabinet het plan van de EU om voldoende beschikbaarheid van kritieke grondstoffen te bereiken: NL non-paper on the Action Plan on Critical Raw Materials and the Critical Raw Materials Act | Publicatie | Rijksoverheid.nl.
[19] Kamerstukken 26 643 en 30 821, nr. 1007.

analyse worden acties geformuleerd om de weerbaarheid te versterken (stap 3). Die acties kunnen zowel sectoraal als sectoroverstijgend van aard zijn.

De aanpak is cyclisch ingericht omdat vitale processen constant onderhevig zijn aan ontwikkelingen en het verhogen van de weerbaarheid een continu proces is. Zo kan met het uitvoeren van zogeheten *quickscans* gecontroleerd worden of de weerbaarheidsanalyse up-to-date is of aanpassing behoeft (stap 4). Dit kan bijvoorbeeld naar aanleiding van een actualiteit als de Covid-19-crisis of de illegale Russische oorlog in Oekraïne.

III. Verankeren van de samenwerking en verantwoordelijkheden: minder vrijblijvend en meer ondersteuning

De veranderende veiligheidscontext vraagt om een meer richtinggevende en minder vrijblijvende aanpak. Daarom zet het kabinet in op rechten en plichten voor alle vitale aanbieders en een verankering hiervan in de wet- en regelgeving. Op die manier verhogen we zowel de fysieke als digitale en economische weerbaarheid.

Vanwege de grensoverschrijdende verbondenheid van de vitale infrastructuur is inzet niet alleen op nationaal niveau, maar ook op Europees en internationaal niveau noodzakelijk. Bepaalde risico's, zoals strategische afhankelijkheden en cascade-effecten, stoppen niet bij de grens. Het kabinet verwelkomt dan ook de twee Europese richtlijnen die een (wettelijk) kader bieden voor het versterken en waarborgen van de digitale en fysieke weerbaarheid van onder meer de vitale infrastructuur. De herziening van de richtlijn netwerk- en informatiebeveiliging (de NIS2-richtlijn) en de richtlijn veerkrachtige kritieke entiteiten (de CER-richtlijn) zijn in december 2022 aangenomen en gepubliceerd.[20, 21] Uw Kamer is eerder over deze richtlijnen en de Nederlandse inzet tijdens het onderhandelingstraject geïnformeerd.[22] Deze CER- en NIS2-richtlijn worden geïmplementeerd in de Nederlandse wet- en regelgeving.[23]

De komende tijd wordt door het kabinet gewerkt aan de totstandkoming van de wetsvoorstellen ter implementatie van deze richtlijnen. De conceptwet- en regelgeving zal naar verwachting dit najaar in consultatie worden gebracht, zodat ook de betrokken bedrijven en organisaties kennis kunnen nemen van de wetsvoorstellen en hieraan kunnen bijdragen. Op dat moment kan ook meer duidelijkheid geboden worden over de concrete vertaling van de richtlijnen naar nationale wetgeving, zodat organisaties zich kunnen voorbereiden. De financiële gevolgen van de implementatie van de CER- en NIS2-richtlijn worden de komende tijd nader in kaart gebracht. Over de precieze inhoud van de implementatiewetgeving en bijbehorende implementatiekeuzes zal uw Kamer bij de parlementaire behandeling van de wetsvoorstellen separaat worden geïnformeerd.[24] Hieronder wordt kort ingegaan op de hoofdlijnen van de nieuwe wet- en regelgeving.

---

[20] EUR-Lex – 32022L2557 – EN – EUR-Lex (europa.eu).

[21] EUR-Lex – 32022L2555 – EN – EUR-Lex (europa.eu).

[22] Kamerstuk 22 112, nrs. 3053 en 3054.

[23] Zie ook de website voor de NCTV: Implementatie CER en NIS2 richtlijnen | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl).

[24] De EC heeft ook een Raadsaanbeveling vastgesteld waarin onder meer is opgeroepen om, mede in het licht van de veranderende geopolitieke situatie, de CER- en NIS2-implementatie waar mogelijk te versnellen. Het kabinet verwelkomt deze aanbeveling, maar wil tegelijkertijd niet afdoen aan een zorgvuldige implementatie en kwaliteit. Over de appreciatie van de Raadsaanbeveling is uw Kamer reeds geïnformeerd (Kamerstuk 22 112, nr. 3556).

Om ervoor te zorgen dat er passende beveiligingsmaatregelen genomen worden krijgen bedrijven en organisaties (entiteiten) die onder deze wetgeving gaan vallen te maken met wettelijke verplichtingen. Entiteiten moeten passende en evenredige weerbaarheidsverhogende maatregelen nemen, zodat zij beter in staat zijn incidenten waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van de processen onder druk kan komen te staan te voorkomen, te bestrijden en ervan te herstellen (de zorgplicht). Om ondersteuning te kunnen bieden en te waarborgen dat de overheid zicht houdt op de gevolgen van incidenten die zich desondanks voordoen, geldt voor organisaties die onder deze wetgeving vallen een meldplicht voor incidenten die significante consequenties (kunnen) hebben voor de continuïteit van hun dienstverlening.

Een belangrijk onderdeel van een minder vrijblijvende aanpak is ook het toezicht op de naleving van de wet- en regelgeving. Er zal daarom op zowel de fysieke, als de digitale weerbaarheid toezicht komen voor entiteiten die onder deze regelgeving worden gebracht. Samen met de betrokken vakdepartementen en toezichthouders wordt uitgewerkt hoe de wettelijke kaders voor dit toezicht nader kunnen worden vormgegeven.

Daarnaast zal er binnen de Aanpak vitaal worden ingezet op een uitgebreidere ondersteuning aan bedrijven en organisaties om hen in staat te stellen hun verantwoordelijkheid en plichten voor de weerbaarheid van vitale processen zo goed mogelijk te vervullen. Bijvoorbeeld door het geven van advies, een zorgvuldige informatie-uitwisseling en het verlenen van bijstand. Op die manier worden aanbieders geholpen met het inzichtelijk maken van en voorbereiden op dreigingen en risico's. Voor de versterking van de crisisbeheersing en de meerjarige landelijke agenda zijn en worden er in samenwerking tussen Rijk, veiligheidsregio's en betrokken aanbieders landelijke crisisplannen ontwikkeld voor de uitval van vitale processen.[25] Vanwege de grensoverschrijdende verbondenheid van de vitale infrastructuur, is het hierbij ook van belang dat er, waar mogelijk, informatie wordt gedeeld met internationale partners. Het Nationaal Cyber Security Centrum (NCSC) heeft als centraal informatieknooppunt en expertisecentrum voor cybersecurity een belangrijke rol in de informatie-uitwisseling over digitale risico's.[26] Daarnaast is het van belang om informatie over fysieke dreigingen en risico's beter te delen. De mogelijkheden om dit beter vorm te geven worden momenteel verkend. Eveneens wordt gekeken hoe sectorspecifieke (vertrouwelijke) informatie beter verstrekt kan worden.

Rolverdeling: taken en verantwoordelijkheden binnen de Aanpak vitaal

De primaire verantwoordelijkheid voor de bescherming van vitale processen ligt bij de vitale aanbieders zelf. Zij hebben inzicht in dreigingen, kwetsbaarheden en risico's en nemen passende maatregelen om zich hiertegen te beschermen.

De beoordeling of een proces of dienst vitaal is wordt gemaakt door het verantwoordelijke vakdepartement, in overleg met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Hierbij wordt geanalyseerd of bij verstoring, uitval of manipulatie van een proces of dienst dermate ernstige gevolgen kunnen optreden dat deze de nationale veiligheid kunnen schaden. Aan de hand van specifieke criteria en drempelwaarden wordt de potentiële impact

[25] Kamerstuk 29 517, nr. 225.
[26] Nederlandse Cybersecuritystrategie 2022–2028, NCTV, 2022 (Bijlage bij Kamerstuk 26 643, nr. 925).

van uitval of verstoring van het proces bepaald. Het vakdepartement stelt algemene kaders vast voor de vitale sectoren die onder haar systeemverantwoordelijkheid vallen. Daarnaast kunnen vakdepartementen beleid of sectorale regelgeving ontwikkelen om de weerbaarheid van sectoren te verhogen. Toezichthouders zijn belast met het toezicht op de naleving van de wettelijke verplichtingen.

De coördinatie van de Aanpak vitaal valt onder de verantwoordelijkheid van de Minister van Justitie en Veiligheid. Namens de Minister voert de NCTV de sectoroverstijgende regie op de bescherming van vitale infrastructuur en let daarbij op de samenhang en effectiviteit van weerbaarheidsverhogende maatregelen. Waar nodig worden instrumenten ontwikkeld om kennis over dreigingen te bundelen en vitale aanbieders en vakdepartementen te ondersteunen. Daarnaast ontwikkelt de NCTV samen met vakdepartementen specifiek beleid en wet- en regelgeving waarmee vitale infrastructuur kan worden beschermd, bijvoorbeeld tegen ongewenste overnames of investeringen.

Bovenstaande rolverdeling geldt zowel voor de huidige als beoogde aanpak.

Tot slot

Bovenstaande uitgangspunten en maatregelen leiden tot een aanpak ter bescherming van de vitale infrastructuur die aansluit bij het huidige dreigingslandschap en de doorontwikkeling van het Europese beleid. De eerst stappen hiertoe zijn gezet. De komende tijd zal het kabinet zich inspannen om de wettelijke rechten en plichten die volgen uit de CER- en de NIS2-richtlijn nader uit te werken, zodat deze zo snel mogelijk in werking kunnen treden. Dit doet het kabinet graag zoveel mogelijk met input van de vitale aanbieders zelf, aangezien zij primair verantwoordelijk zijn voor de bescherming van de vitale processen.

De beoogde aanpassingen vragen een stevige inzet van alle betrokken actoren. De regie voor de bescherming van de vitale infrastructuur ligt bij de Rijksoverheid, maar voor een veilige en weerbare samenleving is de inzet van iedereen nodig: niet alleen van de overheid in al haar geledingen, maar ook van burgers, bedrijven en maatschappelijke organisaties. Tegelijkertijd kunnen dreigingen niet volledig worden weggenomen en bestaat er geen absolute veiligheid. Samen zijn we verantwoordelijk om voorbereid te zijn op als het onverhoopt toch misgaat.[27] Het kabinet blijft zich evenwel uiteraard onverminderd inzetten op het verhogen van de weerbaarheid van onze vitale infrastructuur.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

[27] Zie ook Home | Denk vooruit.