Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dreigingslandschap Vitale Infrastructuur

Inzicht in de stapeling van toenemende en veranderende dreigingen

Foto omslag: *De Oosterscheldekering beschermt Nederland bij dreigend hoogwater. Uitval van systemen kan ernstige gevolgen hebben.*

Inhoud

Samenvatting 4

1. Inleiding 7

2. Denkkader dreigingen, NV-belangen en weerbaarheid van de vitale infrastructuur 10

3. Moedwillige dreigingen voor de vitale infrastructuur 15

3.1 Statelijke actoren vormen een toenemende dreiging voor vitale infrastructuur 15

3.1.1 Sabotage vitale infrastructuur door statelijke actoren 16

3.1.2 Pre-positionering vitale infrastructuur door statelijke actoren 18

3.1.3 Cyberaanvallen door statelijke actoren en hacktivisten 18

3.1.4 Desinformatie 20

3.1.5 Economische druk en strategische afhankelijkheden 20

3.2 Terrorisme en gewelddadig extremisme: een mogelijke dreiging voor vitale infrastructuur 23

3.3 Activisme richt zich ook op vitale infrastructuur 24

3.4 Criminele activiteiten: een mogelijke dreiging voor vitale infrastructuur 25

4. Natuurlijke dreigingen voor de vitale infrastructuur 28

4.1 Klimaatverandering vormt een toenemende dreiging voor de vitale infrastructuur 28

4.1.1 Extreem weer als gevolg van klimaatverandering 28

4.1.2 Stijging zeespiegel als gevolg van klimaatverandering 30

4.2 Aardbevingen 30

4.3 Dreiging van ruimteweer voor de vitale infrastructuur 30

4.4 Dreiging van infectieziekten voor de vitale infrastructuur 31

5. Dreigingen voortkomend uit het falen van vitale processen zelf 33

5.1 Menselijk- en systeemfalen 33

5.2 Keteneffecten 34

6. Politieke, economische, sociale en technologische factoren 37

6.1 Toenemende afhankelijkheid digitale systemen 37

6.2 Technologische ontwikkeling 38

6.3 Energietransitie 39

6.4 Krapte op de arbeidsmarkt 39

6.5 Economische ontwikkelingen 40

7. Conclusie 42

Bronnen 43

Samenvatting

De Nederlandse vitale infrastructuur wordt geconfronteerd met een stapeling van uiteenlopende, toenemende en veranderende dreigingen. Deze dreigingen, waaronder geopolitieke spanningen, klimaatverandering en menselijk- en systeemfalen, kunnen leiden tot verstoring of uitval van vitale processen. Dergelijke verstoring of uitval kunnen een dreiging vormen voor de nationale veiligheid.

Dit eerste dreigingslandschap biedt een overzicht van de belangrijkste dreigingen voor de vitale infrastructuur en inzicht in recente ontwikkelingen met betrekking tot die dreigingen. Daarnaast biedt het dreigingslandschap vakdepartementen en vitale aanbieders een denkkader dat hen kan helpen voor specifieke vitale processen beter inzicht te krijgen in dreigingen, de weerbaarheid, de veiligheidsbelangen die worden geraakt bij verstoring of uitval en de risico's voor de nationale veiligheid die daar uit voortkomen. Dit dreigingslandschap kan daarmee door vakdepartementen en vitale aanbieders worden gebruikt als startpunt voor het maken van risico- en weerbaarheidsanalyses voor de verschillende vitale processen die in het kader van de cyclus vitaal en ten behoeve van de Wet weerbaarheid kritieke entiteiten (Wwke) zullen worden gemaakt.

Denkkader dreigingen, NV-belangen en weerbaarheid van de vitale infrastructuur

- Om een goede inschatting te kunnen maken van risico's voor de vitale processen, en daarmee voor de nationale veiligheid, is inzicht in drie aspecten noodzakelijk: de dreigingen die op een vitaal proces afkomen, de weerbaarheid van vitale processen en de mate waarin de nationale veiligheidsbelangen worden geraakt. Risico's voor de nationale veiligheid bestaan wanneer een vitaal proces wordt geconfronteerd met dreigingen, onvoldoende weerbaar is voor die dreigingen en wanneer verstoring of uitval van een vitaal proces er toe leidt dat één of meerdere nationale veiligheidsbelangen in het geding komen.
- Een dreiging is de waarschijnlijkheid dat een opzettelijke of niet-opzettelijke gebeurtenis zich voordoet die kan leiden tot verstoring of uitval van vitale processen of die hun integriteit en vertrouwelijkheid kan aantasten, waarbij één of meerdere nationale veiligheidsbelangen in het geding komen. Dit dreigingslandschap onderscheidt drie soorten dreigingen voor de vitale infrastructuur: moedwillige dreigingen, natuurlijke dreigingen en dreigingen die voortkomen uit het falen van vitale processen zelf.
- De zes nationale veiligheidsbelangen zijn territoriale-, fysieke, economische en ecologische veiligheid, sociale en politieke stabiliteit en de internationale rechtsorde en stabiliteit. Hoewel de continuïteit van vitale processen onderdeel is van de economische veiligheid, kan verstoring of uitval van een vitaal proces impact hebben op alle nationale veiligheidsbelangen.
- Weerbaarheid is het vermogen van de samenleving om voorbereid te zijn op maatschappelijke (en ecologische) ontwrichting, deze te weerstaan, te absorberen en/of een nieuw evenwicht te bereiken. De weerbaarheid van vitale processen wordt bepaald door het beleid van vitale aanbieders, het overheidsbeleid en de sterktes en kwetsbaarheden van Nederland en de vitale infrastructuur.

Moedwillige dreigingen voor de vitale infrastructuur

- Vitale processen kunnen te maken krijgen met moedwillige dreigingen vanuit o.a. statelijke actoren, terrorisme en gewelddadig extremisme, activisme en criminele activiteiten. Deze kunnen leiden tot verstoring of uitval. Daarnaast kunnen deze, bijvoorbeeld bij spionage en pre-positionering voor sabotage, de integriteit en vertrouwelijkheid van vitale processen onder druk zetten.
  - **Statelijke actoren** vormen een toenemende dreiging voor vitale infrastructuur. Door oorlogen, geopolitieke spanningen en groeiende competitie tussen grootmachten is de wereld rondom Nederland en de Europese Unie instabieler geworden. Met name Rusland en China vormen op verschillende manieren een dreiging voor de Nederlandse vitale infrastructuur. Dit uit zich onder andere in een toename van de inzet van hybride instrumenten, zoals sabotage, spionage en pre-positionering, cyberaanvallen, desinformatie, economische druk en misbruik van strategische afhankelijkheden.
  - Vitale infrastructuur kan een aantrekkelijk doelwit zijn voor **sabotage** door statelijke actoren. Naast maatschappelijke ontwrichting kan sabotage van vitale infrastructuur ook tot doel hebben om druk op landen uit te oefenen, de autonomie van andere landen aan te tasten of te testen hoe landen en de NAVO reageren op sabotageacties. Er zijn in Nederland geen recente voorbeelden geweest van geslaagde fysieke sabotage van vitale infrastructuur door statelijke actoren. Verschillende Europese voorvallen laten echter zien dat vitale infrastructuur kwetsbaar is voor hybride aanvallen en dat actoren ook bereid zijn om daadwerkelijk tot sabotage over te gaan. Zo houden westerse landen Rusland er voor verantwoordelijk dat het land de afgelopen jaren op verschillende plekken in Europa aanslagen en sabotage heeft gepleegd of dit heeft gepoogd te doen. In enkele gevallen waren ook deelprocessen van vitale sectoren doelwit. In de afgelopen jaren hebben er daarnaast verschillende incidenten rond onderwaterinfrastructuur in Europese

wateren plaatsgevonden. Ook is er recent een grote toename zichtbaar in het verstoren van GPS signalen door *jamming* en *spoofing* die de lucht- en scheepvaart raakt.

- Statelijke actoren kunnen ook voorbereidingshandelingen voor sabotage uitvoeren of pogen een positie in de vitale infrastructuur van andere landen te verkrijgen zonder (direct) tot sabotage over te gaan. Het doel van **spionage en pre-positionering** is soms om op een later moment de vitale infrastructuur wel te kunnen saboteren, om druk op andere landen uit te oefenen of om de autonomie van landen aan te tasten. Zo brengt Rusland de vitale maritieme infrastructuur in het Nederlandse deel van de Noordzee in kaart en onderneemt het land activiteiten die duiden op spionage en voorbereidingshandelingen voor verstoring en sabotage.
- Statelijke actoren zetten ook **cyberaanvallen** in om hun politieke, militaire en/of economische doelen te bereiken. Verschillende voorbeelden in Europa en de VS laten zien hoe o.a. China, Rusland en Iran cyberaanvallen op westerse overheden en vitale aanbieders uitvoeren. Hoewel cyberaanvallen op vitale infrastructuur in Nederland tot op heden geen ontwrichtende impact op de nationale veiligheid hebben gehad zijn deze aan de orde van de dag. Statelijke actoren gebruiken cyberaanvallen o.a. om toegang tot vitale processen te verkrijgen en deze bijvoorbeeld op een later moment te kunnen verstoren. Daarnaast kunnen ze cyberaanvallen gebruiken voor spionage en voor financieel gewin. In de praktijk is er sprake van een vermenging tussen statelijke actoren en hacktivisten die uit ideologische overwegingen cyberaanvallen uitvoeren.
- Hoewel er weinig bekend is over de impact van **desinformatie** op het functioneren van de vitale infrastructuur, is dit ook een hybride dreiging die invloed kan hebben op vitale aanbieders en processen.
- In tijden van toenemende concurrentie tussen grootmachten proberen statelijke actoren **economische druk en strategische afhankelijkheden** te gebruiken om invloed uit te oefenen. Bijvoorbeeld door middel van handelsbeperkende maatregelen, door misbruik te maken van de aanwezigheid van buitenlandse bedrijven in de Nederlandse vitale infrastructuur of door misbruik te maken van strategische afhankelijkheden. Strategische afhankelijkheden kunnen ook een dreiging voor de continuïteit van vitale processen vormen wanneer levering onderbroken wordt door een conflict elders in de wereld of doordat de afhankelijkheid de Nederlandse open strategische autonomie beperkt. Strategische afhankelijkheden bestaan ten opzichte van landen, maar ook ten opzichte van één of enkele (tech)bedrijven.

- Ook **terroristen en gewelddadig extremisten** kunnen een dreiging vormen voor de vitale infrastructuur. In Nederland zijn er geen ontwrichtende terroristische of extremistische aanslagen op vitale infrastructuur gepleegd. Wel laten accelerationistische publicaties en buitenlandse voorbeelden zien dat vitale processen doelwit van terroristen en gewelddadig extremisten kunnen zijn. Daarnaast kunnen vitale aanbieders geconfronteerd worden met medewerkers met extremistisch gedachtengoed, zoals soevereinen en rechts-extremisten.
- Verschillende protesten en **activistische acties** in Nederland en Europa hebben de afgelopen jaren laten zien dat ook activisten en demonstranten zich kunnen richten op vitale sectoren of dat hun activiteiten hier effect op kunnen hebben. Verschillende acties hebben de afgelopen jaren geleid tot kortdurende hinder van vitale infrastructuur zoals luchthavens, weginfrastructuur en een sluizencomplex. De nationale veiligheidsbelangen kwamen hierbij niet in het geding.
- Ook **criminele activiteiten** kunnen een dreiging voor de vitale infrastructuur vormen. Het gaat hierbij vaak om cyberaanvallen door criminelen, maar het kan ook om ondermijnende criminaliteit of fysieke handelingen gaan. Cybercriminelen handelen vanuit financieel motief en hebben niet de (primaire) intentie om de maatschappij te ontwrichten. Hoewel criminele cyberaanvallen de afgelopen jaren in Nederland niet tot maatschappelijke ontwrichting hebben geleid, laten verschillende incidenten wel zien hoe vitale sectoren door cyberaanvallen geraakt kunnen worden.

Natuurlijke dreigingen voor de vitale infrastructuur

- Vitale processen kunnen te maken krijgen met verschillende natuurlijke dreigingen. Met name de gevolgen van **klimaatverandering**, die versnelt en ernstiger wordt dan eerder gedacht, vormen een toenemende dreiging voor de vitale infrastructuur.
- Door klimaatverandering worden de wateropgaven voor Nederland substantieel groter. In de zomer nemen zoetwatertekorten toe, er ontstaat meer wateroverlast door regenbuien en de gevolgen van overstromingen worden groter. Wateroverlast kan ontwrichtend werken wanneer de functies van vitale netwerken uitvallen. De afgelopen jaren leidde extreme neerslag in verschillende Europese landen onder andere tot stroomuitval, het stilleggen van het openbaar vervoer en het sluiten van een vliegveld. Klimaatverandering leidt ook tot extreme hitte én droogte in de zomer. Bij langdurige droogte kunnen vitale processen, zoals de drinkwatervoorziening en binnenvaart, onder druk komen te staan. Daarnaast nemen natuurbranden toen en zullen deze vaker tot schade en uitval van vitale infrastructuur leiden.
- Als gevolg van de versnellende klimaatverandering versnelt ook de wereldwijde zeespiegelstijging. In Nederland zal zeespiegelstijging vooral gevolgen hebben voor de waterveiligheid en de beschikbaarheid van zoetwater.
- Er zijn geen recente voorvallen van verstoring of uitval van vitale processen door een aardbeving in Nederland bekend.
- Sommige vitale processen maken gebruik van geavanceerde technologieën die kwetsbaar kunnen zijn voor **ruimteweer**, zoals zonnevlammen, coronale massa-ejecties en protonenstormen. Ruimteweer kan onder andere communicatie en navigatie tijdelijk verstoren of satellieten beschadigen.

Dreigingen voortkomend uit het falen van vitale processen zelf

- De nationale veiligheid kan ook in het geding komen wanneer vitale processen uitvallen door menselijke fouten, systeemfalen of door keteneffecten.
- Bij **menselijk falen** is er sprake van uitval of verstoring van een vitaal proces door een onopzettelijke menselijke fout. Bij **systeemfalen** ligt de oorzaak in een technische fout in het systeem zelf. Verschillende voorbeelden, zoals de CrowdStrike- en NAFIN-storingen, laten zien dat een ogenschijnlijk kleine technische of menselijke fout grote gevolgen kan hebben voor vitale processen en in vergaande gevallen zelfs een dreiging voor de nationale veiligheid kan vormen.
- Door onderlinge afhankelijkheden binnen de vitale infrastructuur kan een verstoring binnen één vitaal proces leiden tot **keteneffecten** in andere vitale processen. Door de complexiteit van systemen, toenemende afhankelijkheden tussen systemen en processen en veel onderlinge en verborgen afhankelijkheden is het moeilijk een goede inschatting te maken van de keteneffecten van verstoring van vitale processen. Vitale processen zijn daarnaast ook verbonden met allerlei niet-vitale processen. Verstoringen van deze niet-vitale processen kunnen eveneens grote keteneffecten hebben op vitale processen

Politieke, economische, sociale en technologische factoren

- Verschillende politieke, economische, sociale en technologische factoren beïnvloeden de vitale infrastructuur zelf, de dreigingen op en de weerbaarheid van de vitale infrastructuur.
- Belangrijke ontwikkelingen zijn onder andere de toenemende afhankelijkheid van vitale processen van complexe digitale systemen. Daarnaast beïnvloeden technologische ontwikkelingen, zoals kunstmatige intelligentie, ruimte-technologie en quantumtechnologie, de veiligheidsomgeving van vitale processen. Ook de energietransitie heeft gevolgen voor de vitale infrastructuur. Krapte op de arbeidsmarkt zorgt voor personeelstekorten bij vitale aanbieders, waardoor deze minder weerbaar worden tegen dreigingen. Tot slot kunnen economische ontwikkelingen wereldwijd invloed hebben op vitale processen.

1. Inleiding

De Nederlandse samenleving is sterk afhankelijk van vitale processen, zoals elektriciteit, toegang tot internet, drinkwater en betalingsverkeer. Deze processen zijn vitaal omdat verstoring of uitval grote gevolgen kan hebben voor het functioneren van de Nederlandse en Europese economie en maatschappij. Dergelijke verstoring of uitval kunnen een dreiging vormen voor de nationale veiligheid.[1]

De vitale infrastructuur wordt geconfronteerd met een stapeling van uiteenlopende en toenemende dreigingen. Geopolitieke spanningen vormen een toenemende dreiging voor onze vitale infrastructuur. Door oorlogen en de concurrentie tussen grootmachten zoals Rusland en China, is Nederland doelwit van hybride aanvallen. Onder hybride aanvallen verstaan we de inzet van een mix van civiele en militaire instrumenten om bepaalde strategische doelstellingen te bereiken, zonder dat er sprake is van een gewapend conflict. Hybride instrumenten worden ingezet door statelijke actoren en niet-statelijke actoren die met een staat samenwerken.[2] Deze aanvallen kunnen de vorm aannemen van onder andere fysieke en digitale spionage en sabotage, desinformatie en economische destabilisatie. Geopolitieke ontwikkelingen kunnen bijvoorbeeld leiden tot verstoringen in toeleveringsketens, wat grote gevolgen kan hebben voor de vitale infrastructuur.

Daarnaast vormen de gevolgen van klimaatverandering een toenemende dreiging voor de vitale infrastructuur. Door de opwarming van de aarde neemt de kans op weersomstandigheden zoals extreme hitte, droogte en neerslag toe. Deze extreme weersomstandigheden kunnen leiden tot verstoringen of uitval van vitale processen zoals energievoorzieningen, waterbeheer en transport. Hoewel de precieze gevolgen van klimaatverandering moeilijk te voorspellen zijn, is het duidelijk dat de combinatie van verschillende klimaatontwikkelingen een toenemende dreiging vormt voor de soms kwetsbare vitale processen.

Verschillende recente incidenten, zoals de CrowdStrike-storing in juli 2024[1], laten zien dat ook menselijke fouten, systeemfalen en keteneffecten vitale processen kunnen verstoren. Tot slot beïnvloeden verschillende politieke, economische, sociale en technologische factoren de dreigingen voor en weerbaarheid van vitale infrastructuur. Zo maken de toenemende afhankelijkheid van digitale systemen, krapte op de arbeidsmarkt en fragmentatie van de wereldeconomie de vitale infrastructuur minder weerbaar voor dreigingen en kunnen technologische ontwikkelingen bestaande dreigingen versterken.

Vitale processen, -infrastructuur en -aanbieders

Binnen de Aanpak Vitaal van de Rijksoverheid wordt gesproken over de bescherming van vitale processen. Voorbeelden hiervan zijn 'keren en beheren van de waterkwantiteit', 'internet en datadiensten' of 'toonbankbetalingsverkeer'. Een vitaal proces is een proces waarvan uitval, verstoring of manipulatie tot dusdanig ernstige effecten kan leiden dat dit de nationale veiligheid kan schaden en daarmee maatschappelijke ontwrichting kan veroorzaken. Het is aan ieder vakdepartement om middels een vitaalbeoordeling te beoordelen welke processen binnen hun beleidsdomein vitaal zijn. In de Wet weerbaarheid kritieke entiteiten (Wwke) wordt gesproken over het borgen van de continuïteit van essentiële diensten binnen de Europese Unie. Een essentiële dienst is een dienst die van cruciaal belang is voor de instandhouding van vitale maatschappelijke functies, economische activiteiten, de volksgezondheid en openbare veiligheid of het milieu. Deze essentiële diensten kunnen worden gezien en aangemerkt als vitaal proces. De vitale processen samen vormen de vitale infrastructuur van Nederland.[3]

Binnen een vitaal proces is één of zijn meerdere organisaties, zoals private bedrijven, publieke organisaties, zelfstandige bestuursorganen en onderdelen van de Rijksoverheid belangrijk voor de continuïteit en weerbaarheid van het proces. Deze organisaties worden aangeduid als vitale aanbieders. Zie voor een overzicht van alle vitale processen, een uitgebreide toelichting van de Aanpak Vitaal van de Rijksoverheid en de daarin gebruikte definities de website van de NCTV.

Doel en afbakening dreigingslandschap

Dit eerste dreigingslandschap vitale infrastructuur geeft een overzicht van de belangrijkste dreigingen voor de vitale infrastructuur en inzicht in recente ontwikkelingen met betrekking tot die dreigingen. Op basis daarvan kan de komende jaren getoetst worden of gebeurtenissen passen binnen de in dit dreigingslandschap beschreven dreigingen of dat deze daarvan afwijken. Dit dreigingslandschap kan daarmee worden gezien als een referentiepunt.

Om een goed beeld te krijgen van risico's voor de vitale processen is naast inzicht in dreigingen ook inzicht nodig in weerbaarheid en de mate waarin de nationale veiligheidsbelangen worden geraakt (zie hoofdstuk 2 voor een toelichting op deze belangen). Weerbaarheid en nationale veiligheidsbelangen worden in dit

[1] Hierbij leidde een foutieve update van de software van CrowdStrike in verschillende landen tot uitval en verstoring van vitale processen. Zie ook paragraaf 5.1.

dreigingslandschap alleen kort besproken. Door de breedte van de vitale infrastructuur kan er, op basis van openbare bronnen, maar beperkt inzicht in deze aspecten worden gegeven.

Daarnaast biedt het dreigingslandschap vakdepartementen en vitale aanbieders een denkkader dat hen kan helpen voor specifieke vitale processen beter inzicht te krijgen in dreigingen, de weerbaarheid, de veiligheidsbelangen die worden geraakt bij verstoring of uitval en de risico's voor de nationale veiligheid die daar uit voortkomen.

Dit dreigingslandschap kan daarmee door vakdepartementen en vitale aanbieders worden gebruikt als startpunt voor het maken van risico- en weerbaarheidsanalyses voor de verschillende vitale processen die in het kader van de cyclus vitaal en ten behoeve van de Wet weerbaarheid kritieke entiteiten (Wwke) zullen worden gemaakt. De vitale infrastructuur bestaat uit een groot aantal diverse vitale processen en aanbieders. Deze hebben op hun beurt weer te maken met een breed scala aan (potentiële) dreigingen. De in dit dreigingslandschap beschreven dreigingen zijn relevant voor de meeste vitale processen. Het is echter niet mogelijk om hier een gedetailleerd totaaloverzicht te geven van alle denkbare dreigingen voor alle vitale processen en aanbieders. Daarvoor zijn de dreigingen waar alle individuele vitale processen en aanbieders mee te maken kunnen krijgen te veelomvattend, uiteenlopend en soms te specifiek voor één vitaal proces.

Dit dreigingslandschap is uitsluitend gebaseerd op openbare bronnen en sluit zo veel mogelijk aan bij bestaande dreigingsproducten, zoals het Dreigingsbeeld Statelijke Actoren, het Cybersecuritybeeld Nederland, het Dreigingsbeeld Terrorisme Nederland, de Rijksbrede Risicoanalyse Nationale Veiligheid, de Trendanalyse Nationale Veiligheid 2024, het Dreigingsbeeld militaire en hybride dreigingen, de jaarverslagen van de AIVD en de MIVD en de Deltascenario's. Daarbij wordt in dit dreigingslandschap, op basis van de bestaande inzichten, zo veel mogelijk expliciet de vertaling naar de vitale infrastructuur gemaakt.

Leeswijzer

Dit dreigingslandschap begint in hoofdstuk 2 met een toelichting op de driehoek van dreigingen, nationale veiligheidsbelangen en de weerbaarheid van de vitale infrastructuur. Hoofdstuk 3 biedt een overzicht van de belangrijkste moedwillige dreigingen voor de vitale infrastructuur. Daarbij zal worden ingegaan op de dreiging vanuit statelijke actoren, terrorisme, activisme en criminele activiteiten. Hoofdstuk 4 gaat over natuurlijke dreigingen voor de vitale infrastructuur, waaronder de gevolgen van klimaatverandering, ruimteweer, infectieziekten en aardbevingen. Hoofdstuk 5 gaat over het falen van vitale processen zelf en keteneffecten die hier uit kunnen ontstaan. Hoofdstuk 6 beschrijft de belangrijkste politieke, economische, sociale en technologische factoren die van invloed zijn op dreigingen, weerbaarheid en de vitale infrastructuur zelf.

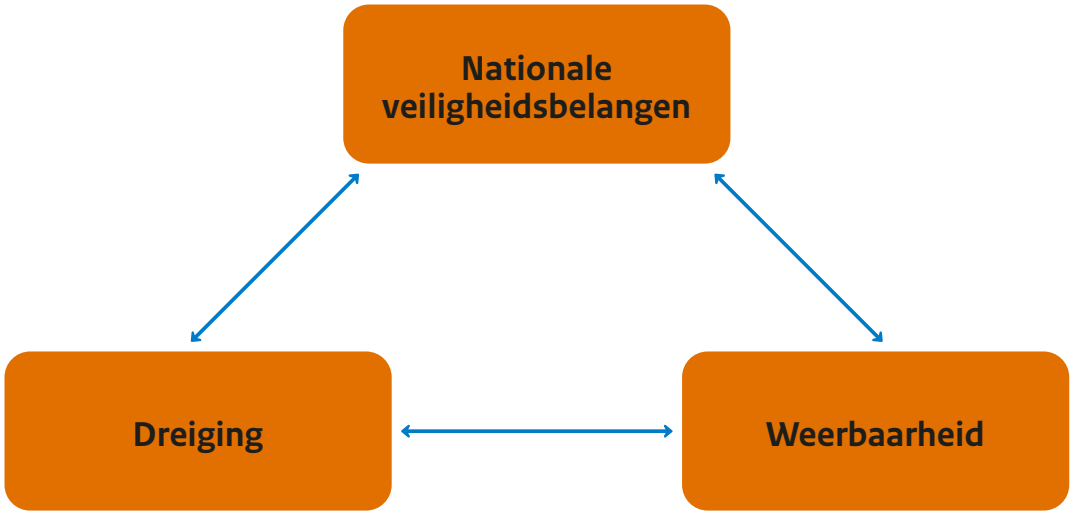
Verschillende stuwen beschermen steden in Nederland tijdens hoogwater. Zo ook deze stuw bij Borgharen die veel water verwerkt bij een hoge waterstand in de Maas.

2. Denkkader dreigingen, NV-belangen en weerbaarheid van de vitale infrastructuur

Om een goede inschatting te kunnen maken van de risico's voor de vitale processen, en daarmee voor onze nationale veiligheid, is inzicht in drie aspecten noodzakelijk: de dreigingen die op een vitaal proces afkomen, de weerbaarheid van vitale processen en de mate waarin de nationale veiligheidsbelangen worden geraakt. Risico's voor de nationale veiligheid bestaan wanneer een vitaal proces wordt geconfronteerd met dreigingen, onvoldoende weerbaar is voor die dreigingen en wanneer verstoring of uitval van een vitaal proces er toe leidt dat één of meerdere nationale veiligheidsbelangen in het geding komen. Deze risico's kunnen er ook zijn zonder dat ze zich manifesteren in concrete incidenten, bijvoorbeeld omdat de vitale infrastructuur zeer weerbaar is tegen een dreiging.

Zonder weerbaarheidsverhogende maatregelen zou de stijgende zeespiegel bijvoorbeeld een grote dreiging voor grootschalige overstromingen vormen. Nederland ligt immers voor 26% onder zeeniveau en circa 60% van het land is gevoelig voor overstromingen.[4] Bij een grootschalige overstroming zouden verschillende nationale veiligheidsbelangen in het geding komen. Dankzij dijkversterkingen, stormvloedkeringen, zandsuppleties en pompen voor waterveiligheid is Nederland echter weerbaar tegen (waarschijnlijk) 3 meter zeespiegelstijging en is het risico op overstromingen door de zeespiegelstijging klein.[5]

Bij analyses met betrekking tot de nationale veiligheid is de driehoek van dreigingen, te beschermen belangen en de weerbaarheid het uitgangspunt (zie figuur 1).



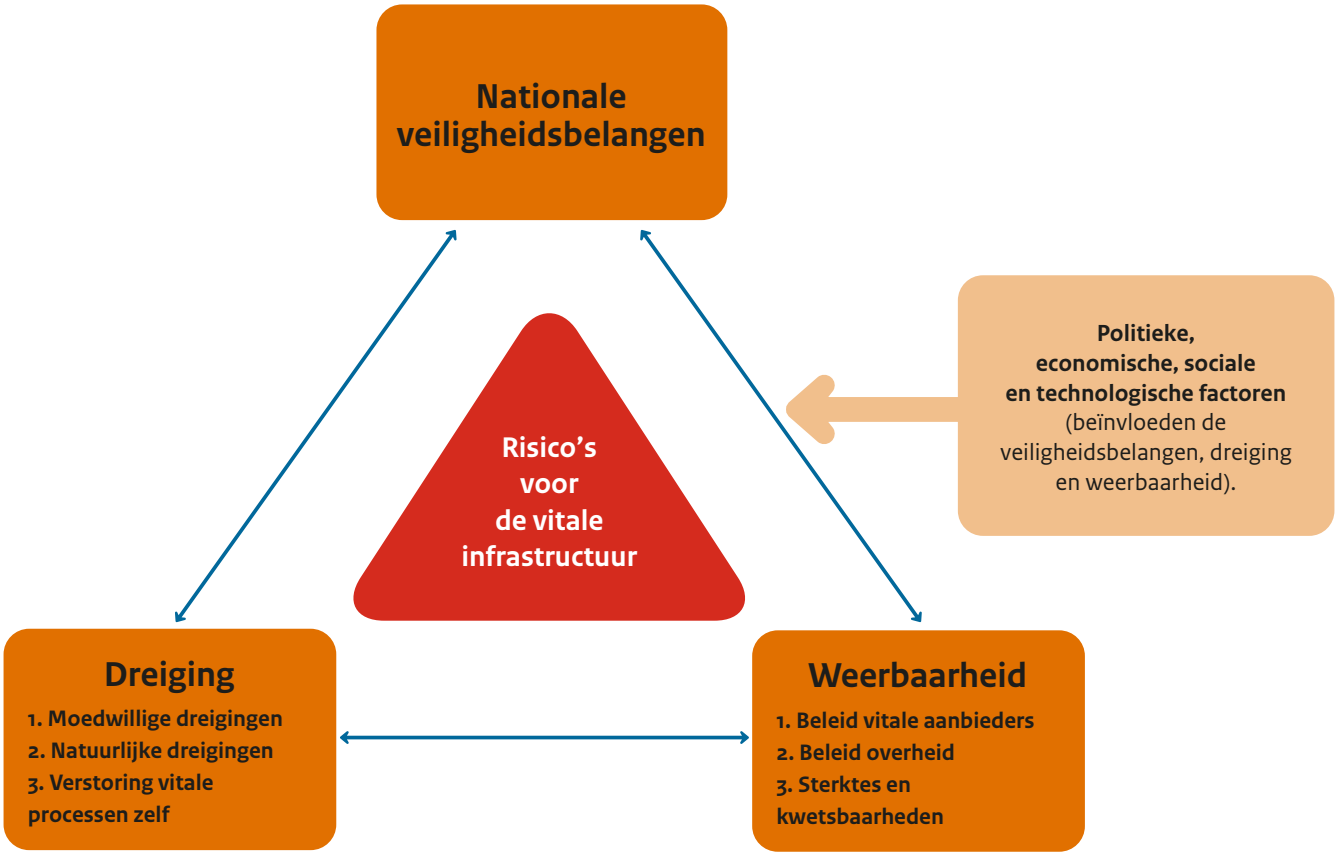
Figuur 1: De algemene driehoek van dreiging, belang en weerbaarheid.

Dreigingen

Een dreiging is de waarschijnlijkheid dat een opzettelijke of niet-opzettelijke gebeurtenis zich voordoet die kan leiden tot verstoring of uitval van vitale processen of die hun integriteit en vertrouwelijkheid kan aantasten, waarbij één of meerdere nationale veiligheidsbelangen in het geding komen.[2] Dit dreigingslandschap onderscheidt, in lijn met de Rijksbrede Risicoanalyse Nationale Veiligheid, drie soorten dreigingen voor de vitale infrastructuur: moedwillige dreigingen, natuurlijke dreigingen en dreigingen die voortkomen uit het falen van vitale processen zelf.[6]

Vitale infrastructuur is een aantrekkelijk doelwit voor kwaadwillenden, zoals statelijke actoren. Dit komt onder andere door de potentiële maatschappelijke impact van verstoring en uitval of het in het geding komen van de integriteit en vertrouwelijkheid van vitale processen.[7] Verschillende voorbeelden in dit dreigingslandschap laten zien dat de vitale infrastructuur kwetsbaar is. Er is soms maar weinig voor nodig om vitale processen, zoals energie, telecommunicatie, de transportsector en drinkwatervoorziening te ontwrichten.[8] Daarnaast kunnen ook natuurlijke fenomenen, zoals extreem weer en natuurrampen, vitale processen verstoren.[9] Door klimaatverandering ontstaan er steeds vaker extreme weersomstandigheden en wordt het steeds waarschijnlijker dat vitale infrastructuur door natuurlijke oorzaken verstoord raakt.[10] Tot slot kunnen menselijke of systeemfouten ook leiden tot verstoring of uitval van vitale infrastructuur.[11]

Omdat vitale processen geconfronteerd worden met een opeenstapeling van uiteenlopende dreigingen kunnen meerdere dreigingen zich gelijktijdig voordoen waarbij het risico op verstoring of uitval van vitale processen toeneemt. Zo geldt bijvoorbeeld dat een cyberaanval bij een enkelvoudig incident over het algemeen gemitigeerd kan worden. Wanneer een aanval wordt gecombineerd met een andere gebeurtenis zal dit moeilijker zijn. Denk bijvoorbeeld aan een aanval op spoorvervoerders tijdens groot onderhoud aan het spoor of een aanval op waterbeheerders tijdens een grote storm.[12]



Figuur 2: De driehoek van dreiging, belang en weerbaarheid van de vitale infrastructuur.

[2] Er worden in verschillende studies en analyses soms iets van elkaar verschillende definities voor dreigingen gebruikt. Dit is de definitie die in dit dreigingslandschap, specifiek voor de vitale infrastructuur, wordt gehanteerd.

Een verstoring van een vitaal proces kan 'eigenstandig' zijn en heeft in dat geval geen effect op andere vitale processen. Omdat een belangrijk kenmerk van de vitale infrastructuur is dat vitale processen van elkaar afhankelijk zijn, kunnen ook keteneffecten (ook wel cascade-effecten genoemd) optreden. Hierbij worden meerdere processen geraakt.[13] Bij een overstroming kan uitval van de stroomvoorziening bijvoorbeeld impact hebben op onderdelen van het internet of op het functioneren van ziekenhuizen.[14]

Nationale veiligheidsbelangen

Vitale processen en aanbieders krijgen met tal van dreigingen te maken. Er is echter pas sprake van een dreiging voor de nationale veiligheid wanneer een of meerdere nationale veiligheidsbelangen in het geding zijn. De zes nationale veiligheidsbelangen zijn:

1. *Territoriale veiligheid*: dit belang omvat onder andere de integriteit van het Nederlandse grondgebied, de integriteit van de digitale ruimte (IT-netwerken en informatiesystemen) en de integriteit van het bondgenootschappelijk grondgebied.
2. *Fysieke veiligheid*: dit belang omvat het ongestoord functioneren van individuen. Deze kan bijvoorbeeld in het geding komen door ongelukken, aanslagen, ziekten of gebrek aan primaire levensbehoeften.
3. *Economische veiligheid*: dit belang omvat het ongestoord functioneren van Nederland als een effectieve en efficiënte economie. Hierbij gaat het onder andere over de continuïteit van vitale processen, het mitigeren van risicovolle strategische afhankelijkheden en het voorkomen van de ongewenste overdracht van kennis en technologie.
4. *Ecologische veiligheid*: dit belang omvat het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in Nederland. Deze komt in het geding wanneer de natuur en het milieu langdurig worden aangetast.
5. *Sociale en politieke stabiliteit*: dit belang omvat het ongestoord voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtstaat en de daarin gedeelde waarden.
6. *Internationale rechtsorde en stabiliteit*: dit belang gaat over het goed functioneren van het internationale stelsel van normen en afspraken, gericht op het bevorderen van de internationale vrede en veiligheid.[15]

Een uitgebreide toelichting op de nationale veiligheidsbelangen is terug te vinden in de Leidraad risicobeoordeling Rijksbrede Risicoanalyse Nationale Veiligheid.

Hoewel de continuïteit van vitale processen onderdeel is van de economische veiligheid, kan verstoring of uitval van een vitaal proces impact hebben op alle nationale veiligheidsbelangen.[16] Bij een grote en langdurige storing in de elektriciteitsvoorzieningen en/of digitale infrastructuur kan bijvoorbeeld niet alleen de economische veiligheid worden aangetast, maar kan er ook sociale onrust ontstaan. Daarnaast kan de fysieke veiligheid in het geding komen wanneer bijvoorbeeld ziekenhuizen geen essentiële zorg meer kunnen verlenen.

Weerbaarheid

Er bestaan verschillende definities van weerbaarheid. Onderzoeksbureau RAND onderzocht de verschillende manieren waarop het concept weerbaarheid wordt gebruikt en geïnterpreteerd in Nederlandse beleidsdocumenten over nationale veiligheid. Op basis daarvan stelden zij een werkdefinitie op van weerbaarheid in het kader van de nationale veiligheid. Deze luidt: *weerbaarheid is het vermogen van de samenleving om voorbereid te zijn op maatschappelijke ontwrichting, deze te weerstaan, te absorberen en/of een nieuw evenwicht te bereiken.*[17] Hoewel verstoringen of uitval van vitale processen waarbij één of meerdere nationale veiligheidsbelangen in het geding komen vaak zullen leiden tot maatschappelijke ontwrichting, is het in de context van de vitale infrastructuur ook mogelijk dat er sprake is van ecologische ontwrichting, zonder grote maatschappelijke effecten. Dat kan bijvoorbeeld het geval zijn wanneer uitval of verstoring van een vitaal proces grote en langdurige schade aan de natuur of het milieu toebrengt, zonder dat mensen hier (op grote schaal) door worden geraakt.

De definitie van RAND komt grotendeels overeen met de definitie van weerbaarheid in de Wet weerbaarheid kritieke entiteiten (Wwke)[3], die weerbaarheid definieert als *het vermogen van een kritieke entiteit om een incident te voorkomen, te beperken en te beheersen, en om bescherming te bieden en bestand te zijn tegen, te reageren op of, zich aan te passen aan en te herstellen van een incident.*[18]

In dit dreigingslandschap gaan we ervan uit dat de weerbaarheid van vitale processen en de vitale infrastructuur als geheel door drie aspecten wordt bepaald:

1. *Het beleidsinstrumentarium van vitale aanbieders* gericht op het voorkomen en mitigeren van dreigingen. Het merendeel van de vitale processen is in handen van private partijen. Zij zijn primair verantwoordelijk voor de continuïteit en weerbaarheid van vitale processen en nemen passende maatregelen om deze te beschermen tegen dreigingen. De weerbaarheid van vitale processen wordt mede bepaald door de mate waarin vitale aanbieders voorbereid zijn op ontwrichting, deze kunnen weerstaan, absorberen en/of een nieuw evenwicht kunnen bereiken. Vitale aanbieders bevorderen hun weerbaarheid onder andere met preventieve maatregelen, continuïteits- en crisismanagement. Denk hierbij bijvoorbeeld aan cybersecurity-maatregelen om digitale aanvallen te weerstaan, screening van personeel om *insider threats* te voorkomen of het aanpassen van infrastructuur en materieel op de veranderende klimaatomstandigheden.
2. *Het beleidsinstrumentarium van de overheid.* Vakdepartementen stellen kaders op voor de sectoren die onder hun verantwoordelijkheid

[3] De Wwke is de nationale wetgeving ter implementatie van de Europese CER-richtlijn (Critical Entities Resilience) en richt zich op de bescherming van kritieke entiteiten tegen alle natuurlijk en door de mens veroorzaakte risico's.

vallen. Dit omvat onder andere sectorale beleid-, wet- en regelgeving. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft een coördinerende rol bij de bescherming van de vitale infrastructuur. Hierbij gaat het om de sector-overstijgende aanpak zoals het opstellen van algemene beleid-, wet- en regelgeving en het ontwikkelen van weerbaarheids-verhogende instrumenten zoals de Cyclus Vitaal. De weerbaarheid van vitale processen wordt mede bepaald door de mate waarin het overheidsbeleid vitale aanbieders en de samenleving voorbereidt op ontwrichting, deze kan weerstaan, absorberen en/of een nieuw evenwicht bereiken. Zie voor een uitgebreide toelichting op alle betrokken overheidsorganisaties en hun rollen en verantwoordelijkheden de website van de NCTV.

3. *Sterktes en kwetsbaarheden* van Nederland en de vitale infrastructuur. Het gaat hierbij om zaken zoals geografische, ruimtelijke, maatschappelijke en economische kenmerken die invloed hebben op de mate waarin vitale processen ontvankelijk zijn voor dreigingen. Zo heeft Nederland bijvoorbeeld een kleine en open economie die gericht is op internationale handel. Hierdoor is de economie kwetsbaar voor internationale (economische) ontwikkelingen die bijvoorbeeld de financiële positie of toeleveringsketens van vitale aanbieders kunnen beïnvloeden.[19] En de geografische ligging als toegangspoort tot Europa en de rol van Nederland als logistieke spil binnen de NAVO maakt de vitale infrastructuur bijvoorbeeld kwetsbaar voor hybride aanvallen.[20] En het feit dat Nederland een laaggelegen en tevens dichtbevolkte rivierdelta is, waar de grote Europese rivieren Rijn, Maas en Schelde de zee in stromen, maakt het land en delen van de vitale infrastructuur (zonder weerbaarheidsverhogende maatregelen) kwetsbaar voor overstromingen.[21]

Voor een goed begrip van de weerbaarheid van individuele vitale processen en de vitale infrastructuur als geheel is het dus noodzakelijk inzicht te hebben in de effectiviteit van het beleidsinstrumentarium van vitale aanbieders en de overheid en de sterktes en zwaktes die van invloed zijn op de ontvankelijkheid van de vitale infrastructuur voor dreigingen. Omdat het te omvangrijk en complex is dit voor de gehele vitale infrastructuur in kaart te brengen en bovendien onderdeel zal zijn van de weerbaarheids-analyses die de vakdepartementen in het kader van de Cyclus Vitaal gaan maken valt dit buiten de scope van dit dreigingslandschap.

Politieke, economische, sociale en technologische factoren

De vitale infrastructuur zelf, de weerbaarheid ervan en de dreigingen waarmee vitale processen worden geconfronteerd, worden daarnaast beïnvloed door verschillende politieke, economische, sociale en technologische (PEST) factoren. Deze kunnen ervoor zorgen dat dreigingen worden versterkt of juist afnemen of dat vitale infrastructuur ontvankelijk of juist weerbaarder wordt voor de dreigingen. Denk aan technologische ontwikkelingen zoals AI die bestaande dreigingen versterken of krapte op de arbeidsmarkt die vitale aanbieders minder weerbaar maakt door tekort aan technisch personeel.

In de Noordzee liggen vitale infrastructuren, denk daarbij aan internetkabels en gaspijpleidingen. De Kustwacht houdt verdachte activiteiten op zee in de gaten om sabotage voortijdig op te sporen.

3. Moedwillige dreigingen voor de vitale infrastructuur

Vitale processen kunnen te maken krijgen met verschillende moedwillige dreigingen. Hieronder wordt ingegaan op de dreiging vanuit statelijke actoren, terrorisme en gewelddadig extremisme, activisme en criminele activiteiten op de vitale infrastructuur. Met name hybride aanvallen door statelijke actoren of hun proxies vormen een toenemende dreiging voor vitale processen. Deze kunnen niet alleen leiden tot verstoring of uitval, maar kunnen ook de integriteit en vertrouwelijkheid van vitale processen onder druk zetten. Dit is bijvoorbeeld het geval bij spionage en pre-positionering voor sabotage.

In sommige gevallen richten kwaadwillende actoren zich doelbewust op een specifiek deel van de vitale infrastructuur. Regelmatig gaan actoren zoals staten en criminelen echter ook opportunistisch te werk. Ze kijken dan hoe ze hun doelen het best kunnen bereiken en richten hun activiteiten, zoals cyberaanvallen, op een breed scala aan systemen en (vitale) infrastructuur waar de aanvallers zelf geen specifieke kennis van hebben. Zeker wanneer vitale processen een lage weerbaarheid hebben kunnen ze in zo'n geval slachtoffer worden van deze activiteiten.

3.1 Statelijke actoren vormen een toenemende dreiging voor vitale infrastructuur

Door oorlogen, geopolitieke spanningen en groeiende competitie tussen grootmachten is de wereld rondom Nederland en de Europese Unie instabieler geworden. De Europese veiligheidssituatie is daardoor in rap tempo verslechterd.[22] Met name Rusland en China vormen op verschillende manieren een dreiging voor de Nederlandse vitale infrastructuur.[23]

Rusland zoekt de confrontatie met het Westen en gebruikt daarbij een breed arsenaal aan middelen om westerse landen schade toe te brengen en zijn eigen positie te verbeteren.[24] Dit doet Rusland onder andere door middel van fysieke en digitale sabotage, het verzamelen van informatie over onze vitale infrastructuur en het verspreiden van desinformatie.[25] Ook China streeft naar een leidende rol in de wereld en daagt daarbij de bestaande wereldorde uit. Het land gebruikt verschillende middelen om zijn invloed te vergroten, waaronder spionage, economische investeringen, technologische ontwikkeling en het in zijn eigen voordeel veranderen van internationale instituties. De Chinese ambities hebben gevolgen voor Nederland, zoals economische afhankelijkheid en geavanceerde cyberaanvallen.[26] Rusland en China werken daarnaast economisch, politiek en militair samen. Zo draagt China direct en indirect bij aan het in stand houden van de Russische oorlogsinspanningen in Oekraïne.[27]

De steeds hardere concurrentie tussen grootmachten uit zich onder andere in een toename van de inzet van hybride instrumenten.[28] Ze blijven hiermee onder de drempel van een gewapend conflict, maar kunnen wel de Nederlandse vitale infrastructuur en de nationale veiligheid schaden.[29]

In deze paragraaf worden de volgende hybride dreigingen door statelijke actoren voor de vitale infrastructuur beschreven: sabotage, spionage en pre-positionering, cyberaanvallen, desinformatie, economische druk en misbruik van strategische afhankelijkheden.

Een militair conflict wordt meestal voorafgegaan door dergelijke hybride dreigingen.[30] Voor het eerst in lange tijd is het reëel dat Nederland, via de collectieve verdedigingsclausule in het NAVO-verdrag (artikel 5), direct betrokken raakt bij een grootschalig gewapend conflict. Dat conflict hoeft zich niet in Nederland af te spelen. De Nederlandse vitale infrastructuur kan ook een doelwit worden wanneer Nederland betrokken raakt bij een gewapend conflict in een andere NAVO-lidstaat of wanneer deze zich in de nabijheid van Nederland afspeelt.[31] Ruslands optreden in en agressie tegen Oekraïne vormen daarbij de grootste dreiging. De hervorming van de Russische krijgsmacht is namelijk gericht op een toekomstig conflict

met de NAVO. Ook blijft het land stappen zetten op de escalatieladder tegen de NAVO. In deze dynamiek bestaat het risico tot ongewilde escalatie.[32]

3.1.1 Sabotage vitale infrastructuur door statelijke actoren

Vitale infrastructuur kan een aantrekkelijk doelwit zijn voor sabotage door statelijke actoren.[33] Nederland is een digitaal en fysiek knooppunt en toegangspoort tot Europa. Onder andere hierdoor is de Nederlandse vitale infrastructuur in principe een interessant doelwit voor sabotage, bijvoorbeeld om logistieke steun naar Oekraïne of militaire troepenaanvoer naar Oost-Europa te verstoren.[34] Naast maatschappelijke ontwrichting kan sabotage van vitale infrastructuur ook tot doel hebben om druk op landen uit te oefenen, de autonomie van andere landen aan te tasten of te testen hoe landen en de NAVO reageren op sabotageacties.

Er zijn in Nederland geen recente voorbeelden geweest van geslaagde fysieke sabotage van vitale infrastructuur die ondubbelzinnig verbonden kunnen worden met statelijke actoren.[35] Verschillende Europese voorvallen laten echter zien dat vitale infrastructuur kwetsbaar is voor hybride aanvallen en dat actoren ook bereid zijn om daadwerkelijk tot sabotage over te gaan. Daarnaast kan sabotage van vitale infrastructuur bij Europese bondgenoten door ketenafhankelijkheden ook impact op de nationale veiligheid hebben.[36]

Hieronder worden drie ontwikkelingen nader uitgelicht die inzicht geven in de huidige dreiging van sabotage van vitale infrastructuur door statelijke actoren:

1. De toename van Russische sabotageacties in Europa.
2. Recente sabotageacties gericht op onderwaterinfrastructuur.
3. De toename van moedwillige verstoringen van GNSS-signalen.

Toename Russische sabotageacties in Europa

Westerse landen houden Rusland er voor verantwoordelijk dat het land de afgelopen jaren op verschillende plekken in Europa aanslagen en sabotage heeft gepleegd of dit heeft gepoogd te doen. In enkele gevallen waren ook deelprocessen van vitale sectoren doelwit. Soms maakt het land hierbij gebruik van proxies om de eigen betrokkenheid te verhullen.[37] Onderzoek van de Universiteit Leiden toont een sterke toename in 2024 van het aantal Russische sabotageacties gericht op Europese landen.[38] Volgens de Strategische Monitor 2025 van The Hague Centre for Strategic Studies (HCSS) is het aantal Russische hybride aanvallen op Europa in 2024 ruim verdubbeld ten opzichte van het jaar ervoor[4].[39] Het doel van deze sabotageacties is meerledig. Enerzijds richt sabotage zich op het vertragen van westerse leveranties aan Oekraine. Anderzijds richten deze activiteiten zich op het zaaien van verdeeldheid en het aanjagen van angst in het Westen. Daarnaast kan Rusland door middel van de sabotageactiviteiten testen waar het Westen rode lijnen trekt als het gaat om Russische agressie op het eigen grondgebied.

In april 2024 zijn er in Duitsland bijvoorbeeld twee Duits-Russische staatsburgers gearresteerd die namens Rusland met explosieven en brandstichting militaire en industriële infrastructuur wilden aanvallen.[40] Volgens de Duitse federale openbaar aanklager wilde een van de mannen onder andere spoorwegen aanvallen die worden gebruikt voor militaire transporten.[41] Diezelfde maand werden er in het Verenigd Koninkrijk twee mannen aangeklaagd omdat ze brand hadden gesticht in een pakhuis met hulpgoederen voor Oekraïne. Britse aanklagers beschuldigen hen ervan voor de Russische overheid te werken.[42] In 2024 vonden er daarnaast verschillende incidenten plaats met pakketjes met explosieven bij overslagpunten voor luchtvracht in Polen, Duitsland en het Verenigd Koninkrijk. Volgens verschillende westerse inlichtingendiensten zit de Russische militaire inlichtingendienst GRU hierachter.[43]

Ook in ieder geval één persoon was doelwit van Russische acties. In juli 2024 werd bekend dat Amerikaanse inlichtingendiensten Russische plannen hadden ontdekt om de CEO van de Duitse wapenfabrikant Rheinmetall te vermoorden.[44]

In Tsjechië heeft Rusland meermaals geprobeerd de signaleringssystemen van de Tsjechische spoorwegen te verstoren.[45] Ook in Nederland is sabotage van fysieke infrastructuur, zoals havens en spoorwegen een reële dreiging. Voor de zogenoemde *Host Nation Support* van de NAVO worden de havens in Rotterdam, Vlissingen en de Eemshaven gebruikt voor het verplaatsen van militair personeel en materieel.[46] Militair materieel dat in de havens wordt opgeladen wordt vervolgens via het spoor en de weg Europa in gestuurd. Dit maakt Nederland nu al een mogelijk militair-logistiek doelwit. Indien de NAVO aan de oostflank van Europa in oorlog raakt zal dit alleen maar toenemen.[47]

Recente sabotageacties gericht op onderwaterinfrastructuur

In de afgelopen jaren hebben verschillende incidenten rond onderwaterinfrastructuur in Europese wateren plaatsgevonden. Door de sterke groei van de hoeveelheid onderzeese infrastructuur en de groeiende afhankelijkheid hiervan is dit een aantrekkelijker doelwit van kwaadwillende actoren geworden.[48] Zo maken internetkabels wereldwijde connectiviteit mogelijk en is het netwerk in Europa essentieel voor financiële transacties.[49] Doordat een groot deel van deze infrastructuur op de zeebodem buiten territoriale wateren ligt, is bescherming en monitoring lastig. De heimelijke benaderbaarheid maakt de onderzeese infrastructuur aantrekkelijk voor hybride conflictvoering. Kwaadwillende actoren kunnen met verstoring van deze infrastructuur grote schade veroorzaken, zonder zelf veel risico te lopen. Het blijft soms onduidelijk wie de daders zijn en het is moeilijk vast te stellen of er echt sprake is van

4 Het rapport van HCSS bracht voor 2023 24 voorbeelden van Russische hybride activiteiten in kaart, voor 2024 waren dat 55 voorbeelden.

moedwillige sabotage.[50] Storingen in onderzeese kabels kunnen namelijk ook onbedoeld worden veroorzaakt door visserij, scheepsankers of grondbewegingen.[51]

Hieronder worden de belangrijkste recente voorbeelden van incidenten rond onderzeese communicatiekabels, stroomverbindingen en pijpleidingen benoemd waarbij sprake is of zou kunnen zijn van sabotage. In januari 2022 werd één van de twee glasvezelkabels tussen Noorwegen en Spitsbergen vernield, waardoor communicatie met het vasteland beperkt werd.[52] In september 2022 werden drie pijpleidingen van Nord Stream 1 en 2 (deze bestaan elk uit twee identieke pijpleidingen) op de bodem van de Oostzee opgeblazen. Nord Stream voorzag Europa van Russisch gas. Drie Oekraïense staatsburgers worden verdacht van deze sabotageactie.[53] In oktober 2022 werden meerdere Franse en Schotse kabels tegelijkertijd doorgeknipt, waardoor de Shetland eilandengroep van de buitenwereld werd afgesloten en drie belangrijke Franse communicatielijnen onbruikbaar raakten.[54] In oktober 2023 raakten een gaspijplijn en een communicatiekabel tussen Finland en Estland beschadigd.[55] Volgens Finland was deze schade opzettelijk ontstaan en onderzoek van de Finse autoriteiten wees uit dat dit waarschijnlijk het gevolg was van een Chinees containerschip dat zijn anker over meer dan 180 kilometer van de Baltische zeebodem heeft gesleept. Er waren zes maanden nodig om de schade te herstellen. Dankzij nieuwe LNG-infrastructuur die na 2022 versneld is aangelegd beschikte Finland wel over voldoende gasaanvoer.[56] Begin 2024 werden er in de Rode Zee, mogelijk door Houthi-milities, vier grote onderzeese internetkabels vernield.[57] In november 2024 zijn twee onderwaterkabels in de Oostzee beschadigd geraakt, waarschijnlijk door het koopvaardijschip Yi Peng 3. Eén kabel loopt tussen Zweden en Litouwen en de andere tussen Duitsland en Finland.[58] In december 2024 vielen de stroomverbinding Estlink 2 en diverse datakabels tussen Finland en Estland uit. Volgens Finland door een Russische sabotageactie met de Eagle S. Deze olietanker zou door Rusland worden gebruikt voor spionage- en sabotageactiviteiten.[59]

Een voorbeeld uit januari 2025 laat zien hoe onderzeese kabels ook onbedoeld verstoord kunnen raken. In die maand was er sprake van een breuk in een glasvezelkabel op de bodem van de Oostzee tussen Zweden en Letland. Aanvankelijk vermoedde de Zweedse politie dat dit het gevolg was van sabotage door de Russische schaduwvloot. Nader onderzoek wees uit dat er geen sprake was van opzet, maar dat het schip genaamd de Vezhen vanwege zware wind de ankers had laten zakken en daarmee onbedoeld de kabel kapot heeft getrokken.[60]

De toename van moedwillige verstoringen van GNSS-signalen

Ook het verstoren van global navigation satellite system (GNSS) signalen is een vorm van hybride aanvallen die een dreiging vormt voor de vitale infrastructuur. Er zijn wereldwijd vier grote GNSS-systemen die worden gebruikt voor tijd- en plaatsbepaling. Het Amerikaanse GPS is hiervan de bekendste. Daarnaast is er het Europese Galileo, het Russische GLONASS en het Chinese Beidou. Veel vitale processen, zoals luchtvaart, energievoorzieningen en digitaal betalingsverkeer, zijn afhankelijk van GNSS voor tijd- en plaatsbepaling.[61] Recent is met name een grote toename zichtbaar in het verstoren van GPS signalen door *jamming* en *spoofing* die de lucht- en scheepvaart raakt.

Bij GPS-jamming wordt het signaal helemaal verstoord terwijl bij spoofing het signaal opzettelijk wordt overstemd door een ander foutief signaal. [62] Dat overstemmen gebeurt op dezelfde frequentie als het GPS-signaal waarbij gebruik wordt gemaakt van een krachtiger signaal.[63] Omdat ze vanuit de ruimte worden verzonden zijn GNSS-signalen niet zo sterk. Met een kleine zender kunnen kwaadwillende actoren zo'n signaal al flink verstoren.[64]

Zowel het Nederlandse Analysebureau Luchtvaartvoorvallen als het Europese Agentschap voor de Luchtvaart (EASA) melden sinds 2023 meer meldingen over verstoring van het gps-signaal van vliegtuigen.[65] Deze verstoringen doen zich voornamelijk boven Oost-Europa en het Midden-Oosten voor.[66] In 2023 waren er ongeveer 600 meldingen over jamming en spoofing. Bij ongeveer 150 van deze meldingen was sprake van spoofing, terwijl er in de jaren 2018 tot en met 2022 überhaupt geen meldingen over spoofing werden gedaan.[67] In 2024 werden er alleen al m.b.t. spoofing 1318 meldingen bij het Analysebureau Luchtvaartvoorvallen gedaan.[68]

Bij verstoring van GPS-signalen moeten vliegtuigen terugvallen op andere onafhankelijke navigatiesystemen.[69] Soms moeten piloten, die bijvoorbeeld uit de richting van Rusland vliegen, voor het bepalen van hun locatie om hulp vragen aan de verkeerstoren, omdat hun GNSS-navigatie nog niet hersteld is.[70] Daarnaast wordt ook de scheepvaart geraakt door GNSS verstoringen.[71] Zo meldde de Finse kustwacht eind 2024 dat de satellietnavigatie op de Oostzee sinds april dat jaar in toenemende mate wordt verstoord, waardoor schepen op zee verdwalen. In een aantal gevallen moest de Finse kustwacht ingrijpen om te voorkomen dat schepen te dicht bij eilanden of in ondiep water terechtkwamen.[72]

GPS-spoofing is een effectief middel tegen onder andere drones, precisiewapensystemen en raketsystemen. Veel incidenten met GPS-spoofing die burgervliegtuigen treffen, hebben dan ook betrekking op (de randen van) conflictgebieden.[73] De website GPSJAM brengt dagelijks GPS-verstoringen in beeld. Deze kaarten laten zien dat deze verstoringen zich concentreren rond de Baltische staten, de Oostzee, Oekraïne en het Midden-Oosten.[74] Naast plaatselijke jamming en spoofing kunnen GNSS-systemen ook veel grootschaliger uitvallen. Verschillende statelijke actoren beschikken over anti-satelliet- of counterspacewapens en cyberwapens die zij gebruiken richting satellietsystemen. Zo hebben Rusland, China, Iran en Noord-Korea in het verleden operaties tegen GPS uitgevoerd.[75]

De gevolgen van grootschalige en langdurige uitval van GNSS-systemen voor de vitale infrastructuur kunnen groot zijn, omdat veel vitale processen afhankelijk zijn van GNSS voor een exacte bepaling van locatie en tijd. Nauwkeurige tijd- en plaatsbepaling is bijvoorbeeld essentieel voor het navigeren van (autonoom) wegverkeer, het monitoren van de drinkwater-voorziening, het synchroniseren van energievoorzieningen, digitaal betalingsverkeer en een correcte werking van moderne netwerken zoals 5G.[76] De precieze afhankelijkheden van vitale processen van GNSS en de potentiële impact van een verstoring zijn echter niet geheel duidelijk.[77]

3.1.2 Pre-positionering vitale infrastructuur door statelijke actoren

Statelijke actoren kunnen ook voorbereidingshandelingen voor sabotage uitvoeren of pogen een positie in de vitale infrastructuur van anderen landen te verkrijgen zonder (direct) tot sabotage over te gaan. Het doel van spionage en pre-positionering is soms om op een later moment de vitale infrastructuur wel te kunnen saboteren. Statelijke actoren kunnen pre-positionering echter ook gebruiken als drukmiddel naar andere landen en om de autonomie van landen aan te tasten. Spionage kan een doel op zich zijn of voorafgaan aan pre-positionering of sabotage om eerst een beter beeld van vitale infrastructuur en kwetsbaarheden daarin te verkrijgen. Gezien de complexiteit en verwevenheid van onze vitale infrastructuur kan het lastig zijn te achterhalen of een statelijke actor of daaraan gelieerde proxies in bepaalde systemen aanwezig zijn.[78]

Onder andere de vitale infrastructuur in de Noordzee is kwetsbaar voor spionage en sabotage. Op de bodem van de Noordzee liggen duizenden kilometers aan datakabels die belangrijk zijn voor de connectiviteit van Nederland. Daarnaast liggen er in de Noordzee belangrijke gaspijpleidingen en elektriciteitskabels ten behoeve van de energievoorziening en wordt de Noordzee, onder andere door windmolenparken op zee, steeds belangrijker voor de nationale energiebehoefte en de energietransitie van Nederland.[79] De komende jaren wordt de vitale infrastructuur op de Noordzee fors uitgebreid en daarmee zal ook onze afhankelijkheid hiervan toenemen.[80] In het jaarverslag van 2023 beschrijft de MIVD dat Rusland de vitale maritieme infrastructuur in het Nederlandse deel van de Noordzee, zoals internetkabels, gasleidingen en windmolenparken in kaart brengt en activiteiten onderneemt die duiden op spionage en voorbereidingshandelingen voor verstoring en sabotage.[81]

3.1.3 Cyberaanvallen door statelijke actoren en hacktivisten

Statelijke actoren zetten cyberaanvallen in om hun politieke, militaire en/of economische doelen te bereiken. Statelijke cyberaanvallen staan niet op zichzelf, maar zijn onderdeel van een bredere gereedschapskist die statelijke actoren hanteren. Zo kunnen cyberaanvallen in samenhang met elkaar en in combinatie met andere, niet-digitale, methoden uit die gereedschapskist worden uitgevoerd.[82] Cyberaanvallen zijn aantrekkelijk omdat ze moeilijk te herleiden kunnen zijn naar de daders en relatief goedkoop kunnen worden uitgevoerd in verhouding tot de schade die ze kunnen aanrichten.[83] Zie voor een overzicht van verschillende typen cyberaanvallen het Cybersecuritybeeld Nederland 2024.

Verschillende cyberaanvallen hebben verschillende beoogde uitkomsten. Zo kunnen statelijke actoren cyberaanvallen inzetten om toegang te verkrijgen en te houden tot vitale processen. Die toegang kunnen zij dan op een later moment, bijvoorbeeld in het geval van een conflict, misbruiken om vitale processen zoals energievoorzieningen of telecomnetwerken te verstoren.[84] Daarnaast kunnen statelijke actoren ook cyber-aanvallen tegen vitale processen inzetten met spionage als doel, bijvoorbeeld vanwege de grote hoeveelheden data waarmee bepaalde sectoren werken. Zo proberen statelijke actoren data te stelen in de (Europese) reis- en luchtvaartsector om personen die voor hen interessant zijn te identificeren, op te sporen of te volgen.[85] Tot slot kunnen cyberaanvallen op vitale infrastructuur ook worden ingegeven door financieel gewin.[86]

Cyberaanvallen op vitale infrastructuur hebben in Nederland tot op heden geen ontwrichtende impact op de nationale veiligheid gehad.[87] Toch zijn geavanceerde cyberaanvallen op de Nederlandse vitale infrastructuur aan de orde van de dag.[88] Het CSBN 2024 concludeerde dat cyberaanvallen van statelijke actoren het nieuwe normaal lijken te zijn. Onder andere Rusland en China intensiveren hun cyberactiviteiten en verbreden hun capaciteiten met de inzet van niet-statelijke actoren. Daarnaast ondervindt Nederland de impact van cyberaanvallen die doorwerken binnen het digitale ecosysteem.[89] Ook signaleert het CSBN dat dergelijke actoren in toenemende mate *edge devices*, zoals firewalls, VPN-servers en routers, aanvallen. Kwaadwillende gebruiken dergelijke systemen aan de rand van een netwerk als toegangspunt voor het achterliggende netwerk en proberen onder andere een achterdeur in te bouwen om zo toegang te blijven houden.[90]

Naast statelijke actoren is er de laatste jaren ook veel aandacht voor hacktivistische cyberaanvallen. Hacktivisten voeren uit ideologische overwegingen cyberaanvallen uit. Geopolitieke spanningen, conflicten en maatschappelijk controversiële onderwerpen kunnen triggers zijn voor hacktivisme. Zo is de oorlog tegen Oekraïne een trigger geweest, maar ook het conflict tussen Israël en Hamas leidde tot een toename van cyberaanvallen. Sinds eind 2023, kort na het uitbreken van het conflict tussen Israël en Hamas, meldde Microsoft een stijging in het aantal meldingen van aanvallen tegen OT-systemen van Israëlische makelij. Waarschijnlijk was deze doelwitkeuze gelegen in het gebruik van apparatuur van een Israëlische firma en niet tegen de getroffen organisaties zelf. Door zo'n cyberaanval op een lokale drinkwater-voorziening die gebruikt maakt van digitale apparatuur van Israëlische makelij, kwamen inwoners van een Iers dorp in november 2023 twee dagen zonder water te zitten.[91]

In de praktijk is er sprake van een vermenging tussen hacktivisten en statelijke actoren.[92] Zo wordt de laatste jaren een groter deel van de Russische digitale spionage-, sabotage- en beïnvloedings-activiteiten uitgevoerd door hacktivistische collectieven. Soms betreft het zogenoemde cover-operaties en soms zijn het daadwerkelijk hacktivistische groeperingen die handelden in het verlengde van de Russische staat.[93]

Voorbeelden cyberoperaties van statelijke actoren en hacktivisten

Verschillende voorbeelden in Europa en de VS laten zien hoe statelijke actoren zoals China, Rusland en Iran cyberaanvallen op westerse overheden en vitale aanbieders uitvoeren.

Cyberaanvallen door Chinese actoren

China zet zijn cyberprogramma's al jaren in voor (pre-positionering voor mogelijke) sabotage, (economische en politieke) spionage en beïnvloedingsoperaties gericht op verschillende Westerse landen.[94] Het tempo van Chinese cyberoperaties op westerse doelwitten ligt hoog en de Chinese inlichtingendiensten schroeven hun activiteiten om westerse doelwitten aan te vallen steeds verder op.[95]

Begin 2024 maakte de MIVD melding van de aanwezigheid van malware genaamd COATHANGER op een losstaand computernetwerk van Defensie, dat minder dan 50 gebruikers telde. Deze malware was afkomstig van een Chinese statelijke actor. De aangetroffen malware installeerde een 'achterdeurtje' door gebruik te maken van een bekende kwetsbaarheid in FortiGate apparaten. China gebruikt dit type malware voor spionage op computernetwerken.[96] Omdat de malware toegang had gekregen tot een geïsoleerd researchnetwerk bleef de schade beperkt. [97]

In 2023 maakten de Verenigde Staten en Microsoft bekend dat hackers van het aan China gelinkte Volt Typhoon de vitale infrastructuur van Amerika hadden geïnfiltreerd. De hackers zouden sinds medio 2021 actief zijn en voorbereidingsactiviteiten voor digitale sabotage uitvoeren.[98] Volgens Amerikaanse functionarissen zou China ernaar streven de verkregen toegang tot Amerikaanse vitale infrastructuur te benutten in het geval van een oorlog of conflict.[99]

In september 2024 werd bekend dat een andere Chinese hackers-groep, bekend als Salt Typhoon, al ruim twee jaar een omvangrijke cyberspionagecampagne op telecomproviders uitvoerde. Hiervan waren minstens acht Amerikaanse telecomproviders en tientallen andere landen slachtoffer. Hoewel de hackers brede toegang hadden bij de telecomorganisaties, zouden ze voornamelijk geïnteresseerd zijn geweest in prominente individuen. Om tot die individuen te komen zou er wel van een groot aantal Amerikanen metadata van telefoongesprekken en sms-berichten zijn gestolen.[100] Volgens berichtgeving in The Wall Street Journal zou deze hackersgroep ook toegang hebben gekregen tot tapsystemen van Amerikaanse opsporingsdiensten.[101]

Cyberaanvallen door Russische actoren

De afgelopen jaren zijn er ook verschillende voorbeelden van cyberaanvallen door Russische statelijke actoren en pro-Russische hacktivisten in de openbaarheid gekomen. In september 2024 waarschuwde de MIVD bijvoorbeeld, samen met internationale partners, voor Russische cyberoperaties van GRU-eenheid 29155. De focus van de hackers van deze Russische militaire geheime dienst ligt onder meer op het in beeld krijgen en verstoren van westerse hulp aan Oekraïne. Hun cyberoperaties zijn er mogelijk ook op gericht om fysieke sabotage, waar deze eenheid al langer mee in verband gebracht wordt, te ondersteunen. Hun operaties richten zich met name op westerse overheden en vitale infrastructuur. Het is een eenheid waarmee Nederland, onder andere vanwege de rol als belangrijk doorvoerland, rekening moet houden. In andere westerse landen heeft de GRU-eenheid wel cyberoperaties ontplooid gericht op logistieke sectoren die hulp aan Oekraïne leveren of daar een rol in hebben.[102]

In februari 2022, slechts een uur voor de Russische invasie in Oekraïne, werd een grootschalige cyberaanval uitgevoerd op het Amerikaanse satellietbedrijf Viasat. Door het wissen van grote hoeveelheden data met wiper malware werd tijdelijk zowel de communicatie aan Oekraïense zijde als satellietcommunicatie in meerdere Europese landen verstoord.[103] Daarnaast werd in april 2024 in Nederland de uitzending van kinderzender BabyTV onderbroken waarna er een tijdlang Russische propaganda zichtbaar was. Deze signal hijacking, waarbij vanaf een alternatief station een sterk signaal naar de satelliet wordt gezonden, was niet gericht op BabyTV, maar was nevenschade van een bredere actie gericht op verstoring van uitzendingen van Oekraïense zenders.[104] Deze aanvallen staan niet op zichzelf, maar waren onderdeel van een grootschalige Russische cybercampagne in het kader van de oorlog tegen Oekraïne. Onderzoek van het Center for Security Studies identificeerde 124 cyberoperaties tegen de ruimtevaartsector in het kader van de oorlog in Oekraïne. Deze waren allemaal gericht op ruimte-systemen en bedrijven op aarde en niet op systemen in de ruimte. Het betrof voornamelijk Distributed Denial of Service (DDoS) aanvallen. Het onderzoek identificeerde daarnaast 35 actoren, waaronder hacktivisten en statelijke actoren aan beide zijden van het conflict, die deze cyberaanvallen uitvoerden.[105]

In juni 2023 waren websites van Nederlandse havens tijdelijk onbereikbaar als gevolg van DDoS-aanvallen door een pro-Russische hacktivistische groepering.[106] In augustus 2023 waren de websites van verschillende Nederlandse luchthavens doelwit van DDoS-aanvallen door pro-Russische hacktivisten, alleen de website van Groningen Airport Eelde was hierdoor tijdelijk onbereikbaar.[107] In juli 2024 werden in de VS hackers van hacktivistengroep de Cyber Army of Russia Reborn (CARR) veroordeeld voor cyber-aanvallen op vitale infrastructuur, zoals waterinfrastructuur en energiebedrijven.[108]

Cyberaanvallen door Iraanse actoren
Dat ook Iran een digitale dreiging voor overheidsorganisaties en vitale aanbieders kan vormen laten aanvallen op Albanië zien. Deze aanvallen moeten worden gezien in de specifieke geopolitieke context van beide landen. Iran en Albanië staan al geruime tijd op gespannen voet met elkaar. De voorbeelden laten wel zien dat Iran relevante cybercapaciteiten heeft en bereid is deze in te zetten ten behoeve van zijn eigen geopolitieke belangen.

In 2022 werden de overheidsnetwerken van Albanië getroffen door een cyberaanval. Albanië en de VS houden Iran hiervoor verantwoordelijk.[109] Door de aanval werden meerdere Albanese overheidswebsites en digitale diensten onbereikbaar en volgens de Albanese premier had de aanval het hele land plat kunnen leggen.[110] Eind 2023 waren het Albanese parlement en het telecombedrijf One Albania doelwit van cyberaanvallen. De exacte omvang en reikwijdte van de aanvallen zijn niet bekend. Een aan Iran gelinkte hackersgroep, genaamd Homeland Justice, heeft via hun Telegram-kanaal de verantwoordelijkheid voor de aanvallen opgeëist. Ze beweerden ook nog een tweede telecombedrijf en de nationale luchtvaartmaatschappij Air Albania te hebben gehackt.[111]

3.1.4 Desinformatie

Ook desinformatie is een hybride dreiging die invloed kan hebben op vitale aanbieders en processen. Desinformatie is het doelbewust verspreiden van misleidende informatie, bijvoorbeeld om meningen te beïnvloeden, geld te verdienen of schade aan de Nederlandse samenleving aan te brengen.[112] Statelijke actoren verspreidden bijvoorbeeld desinformatie tijdens de COVID-19 pandemie, rondom de oorlog in Oekraïne en bij recente verkiezingen.[113] Hoewel er weinig bekend is over de daadwerkelijke impact van desinformatie op het functioneren van vitale processen, uiten vitale aanbieders zorgen over de potentiële gevolgen, met name voor hun medewerkers. Daarnaast waarschuwde De Nederlandse Bank eind 2024 in het rapport 'Weerbaarheid in een gure wereld', dat ook financiële instellingen te maken kunnen krijgen met de verspreiding van desinformatie. Bijvoorbeeld wanneer kwaadwillende actoren nepnieuws zouden verspreiden over de financiële positie van banken om maatschappelijke ontwrichting teweeg te brengen.[114]

3.1.5 Economische druk en strategische afhankelijkheden

In tijden van toenemende concurrentie tussen grootmachten proberen statelijke actoren economische afhankelijkheden te gebruiken om invloed uit te oefenen.[115] Bijvoorbeeld door middel van handelsbeperkende maatregelen, door misbruik te maken van de aanwezigheid van buitenlandse bedrijven in de Nederlandse vitale infrastructuur of door misbruik te maken van strategische afhankelijkheden. Dit soort vormen van economische druk kunnen ook invloed hebben op de integriteit en beschikbaarheid van vitale processen, bijvoorbeeld wanneer zij essentiële grondstoffen, diensten en producten niet meer kunnen importeren. Daarnaast bestaat het risico dat er voor sommige essentiële onderdelen (op termijn) geen alternatieven bestaan uit landen zonder tegengestelde (geopolitieke) belangen.

Er hoeft niet altijd sprake te zijn van een doelbewuste strategie vanuit statelijke actoren om onderdeel te worden van de Nederlandse vitale infrastructuur of om strategische afhankelijkheden te creëren en hier misbruik van te maken. Er kan ook sprake zijn van een economische overeenkomst, die er tegelijkertijd voor zorgt dat buitenlandse bedrijven een positie in de vitale infrastructuur of de toeleverancierssketens van vitale aanbieders krijgen en waar statelijke actoren (op een later moment) misbruik van kunnen maken. Daarmee kan bijvoorbeeld de aanwezigheid van Chinese bedrijven in de toeleverancierssketens van vitale processen een dreiging voor vitale processen zijn of worden. Vitale aanbieders kunnen hierdoor bijvoorbeeld een gelegenheidsdoelwit worden van Chinese economische druk, waaronder misbruik van strategische afhankelijkheden.

Economische druk door China

Er zijn steeds meer Chinese bedrijven aanwezig in de Europese markt. Onder andere in het ecosysteem van diverse vitale sectoren, zoals havens en fysieke infrastructuur, de energiesector en de telecomsector. In tijden van toenemende geopolitieke spanning kan China middels deze bedrijven druk op Europa en Nederland uitoefenen voor politieke en strategische doeleinden.[116]

Onderzoek van de European Parliamentary Research Service laat zien dat China zeer geregeld economische druk uitoefent op andere landen en bedrijven voor politieke doeleinden. China zet dergelijke economische druk ook in richting de Europese Unie. Door druk uit te oefenen op prominente bedrijven of sectoren probeert Beijing anderen af te schrikken om bepaalde lijnen te overschrijden. Die rode lijnen betreffen niet alleen kwesties als soevereiniteit en nationale veiligheid, maar ook China's internationale imago en de behandeling van Chinese bedrijven in het buitenland.[117]

China zet vaak een combinatie van methoden in om economische druk uit te oefenen. Overheden krijgen vooral te maken met handelsrestricties in de vorm van import- en (in mindere mate) exportbeperkingen. Concrete maatregelen die China inzet zijn het verhogen van douanetarieven, het selectief toepassen van binnenlandse en internationale regelgeving, gerichte douanecontroles, het weigeren van vergunningen of het opleggen van onofficiële embargo's. Daarnaast heeft China in 2020 een nieuwe exportcontrolewet aangenomen die het mogelijk maakt om de uitvoer van goederen, technologieën en diensten te controleren om de (vaag gedefinieerde) nationale veiligheid en belangen te beschermen.[118]

Onderzoekers van denktank Merics brachten 123 gevallen van economische druk door China in kaart tussen 2010 en 2022, waarbij er in de laatste vier jaar een duidelijke stijging zichtbaar was. Volgens de onderzoekers is dit waarschijnlijk slechts het topje van de ijsberg, omdat China de maatregelen vaak niet publiek

maakt, ze soms opzettelijk moeilijk detecteerbaar lijkt te maken en bedrijven ze zelf ook niet graag melden uit angst voor represailles van de Chinese autoriteiten en Chinese consumenten. Bedrijven in de consumenten- en landbouwgoederen-, grondstoffen- en dienstensector zijn het vaakst doelwit van Chinese economische druk.[119] Het bekendste voorbeeld van economische druk vanuit China zijn de importrestricties die het land op Litouwen opgelegde na de opening van een '*Taiwanese representative office*' in Vilnius in november 2021. China verlaagde de Litouwse import met bijna 90%.[120]

Recenter onderzoek van het International Institute for Strategic Studies laat zien dat China sinds 2024 zijn strategie voor het uitoefenen van economische druk verlegt van informele handelsverboden en symbolische wijzigingen in wet- en regelgeving naar het actief opleggen van formele exportcontroles. Vooralsnog lijken deze exportcontroles zich vooral op de Verenigde Staten te richten. Hiermee kopieert China de exportcontroles van de Verenigde Staten tegen Chinese technologiebedrijven. Daarbij stelt China ook steeds vaker expliciet waar deze maatregelen een reactie op zijn en neemt het deze tegenmaatregelen tegenwoordig zeer snel.[121]

Daarnaast biedt China goederen aan op de Europese markt tegen prijzen waartegen Nederlandse bedrijven niet kunnen concurreren. Hierdoor kunnen Nederlandse en Europese bedrijven uit de markt geconcurreerd worden en vergroten bestaande of ontstaan er mogelijk nieuwe strategische afhankelijkheden van China. Het land is onder andere een onmisbare speler in de energietransitie. Zo voert China bewust beleid om een monopolie op zonnepanelen te behouden.[122] Hetzelfde speelt in de chemische industrie. Nederlandse bedrijven die vezels maken voor defensiematerieel, zoals kogelwerende vesten, kunnen niet concurreren met de prijzen van Chinese bedrijven. Deze Chinese bedrijven ontvangen staatssteun en bieden hun producten aan tegen zeer lage prijzen. De Koninklijke Vereniging van de Nederlandse Chemische Industrie (VNCI) waarschuwde eind 2024 dan ook dat Europa moet uitkijken voor het vertrek van zijn basischemie.[123]

Economische druk door de VS

De VS zullen Nederland en de Europese Unie waarschijnlijk steeds vaker aansporen tot restrictief optreden richting landen zoals China en Rusland.[124] De VS gebruikt exportcontroles richting China om onder andere de Chinese technologische innovatie en militaire modernisering af te remmen.[125] Onder de nieuwe regering Trump is een voortzetting van het huidige handelsconflict met China te verwachten. Omdat Europa sterk afhankelijk is van de VS is de ruimte om dit te negeren beperkt. Dit kan leiden tot economische represailles vanuit landen als China, zoals het sluiten van markten voor Europese bedrijven en een exportverbod van kritieke grondstoffen en strategische goederen en diensten naar Nederland en de EU. Wanneer dit tot tekorten in Nederland leidt, kan het functioneren van vitale processen onder druk komen te staan.[126]

Strategische afhankelijkheden

Strategische afhankelijkheden[5] van bepaalde grondstoffen, goederen en diensten kunnen een dreiging vormen voor de continuïteit van vitale processen. Dit kan zijn doordat statelijke actoren bewust misbruik maken van deze afhankelijkheden. Ook wanneer dit niet het geval is kan een te grote afhankelijkheid van bepaalde goederen en diensten een dreiging voor vitale processen vormen. Bijvoorbeeld wanneer levering onderbroken wordt door een conflict elders in de wereld of doordat de afhankelijkheid de Nederlandse open strategische autonomie beperkt. Strategische afhankelijkheden kunnen niet alleen bestaan ten opzichte van landen, maar bestaan soms ook ten opzichte van één of enkele (tech)bedrijven.

Met name met betrekking tot China bestaan er strategische afhankelijkheden die risicovol kunnen zijn voor de continuïteit van vitale processen. Ook van Rusland zijn er dergelijke afhankelijkheden, maar die zijn veel kleiner dan die van China. Hierdoor zou de schade bij een extreme en plotselinge ontkoppeling van China ook aanzienlijk groter zijn.[127] Daarnaast zijn er ook afhankelijkheden van onder andere Taiwan en de VS die van invloed kunnen zijn op de vitale processen. Hieronder worden ter illustratie verschillende voorbeelden van strategische afhankelijkheden van China, Rusland, Taiwan en de Verenigde Staten benoemd. Dit is echter geen uitputtend overzicht van alle denkbare strategische afhankelijkheden voor de gehele vitale infrastructuur.

Strategische afhankelijkheden grondstoffen

Nederland en de EU zijn voor kritieke grondstoffen sterk afhankelijk van China.[128] Zonder kritieke grondstoffen die door China worden gewonnen of geraffineerd zouden veel vitale processen essentiële eindproducten missen die nodig zijn om te blijven functioneren. Door de toenemende spanning tussen China enerzijds en de VS en de EU anderzijds zou de leveringszekerheid van kritieke grondstoffen onder druk kunnen komen te staan.[129]

Onderzoek van The Hague Centre for Strategic Studies (HCSS) naar de risico's van de afhankelijkheid van Chinese grondstoffen voor vitale sectoren laat zien dat deze kritieke grondstoffen in tal van apparaten nodig zijn. Voorbeelden hiervan zijn windturbines, helikopters, jachtvliegtuigen, beveiligingscamera's, drones en mobile technologie, variërend van smartphones en computers tot ICT-toepassingen voor online betalingen. Drones bevatten bijvoorbeeld de voornamelijk door China gewonnen of verwerkte grondstoffen silicium, kobalt, gallium en germanium.[130] Dergelijke kritieke grondstoffen zijn cruciaal voor het functioneren

5 Een afhankelijkheid is strategisch wanneer een product of dienst cruciaal is voor het borgen van publieke belangen van Nederland en/of de EU, of de afhankelijkheid een risico vormt voor de continuïteit van vitale processen of de toegang tot gevoelige informatie voor derden. Een strategische afhankelijkheid kan risicovol zijn, wanneer er een hoog risico op leveringsonderbrekingen is. Dit hangt af van de marktconcentratie en de mogelijkheid tot substitutie, de aard van de betrekkingen met het land waarvan we afhankelijk zijn en de mate van wederzijdse afhankelijkheid.

van vitale processen, zoals in het defensie- en veiligheidsdomein, duurzame energiesysteem, duurzame mobiliteit en ICT.[131]

Ook windturbines en zonnepanelen, die een steeds groter deel van de Nederlandse en Europese energieproductie uitmaken, maken gebruik van kritieke grondstoffen. Voor windturbines zijn zeldzame aardmetalen, kobalt en permanente magneten nodig die vrijwel allemaal in China worden geproduceerd. De productie van zonnepanelen is afhankelijk van silicium, germanium en gallium.[132]

Ook in de zorg zijn er strategische afhankelijkheden van China, bijvoorbeeld op het gebied van antibiotica en grondstoffen voor de farmaceutische industrie.[133] Daarnaast zijn de meeste moderne medische procedures afhankelijk van apparaten die rijk zijn aan de eerder genoemde kritieke grondstoffen. Voorbeelden hiervan zijn beademingsapparatuur, pacemakers, MRI-scanners, röntgenfoto's en echografieën.[134]

Nederland is, volgens een publicatie van de NOS, voor de productie van nucleaire geneeskunde afhankelijk van Rusland. Radioactieve stoffen worden steeds vaker gebruikt voor medisch onderzoek en voor de behandeling van verschillende soorten kanker. Hiervoor zijn bewerkte grondstoffen nodig die vrijwel alleen in Rusland worden gemaakt.[135]

Strategische afhankelijkheden halfgeleiders

Het onderzoek van HCSS schetst ook de afhankelijkheid van de Nederlandse vitale infrastructuur van halfgeleiders uit Taiwan. De toelevering hiervan zou kunnen wegvallen of beperkt worden in het geval van een Chinese blokkade en/of invasie van Taiwan. Verschillende vitale processen zijn in meer of mindere mate afhankelijk van Taiwanese halfgeleiders[6]. In de medische sector speelt Taiwan een belangrijke rol in de levering van chips voor medische apparaten, zoals beademingssystemen, diagnostische apparaten en pacemakers. In het defensie- en veiligheidsdomein spelen geavanceerde Taiwanese chips een belangrijke rol in militaire- en politieapparatuur. Daarnaast zijn ze nodig voor nieuwe technologieën, zoals AI en drones, die op steeds grotere schaal zullen worden gebruikt. Taiwanese chips worden daarnaast gebruikt in de energiesector, in de auto-industrie en tal van ICT-toepassingen.[136]

Strategische afhankelijkheden digitale infrastructuur

Ook strategische afhankelijkheden op het gebied van digitale infrastructuur spelen een rol binnen vitale processen. Digitale infrastructuur is een essentieel onderdeel in de bedrijfsprocessen van vitale sectoren zoals energie, telecom, de financiële sector en weg- en spoorbeheer. De Nederlandse digitale infrastructuur wordt echter grotendeels door grote techbedrijven uit niet-Europese landen beheerd en ontwikkeld.[137] Doordat data en digitale dienstverlening worden verplaatst naar andere landen en digitale innovatie in toenemende mate plaatsvindt buiten de EU nemen de strategische afhankelijkheden van andere landen, met name de VS en China, in het digitale domein toe. Deze afhankelijkheden kunnen risico's met zich meebrengen. Bijvoorbeeld wanneer statelijke actoren via digitale technologie en diensten toegang krijgen tot gevoelige informatie en vitale processen. Ook beperkt het de Nederlandse digitale strategische autonomie en kunnen de Nederlandse publieke waarden en publieke belangen op het spel komen te staan.[138]

Op het gebied van clouddiensten zijn er bijvoorbeeld afhankelijkheden van Amerika. Een klein aantal Amerikaanse bedrijven, Amazon Web Services, Microsoft Azure, en Google, domineren 70 tot 80 procent van de Europese markt voor clouddiensten.[139] De macht van de grootste cloudbedrijven groeit daarnaast omdat bedrijven eenmaal gekozen, door technische, organisatorische en financiële barrieres, moeilijk van aanbieder kunnen wisselen. Zelfs als gebruik wordt gemaakt van Europese of Nederlandse aanbieders, bestaat de kans dat ook die gebruik maken van diensten van deze cloudaanbieders.[140] Veel data van Nederlandse banken staan bijvoorbeeld in clouds van deze Amerikaanse techbedrijven.[141] Deze strategische afhankelijkheid heeft implicaties voor de Nederlandse digitale open strategische autonomie. Zo is door de afhankelijkheid van Amerikaanse bedrijven wetgeving in de VS ook in meer of mindere mate van toepassing op Nederlandse organisaties. Daarnaast kan Nederland maar beperkt toezicht op deze bedrijven uitoefenen. Ook kan er een *single point of failure* ontstaan. Een storing of cyberaanval op een van de drie grootste aanbieders kan wereldwijde doorwerking krijgen.[142]

In de ontwikkeling van AI-toepassingen hebben grote Amerikaanse en Chinese private techbedrijven tot nu toe de overhand en loopt de Europese markt achter. Europa is dan ook grotendeels afhankelijk van de grote techbedrijven voor het verkrijgen van de nieuwste AI-gerelateerde software en diensten, zoals modellen voor beeldherkenning en AI-managementtools. Naarmate de digitalisering van processen en de afhankelijkheid van AI-technologie voor basisvoorzieningen toeneemt, en daar de software en diensten van tech-giganten de enige uitkomst voor bieden, neemt de afhankelijkheid van diezelfde bedrijven toe. De toegankelijkheid en betrouwbaarheid van de software is immers in grote mate afhankelijk van de aanbieder. Bovendien mengen grote techbedrijven zich ook in de discussie met overheden in de wijze waarop democratische vrijheden gewogen moeten worden.[143]

Ook op het gebied van applicaties en diensten heeft Europa een zwakke positie, met name ten opzichte van de VS en op sommige gebieden ook van China. Dit geldt bijvoorbeeld voor sociale media, kantoorsoftware en cybersecurity.[144] Ook hiervoor geldt dat dit in

6 Met name Taiwan Semiconductor Manufacturing Corporation (TSMC) speelt een centrale rol in de toeleveringsketen van halfgeleiders. TSMC produceert 92% van 's werelds meest geavanceerde logic chips, oftewel "cutting-edge" chips (d.w.z. <10 nanometer). Taiwanese bedrijven, waaronder TSMC en United Microelectronics Corporation (UMC), produceren ook een aanzienlijk deel van minder geavanceerde chips, oftewel "trailing-edge" en "mature" chips (d.w.z. _10nm). In totaal is Taiwan goed voor meer dan 20% van de wereldwijde halfgeleiderproductie, meer dan elk ander land ter wereld.

sommige gevallen een dreiging voor de nationale veiligheid kan vormen. Bijvoorbeeld wanneer statelijke actoren, zoals China, applicaties en diensten gebruiken voor statelijke inmenging, economische spionage en sabotage van vitale processen.[145]

3.2 Terrorisme en gewelddadig extremisme: een mogelijke dreiging voor vitale infrastructuur

Terroristen en gewelddadig extremisten kunnen een dreiging vormen voor de vitale infrastructuur. In Nederland zijn er geen ontwrichtende terroristische of extremistische aanslagen op vitale infrastructuur gepleegd. Wel laten accelerationistische[7] publicaties en buitenlandse voorbeelden zien dat vitale processen doelwit van terroristen en gewelddadig extremisten kunnen zijn. Daarnaast kunnen vitale aanbieders geconfronteerd worden met medewerkers met extremistisch gedachtengoed, zoals soevereinen en rechts-extremisten.

Terroristische dreiging Nederland en vitale infrastructuur

Er is een reële kans dat er een terroristische aanslag in Nederland zal plaatsvinden. Zoals in het Dreigingsbeeld Terrorisme Nederland (DTN) beschreven is de dreiging vanuit jihadisme en andere radicaal-islamitische kringen hoog. Er bestaat een reële kans dat personen uit het rechts-terroristische online milieu de daad bij het woord voegen en overgaan tot geweld. Daarnaast zijn nieuwe rechts-extremistische groepen, waarvan sommige leden terroristische gedachtegoed aanhangen, meer actiebereid. Ook gaat er vanuit een kleine groep soevereinen een geweldsdreiging uit.[146]

Hoewel er vanuit jihadistische groepen doorgaans weinig aandacht is voor vitale infrastructuur, zijn er wel voorbeelden van oproepen tot het plegen van aanslagen op de luchtvaartsector. Zoals in het DTN van juni 2024 beschreven riep Al Qa'ida op het Arabisch Schiereiland (AQAS) in een video op tot aanslagen op burgerluchtvaarttoestellen van Amerikaanse, Britse en Frans-Nederlandse luchtvaartmaatschappijen, waaronder die van Air-France-KLM. Ondanks deze uitingen is de dreiging vanuit Al Qa'ida en haar regionale afdelingen in Nederland en tegen Nederlandse belangen in het buitenland, waaronder de burgerluchtvaart, waarschijnlijk beperkt.[147] Daarnaast zijn er in perioden van grote media-aandacht voor bosbranden in verschillende delen van de wereld soms oproepen in jihadistische propaganda om dergelijke branden te stichten, om zo schade aan te richten en slachtoffers te maken. Er zijn voor zover bekend geen bosbranden daadwerkelijk veroorzaakt door terroristen of extremisten met een ideologisch motief.[148]

Dat rechtsterroristische organisaties hun aanslagen mogelijk ook op vitale infrastructuur kunnen richten blijkt uit accelerationistische publicaties waarin wordt omschreven dat grootschalige aanslagen op vitale infrastructuur, zoals het stroomnetwerk, telecommunicatie en olietransport, moeten bijdragen aan de beoogde ontketening van een rassenoorlog.[149] Het DTN van december 2023 verwees in dit kader naar het *Terrorgram Collective* waarop onder andere handleidingen worden verspreid voor het maken van bommen en het saboteren van vitale infrastructuur. *Terrorgram Collective* is een belangrijke bron voor rechtsextremisten en accelerationisten wereldwijd die bestaat uit een online netwerk van verschillende kanalen op de communicatie-app Telegram.[150] De dreiging voor concrete rechts-terroristische aanslagen op vitale infrastructuur in Europa lijkt echter beperkt. In Europa komt de dreiging van rechtsterroristen veelal vanuit enkelingen, vaak kwetsbare minderjarige of jongvolwassenen, die in korte tijd online radicaliseren en op kleine schaal geweld plegen. Een aanslag op vitale infrastructuur vereist een bepaalde mate van organisatie en voorbereiding die bij deze enkelingen vooralsnog veelal ontbreekt.[151]

Buitenlandse terroristische aanslagen op vitale infrastructuur

Aanslagen in het buitenland laten zien dat terroristische en extremistische groepen zich kunnen richten op (deelprocessen van) vitale infrastructuur. In maart 2024 stak bijvoorbeeld in Duitsland de links-extremistische groep *Vulkangruppe* een elektriciteitsmast in de buurt van een Teslafabriek in brand. De groep wilde hiermee de fabriek saboteren. De brand veroorzaakte een stroomstoring die naast de fabriek ook tienduizenden inwoners in de regio trof.[152] In tegenstelling tot Nederland heeft Duitsland een omvangrijke, radicale en actieve extreem-linkse scene. De dreiging van aanslagen op vitale infrastructuur door links-extremisten in Duitsland is de afgelopen tijd ook toegenomen. Het is echter onwaarschijnlijk dat dit grote invloed heeft op de kleine groep links-extremisten in Nederland.[153]

In juli 2024, bij de start van de Olympische spelen, werden de Franse spoorwegen gesaboteerd. Vermoedelijk is dit door een links-extremistische groepering gedaan, al hebben de Franse autoriteiten niet alle daders vastgesteld. Op drie plekken werd langs het Franse spoor schade aan apparatuur aangericht. Er werden tientallen ondergrondse glasvezelkabels doorgebrand waarop veiligheidsinformatie voor machinisten wordt verzonden. Door deze sabotage werden treinen geannuleerd en werden honderdduizenden reizigers gedupeerd.[154] Ook glasvezelkabels van telecombedrijven zijn op meerdere plaatsen in Frankrijk doorgeknipt. Hierdoor werden verschillende providers getroffen en werd plaatselijk vaste en mobiele telefonie gehinderd.[155] Dit verschijnsel was niet nieuw, het doorknippen van glasvezelkabels gebeurde in Frankrijk ook al ruim voor de Olympische Spelen.[156]

7 Het accelerationisme is rechts-extremistisch gedachtegoed waarbij d.m.v. terroristisch geweld chaos wordt nagestreefd, om zo een rassenoorlog en de vervanging van de democratie door een nationaalsocialistische en witte etnostaat te bespoedigen.

In de Verenigde Staten voerde in 2022 een vermoedelijk extreemrechtse groepering een aanval op een elektriciteitsnet uit waardoor 45.000 inwoners zonder stroom kwamen te zitten.[157] Bij verschillende andere incidenten in de VS was dit ook een vermoeden.[158]

Medewerkers met extremistisch gedachtengoed

Vitale aanbieders kunnen geconfronteerd worden met medewerkers met verschillende vormen van extremistisch gedachtengoed. Deze kunnen een insider threat vormen, bijvoorbeeld wanneer zij toegang hebben tot gevoelige informatie of systemen.

Het DTN van juni 2024 beschrijft bijvoorbeeld dat defensie een aantrekkingskracht uitoefent op rechts-extremisten. Dit komt onder andere doordat ze hier wapen- en gevechtservaringen op kunnen doen en door de associatie met broederschap en masculiniteit.[159]

Het DTN van december 2024 beschrijft in dit kader dat verschillende organisaties in Nederland worden geconfronteerd met personen die zichzelf 'autonoom' of 'soeverein' verklaren. Personen die zich soeverein noemen, geloven dat de Nederlandse overheid geen legitieme macht over hen uitoefent en dat ze zelf mogen bepalen of de Nederlandse wet- en regelgeving op hen van toepassing is. Deze soevereinen hebben veelal de wens om een alternatieve wereld te creëren, onafhankelijk van de instituties.[160] In totaal zijn er in Nederland enkele tienduizenden aanhangers van het soevereine gedachtegoed. Enkele tientallen tot honderd van hen geloven dat een gewelddadige confrontatie met de overheid uiteindelijk onvermijdelijk zal zijn. In Nederland zijn in beperkte mate zelfverklaarde soevereinen werkzaam bij overheidsinstituties of in vitale sectoren. Sommigen van hen hebben in verband met hun functie toegang tot gevoelige informatie. Hun zelfverklaarde soevereiniteit kan op gespannen voet staan met de professionele integriteit verbonden aan hun werk.[161]

3.3 Activisme richt zich ook op vitale infrastructuur

Verschillende protesten en activistische acties in Nederland en Europa hebben de afgelopen jaren laten zien dat ook activisten[8] en demonstranten zich kunnen richten op vitale sectoren of dat hun activiteiten hier effect op kunnen hebben. Omdat er geen systematisch onderzoek naar activisme in relatie tot vitale infrastructuur wordt gedaan is niet vast te stellen of er de laatste jaren sprake is van een toename van activisme gericht op vitale aanbieders. Wel zijn er de afgelopen jaren verschillende voorbeelden geweest van acties die hebben geleid tot kortdurende hinder van vitale infrastructuur zoals luchthavens, weginfrastructuur en een sluizencomplex. Hierbij kwamen de nationale veiligheidsbelangen niet in het geding. Wanneer de omvang, frequentie en/of duur van dergelijke activiteiten toenemen, zou dit een dreiging voor de nationale veiligheid kunnen gaan vormen.

Zo hebben de afgelopen jaren verschillende acties plaatsgevonden gericht op de luchtvaartsector. In november 2022 drongen klimaatactivisten van Greenpeace en Extinction Rebellion binnen op het luchthaventerrein op Schiphol-Oost. Hier namen zij plaats onder privéjets om zo te voorkomen dat ze konden opstijgen. Ook ketenden enkele actievoerders zichzelf vast aan toestellen.[162] In maart 2024 blokkeerde Extinction Rebellion verschillende toegangswegen naar de kunstbeurs Tefaf in Maastricht, om actie te voeren tegen privéjets die voor de kunstbeurs op Maastricht Aachen Airport landden.[163] In december 2024 werden klimaatactivisten van Extinction Rebellion op Schiphol gearresteerd nadat ze met vliegtickets achter de securitycontrole waren gekomen en daar een grote hoeveelheid bruine vloeistof op de vloer hadden gegoten om te protesteren tegen KLM's spaarprogramma.[164]

In Duitsland blokkeerden klimaatactivisten van *Letzte Generation* in juli 2024 start- en landingsbanen op de luchthaven van Frankfurt. Daarbij lijmden ze zichzelf vast op het asfalt. Het vliegverkeer werd hierdoor urenlang stilgelegd en 270 van de 1.400 geplande vluchten werden die dag geannuleerd.[165] In mei dat jaar hadden klimaatactivisten ook al de toegangswegen naar de startbaan van de luchthaven van München geblokkeerd.[166]

Activisten richten zich ook op maritieme infrastructuur. In juli 2024 blokkeerde Extinction Rebellion cruciale toegangswegen naar de Rotterdamse haven.[167] Extinction Rebellion en zusterorganisatie Geef Tegengas bezetten in september 2024 de Botlekbrug, een belangrijke schakel voor weg-, spoor- en scheepvaartverkeer voor de Rotterdamse haven en de Maasvlakte. Zij deden dit uit protest tegen uitbreiding van de gasindustrie.[168] In augustus 2024 blokkeerde Extinction Rebellion de doorgang van het sluizencomplex IJmuiden door actievoerders aan het hek van de Noordersluis vast te lijmen en te ketenen. De acties richtten zich tegen de cruisevaart, maar met de blokkade werd het hele scheepvaartverkeer in het Noordzeekanaal gehinderd.[169] In juni 2024 bezetten Greenpeace-activisten een boorplatform bij Schiermonnikoog om actie te voeren tegen gaswinningsplannen ten noorden van het eiland.[170]

Activisten maken daarnaast gebruik van snelwegen om de maatschappelijke impact van hun acties te vergroten. Extinction Rebellion blokkeerde de afgelopen jaren bijvoorbeeld meermaals de A12 en de A10, uit protest tegen fossiele subsidies.[171] Ook boerenprotesten zorgden er in Nederland meermaals voor dat snelwegen werden geblokkeerd. Tijdens acties werd verkeer platgelegd met o.a. tractoren, hooibalen en brandstichting.[172]

8 Activisten willen anderen overtuigen van een bepaald standpunt, maar streven daarbij geen ondemocratische doelen na en hanteren ook geen ondemocratische methodes. Soms overtreden activisten wel de wet, maar niet met als doel de democratische rechtsorde te ondermijnen.

3.4 Criminele activiteiten: een mogelijke dreiging voor vitale infrastructuur

Ook criminele activiteiten kunnen een dreiging voor de vitale infrastructuur vormen. Het gaat hierbij vaak om cyberaanvallen door criminelen, maar het kan ook om ondermijnende criminaliteit of fysieke handelingen, zoals koperdiefstal, gaan.

Cybercriminaliteit gericht op vitale infrastructuur

Cybercriminelen handelen vanuit financieel motief en hebben niet de (primaire) intentie om de maatschappij te ontwrichten. Desondanks kunnen hun aanvallen zoveel impact veroorzaken dat ze nationale veiligheidsbelangen raken. De capaciteit van sommige cybercriminelen is te vergelijken met die van statelijke actoren.[173]

In het verleden gaven sommige criminele groepen aan zich niet op vitale infrastructuur te richten. Dat zou niet verstandig zijn omdat zij zich zo in de kijker zouden spelen van inlichtingen- en opsporingsinstanties. Aan de andere kant zou in vitale sectoren de neiging kunnen bestaan om sneller losgeld te betalen vanwege het belang van de bedrijfscontinuïteit. Daardoor zou dit toch een aantrekkelijk doelwit kunnen zijn voor criminelen. In de praktijk zullen criminelen vaak opportunistisch zijn. Dat betekent dat het doelbewust aanvallen van vitale infrastructuur door cybercriminelen niet structureel gebeurt, maar ook niet principieel is uitgesloten.[174]

Hoewel criminele cyberaanvallen de afgelopen jaren in Nederland niet tot maatschappelijke ontwrichting hebben geleid, laten verschillende incidenten wel zien hoe vitale sectoren door cyberaanvallen geraakt kunnen worden. Dit geldt bijvoorbeeld voor de energiesector. Zo konden Nederlandse windmolens op Windpark Oude Maas begin 2022 niet proefdraaien door een ransomware-aanval op de Duitse windmolenfabrikant Nordex. In Denemarken werd de energiesector in mei 2023 door een grote cyberaanval getroffen. In totaal werden er 22 energiebedrijven via kwetsbaarheden in firewalls van fabrikant Zyxel gecompromitteerd.[175] Uit onderzoek van SektorCERT, het cybersecuritycentrum voor de Deense vitale sectoren, is gebleken dat de aanval mogelijk was omdat bedrijven hadden nagelaten beveiligingsupdates te installeren.[176] Dankzij sensoren van SektorCERT werd de aanval snel opgemerkt en kon worden voorkomen dat er een grootschalige storing in de energievoorziening ontstond.[177]

Ook de maritieme sector werd de afgelopen jaren slachtoffer van cybercriminelen. In maart 2023 werd maritiem dienstverlener Royal Dirkzwager getroffen door een ransomware-aanval van de Play ransomwaregroep. Royal Dirkzwager registreert alle in- en uitgaande zeeschepen in de Rotterdamse haven. Het bedrijf kon verschillende diensten niet aan klanten aanbieden, waaronder het systeem dat klanten een real-time overzicht geeft van wanneer schepen arriveren en de ROAM-service voor het monitoren van scheepsverkeer.[178] Daarnaast lekte de hacker vertrouwelijke gegevens van de organisatie, waaronder werknemers-ID's, paspoorten en contracten. Het bedrijf had ongeveer een week nodig om zijn systemen volledig te herstellen en de diensten te hervatten.[179]

Het CSBN 2024 laat zien dat zorgorganisaties regelmatig slachtoffer zijn van cyberaanvallen. Daarbij gaat het vaak om ransomware en/of afpersing met gestolen gegevens. Een groot deel daarvan vond plaats in het buitenland en had impact op de te verlenen zorg.[180] In het Verenigd Koninkrijk werden in juni 2024 bijvoorbeeld in verschillende ziekenhuizen operaties en bloedtransfusies geannuleerd, nadat een toeleverancier van pathologische diensten slachtoffer was geworden van een ransomware-aanval van Russische cybercriminelen van de Qilin-groep.[181] In juli 2024 werden in de Verenigde Staten bloedbanken slachtoffer van een ransomware-aanval. Hierdoor moesten meer dan 250 ziekenhuizen hun protocollen voor bloedtekort activeren.[182] Hoewel ook in Nederland een aantal zorginstellingen geraakt werd door cyberaanvallen, had dit voor zover bekend geen impact op de te verlenen zorg. Wel werden organisaties afgeperst met gestolen gegevens en werden gegevens gelekt.[183]

Ondermijnende criminaliteit

Ondermijnende criminaliteit vormt niet alleen een dreiging voor de samenleving en rechtsstaat, maar kan ook een dreiging voor vitale infrastructuur vormen. Dit is vooral zichtbaar in zeehavens, waar de georganiseerde criminaliteit infrastructuur onder ander gebruikt voor drugshandel. Omdat criminelen gebruik maken van de infrastructuur zijn zij niet gebaat bij schade aan of sabotage daarvan. Hun activiteiten kunnen het functioneren van deze infrastructuur echter wel onder druk zetten. Logistieke processen worden bijvoorbeeld verstoord door illegale uithalers op terminals. Daarnaast worden havenmedewerkers en inspecties onder druk gezet, geïntimideerd of geronseld. Uit angst hier ook slachtoffer van te worden kiezen sommige medewerkers ervoor in andere sectoren te gaan werken. Hierdoor is het moeilijk om het personeel voor havens te krijgen die wel nodig is om de infrastructuur draaiende te houden.[184]

Koperdiefstal

Een voorbeeld van criminele activiteiten die direct hinder veroorzaken voor vitale infrastructuur is de diefstal van koper, onder andere in bliksemafleiders, bekabeling en spoorstaven, rond het spoor. Op het getroffen spoor is vaak geen of alleen beperkt en langzaam rijdend treinverkeer mogelijk.[185] Door maatregelen, zoals cameratoezicht en het plaatsen van hekken zijn gevallen van koperdiefstal op het spoor de afgelopen jaren wel sterk gedaald.[186] Naast spoorwegen hebben ook energiebedrijven, zoals bij zonneparken, te maken met koperdiefstal.[187]

Insider threats

Insider threats kunnen bij de verschillende dreigingen een rol spelen. Sommige insiders handelen vanuit persoonlijke motieven zoals frustratie, politieke overtuigingen of financieel gewin. Anderen werken vrijwillig of gedwongen mee aan de kwaadaardige handelingen van statelijke actoren, terroristen, activisten of criminelen. Insider threats kunnen ook onbewust zijn en door onoplettend handelen een vitale aanbieder blootstellen aan een dreiging. Tot slot kunnen insiders ook personen zijn die bewust regels, zoals beveiligingsrichtlijnen, negeren. Hierdoor maken zij een vitale aanbieder kwetsbaar voor dreigingen of systeemfalen. Insiders kunnen binnen een vitale aanbieder zelf zitten of in de soms complexe keten van toeleveranciers. [188]

Het Insider Risk Trend Report 2025 van Signpost Six brengt de verschillende trends op het gebied van insider threats in kaart. Zo zijn geldproblemen de belangrijkste drijfveer voor insider threats. Daarnaast leidt de verbetering van cyber- en fysieke beveiliging bij bedrijven er toe dat kwaadwillende actoren er voor kiezen om insiders te rekruteren voor onder andere spionage, pre-positionering en sabotage.[189]

Klimaatverandering zorgt ook in Nederland steeds vaker voor extreme weersomstandigheden. Natuurlijke elementen vormen een toenemende dreiging voor de vitale infrastructuur.

4. Natuurlijke dreigingen voor de vitale infrastructuur

Vitale processen kunnen te maken krijgen met verschillende natuurlijke dreigingen. Met name de gevolgen van klimaatverandering vormen een toenemende dreiging voor de vitale infrastructuur.
Hieronder wordt ingegaan op de dreiging door klimaatverandering, aardbevingen, ruimteweer en infectieziekten.

4.1 Klimaatverandering vormt een toenemende dreiging voor de vitale infrastructuur

Klimaatverandering versnelt en wordt ernstiger dan eerder werd gedacht. Dit creëert nieuwe en versterkt bestaande dreigingen.[190] Op basis van klimaatmodellen verwacht het Intergovernmental Panel on Climate Change (IPCC) dat het wereldwijde klimaat rond 2033 al 1,5 graden is opgewarmd. In Europees Nederland gaat de opwarming ongeveer twee keer zo snel als wereldwijd en is het nu al 2,3 graden warmer dan rond 1900.[191] Hierdoor krijgt Nederland nu en in de komende jaren al te maken met ernstige, directe en indirecte gevolgen van klimaatverandering.[192] Zo stijgt de zeespiegel en ontstaan er steeds vaker extreme weersomstandigheden. Enerzijds zullen hitte en droogte toenemen en anderzijds zal het vaker extreem hard regenen. Het wordt daardoor steeds waarschijnlijker dat Nederland te maken krijgt met verstoring of uitval van vitale infrastructuur als gevolg van klimaatverandering.[193]

Tegelijkertijd zijn de exacte gevolgen van klimaatverandering en de precieze impact daarvan op vitale processen moeilijk in te schatten.[194] Het Planbureau voor de Leefomgeving (PBL) concludeert in het rapport 'Klimaatrisico's in Nederland - De huidige stand van zaken' dat een compleet overzicht van complexe risico's als gevolg van klimaatverandering lastig te schetsen is vanwege het grote aantal mogelijke combinaties, de stapelingen van klimaatrisico's, de keteneffecten en de neveneffecten van klimaatadaptatie. De optelsom van meerdere risico's kan dan ook groter uitpakken dan verwacht.[195] Denk hierbij bijvoorbeeld aan de opeenstapeling van extreme regenval én hoge rivierafvoeren én een hogere zeespiegel, waardoor afwatering extra lastig wordt.[196]

Daarnaast is de omvang en snelheid van de impact van klimaatverandering afhankelijk van specifieke omstandigheden, de maatschappelijke context en de uitvoering van klimaatadaptatiebeleid. De toegenomen afhankelijkheid van burgers en bedrijven van onder andere elektriciteit-, ICT- en logistieke netwerken maakt Nederland tevens kwetsbaarder voor de gevolgen van klimaatverandering op dergelijke vitale infrastructuur.[197] Daarbij geldt dat extreem weer meerdere vitale processen tegelijkertijd kan raken en dat een grotere kans op natuurlijke dreigingen ook betekent dat de kans op het samenvallen van verschillende dreigingen toeneemt.[198]

4.1.1 Extreem weer als gevolg van klimaatverandering

De Deltascenario's[9] van het Nationale Deltaprogramma laten verschillende mogelijke toekomstbeelden zien op basis van een plausibele bandbreedte van de klimaatverandering, de inspanning van Nederland om uitstoot van broeikasgassen terug te dringen en socio-economische ontwikkelingen.[199] Voor alle scenario's geldt dat de wateropgaven voor Nederland substantieel groter worden. In de zomer nemen zoetwatertekorten toe, er ontstaat meer wateroverlast door regenbuien en de gevolgen van overstromingen worden groter.[200]

Extreme neerslag

Door klimaatverandering neemt het aantal zware buien met veel neerslag toe.[201] In de zomer door piekbuien en in de winter door lange periodes met regen.[202] Dit kan zo extreem worden dat het watersysteem dit niet meer op kan vangen, met frequentere overstromingen tot gevolg.[203] Wateroverlast kan ontwrichtend werken

9 In 2024 is een nieuwe set Deltascenario's opgesteld door Deltares , in opdracht van de Deltacommissaris en het ministerie van IenW. Ze zijn gebaseerd op de nieuwste inzichten van o.a. KNMI, Planbureau voor de Leefomgeving en Wageningen Universiteit.

wanneer de functies van vitale netwerken uitvallen, zoals het elektriciteitsnet, gasnet of communicatienetwerken en internet. Wegen kunnen onbegaanbaar worden en ziekenhuizen, transformatorstations en rioolwaterzuiveringen kunnen uitvallen door wateroverlast.[204] De afgelopen jaren leidde extreme neerslag in verschillende Europese landen onder andere tot stroomuitval, het stilleggen van het openbaar vervoer en het sluiten van een vliegveld.[205]

Een voorbeeld hiervan is de extreme neerslag in juli 2021 in Zuid-Limburg, de Ardennen en de Eifel. Een groot weersysteem zorgde daar voor wateroverlast en overstromingen. In Zuid-Limburg viel lokaal meer dan 160 mm neerslag in 48 uur. In de Ardennen en de Eifel viel op een aantal locaties zelfs meer dan 250 mm in 48 uur. In het buitenland vielen 200 slachtoffers en was er langdurige uitval van essentiële voorzieningen zoals elektriciteit en transport. In Nederland is lokaal kort infrastructuur uitgevallen en beschadigd. De hersteltijd van sommige locaties was een half jaar.[206]

In oktober 2024 veroorzaakte extreme neerslag in Valencia de zwaarste overstromingen in Spanje van deze eeuw.[207] Hierbij vielen ruim 200 doden en grote delen van de infrastructuur raakten beschadigd. In sommige plekken rond Valencia viel op één dag 400 millimeter regen. Hierbij is een duidelijke link met klimaatverandering. De warme Middellandse Zee zorgde voor extra verdamping en warme lucht zorgde voor extra hevige regenval. Een zogenaamde koudeput zorgde ervoor dat het regenfront op dezelfde plek bleef hangen.[208]

In het Caribisch deel van het Koninkrijk neemt daarnaast de kans op zware orkanen toe en duurt het orkaanseizoen steeds langer. In 2022 viel op sommige plekken op Bonaire de stroomvoorziening uit, na zware regenval die delen van het eiland onder water zette.[209]

Door klimaatverandering neemt ook de kans op valwinden toe.[210] Deze kunnen tijdens zware onweersbuien ontstaan doordat lucht door zeer zware regenval sterk afkoelt. De koude lucht valt op het aardoppervlak en zorgt voor zeer zware windstoten.[211] In juni 2021 werd bijvoorbeeld de gemeente Leersum getroffen door een valwind. Deze valwind veroorzaakte naast negen gewonden en schade aan huizen ook zeven gaslekken door omgevallen bomen.[212] In de gemeente Oosterwolde waaiden als gevolg van een extreme valwind vier hoogspanningsmasten om.[213]

Extreme hitte en droogte in de zomer

Klimaatverandering leidt ook tot extreme hitte én droogte in de zomer. Bij langdurige droogte kunnen vitale processen, zoals de drinkwatervoorziening en binnenvaart, onder druk komen te staan.[214] Daarnaast nemen natuurbranden toen en zullen deze vaker tot schade en uitval van vitale infrastructuur leiden.

Zoetwatertekorten

De Deltascenario's laten zien dat er in de zomer steeds vaker onvoldoende zoetwater zal zijn. Door toenemende verdamping, langere perioden van droogte, lagere rivierafvoeren en verzilting van grondwater neemt het zoetwateraanbod af.[215] Grondwater verzilt onder andere door bodemdaling en de verminderde waterafvoer van rivieren in perioden van extreme droogte. [216] Daarnaast draagt de stijgende zeespiegel via grondwater, rivieren en zeesluizen bij aan verzilting, vooral in kustgebieden.[217] Tegelijkertijd neemt de watervraag toe voor doorspoeling van watersystemen (verziltingsbestrijding), beregening van landbouwgebieden, drinkwater, natuur en vernatting van laagveen. De Deltascenario's concluderen dat het naar verwachting in 2050 steeds lastiger wordt om voldoende zoetwater beschikbaar te houden voor alle huidige functies.[218]

Drinkwatervoorzieningen onder druk

Naast grondwater wordt ook oppervlaktewater gebruikt voor de winning van drinkwater. Deze waterbronnen staan niet alleen onder druk door toenemende droogte en verzilting. Voor zowel grond- als oppervlaktewater geldt dat de kwaliteit onder druk staat door gewasbeschermingsmiddelen, nitraat uit mest en de reststoffen van medicijnen en cosmetica. Daarnaast neemt de vraag naar drinkwater door bevolkings- en economische groei toe. Er zijn dus verschillende factoren die er samen voor zorgen dat de kwetsbaarheid van de drinkwatervoorziening is toegenomen.[219] In 2023 waarschuwde het RIVM dat er regionaal sprake is van tekorten in het aanbod van drinkwater en dat er zonder maatregelen vanaf 2030 naar verwachting bij alle tien drinkwaterbedrijven sprake van een tekort zal zijn.[220] Zonder maatregelen zou het om een tekort van ruim 100 miljoen kubieke meter gaan, dat is iets minder dan het verbruik in een provincie als Overijssel. Ook nu al hebben drinkwaterbedrijven soms onvoldoende drinkwater, waardoor ze nee aan bedrijven moeten verkopen.[221] Een actieplan van de Rijksoverheid, provincies en drinkwaterbedrijven moet dit tekort in 2030 voorkomen.[222]

Effect droogte en hitte op vitale processen

Verschillende voorbeelden laten zien hoe droogte en hitte een dreiging voor vitale processen kunnen vormen. In de zomer van 2022 veroorzaakte droogte bijvoorbeeld een sterk verminderde diepgang op de binnenvaarwegen en daarmee fors lagere laadvermogens. De vaker voorkomende droge periodes vereisen onder andere aanpassingen aan de infrastructuur, logistiek en scheepsconstructies om het potentieel van de binnenvaart optimaal te kunnen blijven benutten.[223] Ook waterkeringen en dijken zijn gevoelig voor droogte. In dijken kunnen bij extreme droogte scheuren ontstaan en waterkeringen kunnen beschadigd raken.[224] Bij veendijken komt scheurvorming door droogte het vaakst voor.[225]

Hitte en droogte veroorzaken daarnaast problemen aan het spoor. Beweegbare spoorbruggen kunnen door hitte bijvoorbeeld uitzetten en daardoor niet meer open of dicht. Door hoge temperaturen neemt daarnaast de kans op spoorspatting toe, waardoor er knikken in de rails komen. Wanneer droogte leidt tot bodemdaling kunnen er ongelijke verzakkingen van het spoor of perrons ontstaan.[226]

Ook op de (chemische) industrie kan de toenemende droogte effect hebben, zoals een tekort aan proces- en koelwater, een tekort aan bluswater en beperkte aanvoer van grondstoffen of producten als gevolg van een lage waterstand.[227]

Natuurbranden

Het risico op natuurbranden in Nederland is hoog. Volgens het Natuurbrandsignaal '23[10] zullen natuurbranden door klimaatverandering intenser worden en zal Nederland vaker geconfronteerd worden met onbeheersbare natuurbranden, die met de huidige tactiek, techniek en capaciteit van de brandweer steeds moeilijker te bestrijden zijn.[228] Ook hier spelen de stijgende temperatuur, toenemende droogte in de zomer en dalende grondwaterstand een belangrijke rol. Hierdoor wordt vegetatie meer en vaker brandbaar. In de lente en de zomer zal hierdoor vaker directe en indirecte schade en uitval van vitale infrastructuur zijn. Doordat de natuur en de fysieke leefomgeving in Nederland sterk verweven zijn kunnen natuurbranden bovendien snel aanzienlijke schade aan vitale infrastructuur veroorzaken. [229] Bermbranden kunnen er bijvoorbeeld voor zorgen dat (spoor) wegen afgesloten moeten worden vanwege de benodigde ruimte voor hulpdiensten of slecht zicht als gevolg van de rook. Een groot deel van het hoofdwegennet is gevoelig voor afsluiting door rook van langdurige vlammende of smeulende natuurbranden en zelfs kleinere branden kunnen potentieel grote maatschappelijke impact hebben wanneer ze voorkomen op kritieke punten van het hoofdwegennet.[230] Bij een onbeheersbare brand kunnen ook elektriciteit, telecommunicatie of drinkwatervoorziening geraakt worden. Bij uitval van een kritieke transformator kan een lokale natuurbrand zelfs zorgen voor regionale uitval van elektriciteit.[231] Door een toename van (gelijktijdige) natuurbranden zal er ook een grotere druk op het brandweersysteem ontstaan, waardoor de hulpvraag groter kan worden dan de beschikbaarheid van brandweermiddelen.[232]

4.1.2 Stijging zeespiegel als gevolg van klimaatverandering

Als gevolg van de versnellende klimaatverandering versnelt ook de wereldwijde zeespiegelstijging. Ook aan de Nederlandse kust is deze zeespiegelstijging zichtbaar. Nu is de stijging enkele millimeters per jaar (3,7 millimeter). Afhankelijk van de uitstoot van broeikasgassen is de verwachte cumulatieve zeespiegelstijging in 2050 16 tot 38 centimeter.[233] Volgens de laatste klimaatscenario's van het KNMI (2023) stijgt de zeespiegel voor de Nederlandse kust tot 2100 waarschijnlijk maximaal 1,2 meter. Na 2100 hangt het tempo van de zeespiegelstijging steeds meer af van de mate van opwarming en het al dan niet instabiel worden van delen van de Antarctische ijskap. Als de Antarctische ijskappen instabiel worden, kan deze stijging zelfs oplopen tot 2,5 meter in 2100 en 17,5 meter in 2300. De kans hierop is klein, maar de gevolgen van een dergelijke zeespiegelstijging zouden erg groot zijn.[234]

In Nederland zal zeespiegelstijging vooral gevolgen hebben voor de waterveiligheid en de beschikbaarheid van zoetwater. Uit onderzoek van het Kennisprogramma Zeespiegelstijging blijkt dat Nederland zich met de huidige aanpak van dijkversterkingen, stormvloedkeringen, zandsuppleties en pompen voor waterveiligheid technisch gezien waarschijnlijk tot 3 meter zeespiegelstijging tegen overstromingen kan blijven beschermen. Dat vraagt wel om grote inspanning en aanpassingen in het ruimtegebruik, want bij de doorgaande zeespiegelstijging zijn steeds omvangrijkere zandsuppleties en steeds verdergaande versterkingen van waterkeringen nodig. Daarnaast moeten de stormvloedkeringen veel vaker sluiten en uiteindelijk worden vervangen.[235]

4.2 Aardbevingen

Aardbevingen kunnen in potentie tot verstoring of uitval van vitale processen leiden. Onder andere doordat veel vitale infrastructuur, zoals leidingen en kabels, in de ondergrond aanwezig zijn.[236]
Er zijn echter geen recente voorvallen van verstoring of uitval van vitale processen door een aardbeving in Nederland bekend.
Een aardbeving is een trilling of schokkende beweging van de aardkorst. Aardbevingen kunnen een natuurlijke oorzaak hebben of worden geïnduceerd door de mens. Beide typen aardbevingen komen in Nederland voor.[237] Aardbevingen worden niet beïnvloed door klimaatverandering. Doordat de gaswinning in het Groningenveld eind 2023 is gestopt neemt daar zowel de waarschijnlijkheid als de kracht van de aardbevingen af.[238]
De meeste natuurlijke bevingen komen in Nederland in Limburg voor.[239] In 2024 vonden er in Nederland 47 aardbevingen plaats, waarvan 40 geïnduceerde en 7 natuurlijke aardbevingen. Dit aantal is lager dan in 2023, toen waren er 62 aardbevingen.[240]

4.3 Dreiging van ruimteweer voor de vitale infrastructuur

Sommige vitale processen maken gebruik van geavanceerde technologieën die kwetsbaar kunnen zijn voor ruimteweer.[241]
Er zijn verschillende ruimteweerfenomenen die van invloed kunnen zijn op vitale infrastructuur. Deze fenomenen vinden allemaal hun oorsprong in de activiteiten van de zon. De zon maakt een cyclus van 11 jaar door. In deze zonnecyclus zijn er periodes waarin de zon heel actief is en periodes waarin de zon juist rustig is. [242]

[10] Het rapport Natuurbrandsignaal '23 is opgesteld door een consortium bestaande uit het Nederlands Instituut Publieke Veiligheid (NIPV), het Koninklijk Nederlands Meteorologisch Instituut (KNMI), Wageningen Universiteit & Research (WUR), de Vrije Universiteit Amsterdam (VU) en Deltares.

Er zijn drie belangrijke fenomenen die de zon produceert en die ruimteweer op aarde veroorzaken:

1. *Zonnevlammen* (solar flares). Dit zijn intense uitbarstingen van energie in de vorm van elektromagnetische straling, zoals röntgenstraling. Ze kunnen tijdelijke verstoringen veroorzaken in communicatie en navigatie.
2. *Coronale massa-ejecties* (CME's). Hierbij komt er een grote hoeveelheid zonneplasma met geladen deeltjes, zoals protonen en elektronen, vrij van de zon. Wanneer deze deeltjes de aarde bereiken, kunnen ze een geomagnetische storm veroorzaken, die de magnetosfeer van de aarde verstoort.
3. *Protonenstormen*. Deze stormen bestaan uit zeer snel bewegende protonen met een hoge energie. Protonenstormen kunnen schade aan satellieten veroorzaken door deeltjesstraling.[243]

Als zo'n zonnevlam, coronale massa ejectie of protonenstorm naar de aarde is gericht heeft dat effect op onze atmosfeer.[244]

In de jaren 2024 – 2026 zit de aarde in een piek van dit ruimteweer. Zo was er op 10 en 11 mei 2024 wereldwijd bijvoorbeeld een geomagnetische storm van de zwaarste categorie. Geomagnetische stormen kunnen invloed hebben op de hogere lagen van de atmosfeer, zoals de thermosfeer en ionosfeer. Dit kan storingen veroorzaken in radiocommunicatie en satellietnavigatie-systemen.[245] Lange-afstandscommunicatie is van groot belang voor de luchtvaart en bij een zeer verstoorde ionosfeer kan dit contact moeilijk of zelfs onmogelijk worden. Doordat ruimteweer de ionosfeer verstoort, kan het ook zijn dat satellietsignalen door de ionosfeer verstoord worden.[246] Zoals beschreven in paragraaf 3.1.1. zijn veel satellieten afhankelijk van GNSS voor tijd- en plaatsbepaling en kan verstoring of uitval hiervan grote keteneffecten veroorzaken.

De mogelijke impact van een geomagnetische storm op satellieten werd onder andere zichtbaar bij de lancering van Starlink-satellieten van SpaceX in februari 2022. Van de 49 gelanceerde satellieten die om een lage baan in de aarde terecht hadden moeten komen gingen er 40 na de lancering verloren als gevolg van een geomagnetische storm. Door de storm was er sprake van veel weerstand en vielen de satellieten terug naar de atmosfeer waarbij ze verbrandden.[247]

In uitzonderlijke gevallen kunnen ook beheerders van elektriciteits-netwerken problemen ondervinden door een zonnestorm.[248] Geomagnetische stormen kunnen het magnetisch veld van de aarde verstoren, wat op zijn beurt elektrische spanningen veroorzaakt in elektriciteitsnetwerken. Deze storingen kunnen leiden tot uitval van netwerken, vooral in gebieden waar de aardkorst slecht geleid is.[249] Deze dreiging bestaat vooral in noordelijke gebieden en deed zich op grote schaal voor het laatst voor in 1989 in Canada. Daar zaten toen miljoenen mensen uren zonder stroom als gevolg van een zware geomagnetische storm. In Nederland zal zich dit niet snel voordoen, door onze geografische ligging, goed geleidende bodem en korte, fijnmazige elektriciteitsnetwerken.[250]

4.4 Dreiging van infectieziekten voor de vitale infrastructuur

De COVID-19-pandemie heeft laten zien dat een grootschalige uitbraak van infectieziekten grote maatschappelijke gevolgen kan hebben. Humane infectieziekten kunnen leiden tot doden en zieken en bij een ernstige pandemie ook een gebrek aan voldoende acute zorg veroorzaken.[251]

Er zijn een aantal ontwikkelingen die op langere termijn een verhoogd risico op een grootschalige uitbraak van infectieziekten kunnen impliceren. Zo zijn er steeds meer diersoorten vatbaar voor de vogelgriep.[252] Sinds een paar jaar raken zoogdieren zoals koeien en sporadisch ook mensen besmet.[253] De variant die in de VS onder koeien rondgaat verspreidt zich momenteel niet van mens-op-mens. De kans op mutaties die dit wel doen wordt echter steeds groter, omdat het virus vrijelijk rondgaat onder zoogdieren in de VS. Verschillende epidemiologen en virologen noemen de situatie in de VS al maanden zorgelijk, ook door het gebrek aan preventieve maatregelen, monitoring en het trage delen van informatie met wetenschappers.[254]

Daarnaast neemt door de opwarming van de aarde de kans op nieuwe pandemieën toe. Dit komt o.a. doordat muggen en teken zich op plekken vestigen waar ze eerst niet zaten. Daar kunnen ze bijvoorbeeld in contact komen met zieke dieren.[255]

Tot slot is er een afnemende bereidheid onder de bevolking tot vaccinatie en zijn er nieuwe ontwikkelingen op het gebied van bioinformatica en AI.[256] Er zijn experts die waarschuwen voor de mogelijkheid dat kwaadwillende actoren AI-modellen in de toekomst zullen gebruiken bij het ontwikkelen van biologische wapens, zoals een besmettelijk virus.[257] Hoewel de huidige modellen hier niet toe in staat zijn, is de mogelijkheid om met toekomstige nog geavanceerdere modellen wel dergelijke wapens te maken iets om goed in de gaten te houden.[258]

Op woensdag 24 augustus 2024 was er een storing in het NAFIN-netwerk, een belangrijk glasvezelnetwerk voor behoud van de nationale veiligheid. Daardoor kwam het vliegverkeer op Eindhoven Airport volledig stil te liggen.

5. Dreigingen voortkomend uit het falen van vitale processen zelf

De nationale veiligheid kan ook in het geding komen wanneer vitale processen uitvallen door menselijke fouten, systeemfalen of door keteneffecten. Het vitale proces valt in zo'n geval dus niet uit door het handelen van kwaadwillende actoren of door natuurlijke dreigingen. Dit soort dreigingen kunnen echter wel bijdragen aan de impact van menselijk- en systeemfalen. Bijvoorbeeld wanneer waterkeringen door een technisch probleem niet werken op het moment van extreem slecht weer met grote hoeveelheden regenval.[259]

5.1 Menselijk- en systeemfalen

Bij menselijk falen is er sprake van uitval of verstoring van een vitaal proces door een onopzettelijke menselijke fout. Bij systeemfalen ligt de oorzaak in een technische fout in het systeem zelf. Verschillende voorbeelden laten zien dat een ogenschijnlijk kleine technische of menselijke fout grote gevolgen kan hebben voor vitale processen en in vergaande gevallen zelfs een dreiging voor de nationale veiligheid kan vormen.

In de zomer van 2024 deden zich twee grootschalige uitvalincidenten voor als gevolg van een softwarefout, waardoor onder andere ziekenhuiszorg, luchtvaart en overheidstaken grote hinder ondervonden. Zo ontstond er in juli 2024 een wereldwijde storing van miljoenen Microsoft systemen door een foutieve update van de software van CrowdStrike.[260] Dit leidde in verschillende landen tot uitval en verstoring van vitale processen. Sommige banken konden tijdelijk geen overboekingen doen, enkele tv-zenders gingen op zwart, haventerminals stonden stil en op veel vliegvelden moesten vluchten worden geannuleerd.[261] Hoewel in Nederland de nationale veiligheid niet in het geding kwam, ondervonden ook hier verschillende vitale processen hinder van de storing. Ziekenhuizen in Emmen, Hoogeveen, Stadskanaal en Doetinchem moesten de zorg tijdelijk afschalen en patiënten voor spoedeisende hulp naar andere ziekenhuizen overbrengen. De luchthavens Schiphol en Eindhoven Airport moesten vluchten annuleren. Bussen in de provincie Utrecht en regio's Amersfoort en Almere werden tijdelijk geschrapt. Klanten van de digitale bank KNAB konden niet in de app van de financiële dienstverlener.[262] De CrowdStrike-storing laat zien hoe kwetsbaar de gedigitaliseerde samenleving is en dat dergelijke storingen kunnen leiden tot grootschalige uitval. Het bestaan van digitale monoculturen, waarin vele organisaties afhankelijk zijn van een klein aantal aanbieders binnen het bredere digitale ecosysteem, kan leiden tot grootschalige effecten.[263]

In augustus 2024 raakten overheidsdiensten en het vliegverkeer Eindhoven verstoord door een softwarefout op een netwerk van Defensie. De oorzaak van de problemen lag in de toegangsverlening tot het zogenoemde Netherlands Armed Forces Integrated Network (NAFIN). Dat is een zwaarbeveiligd netwerk dat onder meer Defensielocaties met elkaar verbindt en ook wordt gebruikt bij datacenters van verschillende ministeries en politiebureaus. Door een fout in de softwarecode ontstond een probleem in de tijdsynchronisatie op het netwerk. Hulpdiensten hadden hierdoor problemen met hun communicatie- en alarmeringssysteem, waardoor ze onderling moeilijker konden communiceren. Ambtenaren van diverse ministeries konden niet inloggen op werksystemen. Eindhoven Airport maakt gebruik van datzelfde netwerk en ondervond ook hinder. Vliegtuigen konden niet opstijgen of landen.[264] Ook de Kustwacht werd door de storing geraakt. Onder andere hun communicatie- en alarmeringssysteem haperden. Daardoor waren ze tijdelijk niet bereikbaar voor schepen in nood, maar ook niet voor de Koninklijke Nederlandse Redding Maatschappij (KNRM) en de luchtverkeersleiding.[265]

Ook het vitale proces 'communicatie met en tussen hulpdiensten middels 112 en C2000' heeft de afgelopen jaren te maken gehad met uitval als gevolg van systeemfalen. In 2019 was het alarmnummer 112 enige tijd onbereikbaar als gevolg van een storing in de systemen van KPN. Deze was ontstaan door het niet goed functioneren van een digitale teller in het telefoonsysteem.[266]

Het C2000 communicatiesysteem, waarmee hulpverleners van de politie, brandweer, ambulance en defensie communiceren, heeft geregeld met verstoring door systeemfalen te maken gehad. Zo ondervonden meldkamers in juni 2023 problemen in het communiceren met hulpverleners op straat door een netwerkprobleem tussen de meldkamers en de C2000 centrale apparatuur.[267] Ook tijdens de nieuwjaarsnacht van 2024/2025 kampte het C2000-systeem met storing, mogelijk door overbelasting.[268]

In april 2024 was er een storing van de Luchtverkeersleiding Nederland (LVNL) die ontstond door een verkeerd uitgevoerde voorbereiding op een update van nieuwe software in het luchtverkeersleidingssysteem (AAA). Er werd eerst teruggevallen op de zogeheten backup-mode van AAA en toen deze ook niet betrouwbaar bleek, is teruggeschakeld naar het backup-systeem (Phoenix). Het vliegverkeer is vervolgens volledig afgebouwd. Na een herstart van AAA werkte het luchtverkeersleidingssysteem weer en kon de normale dienstverlening worden hervat.[269] Een aantal vliegtuigen kon niet opstijgen en een aantal landingen werd omgeleid naar België. Omdat de storing laat op de avond plaatsvond was de impact beperkt.[270]

Menselijk- of systeemfalen kan ook samenvallen met andere dreigingen, zoals extreem weer. Op 2 november 2023 dreigde door zo'n stapeling van dreigingen Amsterdam onder water te lopen. Zware neerslag, storm Ciarán en een storing bij het gemaal IJmuiden zorgden voor hoog water. Door de storing gingen de schuiven (spuikokers) van het gemaal in IJmuiden niet meer dicht. De spuikokers staan bij eb open om overtollig water op zee te spuien maar sluiten zich weer bij vloed. Door het technische probleem sloten ze niet en stonden ze enige tijd open terwijl het al vloed was. Hierdoor kwam er in de vroege ochtend een flinke golf zeewater het Noordzeekanaal in en ging ook het peil van het IJ omhoog. Nadat het probleem was ontdekt, zijn de kleppen door een technische ploeg snel handmatig gesloten. De combinatie van de storing, de hoge waterstand en de storm Ciarán had een waterstand van -12 centimeter tot gevolg, terwijl die normaal -40 centimeter is. Om overstroming van Amsterdam te voorkomen zijn snel de veertien sluizen en waterkeringen bij het IJ gesloten, zodat het waterniveau in de grachten niet verder kon stijgen. Om het waterpeil in de stad weer op het gewenste niveau te krijgen werd Gemaal Zeeburg vervolgens vol aangezet. Door onder andere de sluizen tussen Amsterdam en het IJ te sluiten zakte het peil binnen 24 uur weer naar het gewenste niveau van rond de -40 cm NAP.[271]

In sommige gevallen ontstaan er problemen binnen vitale processen, zonder duidelijk aanwijsbare oorzaak. Een voorbeeld hiervan is het Spoorwegongeval in 2023 bij Voorschoten. In de nacht van 4 april 2023 reed bij station Voorschoten een goederentrein tegen een kraan op lorries aan. De kraan kwam in het andere spoor terecht. Daardoor werd deze ook aangereden door een reizigerstrein. De kraanbestuurder kwam om het leven en twintig personen werden naar een ziekenhuis gebracht. Er was ruim twee weken geen treinverkeer mogelijk tussen Leiden en Den Haag. Onderzoek van de Onderzoeksraad voor Veiligheid wees uit dat er verschillende factoren waren die mogelijk hebben bijgedragen aan het ongeval, maar dat het onderzoek geen directe oorzaak kon achterhalen.[272]

5.2 Keteneffecten

Door onderlinge afhankelijkheden binnen de vitale infrastructuur kan een verstoring binnen één vitaal proces leiden tot keteneffecten in andere vitale processen. Dit wordt ook wel cascade-effecten genoemd.[273] Vitale processen zijn daarnaast ook verbonden met allerlei niet-vitale processen. Verstoringen van deze niet-vitale processen kunnen eveneens grote keteneffecten hebben op vitale processen. De keteneffecten van de eerder genoemde NAFIN-storing (niet vitaal) op o.a. hulpdiensten en vliegverkeer (wel vitaal) zijn hier een goed voorbeeld van.

Het is moeilijk een goede inschatting te maken van de keteneffecten van verstoring van vitale processen. Dit komt doordat de complexiteit van systemen en afhankelijkheden tussen systemen en processen steeds verder toenemen en er veel onderlinge en verborgen afhankelijkheden binnen en tussen vitale processen zijn. Daarbij veranderen deze afhankelijkheden ook steeds door technologische ontwikkeling en vernieuwing van systemen en infrastructuur.[274] Met name de uitval van elektriciteit heeft grote keteneffecten.[275] Elektriciteitsuitval vindt veelal onverwacht plaats. Omdat elektriciteit alleen kan worden getransporteerd wanneer het net op spanning is, heeft het elektriciteitsnet geen bufferwerking. Hierdoor zijn de effecten voor iedereen die getroffen is direct merkbaar. Meestal wordt een elektriciteitsuitval binnen twee uur verholpen en leidt dit niet tot maatschappelijke ontwrichting. Bij een grootschalige of zeer complexe uitval kan de oorzaak mogelijk niet altijd direct vastgesteld worden en is de hersteltijd moeilijk in te schatten.[276] De impact van elektriciteitsuitval op verschillende vitale processen wordt vaak al binnen enkele uren merkbaar.[277] Zo valt door de uitval van elektriciteit met enkele uren de telecomvoorziening uit, waardoor burgers ook geen toegang meer hebben tot 112. Bij grootschalige uitval zijn reguliere communicatiemiddelen, zoals internet en tv, al snel niet meer toegankelijk.[278] Het elektriciteitsnetwerk is een dusdanig essentiële voorziening in de Nederlandse samenleving dat uitval tot ernstige maatschappelijke ontwrichting kan leiden en daarmee een dreiging voor de nationale veiligheid kan vormen.[279]

Ook de aardgas- en elektriciteitsvoorziening zijn nauw met elkaar verweven en kunnen niet (lang) zonder elkaar functioneren. Omdat de apparatuur waarmee de aardgasvoorziening wordt

aangestuurd elektrisch gevoed wordt en er maar beperkt noodvoorzieningen voorhanden zijn functioneert de aardgasvoorziening niet zonder elektriciteit. Zonder aardgas kunnen gasgestookte elektriciteitscentrales dan weer niet functioneren, omdat er geen brandstof is waarmee de gascentrales de generatoren kunnen aandrijven.[280]

Het Analistennetwerk Nationale Veiligheid heeft in de Themarapportage bedreiging vitale infrastructuur (2022) een scenario uitgewerkt voor de uitval van de elektriciteitsvoorziening in Europa. Hoewel een groot deel van de vitale processen enige tijd via een noodstroomvoorziening zou kunnen functioneren, is het onzeker of dit in de praktijk ook zo werkt. Het effect van elektriciteitsuitval op andere vitale processen is weliswaar moeilijk in te schatten, maar het scenario van het ANV laat zien dat stroomuitval in Nederland gedurende 24 uur er toe kan leiden dat treinverkeer (deels) plat komt te liggen, er geen pinbetalingen meer kunnen worden uitgevoerd bij winkels zonder noodstroomvoorziening en objecten zoals gemalen niet lang zullen blijven functioneren.[281]

Door een stroomstoring kan het treinverkeer stil komen te liggen. Zo zorgde een storing in juni 2025 er voor dat er geen treinverkeer mogelijk was van en naar Schiphol.

6. Politieke, economische, sociale en technologische factoren

Verschillende politieke, economische, sociale en technologische factoren (PEST-factoren) beïnvloeden de vitale infrastructuur zelf, de dreigingen op en de weerbaarheid van de vitale infrastructuur. Daarmee hebben ze ook invloed op de impact van concrete incidenten die voortkomen uit dreigingen. Technologische ontwikkeling kan bijvoorbeeld de middelen die kwaadwillende actoren gebruiken om vitale infrastructuur te verstoren veranderen. Tegelijkertijd biedt technologische ontwikkeling vitale aanbieders nieuwe mogelijkheden om hun weerbaarheid tegen dreigingen te vergroten. De vitale infrastructuur zelf kan veranderen door bijvoorbeeld de energietransitie of digitalisering. Dit soort veranderingen hebben op hun beurt ook weer invloed op de dreiging en de weerbaarheid. Hieronder worden de belangrijkste PEST-factoren benoemd.

6.1 Toenemende afhankelijkheid digitale systemen

Een belangrijk kenmerk van de vitale infrastructuur is dat deze steeds afhankelijker wordt van digitale systemen, zoals in de gezondheidszorg en in de logistiek. Daarnaast nemen de complexiteit van systemen en afhankelijkheden tussen systemen en processen toe.[282] Bijvoorbeeld omdat deze met elkaar verbonden worden of omdat vitale processen gebruik maken van dezelfde hard- of software.[283] De onderlinge afhankelijkheden zorgen ervoor dat het moeilijk is in te schatten wat het effect van verstoring van een vitaal proces op andere vitale processen is.[284]

In tijden van toenemende geopolitieke spanningen neemt de dreiging voor verstoring van digitale systemen door cyberaanvallen, sabotage en spionage mogelijk toe.[285] Nederland is daarbij om verschillende redenen een aantrekkelijk doelwit voor kwaadwillende actoren. Zo heeft Nederland een hoogwaardige kenniseconomie en zijn we voorloper op het gebied van bepaalde technologieën. Ook huisvest Nederland verschillende internationale organisaties die informatie verwerken die interessant kan zijn voor kwaadwillenden.[286] Daarnaast is Nederland een aantrekkelijk doelwit, omdat we tot de top 5 van belangrijkste digitale knooppunten wereldwijd behoren.[287] Dit komt onder andere door de aanlanding van tien internationale onderzeese datakabels in Nederland, de aanwezigheid van internet exchanges waaronder Amsterdam Internet Exchange (AMS-IX) en de aanwezigheid van (co-locatie)datacentra. [288] Tot slot maakt de snelle, goedkope en betrouwbare internetinfrastructuur in Nederland het voor kwaadwillenden aantrekkelijk om vanuit Nederland cyberaanvallen te plegen tegen burgers, organisaties of overheden in andere landen.[289]

De meeste moderne (vitale) infrastructuur is vatbaar voor aanvallen waarbij kwaadwillenden digitale systemen binnendringen en manipuleren.[290] Cyberaanvallen vormen door digitalisering bijvoorbeeld een reëel gevaar voor grootschalige uitval van elektriciteitsnetwerken die verschillende energiecentrales verbinden en er voor zorgen dat elektriciteit bij huishoudens en bedrijven terechtkomt. Een succesvolle cyberaanval op een elektriciteitsnetwerk kan een keteneffect veroorzaken met grote fysieke gevolgen. Denk hierbij aan uitval van en schade aan energiecentrales en andere vitale infrastructuur, zoals watervoorzieningen, transport en communicatie.[291]

Ook bij financiële instellingen vinden dagelijks cyberaanvallen plaats.[292] De Europese financiële infrastructuur is onderling sterk met elkaar verbonden en bedrijven in de financiële sector zijn afhankelijk van een beperkt aantal digitale dienstverleners. Met een cyberaanval op één zo'n bedrijf kunnen hackers er meerdere raken en bedrijven kunnen elkaar onderling mogelijk besmetten.[293]

Operationele technologie (OT) is cruciaal voor het aansturen, monitoren en beheren van veel vitale processen. OT-systemen vormen het fundament van belangrijke fysieke processen, zoals de productie en verwerking van grondstoffen, het zuiveren van drinkwater, de bediening van sluizen en distributie van

elektriciteit. Bij incidenten in OT-omgevingen kan ook schade aan industriële apparatuur en de nabije omgeving ontstaan. In uiterste gevallen is het mogelijk dat er slachtoffers vallen. De toenemende integratie van operationele technologie en informatietechnologie (IT) vergroot het aanvalsoppervlak en maakt OT-systemen kwetsbaarder voor cyberaanvallen.[294]

Cyberactoren blijken geïnteresseerd te zijn in het compromitteren van OT, zo zijn er malware-soorten die gebruikt kunnen worden voor de sabotage van OT-systemen.[295] Sinds eind 2023 heeft Microsoft een toename waargenomen in het aantal meldingen van aanvallen gericht op aan internet blootgestelde en slecht beveiligde OT-apparaten.[296]

Doordat digitale processen, in een breder digitaal ecosysteem, in hoge mate met elkaar verbonden zijn, kunnen ook niet-vitale organisaties voor kwaadwillenden een aantrekkelijke springplank zijn naar vitale aanbieders.[297]

6.2 Technologische ontwikkeling

Technologische ontwikkelingen zullen in grote mate de toekomstige veiligheidsomgeving gaan beïnvloeden. Aan de ene kant kunnen technologische ontwikkelingen bestaande dreigingen voor de vitale infrastructuur versterken of deze kwetsbaarder maken voor dreigingen. Aan de andere kant kan nieuwe technologie ook worden gebruikt om de weerbaarheid van vitale infrastructuur te vergroten, bijvoorbeeld in de verdediging tegen (digitale) aanvallen. Daarnaast kan technologie worden gebruikt in het oplossen van maatschappelijke uitdagingen, zoals klimaatverandering, waardoor dreigingen voor de vitale infrastructuur kunnen afnemen.

Geavanceerde technologie wordt wereldwijd steeds breder toegankelijk en beschikbaar. Tussen staten is er sprake van een technologiewedloop, zeker op het gebied van AI, quantumtechnologie en ruimtetechnologie. Tegelijkertijd worden niet-statelijke (commerciële) partijen steeds belangrijker voor de ontwikkeling van nieuwe technologie. Grote technologiebedrijven als SpaceX, Meta en Alphabet (Google) hebben inmiddels grote economische en geopolitieke macht.[298]

Kunstmatige intelligentie

Een goed voorbeeld hiervan is de snelle ontwikkeling van generatieve AI. Sinds de introductie van ChatGPT eind 2022 zijn er wereldwijd vele AI-modellen beschikbaar gekomen die publiekelijk toegankelijk zijn en gratis of relatief goedkoop teksten, afbeeldingen, audio, video en deepfakes kunnen genereren. Ondertussen zijn de Verenigde Staten en China verwikkeld in een AI-techrace, waarin beide landen veel geld in de ontwikkeling van AI investeren. Tegelijkertijd worden deze nieuwe AI-toepassingen voornamelijk door grote techbedrijven ontwikkeld en op de markt gebracht, waardoor er nieuwe afhankelijkheden van deze bedrijven ontstaan.[299] AI versterkt ook bestaande dreigingen voor de vitale infrastructuur, bijvoorbeeld doordat kwaadwillende actoren deze technologie kunnen gebruiken om kwetsbaarheden in de digitale systemen van vitale infrastructuur te zoeken en hier mogelijk cyberaanvallen op uit te voeren.[300]

Naast AI komen robotica en autonome systemen ook steeds breder beschikbaar. Voorheen waren dit soort technologieën voornamelijk in handen van statelijke actoren, maar inmiddels kunnen ook niet statelijke actoren technologieën zoals commercieel verkrijgbare drones en do-it-yourself-kits voor genetische modificatie (biotechnologie) relatief goedkoop gebruiken. Hierdoor kunnen deze technologieën ook door kwaadwillende actoren zoals criminelen of terroristen worden ingezet.[301]

Ruimtetechnologie

Op het gebied van ruimtetechnologie zijn er drie relevante ontwikkelingen voor de nationale veiligheid. Allereerst is er sprake van een militarisering van de ruimte. Staten zoals China, de Verenigde Staten en Rusland integreren de ruimte in conventionele militaire operaties. Daarnaast is er een gebrek aan aandacht voor de digitale veiligheid van ruimtetechnologie. Satellieten worden gebruikt voor een breed scala aan militaire en civiele toepassingen, zoals GPS, aardobservatie en telecommunicatie. Verstoring van GPS kan bijvoorbeeld ontwrichtende keteneffecten op vitale infrastructuur hebben. Er is echter weinig inzicht in de mogelijke kwetsbaarheden van de ruimte infrastructuur. Tot slot is er een toenemende hoeveelheid commerciële partijen actief in de ruimte, dit leidt (mogelijk) tot nieuwe afhankelijkheden van commerciële partijen.[302]

Quantumtechnologie

Toepassingen van quantumtechnologie staan nog in de kinderschoenen, waardoor de potentiële impact deels nog onbekend is. Wel is het vanuit nationale veiligheidsperspectief noodzakelijk nu al te anticiperen op de komst van allerlei quantumtechnologie toepassingen. Met name de komst van de quantumcomputer is voor de vitale infrastructuur relevant.[303] Deze kan naar verwachting gebruikt worden om de huidige cryptografische standaarden te breken, waardoor protocollen en gevoelige gegevens die nu met encryptie goed beveiligd zijn, later alsnog ontcijferd kunnen worden.[304] Quantumcomputers hebben daarmee de potentie om in de toekomst verstoring of uitval van vitale processen te veroorzaken. Het is nog niet duidelijk wanneer deze technologie hiertoe in staat zal zijn, maar voor sommige partijen is het nu al van belang om te beginnen met het implementeren van post-quantumcryptografie.[305] Versleutelde data die nu onderschept en opgeslagen wordt, kan mogelijk namelijk op een later moment ontsleuteld worden met een quantumcomputer. Daardoor vormt een toekomstige krachtige quantumcomputer nu al een risico voor de nationale veiligheid.[306]

6.3 Energietransitie

De energietransitie, waarbij de energievraag wordt beperkt, fossiele brandstoffen worden uitgefaseerd en meer gebruik wordt gemaakt van duurzame energiebronnen, kan gevolgen hebben voor de vitale infrastructuur. Doordat steeds meer bedrijven en huishoudens overstappen op elektriciteit groeit de vraag naar elektriciteit harder dan de groei van de beschikbare capaciteit. Hierdoor komt de leveringszekerheid onder druk te staan en kan het aantal stroomstoringen op regionaal niveau door de krapte op het elektriciteitsnet stijgen. Ook de toenemende afhankelijkheid van zonne- en windenergie heeft effect op de leveringszekerheid. Bij langere periodes van gebrek aan zonne- en windenergie, moeten deze worden opgevangen door andere energiebronnen zoals waterstof of biomassa.[307]

Het effect van de energietransitie op vitale infrastructuur en de onderlinge verwevenheid is goed zichtbaar in de verwevenheid van energievoorzieningen en de digitale infrastructuur. Op veel plekken in Nederland is het elektriciteitsnet zo vol dat er de aankomende jaren geen capaciteit is voor het aansluiten van nieuwe grootverbruikers. De beschikbaarheid van voldoende capaciteit in het elektriciteitsnetwerk op lokaal niveau is echter essentieel voor het functioneren van de digitale infrastructuur. Zo is er extra elektriciteit nodig voor het uitbreiden van het 5g netwerk en het aansluiten van nieuwe woningen op de digitale infrastructuur. Tegelijkertijd is een betrouwbare digitale infrastructuur een voorwaarde voor de energietransitie, omdat intelligente energienetwerken hoge eisen stellen aan digitale connectiviteit.[308]

Daarnaast zijn er voor de energietransitie veel mineralen en metalen nodig waarvoor Europa sterk afhankelijk is van landen zoals China en de Democratische Republiek Congo. De levering van deze materialen kan een knelpunt vormen voor de energietransitie en tegelijkertijd kan de Europese afhankelijkheid van deze materialen als geopolitiek drukmiddel worden ingezet.[309]

Tot slot gaat de energietransitie hand in hand met digitalisering, waardoor de nieuwe energie-infrastructuur, zoals slimme meters en laadpalen, kwetsbaar is voor digitale aanvallen en sabotageacties gericht op het stroomnet.[310] Onderzoek van de Rijksinspectie Digitale Infrastructuur (RDI) laat zien dat de explosieve groei van het aantal zonnepaneelinstallaties gepaard gaat met een toename aan storing van deze installaties. De RDI onderzocht 9 omvormers waarvan er geen één aan de gebruikte normen voor cyberveiligheid voldeed. Hierdoor zijn zonnepaneelinstallaties eenvoudig te hacken en kunnen deze worden uitgeschakeld of ingezet voor DDoS-aanvallen. Daarnaast bleken vijf van de negen omvormers, die de energie die een zonnepaneel produceert omzet naar wisselspanning voor het elektriciteitsnet, zelf storingen te kunnen veroorzaken.[311]

6.4 Krapte op de arbeidsmarkt

De arbeidsmarkt is krap en zal dat door vergrijzing en afvlakkende productiviteitsgroei voorlopig ook blijven.[312] Personeelstekorten kunnen vitale aanbieders minder weerbaar maken tegen dreigingen en in een extreem geval kan personeelstekort zelf ook voor verstoring of uitval van vitale processen zorgen.

De Staatscommissie Demografische Ontwikkelingen 2050 beschrijft in het rapport Gematigde groei dat de vergrijzing van de Nederlandse bevolking in de komende 10 tot 15 jaar piekt en resulteert in een blijvend 'oudere' samenleving naar 2050.[313] Volgens onderzoek van McKinsey kan de krapte op de arbeidsmarkt in 2030 verdrievoudigen tot een tekort van 1,4 miljoen mensen. Bestaande tekorten zullen met name toenemen in technische beroepen, zorg en welzijn.[314]

Het tekort aan personeel met technische expertise kan ertoe leiden dat aanbieders van vitale infrastructuur onvoldoende gekwalificeerd personeel kunnen aantrekken. Vitale aanbieders kunnen hierdoor mogelijk geen state-of-the-art systemen installeren en er kunnen op de lange termijn ook problemen ontstaan wanneer er te weinig technische kennis is over het aansturen en onderhouden van systemen. Juist in geval van een incident is menselijk ingrijpen nodig om verstoring in geautomatiseerde processen op te vangen. Denk aan het handmatig aansturen van bruggen en sluizen, als de geautomatiseerde bediening verstoort raakt of uitvalt. Ook de toenemende complexiteit en afhankelijkheden binnen systemen vragen om specifieke kennis en expertise om deze aan te sturen, te onderhouden en te reageren op incidenten.[315]

Het tekort aan technisch personeel vormt een sluimerende dreiging die er toe kan leiden dat de weerbaarheid van vitale infrastructuur niet op peil kan worden gehouden.[316] Zo waarschuwde de Cyber Security Raad in juli 2024 al in een brief aan de minister van Economische Zaken voor de effecten van tekorten op de cybersecurity arbeidsmarkt op de digitale weerbaarheid en de strategische digitale autonomie van Nederland.[317] Daarnaast kan het voor kwaadwillenden interessant worden om te identificeren bij welke organisaties de grootste tekorten zijn en die daarmee mogelijk de zwakste verdediging hebben.[318]

In de zorg zal er zelfs sprake zijn van een 'dubbele vergrijzing', omdat er door de ouder wordende bevolking aan de ene kant minder zorgpersoneel beschikbaar is en er aan de andere kant meer mensen een beroep op de zorg gaan doen.[319]

6.5 Economische ontwikkelingen

Economische ontwikkelingen wereldwijd kunnen invloed hebben op vitale processen. Denk aan het effect van prijsstijgingen of handelsbeperkingen m.b.t. grondstoffen op vitale aanbieders. Nederland, als kleine, open economie binnen de Eurozone, blijft kwetsbaar voor internationale financiële schokken. Problemen in andere landen kunnen aanzienlijke gevolgen hebben voor onze economie. Bankencrises of andere problemen bij financiële marktpartijen, fiscale crises (in de Eurozone), handelsgeschillen of de geopolitisering van de wereldhandel kunnen daarmee een relatief grote impact op de Nederlandse economie hebben.[320]

De wereldeconomie fragmenteert de laatste jaren steeds meer. Volgens het IMF namen landen in 2023 wereldwijd meer dan 2.500 industriepolitieke maatregelen, waarvan 70% een verstorende werking op de handel heeft. De Nederlandse economie is gevoelig voor deze fragmentatie, omdat onze economie voor een groot deel afhankelijk is van internationale handel. Dit maakt Nederland gevoelig voor verstoringen in mondiale toeleveringsketens en handels- en kapitaalsbeperkingen.[321]

Op de bodem van de Noordzee ligt een netwerk van o.a. internetkabels en elektriciteitskabels van windmolenparken. Een onbemand oppervlaktevaartuig helpt bij het waarborgen van de veiligheid van essentiële onderzeese infrastructuren.

7. Conclusie

Dit dreigingslandschap laat zien dat de vitale infrastructuur te maken heeft met een stapeling van uiteenlopende dreigingen. Met name hybride aanvallen door statelijke actoren, waaronder fysieke en digitale sabotage, spionage en pre-positionering en misbruik van strategische afhankelijkheden vormen een toenemende dreiging. Ook de gevolgen van de alsmaar versnellende klimaatverandering zullen een steeds grotere en deels nog moeilijk in te schatten impact op de vitale infrastructuur hebben.

Wanneer deze dreigingen zich manifesteren in concrete gebeurtenissen en vitale processen hier onvoldoende weerbaar voor zijn ontstaat het risico op verstoring of uitval. Zeker wanneer verschillende dreigingen, waaronder menselijk en systeemfalen, zich gelijktijdig voordoen neemt het risico hierop toe. Daarbij kan de nationale veiligheid in het geding komen. Door complexe, steeds veranderende en soms verborgen onderlinge afhankelijkheden kan verstoring van één vitaal proces daarbij grote keteneffecten hebben op andere vitale processen. Ook laten verschillende voorbeelden van (cyber)spionage en pre-positionering voor sabotage zien dat, ook wanneer er geen sprake is van verstoring of uitval, kwaadwillenden de integriteit en vertrouwelijkheid van vitale processen kunnen aantasten.

Tegelijkertijd zorgen vaak ingrijpende politieke, economische, sociale en technologische ontwikkelingen er voor dat de vitale infrastructuur zelf, de weerbaarheid ervan en de dreigingen waarmee vitale processen worden geconfronteerd veranderen. Dit maakt het voor de nationale veiligheid extra belangrijk om periodiek naar de staat van de driehoek van dreigingen, belang en weerbaarheid van vitale processen te kijken.

Omdat de dreigingen continu veranderen is het belangrijk de kennis hierover actueel te houden. De NCTV draagt hier onder andere aan bij met periodieke analyseproducten zoals het Dreigingsbeeld Statelijke Actoren, het Cybersecuritybeeld Nederland, het Dreigingsbeeld Terrorisme Nederland en verschillende thema-analyses.

De in dit dreigingslandschap beschreven dreigingen onderstrepen het belang van een weerbare vitale infrastructuur. Dat begint bij inzicht in de huidige weerbaarheid van vitale processen, waarin met de weerbaarheidsanalyses die de vakdepartementen per vitaal proces zullen uitvoeren invulling zal worden geven. Hierbij kunnen zij het in dit dreigingslandschap uitgewerkte denkkader en de beschreven dreigingen als startpunt gebruiken.

Bronnen

1 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2022.
https://www.nctv.nl/onderwerpen/vitale-infrastructuur
2 'Hybride dreigingen en maatschappelijke weerbaarheid', Adviesraad Internationale Vraagstukken, 04-06-2024.
https://magazines.defensie.nl/defensiekrant/2022/41/03_hybride-dreiging-gas_41
3 https://www.nctv.nl/onderwerpen/vitale-infrastructuur/aanpak-vitaal
4 Themarapportage klimaat- en natuurrampen, Analistennetwerk Nationale Veiligheid, 2022.
5 'Tussenbalans van het Kennisprogramma Zeespiegelstijging', Kennisprogramma Zeespiegelstijging, november 2023.
6 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2022.
7 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2022.
8 'Hybride dreigingen en maatschappelijke weerbaarheid', Adviesraad Internationale Vraagstukken, 04-06-2024.
9 'Themarapportage bedreiging vitale infrastructuur', Analistennetwerk Nationale Veiligheid, 2022.
10 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2022.
11 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
12 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
13 'Themarapportage bedreiging vitale infrastructuur', Analistennetwerk Nationale Veiligheid, 2022.
14 https://www.nctv.nl/onderwerpen/vitale-infrastructuur
15 'Leidraad Risicobeoordeling Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2019.
16 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2022.
17 'Weerbaarheid becijferd Een methode om weerbaarheid tegen dreigingen voor de nationale veiligheid inzichtelijk te maken', RAND Europe, 2024.
18 https://www.nctv.nl/onderwerpen/vitale-infrastructuur.
19 Weerbaarheid in een gure wereld – Geopolitieke risico's en financiële instellingen', De Nederlandse Bank, november 2024.
20 Kamerbrief over Weerbaarheid tegen militaire en hybride dreigingen, 6 december 2024.
21 Themarapportage klimaat- en natuurrampen, Analistennetwerk Nationale Veiligheid, 2022.
22 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024. 'Nederland in een fragmenterende wereldorde', WRR, 01-07-2024.
23 Kamerbrief over Weerbaarheid tegen militaire en hybride dreigingen, 6 december 2024.
24 Jaarverslag AIVD 2022.
25 Vragen van de leden Bontenbal en Boswijk (beiden CDA) aan de ministers van Buitenlandse Zaken en van Defensie over het artikel 'Russia plotting sabotage across Europe, intelligence agencies warn', Ministerie van Defensie, 18 juni 2024.
26 Jaarverslag AIVD 2023.
27 'Hybride dreigingen en maatschappelijke weerbaarheid', Adviesraad Internationale Vraagstukken, 04-06-2024.
28 'Hybride dreigingen en maatschappelijke weerbaarheid', Adviesraad Internationale Vraagstukken, 04-06-2024.
29 'Themarapportage ongewenste inmenging en beïnvloeding democratische rechtsstaat', Analistennetwerk Nationale Veiligheid, juli 2022.
30 'Dreigingsbeeld militaire en hybride dreigingen', BZK, AIVD en MIVD, December 2024.
31 Kamerbrief over Weerbaarheid tegen militaire en hybride dreigingen, 6 december 2024.
32 'Dreigingsbeeld militaire en hybride dreigingen', BZK, AIVD en MIVD, December 2024.
33 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
34 Kamerbrief over Weerbaarheid tegen militaire en hybride dreigingen, 6 december 2024.
35 Dreigingsbeeld Statelijke Actoren 2, AIVD, MIVD en NCTV, 2022.
36 'Vragen van de leden Bontenbal en Boswijk (beiden CDA) aan de ministers van Buitenlandse Zaken en van Defensie over het artikel 'Russia plotting sabotage across Europe, intelligence agencies warn', Ministerie van Defensie, 18 juni 2024.
37 'Russia plotting sabotage across Europe, intelligence agencies warn', Financial Times, 5 mei 2024.
38 https://dataverse.harvard.edu/file.xhtml?fileId=10787750&version=2.0
39 'Chaos, Orde en Machtspolitiek HCSS Strategische Monitor 2025', HCSS, December 2024.
40 'German spying: Two men held over suspected Russian sabotage plot', BBC, 18 april 2024.

41 'Drie Duits-Russische mannen beschuldigd voor sabotage en spionage in opdracht van Rusland', Het Laatste Nieuws, 2 januari 2025.
42 'Two British men charged with helping Russian intelligence', BBC, 26 april 2024.
43 'Rusland zit achter reeks branden bij DHL-depots in Europa', NRC, 6 november 2024.
44 'CNN: Rusland wilde topman van Duitse wapenfabrikant vermoorden', NOS, donderdag 11 juli 2024.
45 https://english.radio.cz/czech-minister-tells-financial-times-russia-trying-sabotage-critical-8813329
46 'Eemshaven militair terrein: en dan?', Dagblad van het Noorden, 4 januari 2025.
47 'Nederlands spoor speelt cruciale rol in snelle mobilisatie NAVO, maar achterstallig onderhoud is groot probleem', De Telegraaf, 21 april 2024.
https://www.defensie.nl/onderwerpen/internationale-samenwerking/host-nation-support
48 'New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape', HCSS & TNO, mei 2024.
49 'New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape', HCSS & TNO, mei 2024.
50 'New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape', HCSS & TNO, mei 2024.
51 'Europa kwetsbaar voor sabotage', Reformatorisch Dagblad, 22 november 2024.
52 'New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape', HCSS & TNO, mei 2024.
53 'Duitse autoriteiten op het punt aanslagplegers Nord Stream te arresteren, dubieuze rol voor Polen', Volkskrant, 14 augustus 2024.
54 'New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape', HCSS & TNO, mei 2024.
55 'Lek in gaspijplijn tussen Finland en Estland, Finse president spreekt van 'externe activiteit'', NRC, 10 okt 2023.
56 Invisible frontlines Safeguarding the European Energy Infrastructure, Danish Institute for International Studies, 2024.
'A Chinese ship remains the focus of the investigation into Baltic Sea gas pipeline damaged last year', APnews, 25 april 2024.
57 'Kabelbreuken in Rode Zee mogelijk werk van Houthi-strijders', NRC, 27 februari 2024.
58 'Europa kwetsbaar voor sabotage', Reformatorisch Dagblad, 22 november 2024.
59 "Saboteerden Russen stroomkabel Oostzee? 5 vragen over de Estlink 2", De Telegraaf, 26 december 2024.
60 'Kapotvaren glasvezelkabel in Oostzee geen sabotage maar 'ongelukje'', Volkskrant, 3 februari 2025.
61 Kamerbrief Rapport Inventarisatie Kwetsbaarheid Uitval Satellietnavigatie, Ministerie van Infrastructuur en Waterstaat, 7 maart 2023.
62 'Jaarpublicatie Analysebureau Luchtvaartvoorvallen 2023', Inspectie Leefomgeving en Transport (ILT), 15 augustus 2024.
63 'Met grootschalige gps-jamming bereikt elektronische oorlogsvoering ook de NAVO-landen, de Volkskrant, 14 maart 2024.
64 'De wereld draait op tijd. Maar dan moeten we wel exact weten hoe laat het is', De Correspondent, 5 december 2024.
65 'Jaarpublicatie Analysebureau Luchtvaartvoorvallen 2023', Inspectie Leefomgeving en Transport (ILT), 15 augustus 2024.
66 'Valse gps-signalen misleiden passagiersvliegtuigen boven Midden-Oosten', NOS, 16 maart 2024.
67 'Jaarpublicatie Analysebureau Luchtvaartvoorvallen 2023', Inspectie Leefomgeving en Transport (ILT), 15 augustus 2024.
68 https://nos.nl/regio/noord-holland/artikel/597792-extreme-toename-van-meldingen-over-verstoring-gps-signaal-in-nederlandse-cockpits
69 'Valse gps-signalen misleiden passagiersvliegtuigen boven Midden-Oosten', NOS, 16 maart 2024.
70 https://www.navnin.nl/new/2024/09/26/verslag-van-de-workshop-gnss-jamming-en-spoofing-op-12-09-2024/
71 https://www.marinelink.com/blogs/blog/finland-detects-jamming-of-satellite-navigation-and-spoofing-on-102058
https://www.reuters.com/world/europe/finland-warns-hostile-activities-by-russia-2024-10-23/
72 Finland merkt verstoring van navigatiesignalen en 'spoofing' op zee: "Schepen verdwalen", Het Laatste Nieuws, 31 oktober 2024.
73 GPS Spoofing, OPSGROUP, 6 september 2024.
'Valse gps-signalen misleiden passagiersvliegtuigen boven Midden-Oosten', NOS, 16 maart 2024.
74 GPSJAM GPS/GNSS Interference Map
75 'America's Asymmetric Vulnerability to Navigation Warfare: Leadership and Strategic Direction Needed to Mitigate Significant Threats', Marc J. Berkowitz, 18 juli 2024.
76 Kamerbrief Rapport Inventarisatie Kwetsbaarheid Uitval Satellietnavigatie, Ministerie van Infrastructuur en Waterstaat, 7 maart 2023.
https://www.dlr.de/en/media/videos/2021/video-what-would-a-day-without-space-look-like
https://www.strict.nl/blog/inzicht-in-gps-jamming-en-spoofing-toepassingen-gevolgen-en-maatregelen
77 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
78 Jaarverslag MIVD 2023.
79 Kamerbrief voortgang Strategie ter bescherming Noordzee Infrastructuur, Ministerie van Infrastructuur en Waterstaat, 10 juni 2024.
80 Kamerbrief voortgang Strategie ter bescherming Noordzee Infrastructuur, Ministerie van Infrastructuur en Waterstaat, 10 juni 2024.
81 Jaarverslag MIVD 2023.
82 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
83 'New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape', HCSS & TNO, mei 2024.
84 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
85 Cybersecuritybeeld Nederland 2023', NCTV, 3 juli 2023.
86 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
87 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
88 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.

89 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
90 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024
91 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
92 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
93 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
94 Jaarverslag AIVD 2023.
95 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
96 'MIVD onthult werkwijze Chinese spionage in Nederland', Ministerie van Defensie, 6 februari 2024.
97 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
98 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
99 'FBI shuts down China's 'Volt Typhoon' hackers targeting U.S. infrastructure', CNBS, 31 januari 2024.
100 https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications
'Chinese hackers are deep inside America's telecoms networks', The Economist, 12 december 2024.
101 'U.S. Wiretap Systems Targeted in China-Linked Hack', The Wall Street Journal, 5 oktober 2024.
102 https://www.defensie.nl/actueel/nieuws/2024/09/05/mivd-waarschuwt-russen-hebben-het-gemunt-op-westerse-hulp-aan-oekraine
103 'Cybersecuritybeeld Nederland 2023', NCTV, 3 juli 2023.
104 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
105 "Hacking the Cosmos: Cyberoperations against the space sector – A case study from the ware in Ukraine, Center for Security Studies – ETH Zürich, oktober 2024.
106 'Pro-Russische groep legt websites Nederlandse havens plat', RTL Nieuws, 14-06-2023.
107 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
108 https://therecord.media/cyber-army-russia-us-sanctions
109 Jaarverslag AIVD 2023.
110 'Albanië verbreekt diplomatieke banden met Iran na cyberaanval', NOS, 8 september 2022.
111 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
112 https://www.nctv.nl/onderwerpen/desinformatie
113 'Weerbaarheid in een gure wereld – Geopolitieke risico's en financiële instellingen', De Nederlandse Bank, november 2024.
114 'Weerbaarheid in een gure wereld – Geopolitieke risico's en financiële instellingen', De Nederlandse Bank, november 2024.
115 'New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape', HCSS & TNO, mei 2024.
116 Kamerbrief over ontwikkelingen Chinabeleid, een verschuiving van de balans, 13 januari 2023.
'Hybride dreigingen en maatschappelijke weerbaarheid', Adviesraad Internationale Vraagstukken, 04-06-2024.
117 'China's economic coercion. Evolution, characteristics and countermeasure', European Parliamentary Research Service, November 2022.
118 'China's economic coercion. Evolution, characteristics and countermeasure', European Parliamentary Research Service, November 2022.
119 'Fasten your seatbelts: How to manage China's economic coercion', MERICS, 25-08-2022.
120 'China's economic coercion. Evolution, characteristics and countermeasure', European Parliamentary Research Service, November 2022.
121 'China's use of export controls, International Institute for Strategic Studies', 27 februari 2025.
122 'Groene zonnepanelen uit nederland: China's bijna-monopolie op zonne-energie', De Groene Amsterdammer, 12 juni 2024.
123 'Ons leger loopt gevaar'; Nederland dreigt productie ijzersterke vezel te verliezen aan Chinese concurrentie: 'Strategisch risico', De Telegraaf, 09 november 2024.
124 'Strategische Monitor 2023: Barsten en Blokken', Clingendael en HCSS, januari 2024.
125 'China's use of export controls, International Institute for Strategic Studies', 27 februari 2025.
126 'Strategische Monitor 2023: Barsten en Blokken', Clingendael en HCSS, januari 2024.
127 'Strategische Monitor 2023: Barsten en Blokken', Clingendael en HCSS, januari 2024.
128 Kamerbrief over ontwikkelingen Chinabeleid, een verschuiving van de balans, 13 januari 2023.
129 'Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoffen en Taiwanese chips voor vitale-sectoren.', The Hague Centre for Strategic Studies, April 2023.
130 'Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoffen en Taiwanese chips voor vitale-sectoren.', The Hague Centre for Strategic Studies, April 2023.
131 'Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoffen en Taiwanese chips voor vitale-sectoren.', The Hague Centre for Strategic Studies, April 2023.
132 'Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoffen en Taiwanese chips voor vitale-sectoren.', The Hague Centre for Strategic Studies, April 2023.
133 Kamerbrief over ontwikkelingen Chinabeleid, een verschuiving van de balans, 13 januari 2023.
134 'Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoffen en Taiwanese chips voor vitale-sectoren.', The Hague Centre for Strategic Studies, April 2023.
135 'Nederland te afhankelijk van Rusland voor nucleaire medicijnen', NOS, 22 augustus 2024.

136 'Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoen en Taiwanese chips voor vitale-sectoren.', The Hague Centre for Strategic Studies, April 2023.
137 https://ibestuur.nl/artikel/als-het-gaat-om-digitale-technologie-zijn-we-te-afhankelijk/
138 Jaarverslag en slotwet Ministerie van Economische Zaken en Klimaat 2023.
Agenda Digitale Open Strategische Autonomie
139 'Too late to act? Europe's quest Policy Brief for cloud sovereignty', Clingendael, maart 2024.
140 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
141 'DNB: burgers moeten beseffen dat financiële dienstverlening uit kan vallen', NRC,
21 oktober 2024.
142 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
143 Versterkte dreigingen in een wereld vol kunstmatige intelligentie, NCTV, AIVD en MIVD, december 2024.
144 Agenda Digitale Open Strategische Autonomie
145 Versterkte dreigingen in een wereld vol kunstmatige intelligentie, NCTV, AIVD en MIVD, december 2024.
146 'Dreigingsbeeld Terrorisme Nederland december 2024', NCTV, December 2024.
147 Dreigingsbeeld Terrorisme Nederland, Juni 2024.
148 https://monitoring.bbc.co.uk/product/b00036gf
149 'Dreigingsbeeld Terrorisme Nederland 55', NCTV, Oktober 2021.
'Dreigingsbeeld Terrorisme Nederland 57', NCTV, November 2022.
150 'Dreigingsbeeld Terrorisme Nederland december 2023', NCTV, December 2023.
151 'Dreigingsbeeld Terrorisme Nederland december 2024', NCTV, December 2024.
152 'Kosten van stroomstoring bij Tesla-fabriek lopen 'in de negen cijfers', NOS, 5 maart 2024.
153 'Dreigingsbeeld Terrorisme Nederland december 2024', NCTV, December 2024.
154 'Extreemlinkse activist gearresteerd na sabotage spoorwegen Frankrijk', NOS, 29 juli 2024.
155 'Glasvezelnetwerken gesaboteerd in Frankrijk, Olympische Spelen niet gehinderd', Trouw, 29 juli 2024.
156 'Raadselachtige sabotage treft internet in Frankrijk: 'Een incident op deze schaal is nog nooit gebeurd'', De Volkskrant, 27 april 2022.
157 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
158 The Far-Right's Fascination with the U.S. Electric Grid, UNICORN RIOT, 19 december 2022
159 'Dreigingsbeeld Terrorisme Nederland juni 2024', NCTV, juni 2024.
Jaarverslag MIVD 2023.
160 'Met de rug naar de samenleving Een analyse van de soevereinenbeweging in Nederland', AIVD, Nationale Politie en NCTV, 9 april 2024.
161 Dreigingsbeeld Terrorisme Nederland, NCTV, December 2024.
162 'Ruim 200 klimaatactivisten gearresteerd op Schiphol, alle actievoerders weg', Nos, 5 november 2022.
163 'Noodverordening Maastricht Airport verlengd na protest Extinction Rebellion', NOS, 9 maart 2024.
164 'Bijna 100 klimaatbetogers opgepakt na actie voorbij controles Schiphol', NOS, december.
165 '200 Flugausfälle nach Kleber-Attacke in Frankfurt', Neue Presse, 26 juli 2024.
'Flughafen Frankfurt lahmgelegt', Frankfurter Neue Presse, 26 juli 2024.
166 Politiker reagieren empört auf Flughafen-Blockade, Tagesschau, 18 mei 2024.
167 https://www.rijnmond.nl/nieuws/1853646/extinction-rebellion-weggestuurd-bij-haven-rotterdam-parallelbaan-a15-weer-open
168 https://www.rijnmond.nl/nieuws/1884672/demonstratie-op-de-botlekbrug-is-slechts-het-begin-zeggen-activisten
169 'Extinction Rebellion blokkeert opnieuw doorgang cruiseschip IJmuiden, gemeente ontbindt actie', Trouw, 11 augustus 2024.
170 'Greenpeace-activisten bezetten boorplatform bij Schiermonnikoog', NOS Nieuws, dinsdag 4 juni 2024.
171 https://nos.nl/artikel/2518386-blokkade-extinction-rebellion-beeindigd-a10-is-weer-vrij
Zijn er staatsrechtelijke blokkades op de snelweg voor demonstranten? | Erasmus University Rotterdam (eur.nl)
172 https://www.rtvoost.nl/nieuws/2311207/boeren-voeren-met-branden-en-blokkades-actie-zo-zag-dat-er-maandagavond-uit
https://www.rtl.nl/nieuws/artikel/5317581/boerenprotesten-traktoren
173 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
174 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
175 ''Grootste cyberaanval' op Deense vitale infrastructuur raakte 22 energiebedrijven´, security.nl, 14 november 2023.
176 ''Grootste cyberaanval' op Deense vitale infrastructuur raakte 22 energiebedrijven´, security.nl, 14 november 2023.
177 Invisible frontlines Safeguarding the European Energy Infrastructure, Danish Institute for International Studies, 2024.
178 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
https://www.security.nl/posting/789992/Maritiem+dienstverlener+Royal+Dirkzwager+getroffen+door+ransomware
179 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024
180 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024
181 'Russian crime group behind London hospitals cyber-attack, says expert', The Guardian, 5 juni 2024.

182 'Ransomware attack on major US blood center prompts hundreds of hospitals to implement shortage protocols', The Reford, 31 juli 2024.
183 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
184 https://www.portofrotterdam.com/nl/bouwen-aan-de-haven/veilige-haven/ondermijning
185 https://www.prorail.nl/veelgestelde-vragen/waarom-is-koperdiefstal-zo-n-probleem-op-het-spoor
186 'Aantal koperdiefstallen op het spoor vorig jaar drastisch afgenomen', nu.nl, 9 januari 2023.
187 https://www.bnr.nl/nieuws/bouw-infrastructuur/10546386/koperdiefstal-zonneparken-indirecte-kosten-zijn-een-groot-probleem
188 Zie voor een handreiking over het omgaan met insider threats in het cyberdomein: 'Omgaan met insider threats', Nationaal Cyber Security Centrum, 28 februari 2024.
189 Insider Risk Trend Report 2025, Signpost Six, januari 2025.
190 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
191 'Climate Change 2023 Synthesis report.', IPCC. 2023.
192 'Klimaatrisico's in Nederland; De huidige stand van zaken.', Planbureau voor de Leefomgeving, 14 mei 2024.
193 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2022.
'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
194 'Themarapportage bedreiging vitale infrastructuur', Analistennetwerk Nationale Veiligheid, 2022.
'Klimaatrisico's in Nederland: De huidige stand van zaken zaken', Planbureau voor de Leefomgeving, 14 mei 2024.
195 'Klimaatrisico's in Nederland: De huidige stand van zaken zaken', Planbureau voor de Leefomgeving, 14 mei 2024.
196 'Deltascenarios-2024 - Zicht op water in Nederland', Deltares, april 2024.
197 'Klimaatrisico's in Nederland: De huidige stand van zaken zaken', Planbureau voor de Leefomgeving, 14 mei 2024.
198 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
199 'Deltascenarios-2024 - Zicht op water in Nederland', Deltares, april 2024.
200 'Deltascenarios-2024 - Zicht op water in Nederland', Deltares, april 2024.
201 Koninklijk Nederlands Meteorologisch Instituut (KNMI). (9 oktober 2023). KNMI'23-klimaatscenario's voor Nederland. Beschikbaar via: https://www.knmi.nl/research/ publications/knmi-23-klimaatscenario-s-voor-nederland
202 'Deltascenarios-2024 - Zicht op water in Nederland', Deltares, april 2024.
203 Koninklijk Nederlands Meteorologisch Instituut (KNMI). (9 oktober 2023). KNMI'23-klimaatscenario's voor Nederland. Beschikbaar via: https://www.knmi.nl/research/ publications/knmi-23-klimaatscenario-s-voor-nederland
204 'Deltascenarios-2024 - Zicht op water in Nederland', Deltares, april 2024.
205 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
206 'Juli 2021 overstroming en wateroverlast in Zuid-Limburg', Deltares, 26 april 2022.
207 https://www.knmi.nl/over-het-knmi/nieuws/waarom-viel-er-de-afgelopen-dagen-zoveel-regen-in-spanje
208 'Bizar, maar dit is slechts het begin, minder wordt het niet', Algemeen Dagblad, 2 november 2024.
209 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
210 KNMI: klimaatverandering wordt meer voelbaar, valwind als in Leersum gaat vaker voorkomen, RTV Utrecht, 25 oktober 2021.
211 Themarapportage klimaat- en natuurrampen, Analistennetwerk Nationale Veiligheid, 2022.
212 Themarapportage klimaat- en natuurrampen, Analistennetwerk Nationale Veiligheid, 2022.
213 https://www.rtl.nl/nieuws/nederland/artikel/5237270/kabels-hoogspanningsmast-boerderij-vluchten-valwind
214 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
'Kamerbrief Toekomst binnenvaart', Ministerie van Infrastructuur en Waterstaat, 30 november 2022.
215 'Deltascenarios-2024 - Zicht op water in Nederland', Deltares, april 2024.
216 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
217 'Tussenbalans van het Kennisprogramma Zeespiegelstijging', Kennisprogramma Zeespiegelstijging, november 2023.
218 'Deltascenarios-2024 - Zicht op water in Nederland', Deltares, april 2024.
219 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
220 https://www.rivm.nl/nieuws/snel-actie-nodig-om-drinkwatertekort-in-2030-te-voorkomen
221 'Als er niets gebeurt, is straks overal een watertekort. Zo moet het water uit de kraan drinkbaar en betaalbaar blijven', NRC, 12 januari 2025.
222 https://www.nieuwsienw.nl/home_old1717146098/2966196.aspx
223 'Kamerbrief Toekomst binnenvaart', Ministerie van Infrastructuur en Waterstaat, 30 november 2022.
224 https://www.rijkswaterstaat.nl/water/waterbeheer/droogte-en-watertekort/verdeling-water-bij-droogte
225 https://www.onswater.nl/actueel/nieuws/2023/07/19/droogte-zorgt-voor-problemen-voor-nederlandse-dijken
226 Spoorwegen - Klimaatadaptatie
227 https://www.europoortkringen.nl/chemie-informeert-rijk-over-impact-droogte/
228 'Natuurbrandsignaal '23', Nederlands Instituut Publieke Veiligheid, 23 januari 2023.
229 'Kamerbrief Op weg naar een integrale aanpak van natuurbrandbeheersing', Ministerie van Landbouw, Natuur en Voedselkwaliteit, 13 juni 2024.
230 'Natuurbrandsignaal '23', Nederlands Instituut Publieke Veiligheid, 23 januari 2023.

231 'Natuurbrandsignaal '23', Nederlands Instituut Publieke Veiligheid, 23 januari 2023.
232 'Natuurbrandsignaal '23', Nederlands Instituut Publieke Veiligheid, 23 januari 2023.
233 Koninklijk Nederlands Meteorologisch Instituut (KNMI). (9 oktober 2023). KNMI'23-klimaatscenario's voor Nederland. Beschikbaar via: https://www.knmi.nl/research/ publications/knmi-23-klimaatscenario-s-voor-nederland
234 'Tussenbalans van het Kennisprogramma Zeespiegelstijging', Kennisprogramma Zeespiegelstijging, november 2023.
235 'Tussenbalans van het Kennisprogramma Zeespiegelstijging', Kennisprogramma Zeespiegelstijging, november 2023.
236 Themarapportage klimaat- en natuurrampen, Analistennetwerk Nationale Veiligheid, 2022.
237 Themarapportage klimaat- en natuurrampen, Analistennetwerk Nationale Veiligheid, 2022.
238 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
239 Themarapportage klimaat- en natuurrampen, Analistennetwerk Nationale Veiligheid, 2022.
240 https://www.knmi.nl/over-het-knmi/nieuws/jaaroverzicht-aardbevingen-2024
241 'Uitleg over Ruimteweer', KNMI.
242 'KNMI onderzoekt effecten van ruimteweer op ons dagelijks leven', KNMI, 9 mei 2022.
243 https://magazines.defensie.nl/vliegendehollander/2015/05/ruimteweer
244 'KNMI onderzoekt effecten van ruimteweer op ons dagelijks leven', KNMI, 9 mei 2022.
245 https://www.knmi.nl/over-het-knmi/nieuws/geomagnetische-storm-verwacht-door-uitbarsting-op-de-zon
246 'KNMI onderzoekt effecten van ruimteweer op ons dagelijks leven', KNMI, 9 mei 2022.
247 'SpaceX to lose up to 40 Starlink satellites after geomagnetic storm', the Guardian, 9 februari 2022.
248 https://www.knmi.nl/over-het-knmi/nieuws/geomagnetische-storm-verwacht-door-uitbarsting-op-de-zon
249 https://www.knmi.nl/over-het-knmi/nieuws/knmi-onderzoekt-effecten-van-ruimteweer-op-ons-dagelijks-leven
250 https://www.newscientist.nl/nieuws/krachtige-zonnevlam-veroorzaakte-tijdelijke-radiostoring/
251 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2022.
https://www.nctv.nl/onderwerpen/vitale-infrastructuur
252 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
253 'WHO slaat alarm over vogelgriep, al is kans op nieuwe pandemie klein', NOS, 21 april 2024.
254 'Kans op nieuwe pandemie, Amerikaanse aanpak vogelgriep één groot gokspel', NOS. 11 januari 2025.
255 'Bij een nieuwe pandemie is er in Nederland weer een tekort aan IC's en tests', NRC, 22 februari 2024.
256 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
257 'OpenAI: geringe kans dat ChatGPT recept geeft voor biologische wapens', RTLnieuws, 01-02-2024, https://www.rtlnieuws.nl/economie/artikel/5432595/kleine-kans-dat-openai-recept-geeft-voor-biologische-wapens
'Capabilities and risks from frontier AI: A discussion paper on the need for further
research into AI risk', AI Safety Summit, oktober 2023.
258 'Capabilities and risks from frontier AI: A discussion paper on the need for further
research into AI risk', AI Safety Summit, oktober 2023.
'The Operational Risks of AI in Large-Scale Biological Attacks: Results of a Red-Team Study.',Mouton, Christopher A., Caleb Lucas, and Ella Guest (RAND Corporation), 2024. https://www.rand.org/pubs/research_reports/RRA2977-2.html.
259 'Themarapportage bedreiging vitale infrastructuur', Analistennetwerk Nationale Veiligheid, 2022.
260 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
261 'Benut grootste computerstoring ooit als leerzame brandoefening', NRC Handelsblad, 27 juli 2024.
262 Over de hele wereld is er hinder van de computerstoring. Wat is er aan de hand, en hoe kan het opgelost worden?', NRC Handelsblad, 19 juli 2024.
263 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
264 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
265 https://nos.nl/artikel/2535038-extra-schepen-vliegtuig-en-inzet-politie-hielpen-kustwacht-storing-door
266 'Themarapportage bedreiging vitale infrastructuur', Analistennetwerk Nationale Veiligheid, 2022.
267 'Kamerbrief Onderwerp Stand van zaken vernieuwing en vervanging C2000 zomer 2023', Ministerie van Justitie en Veiligheid, 14 juni 2023.
268 'Frustratie over hapering communicatiesysteem politie: 'Problemen spelen al jaren'', NOS, 2 januari 2025.
269 Storing luchtverkeersleidingssysteem
270 'Storing luchtverkeersleiding wordt extern onderzocht', NOS, 25 april 2024.
271 'Klimaatrisico's in Nederland: De huidige stand van zaken zaken', Planbureau voor de Leefomgeving, 14 mei 2024.
272 'Spoorwegongeval Voorschoten', Onderzoeksraad voor Veiligheid, Mei 2024.
273 'Klimaatrisico's in Nederland: De huidige stand van zaken zaken', Planbureau voor de Leefomgeving, 14 mei 2024.
274 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2022.
275 'Klimaatrisico's in Nederland: De huidige stand van zaken zaken', Planbureau voor de Leefomgeving, 14 mei 2024.
276 'Nationaal Crisisplan Elektriciteit', Ministerie van Economische Zaken en Klimaat, februari 2022.
277 'Nationaal Crisisplan Elektriciteit', Ministerie van Economische Zaken en Klimaat, februari 2022.

278 'Nationaal Crisisplan Elektriciteit', Ministerie van Economische Zaken en Klimaat, februari 2022.
279 'Nationaal Crisisplan Elektriciteit', Ministerie van Economische Zaken en Klimaat, februari 2022.
280 'Nationaal Crisisplan Elektriciteit', Ministerie van Economische Zaken en Klimaat, februari 2022.
281 'Themarapportage bedreiging vitale infrastructuur', Analistennetwerk Nationale Veiligheid, 2022.
282 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2022.
283 'Themarapportage bedreiging vitale infrastructuur', Analistennetwerk Nationale Veiligheid, 2022.
284 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2022.
285 'Themarapportage bedreiging vitale infrastructuur', Analistennetwerk Nationale Veiligheid, 2022.
'Nederland in een fragmenterende wereldorde', WRR, 01-07-2024.
286 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024
287 'Nederland in een fragmenterende wereldorde', WRR, 01-07-2024.
288 'De staat van de digitale infrastructuur. De ruggengraat van onze digitale economie.', Ministerie van Economische Zaken en Klimaat, Januari 2024.
289 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024
290 'New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape', HCSS & TNO, mei 2024.
291 Invisible frontlines Safeguarding the European Energy Infrastructure, Danish Institute for International Studies, 2024.
292 'Hybride dreigingen en maatschappelijke weerbaarheid', Adviesraad Internationale Vraagstukken, 04-06-2024.
293 'DNB: burgers moeten beseffen dat financiële dienstverlening uit kan vallen', NRC,
21 oktober 2024.
294 'Cybersecuritybeeld Nederland 2023', NCTV, 3 juli 2023.
295 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
296 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
297 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024.
298 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
299 PM: NCTV AI publicatie
300 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
301 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
302 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
303 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
304 'Bereid je voor op de dreiging van quantum computers', AIVD, september 2021.
'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
305 'Bereid je voor op de dreiging van quantum computers', AIVD, september 2021.
'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
306 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024
307 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
308 De staat van de digitale infrastructuur. De ruggengraat van onze digitale economie.', Ministerie van Economische Zaken en Klimaat, Januari 2024.
309 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
310 'Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse', Analistennetwerk Nationale Veiligheid, 2024.
'Nederlandse hacker kon 4 miljoenzonnepaneelsystemen in 150 landen overnemen', Follow the Money, 12 augustus 2024.
311 'Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen', Rijksinspectie Digitale Infrastructuur, 23 mei 2023.
312 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
'Bouwen aan een toekomstbestendige arbeidsmarkt', McKinsey, juni 2024.
313 'Gematigde groei', **Staatscommissie Demografische Ontwikkelingen 2050, januari 2024.**
314 'Bouwen aan een toekomstbestendige arbeidsmarkt', McKinsey, juni 2024.
315 'Themarapportage bedreiging vitale infrastructuur', Analistennetwerk Nationale Veiligheid, 2022.
316 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 2022.
317 'CSR signaalbrief cybersecurity arbeidsmarkt', Cyber Security Raad, 4 juli 2024.
318 'Cybersecuritybeeld Nederland 2024', NCTV, 28 oktober 2024
319 'Gematigde groei', **Staatscommissie Demografische Ontwikkelingen 2050, januari 2024.**
320 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport', Analistennetwerk Nationale Veiligheid, 2024.
321 'Weerbaarheid in een gure wereld – Geopolitieke risico's en financiële instellingen', De Nederlandse Bank, november 2024.

Uitgave
Nationaal Coördinator
Terrorismebestrijding
en Veiligheid (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

Meer informatie
www.nctv.nl
info@nctv.minjenv.nl
@nctv_nl

Foto's
ANP

Juli 2025