CSR Cyber Security Raad

VERBINDING ONDER DRUK

De weerbaarheid van de (digitale) communicatie-infrastructuur in onveilige tijden

ADVIESRAPPORT

WEERBAARHEID

SAMENVATTING ADVIES

De digitale telecommunicatie- en internetinfrastructuur (hierna: de communicatie-infrastructuur) is de ruggengraat voor Nederland: burgers, overheid, kleine en grote bedrijven zijn hiervan afhankelijk. Uitval van delen van deze infrastructuur kan onze samenleving ontwrichten.

De Nederlandse communicatie-infrastructuur is van hoge kwaliteit en de sector functioneert goed, maar staat onder druk van de geopolitieke verhoudingen die de afgelopen jaren zijn veranderd. Kwaadwillende statelijke actoren hebben cyberoperaties tegen westerse landen geïntensiveerd, waarbij ook de communicatie-infrastructuur doelwit is. De weerbaarheid van de Nederlandse communicatie-infrastructuur moet daarom worden versterkt.

- **De Cyber Security Raad (hierna: de raad) heeft onderzoek verricht naar de communicatie-infrastructuur en vond vijf systeemrisico's (zie schema op volgende pagina).**
- **In dit advies doet de raad enkele dringende aanbevelingen aan het kabinet om deze risico's aan te pakken.**
- **Het advies is tot stand gekomen in nauwe samenwerking met experts uit de betrokken sectoren.**

SYSTEEMRISICO'S	AANBEVELINGEN
1 De geografische concentratie van internetexchange en datacenter-infrastructuur rond Amsterdam	Vergroot de geografische spreiding, decentralisatie en redundantie van infrastructuur
2 Wederzijdse ketenafhankelijkheid tussen energie- en communicatie-infrastructuur	Verbind de communicatie- en energiesector en stel gezamenlijk prioriteiten vast
3 Automatische uitwijk bij (langdurige) uitval	Zorg voor automatische uitwijk voor kritieke communicatie bij langdurige uitval
4 De beperkte capaciteit om langdurige stroomuitval op te vangen	Onderzoek waar noodstroomcapaciteit bij stroomuitval verbeterd kan worden en het herstelvermogen vergroot
5 Afhankelijkheid van delen van de communicatie-infrastructuur van een beperkt aantal leveranciers	Zet in op de strategische autonomie van vitale processen

AANLEIDING

ADVIES

De wereld is in hoog tempo onveiliger en onvoorspelbaarder geworden. Dit is aanleiding voor de raad om te onderzoeken waar de weerbaarheid van de Nederlandse communicatie-infrastructuur verbetering nodig heeft. De raad heeft het advies opgesteld in nauwe samenwerking met experts uit de communicatie- en internetsector. Het onderliggende onderzoek is uitgevoerd door TNO in opdracht van de raad.

Het onderzoek bestaat uit twee delen, met als centrale vraag:

> **Is de Nederlandse digitale communicatie-infrastructuur voldoende weerbaar[1] tegen doelbewuste, geopolitiek gedreven verstoring door een statelijke actor[2]?**

Het voorliggende advies komt voort uit het eerste deel van het onderzoek, en richt zich op de systemische weerbaarheid van de sector[3]. Hierbij ligt de focus op de beschikbaarheid en continuïteit van de communicatie-infrastructuur in tijden van grote dreiging. Een vervolgadvies over de veiligheid van de onderliggende technische protocollen die data- en spraakverkeer mogelijk maken - gebaseerd op het tweede deel van het onderzoek - volgt in de tweede helft van 2026.

Dit advies volgt de logische samenhang van belangen, dreigingen en de risico's die daaruit voortvloeien. Aan de hand van deze risico's zijn de aanbevelingen geformuleerd.

Het belang van de communicatie-infrastructuur voor Nederland

De digitale communicatie-infrastructuur is onmisbaar voor het dagelijks functioneren van de Nederlandse samenleving. Burgers zijn afhankelijk van deze infrastructuur voor bijvoorbeeld communicatie, toegang tot informatie en financiële en nooddiensten. Een grootschalige uitval of verstoring raakt direct het dagelijks leven van miljoenen mensen. Digitale communicatie is in het bijzonder cruciaal voor het functioneren van de samenleving in tijden van verhoogde spanning of crises.

Nederland heeft een vooraanstaande positie als digitale hub van Europa. Zo is de Amsterdam Internet Exchange (AMS-IX) een van de grootste ter wereld.

1 Weerbaarheid wordt omschreven als maatregelen op risico's die voortkomen uit de impact van dreigingen op te beschermen belangen.
2 En criminele samenwerkingsverbanden, die qua kennis, vaardigheden en vasthoudendheid vaak nauwelijks onderdoen voor statelijke actoren.
3 TNO 2025 R12358 - Weerbaarheid digitale communicatie-infrastructuur Nederland, Deel I: Globale verkenning (definitief), 9 januari 2026.

De communicatie-infrastructuur is daarmee een economische factor van belang en maakt Nederland aantrekkelijk voor internationale bedrijven, AI-fabrieken, dataopslag en wetenschappelijk onderzoek.

Het Nederlandse bedrijfsleven is verregaand gedigitaliseerd en zeer afhankelijk van data en connectiviteit voor het leveren van producten en diensten. Verstoring van de infrastructuur heeft direct grote economische schade tot gevolg.
De communicatie-infrastructuur is daarnaast nauw verweven met andere vitale sectoren. Zo zijn communicatienetwerken logischerwijs afhankelijk van energienetwerken, maar geldt met de opkomst van **smart grids** in toenemende mate ook het omgekeerde.

Uitval in de communicatie-infrastructuur heeft directe en ingrijpende gevolgen voor nagenoeg alle vitale sectoren.

Dreigingsbeeld

De AIVD constateert in zijn jaarverslag over 2025 dat Nederland de grootste veiligheidsdreiging in decennia ervaart. Kwaadwillende statelijke actoren hebben hun cyberoperaties tegen westerse landen geïntensiveerd [4], waarbij ook de communicatie-infrastructuur doelwit is.
De inlichtingen- en veiligheidsdiensten hebben in september 2025 het parlement gewaarschuwd dat hybride operaties een voortdurende dreiging vormen voor de Nederlandse samenleving. Deze operaties omvatten heimelijke beïnvloeding, spionage, cyberoperaties en pre-positionering voor sabotage. Beide diensten adviseren een actievere Nederlandse houding in deze hybride confrontatie.

Dreiging met name vanuit Rusland en China

Inlichtingendiensten waarschuwen al geruime tijd dat statelijke actoren - met name uit Rusland en China - op grote schaal opereren in westerse digitale infrastructuren. De aanvallen richten zich niet alleen op geopolitieke tegenstanders, maar ook op bondgenoten en neutrale partijen wanneer dat strategisch opportuun is.

De AIVD waarschuwt [5] dat Rusland zich voorbereidt op een langdurige confrontatie met westerse landen en kwalificeert bepaalde activiteiten als sabotage grenzend aan staatsterrorisme, bedoeld om angst te zaaien en maatschappelijke ontwrichting te veroorzaken. Ook de MIVD heeft concrete cyberoperaties door Russische statelijke actoren waargenomen tegen Nederlandse vitale infrastructuur [6], mogelijk als voorbereiding op sabotage. China vormt de grootste dreiging voor de Nederlandse economische veiligheid: een dreiging die zich uit in spionageactiviteiten, cyberaanvallen en heimelijke verwerving van technologie en kennis.[7]

Het aantal landen dat offensieve cybercapaciteiten ontwikkelt is de afgelopen jaren sterk gegroeid, de zogenaamde proliferatie van geavanceerde cybercapaciteiten.[8] Te verwachten valt dat het offensieve gebruik van AI de groei van het aantal staten (en andere actoren) met geavanceerde cybercapaciteiten verder zal aanjagen.

4 Sommige criminele netwerken beschikken inmiddels over vergaande capaciteiten om zelf inlichtingenonderzoek te doen. Dit betekent dat zware criminele samenwerkingsverbanden methoden gebruiken die voorheen vooral aan staten of inlichtingendiensten werden toegeschreven. Criminele en statelijke actoren zijn hiermee ook in toenemende mate moeilijker te onderscheiden.
5 AIVD Jaarverslag 2025
6 MIVD Jaarverslag 2024
7 AIVD Jaarverslag 2025
8 AIVD Jaarverslag 2024

SABOTAGE

De aanval op Kyivstar (2023)

In 2023 werd Kyivstar, de grootste mobiele netwerk operator in Oekraïne, getroffen door een grootschalige cyberaanval die tot een dagenlange landelijke verstoring van mobiele spraak- en datadiensten leidde. De aanval zou zijn uitgevoerd door een aan Rusland gelieerde hackergroep die zich al maanden eerder in het netwerk van Kyivstar had genesteld. De effecten waren destructief: naar verluid zijn duizenden virtuele servers gewist en had meer dan de helft van de Oekraïense bevolking geruime tijd geen toegang tot mobiele communicatiediensten.

De aanval had ook bredere maatschappelijke effecten, waaronder een verstoring van luchtalarmsystemen, financiële diensten en het openbaar vervoer. De aanval op Kyivstar is een evidente manifestatie van hybride oorlogsvoering en onderstreept de mate waarin vitale infrastructuur een doelwit kan zijn bij geopolitieke geschillen.

PRE-POSITIONERING

De Volt Typhoon-campagne (2021)

De Chinese statelijke actor Volt Typhoon compromitteert sinds 2021 IT-systemen in de Amerikaanse vitale infrastructuren. Het meest aannemelijke doel van deze groep is zich te pre-positioneren voor ontwrichtende of destructieve cyber-aanvallen in het geval van een conflict met de Verenigde Staten. De activiteit is in 2023 ontdekt maar de groep was daarvoor al lange tijd sluimerend in verscheidene vitale infra-structuren (digitale communicatie, maar bijvoorbeeld ook energie, transport en water) aanwezig.

Opvallend is dat Volt Typhoon zich vaak toegang wist te verschaffen door kwetsbaarheden in verouderde of slecht onderhouden apparatuur en zeer effectief was in het ontwijken van detectie-oplossingen. Voor zover bekend heeft de Volt Typhoon-campagne nog niet tot daadwerkelijke verstoring van digitale communicatie-infrastructuur (of andere vitale dienstverlening) geleid, maar de mate waarin deze actor heeft geïnvesteerd in voorbereidende handelingen voor een eventuele ontwrichtende aanval is tamelijk uniek.

Bevindingen en risico's

Stevige basis, nieuwe risico's

Nederland heeft een goed ontwikkeld digitaal communicatielandschap. De Nederlandse internetknooppunten behoren tot de grootste in de wereld, de Nederlandse mobiele netwerken presteren zeer goed in internationale benchmarks en in alle dienstdomeinen is sprake van een competitieve markt met voldoende aanbieders. Het laatste biedt afnemers de mogelijkheid om diensten bij verschillende aanbieders te kopen en daarmee minder gevoelig te zijn voor individuele uitval of verstoring.

Tegelijkertijd is de wereld in hoog tempo onvoorspelbaarder en gevaarlijker geworden. Veel partijen zijn zich bewust van deze veranderende dreiging en hebben daarop een solide fundament aan weerbaarheidsvoorzieningen getroffen. Tegelijkertijd maakt de inherente complexiteit van omvangrijke en gemengde technologieomgevingen het terugdringen van kwetsbaarheden tot een permanent aandachtspunt, zeker in het licht van het verhoogde dreigingsniveau.

De raad signaleert **vijf systeemrisico's** in de communicatie-infrastructuur waar overheid en sector kunnen optreden om de robuustheid naar het voor deze tijd noodzakelijke niveau te brengen.

1 GEOGRAFISCHE CONCENTRATIE

Internetexchanges en datacenters zijn geconcentreerd in de regio Amsterdam. Dit komt voort uit de sterke concentratie van fysieke bekabeling voor **long haul** routes[9] in deze regio en de **low latency** vereisten van bedrijven in de Randstad die kritieke business functies in externe datacenters onderbrengen. De concentratie is historisch te verklaren vanuit efficiency, maar staat haaks op het gangbare ontwerpprincipe om tussen redundante datacenters van één partij voldoende geografische afstand te waarborgen. Deze principes zijn bijvoorbeeld wel toegepast door de aanbieders van vaste en mobiele datadiensten, die hun belangrijkste datacenters geografisch over Nederland hebben gespreid. Door dit gebrek aan geografische spreiding van grote internetexchanges en datacenters, kunnen regionale incidenten, zoals door moedwillige sabotage, nationaal ontwrichtend uitwerken.

2 KETENAFHANKELIJKHEID TUSSEN DE ENERGIE- EN COMMUNICATIE-INFRASTRUCTUUR

De communicatie-infrastructuur is direct afhankelijk van de energiesector. Verstoringen in de stroomvoorziening hebben onmiddellijke gevolgen voor communicatiediensten. Omgekeerd is de energie-infrastructuur in hoge mate afhankelijk van de communicatie-infrastructuur, bijvoorbeeld bij het aansturen van omvormers, laadpalen, thuisbatterijen, klimaatsystemen en energiemanagement op het net. Beide vitale sectoren zijn het centrale zenuwstelsel van de Nederlandse economie en samenleving, daarom is meer onderlinge samenwerking wenselijk.

3 GEEN AUTOMATISCHE UITWIJK

Nederland kent geen formele regeling voor het onderling overnemen van gebruikers van dienst- of infrastructuurdomeinen naar een andere aanbieder indien zich langdurige uitval zou voordoen. Voor mobiele communicatie kan nationale of **disaster roaming** de veerkracht van data- en telefoniediensten verbeteren voor kritieke gebruikers. Wel is 112 altijd bereikbaar via het netwerk van een andere aanbieder.

9 Dit betreft (trans-Atlantische) zeekabels.

4 BEPERKTE CAPACITEIT OM STROOMUITVAL OP TE VANGEN

Basisstations - zoals voor mobiele communicatie - beschikken over batterijcapaciteit in het geval van een stroomuitval. Dankzij deze noodstroom kan veelal gedurende een periode van een aantal uren communicatie blijven plaatsvinden. Bij langere stroomuitval valt de mobiele en andere communicatiedienstverlening weg, terwijl communicatie juist op deze momenten cruciaal is.

5 AFHANKELIJKHEID KRITIEKE PARTIJEN

De Nederlandse connectiviteit, van met name internetexchanges, resolving & registration partijen en aanbieders van satellietdiensten, is vaak afhankelijk van datacenterdiensten van derde partijen met een buitenlandse eigenaar. In de huidige onrustige wereld kan Nederland via deze afhankelijkheden kwetsbaar zijn, bijvoorbeeld door nevenschade bij sabotage gericht op een ander land, handelsblokkades of het anderszins plotseling stoppen van dienstverlening. Sommige aanbieders mitigeren deze afhankelijkheid door infrastructuur van meerdere aanbieders af te nemen of maken gebruik van zowel cloud als on-premises oplossingen.

LESSEN

Lessen uit Oekraïne

De Oekraïense samenleving en vitale infrastructuur, waaronder ook de communicatie-infrastructuur, is verrassend weerbaar gebleken tegen de niet aflatende kinetische en digitale aanvallen vanuit Rusland. Uit vier jaar oorlog zijn veel lessen te leren voor de Nederlandse communicatie-infrastructuur. Efficiëntie en centralisatie, zowel geografisch als qua netwerkarchitectuur, zijn een kwetsbaarheid gebleken. De Oekraïners hebben daarop in snel tempo hun netwerk gedecentraliseerd en redundant gemaakt.

Ook hebben de aanbieders in de communicatie-infrastructuur zich in een vroeg stadium gerealiseerd dat zij niet moeten concurreren op beschikbaarheid en veiligheid. Samen voelen zij de verantwoordelijkheid om het land verbonden te houden. Ook ligt er een sterke focus op snel herstel bij de uitval van stroom en voldoende noodstroomcapaciteit om de uitval van stroom voor langere periodes op te vangen. De belangrijkste lessen vanuit Oekraïne hebben hun weg gevonden naar dit advies van de CSR.

Aanbevelingen

1 VERGROOT DE GEOGRAFISCHE SPREIDING, DECENTRALISATIE EN REDUNDANTIE VAN INFRASTRUCTUUR

De raad adviseert het kabinet om geografische spreiding van peering- en transitcapaciteit[10] actief te stimuleren. Door exchanges en datacenters geografisch te verspreiden en extra netwerkroutes aan te leggen, wordt de robuustheid van de Nederlandse communicatie-infrastructuur verhoogd. Verkeer kan zo bij een storing of aanval automatisch worden omgeleid via andere knooppunten. Tevens adviseert de raad om decentralisatie en redundantie in de gehele communicatie-infrastructuur te versterken, zowel fysiek als logisch.[11] Netwerken met een dichte, onderling verbonden structuur en diverse routeringspaden zijn significant beter bestand tegen sabotage. Hersteltijden van verbindingen na een incident zijn in gedecentraliseerde en gedistribueerde netwerken, zoals het internet, aanzienlijk korter dan in gecentraliseerde architecturen.

2 VERBIND TELECOM- EN ENERGIESECTOR EN STEL GEZAMENLIJK PRIORITEITEN VAST

De raad adviseert het kabinet om een aanpak te ontwikkelen specifiek gericht op de interactie tussen beide sectoren om de kans op en impact van cascadeverstoringen te verkleinen. Dit moet leiden tot afgestemde investeringsplannen in weerbaarheid, aansluitingen en ketenafhankelijkheden, afspraken over prioriteitsherstel, periodieke crisisoefeningen en het beter verbinden van crisisstructuren.

3 ZORG VOOR AUTOMATISCHE UITWIJK VOOR KRITIEKE COMMUNICATIE BIJ LANGDURIGE UITVAL

De raad adviseert het kabinet om zorg te dragen dat, op basis van een verkenning naar roamingmogelijkheden, afspraken tussen aanbieders worden gemaakt, met name gericht op kritieke gebruikers. Daarnaast adviseert de raad het kabinet om aanbieders binnen de vitale infrastructuur te stimuleren tot het gebruik van satellietcommunicatie als back-up. Op die manier is de beschikbaarheid van een kritieke terugvaloptie beter geborgd.

4 VERBETER HET HERSTELVERMOGEN EN DE NOODSTROOMCAPACITEIT BIJ STROOMUITVAL

Hoe sneller schade aan energie-infrastructuur wordt hersteld, hoe kleiner de vervolgschade. De raad adviseert het kabinet daarom ook om dit herstelvermogen van de energie-infrastructuur te vergroten. Daarnaast adviseert de raad het kabinet om samen met de sector een plan te ontwikkelen voor de vergroting van noodstroomcapaciteit op kritieke punten.

5 ZET IN OP DE STRATEGISCHE AUTONOMIE VAN VITALE PROCESSEN

De raad adviseert het kabinet om in lijn met Europese initiatieven[12], zoals de richtlijnen voor strategische autonomie en de Cyberbeveiligingswet, diversificatie in de markt en de leveranciersketen aan te jagen waar de afhankelijkheid van een enkele partij onevenredige veiligheidsrisico's met zich meebrengt. Daarnaast adviseert de raad vitale data en kernnetwerkfuncties zoveel mogelijk binnen de Nederlandse of Europese jurisdictie te borgen.

10 Peering is het uitwisselen van (gratis) verkeer tussen aanbieders, transit is overig verkeer dat naar netwerken gaat waar geen directe verbinding mee is.
11 Logisch betekent hoe data, functies of verbindingen door software worden ingedeeld en geïnterpreteerd.
12 Waaronder het European Tech Sovereignty Package, een set van maatregelen van de Europese Commissie ter versterking van Europa's capaciteiten voor semiconductors, AI Cloud en open source.

CSR Cyber Security Raad

AVIESRAPPORT

WEERBAARHEID

VERBINDING ONDER DRUK

De weerbaarheid van de (digitale) communicatie-infrastructuur in onveilige tijden

Cyber Security Raad
Korte Voorhout 7
2511 CW Den Haag
TEL 070 - 7515 333
E-MAIL info@cybersecurityraad.nl
WWW cybersecurityraad.nl

Postadres
Postbus 20011
2500 EA Den Haag