Position paper NLconnect

Herziening van de Europese Cybersecurity Act (CSA2) potentieel contraproductief voor investeringen in telecomnetwerken en voor de weerbaarheid van Europa

NLconnect vertegenwoordigt de Nederlandse telecom-, breedband- en glasvezelindustrie. Samen werken onze 90 leden aan een Nederland waarin vaste en mobiele connectiviteit veilig, duurzaam en van wereldklasse is. Connectiviteit is de vitale digitale ruggengraat waarop de Nederlandse samenleving en economie draaien.

Nederland behoort internationaal tot de wereldtop op het gebied van digitale connectiviteit, dankzij toonaangevende 5G-, glasvezel- en kabelnetwerken. Deze netwerken vormen het fundament van de bredere digitale sector en zijn onmisbaar voor productiviteit, energietransitie en maatschappelijke veerkracht.

In een wereld van geopolitieke spanningen, cyberdreigingen en andere veiligheidsuitdagingen is het van cruciaal belang dat onze digitale infrastructuur robuust en weerbaar is. Het versterken van cyberweerbaarheid – het doel van de voorgestelde herziening van de Cybersecurity Act (CSA2) – is daarom een legitieme en noodzakelijke ambitie. Onderdelen van de CSA2, zoals de certificeringsprocedure voor de leveranciersketen dragen in positieve zin bij aan dit doel.

NLconnect constateert dat de voorgestelde herziening ook elementen bevat die moeten worden heroverwogen. In de huidige vorm mist het voorstel een basis voor het uitvoeren van een risicobeoordeling van leveranciers voor de ICT-toeleveringsketen voor vaste en mobiele telecomnetwerken. Dit leidt tot disproportionele maatregelen en is potentieel contraproductief voor investeringen in onze netwerken, voor de veiligheid en de continuïteit van telecomnetwerken en voor de weerbaarheid van Europa.

1. Ook vaste netwerken komen in scope

De voorgestelde bepalingen zijn niet beperkt tot mobiele (5G) netwerken. Ook vaste netwerken expliciet vallen binnen de CSA2. Dit betreft toegangsnetwerken (FTTH, kabel), transportnetwerken en transmissie-infrastructuur. Daarmee wordt de reikwijdte van de voorgestelde maatregelen aanzienlijk breder dan de oorspronkelijke vrijwillige 5G-toolbox-benadering voor mobiele netwerken en de recente vrijwillige ICT supply chain toolbox voor vaste netwerken.

Voor vaste netwerken is tot op heden geen gecoördineerde, sectorbrede risico- en impactanalyse uitgevoerd waarin operators en technische experts zijn betrokken.
De voorgestelde uitbreiding betekent dat apparatuur in delen van het netwerk met een laag risicoprofiel eveneens onder generieke vervangingsverplichtingen kan vallen.
Dit staat niet in verhouding tot het risicoprofiel van afzonderlijke componenten en leidt tot onwenselijke economische en operationele gevolgen.

2. **Gebrek aan een risicogebaseerde en proportionele aanpak**
De CSA2 introduceert een vergaand instrumentarium om niet-technische risico's in ICT-toeleveringsketens te adresseren. Het voorstel borgt onvoldoende dat maatregelen proportioneel worden toegepast op basis van concrete risico's en de beoordeling daarvan.

Niet elk netwerkonderdeel, elke functie of elke inzet van producten of diensten van een leverancier kent hetzelfde risicoprofiel. Een generieke uitsluiting van producten of diensten van een leverancier, los van context, gebruik en risicobeperkende maatregelen, kan leiden tot onevenredige economische schade zonder aantoonbare veiligheidswinst.

Wij pleiten voor een duidelijk onderscheid tussen kern- en randfuncties, erkenning van bestaande technische en organisatorische risicobeperkende maatregelen en ruimte voor maatwerk op basis van aantoonbare risicoanalyses.

3. Generieke uitsluitingen leiden tot investeringsonzekerheid
Zoals vermeld kondigt de CSA2 voor de telecomsector generieke uitsluitingen van producten en diensten van leveranciers ('blanket bans') aan, zonder dat daar een kenbare risicobeoordeling aan vooraf is gegaan. De CSA2 geeft de Europese Commissie (naast de lidstaten) een ruime bevoegdheid om verboden op te leggen voor het gebruik van producten en diensten van leveranciers.

De komende jaren zijn substantiële investeringen vanuit onze industrie nodig, onder meer in de versterking van de digitale weerbaarheid van netwerken, maar ook in verduurzaming, capaciteitsverbeteringen en nieuwe technologieën zoals 5G-stand-alone, nieuw spectrum en de voorbereiding op 6G, de nieuwe generatie mobiele netwerken die thans in ontwikkeling is. De gevolgen van de voorgestelde maatregelen

zullen aanzienlijk zijn. Juist in een sector die afhankelijk is van langetermijninvesteringen leidt niet alleen een verbod op het gebruik van producten en diensten van bepaalde leveranciers, maar ook de dreiging ervan tot disproportionele (investerings-) onzekerheid en afnemende investeringsbereidheid (*chilling effect*).

4. Strijdigheid met Nederlandse Visie Digitale autonomie en soevereiniteit: negatieve effecten op waardeketen en weerbaarheid

De recente Nederlandse Visie Digitale autonomie en soevereiniteit (december 2025) formuleert drie kernambities: (i) het verminderen van afhankelijkheden van specifieke leveranciers, (ii) voorkomen van single-vendor lock-in, en (iii) het bevorderen van een open, divers en innovatief ecosysteem.

De CSA2 werkt deze ambities niet in de hand, maar juist tegen. Door het generieke verbodsmodel worden de afhankelijkheden niet verminderd. Het verbodsmodel verkleint het aantal beschikbare leveranciers. Dit leidt juist tot toenemende afhankelijkheden van een beperkt aantal (meestal westerse) leveranciers.
Een versmalling van het leverancierslandschap kan op middellange termijn niet alleen leiden tot verminderde concurrentie (lock-ins, supply risico's en prijsopdrijvende effecten), maar ook tot een groter risico voor de continuïteit en weerbaarheid door (te) grote afhankelijkheid in heel Europa van slechts enkele leveranciers. Minder keuze betekent een grote kwetsbaarheid. Dit ondermijnt de strategische veerkracht die Nederland expliciet nastreeft.[1] (Dreigende) blanket bans kunnen daarbij ook tegenmaatregelen oproepen in andere landen, die bijvoorbeeld Europese leveranciers van hun markt kunnen weren.[2] Het kabinet benadrukt in de Visie daarom terecht dat het categorisch uitsluiten van bepaalde dienstverleners niet past binnen het landenneutrale kabinetsbeleid. De overheid wil juist technologische innovatie stimuleren die bijdraagt aan digitale autonomie en soevereiniteit, en daarbij optimaal gebruikmaken van de innovatiecapaciteit van marktpartijen.[3]

Een algeheel verbod op het gebruik van producten of diensten van een leverancier zou alleen in het uiterste geval mogelijk moeten zijn, als ultimum remedium, indien na een

[1] Visie Digitale autonomie en soevereiniteit, p. 7.
[2] Ter illustratie: recentelijk voerde de VS een algemeen verbod in op import of verkoop van consumentenrouters die niet in dat land zijn gefabriceerd, zie: https://www.bbc.com/news/articles/c74787w149zo
[3] Visie Digitale autonomie en soevereiniteit, p. 9, 12.

uitgebreide risicobeoordeling blijkt dat andere, minder vergaande maatregelen niet mogelijk zijn. Een kernprincipe van netwerkveiligheid en -veerkracht is het gebruik van producten en diensten van meerdere leveranciers. Hierdoor kunnen telecomaanbieders risico's spreiden, lock-in vermijden en sneller inspelen op technische kwetsbaarheden of leveringsproblemen. Indien het aantal toegestane leveranciers structureel wordt beperkt tot een zeer kleine groep, ontstaat juist een nieuwe strategische afhankelijkheid, ditmaal van een beperkt aantal "geautoriseerde" leveranciers.
Dit vergroot de impact van verstoringen, verzwakt de onderhandelingspositie van operators en kan innovatie in de keten afremmen.

Wij benadrukken dat strategische autonomie niet gelijkstaat aan concentratie, maar juist aan een gediversifieerd, concurrerend en transparant leveranciers landschap binnen duidelijke veiligheidskaders. Een beleid dat de facto leidt tot netwerken met producten en diensten van één of een beperkt aantal leveranciers staat haaks op dit uitgangspunt.

5. **Continuïteit van essentiële diensten vereist gefaseerde en flexibele overgangen**
Telecommunicatienetwerken vormen de ruggengraat van de digitale samenleving en zijn essentieel voor openbare veiligheid, economische continuïteit en crisisrespons. Wij achten het daarom van cruciaal belang dat de CSA2 expliciet waarborgen bevat voor de continuïteit van essentiële diensten.

Verplichte en strak getimede uitfasering van bestaande netwerkcomponenten, zonder voldoende ruimte voor gefaseerde migraties, verhoogt het risico op storingen, capaciteitsproblemen en operationele fouten. Dit geldt temeer wanneer meerdere lidstaten gelijktijdig vergelijkbare migraties moeten uitvoeren, wat leidt tot schaarste aan materieel, expertise en implementatiecapaciteit.

Wij pleiten daarom voor flexibele tijdschema's, afgestemd op de essentiële functie van het netwerkonderdeel, de daadwerkelijke risicobeoordeling van het betreffende gebruik, de technische levenscyclus van assets en de beschikbaarheid van veilige en alternatieve producten en diensten die onderling kunnen communiceren.

Zonder deze flexibiliteit dreigt de CSA2 het tegenovergestelde te bereiken van wat wordt beoogd: minder in plaats van meer operationele veerkracht.

Gebrek aan transparantie en voorspelbaarheid
In de CSA2 worden cruciale keuzes uitgesteld naar latere uitvoeringshandelingen, zonder betrokkenheid van de lidstaten en de markt. Dit betreft onder meer de aanwijzing van hoogrisicolanden en leveranciers, de afbakening van sleuteltechnologieën, producten en diensten en de concrete risicobeperkende- en verbodsmaatregelen.

Deze onzekerheid creëert aanzienlijke investeringsrisico's voor telecomaanbieders. Grote infrastructuurinvesteringen kennen lange afschrijvingsperioden en vereisen voorspelbare regelgeving.

NLconnect roept daarom op tot vroegtijdige consultatie van marktpartijen, duidelijke criteria en procedures voor aanwijzing van hoogrisicoleveranciers en toereikende overgangstermijnen na transparante besluitvorming.

6. Uitvoerbaarheid en compensatie voor vervanging
Eventuele maatregelen dienen op landenniveau plaats te vinden. Nederland heeft in eerdere beleidskaders gekozen voor een risicogebaseerde en casus-specifieke aanpak, waarbij risico's zijn beperkt via netwerksegmentatie, aanvullende technische maatregelen en gerichte beperkingen waar dat door de wetgever noodzakelijk werd geacht (Bvit en Rvit). Een generieke Europese verplichting tot versnelde vervanging zou ook onderdelen treffen waarvoor risico's reeds adequaat zijn geadresseerd, mede door toepassing van andere regelgeving.

De kosten voor verplichte vervanging van apparatuur kunnen voor telecomaanbieders oplopen tot tientallen miljarden euro's. Zonder voldoende alternatief aanbod, compensatie uit publieke middelen of voldoende ruime overgangstermijnen zal dit leiden tot uitstel of bevriezing van netwerkupgrades, vertraging van capaciteitsexpansies, hogere kapitaalkosten en uiteindelijk stijgende consumentenprijzen.

Dit effect wordt versterkt doordat telecomaanbieders strenger lijken te worden behandeld dan andere vitale sectoren. Waar in andere sectoren risicobeperkende maatregelen proportioneel kunnen worden toegepast en sancties lager uitvallen, geldt

voor telecom een verplichte vervanging met aanzienlijk zwaardere sancties. Een dergelijke ongelijke benadering ondermijnt het gelijke speelveld.

7. **Operationeel risico door gelijktijdige EU-brede migraties**

De voornoemde maatregelen die op basis van de CSA2 kunnen worden opgelegd kunnen ertoe leiden dat in meerdere lidstaten gelijktijdig grootschalige netwerkvervangingen moeten plaatsvinden. Dit vergroot het systemische risico voor de Europese telecommunicatie-infrastructuur als geheel.

Een dergelijke “migratiepiek” kan immers leiden tot tekorten aan gekwalificeerd personeel, leveringsproblemen bij alternatieve leveranciers en een verhoogde kans op implementatiefouten.

Wij benadrukken dat gespreide implementatie en nationale flexibiliteit noodzakelijk zijn om deze risico’s te mitigeren en de stabiliteit van Europese netwerken te waarborgen.

Tot slot

Een goed functionerende interne markt vereist harmonisatie die bijdraagt aan rechtszekerheid en voorspelbaarheid. Tegelijkertijd moet worden voorkomen dat nieuwe verplichtingen leiden tot stapeling van regels bovenop bestaande kaders, zoals onlangs in de Kamer besproken Cyberbeveiligingswet en Europese cyberbeveiligingsinstrumenten.

Nationale veiligheid is primair een bevoegdheid van lidstaten. Nederland heeft reeds een risicogebaseerd 5G-beleid ingevoerd waarin veiligheidsrisico’s worden geadresseerd via gerichte maatregelen. Een vergaande centralisering op EU-niveau die bestaande nationale afspraken doorkruist, is strijdig met het Europees verdragsrecht en ondermijnt investeringsvoorspelbaarheid.

NLconnect onderschrijft de ambitie om de cyberweerbaarheid van Europa te versterken, en roept het kabinet op zich in te zetten voor een strikt risicogebaseerde, technisch onderbouwde en proportionele benadering en toezicht die door Nederland zelf kan worden uitgevoerd. Zonder die balans dreigt het voorstel de digitale weerbaarheid te verzwakken.

De bijlage bevat enige suggesties voor inbreng vanuit de Kamer naar aanleiding van het BNC-fiche.

Den Haag, 27 maart 2026

Mathieu Andriessen, directeur