Kapteynstraat 1, SBIC - Building suite 220 / 2201 BB Noordwijk

info@cyberveilignederland.nl
www.cyberveilignederland.nl

KvK 71802525

Commissie Digitale Zaken

Noordwijk, 17 september 2025
Ref.: PA902-250917

Betreft: Schriftelijke inbreng Cyberveilig Nederland over de Nationale Digitaliseringsstrategie

Geacht lid van de commissie Digitale Zaken,

Geopolitieke spanningen, technologische innovaties en steeds geavanceerdere cyberdreigingen maken dat stilstand geen optie is. Daar komt bij dat enkele grote internationale technologiebedrijven inmiddels zó dominant zijn dat Nederland, ook als overheid, in een ongezonde afhankelijkheidsrelatie dreigt te belanden[1]. Digitale soevereiniteit en weerbaarheid zijn daarom geen luxe, maar een randvoorwaarde voor onze nationale veiligheid en maatschappelijke stabiliteit. In de Nederlandse Digitaliseringsstrategie (NDS wordt dit probleem dan ook grotendeels geadresseerd.

Nationale Digitaliseringsstrategie (NDS)
De NDS onderstreept het belang van digitale autonomie en weerbaarheid en benoemt dit terecht als één van de nationale prioriteiten. Daarbij wordt expliciet gewezen op de risico's van strategische afhankelijkheden. Cyberveilig Nederland onderschrijft deze analyse volledig[2]. Nu verkiezingen en kabinetsformatie naderen, is dit hét moment om een structurele koerswijziging in te zetten – financieel, bestuurlijk en beleidsmatig – en daadwerkelijk met mensen en middelen te investeren in digitale soevereiniteit en cyberweerbaarheid[3].

Toenemende risico's door afhankelijkheden
Nederland is te sterk afhankelijk van niet-Europese technologie. Deze situatie beperkt onze regie en maakt ons kwetsbaar.

De risico's zijn veelzijdig:

- Geopolitieke druk: buitenlandse staten of bedrijven kunnen via uitsluiting of uitval de beschikbaarheid van diensten en vitale processen inzetten als drukmiddel of zelfs als wapen[4].

[1] Zakelijke gebruikers van IT veroordelen marktgedrag van Broadcom - CIO Platform Nederland
Input cyberveilig nederland aan rondetafelgesprek over digitale soevereiniteit bij de rijksoverheid. - Cyberveilig Nederland
[3] Position paper: tijd voor daadkracht in cyberveiligheid - Cyberveilig Nederland
[4] Kamer wil opheldering over afsluiten e-mail hoofdaanklager ICC door Microsoft - Security.NL

- Complianceproblemen: doordat toezicht, auditing en naleving afhankelijk zijn van buitenlandse diensten en producten, ontstaat het risico dat Nederland niet kan voldoen aan zijn eigen normen.
- Ongewenste toegang tot data: buitenlandse partijen kunnen gevoelige gegevens inzien of de toegang daartoe beperken, manipuleren of stopzetten.
- Technologische achterstand: zonder strategische investeringen lopen we achter bij doorbraken in AI, quantumtechnologie en encryptie. Technologie die onze toekomst gaat bepalen.

Dit alles ondermijnt een van de kerntaken van de overheid: het beschermen van burgers, economie en de democratische rechtsorde.

Specifieke kwetsbaarheden

De grootste kwetsbaarheid ligt momenteel bij de dominantie van enkele, voornamelijk Amerikaanse, cloud- en softwareleveranciers (hyperscalers). Hun lock-in-effecten maken overstappen duur, complex en soms praktisch onmogelijk. Ook de afhankelijkheid van leveranciers van chips en netwerkapparatuur vormt een structureel risico. Het gevolg is dat de Europese en Nederlandse markt voor alternatieven onderontwikkeld blijft zolang hier niet structureel in wordt geïnvesteerd.

Daarbovenop ontbreekt nog vaak gecoördineerd inzicht in waar de “te beschermen belangen” precies liggen. Zowel binnen afzonderlijke (rijks)organisaties als in de bredere maatschappelijke afhankelijkheden ontbreekt overzicht. Zonder dit inzicht kan de impact van uitval of manipulatie van cruciale technologieën onvoldoende worden ingeschat.

Ten slotte speelt ook het tekort aan cyberspecialisten een cruciale rol. Dit tekort vergroot de afhankelijkheid van externe leveranciers en leidt tot risico’s op drie vlakken:

- Datatoegang: externe experts krijgen diepgaande toegangsrechten tot systemen en gevoelige informatie.
- Dienstcontinuïteit: bij beëindiging van contracten of faillissementen kunnen vitale diensten plotseling wegvallen.
- Compliancy: buitenlandse leveranciers voldoen niet altijd aan Europese of nationale normen.

Potentieel van de Nederlandse cybersecuritysector

De Nederlandse cybersecurity sector is voornamelijk een dienstensector. Ten behoeve van de ondersteuning van deze dienstverlening zijn Europese alternatieven beschikbaar, maar die zijn soms minder gebruiksvriendelijk of duurder. Met gerichte stimulering en een duidelijke koppeling aan strategische investeringen – bijvoorbeeld door de NAVO-norm te verhogen – zien we hierop volop kansen voor de Nederlandse sector. We staan immers al internationaal hoog aangeschreven op het gebied van cryptografie en innovatieve softwareontwikkeling.

De rol van de overheid: autonomie in de inkoopstrategie

Digitale soevereiniteit moet structureel onderdeel worden van de risicobeoordeling bij aanbestedingen van het Rijk. Alleen zo voorkomen we dat korte termijn kostenbesparingen leiden tot langdurige afhankelijkheden. Door zelf op te treden als launching customer kan de overheid veilige, interoperabele en Europese alternatieven stimuleren. Dit vergroot de regie over kritieke processen en data, en versterkt onze weerbaarheid tegen geopolitieke druk.

Een betere inkoopstrategie is hierbij noodzakelijk. Concreet betekent dit dat in aanbestedingen eisen moeten worden opgenomen over:

- continuïteitsclausules;
- expliciete afspraken over dataportabiliteit;
- waarborgen voor leveringszekerheid.

Zo wordt voorkomen dat Nederland afhankelijk blijft van één leverancier of van niet-Europese partijen. Nieuwe wetten en regels zoals de ABRO, de Cyberbeveiligingswet en de Cyber Resilience Act kunnen hierbij ondersteunend werken, mits deze ook in de uitvoering consequent worden toegepast.

Conclusie: regie en daadkracht noodzakelijk

De kern van het probleem is dat het binnen de Nederlandse (Rijks)overheid ontbreekt aan regie en daadkracht, daarom adviseren wij vanuit CVNL om:

1. Grip te krijgen op bestaande afhankelijkheden van buitenlandse grootmachten;
2. Te investeren in strategische technologieën zoals encryptie, quantumtechnologie en kunstmatige intelligentie;
3. Te leren van Europese bondgenoten[5] en gezamenlijk alternatieven ontwikkelen;
4. Proactief overheidsbeleid te voeren in samenwerking met de markt, gericht op soevereiniteit en weerbaarheid.

Zonder deze koers dreigen we dezelfde fouten te maken als bij de te late overstap naar de cloud: te afhankelijk, te weinig soeverein, en onvoldoende voorbereid op geopolitieke risico's.

Cyberveilig Nederland staat klaar om, samen met de overheid en de markt, de noodzakelijke stappen te zetten. Nu is het moment om de digitale weerbaarheid en autonomie van Nederland structureel te verankeren.

[5] Deens Ministerie van Digitalisering maakt overstap naar Linux en LibreOffice – HCC