Duiding van het coalitieakkoord 2026–2030 voor de leden van Cyberveilig Nederland

Het nieuwe coalitieakkoord van D66, VVD en CDA bevat een reeks maatregelen die direct of indirect impact hebben op de digitale veiligheid van Nederland. Hoewel cybersecurity niet als afzonderlijk thema is uitgewerkt, raken verschillende passages aan onze sector: van de oprichting van een Nederlandse Digitale Dienst tot investeringen in defensieve en offensieve cybercapaciteiten, de vereenvoudiging van de AVG, de implementatie van de Cyberbeveiligingswet en de ambitie om Nederland koploper te maken in een digitale wereld.

Voor Cyberveilig Nederland is het belangrijk om te begrijpen waar kansen ontstaan, waar risico's liggen en op welke punten wij als sector een rol kunnen en moeten spelen. In de onderstaande analyse duiden we de belangrijkste onderdelen van het akkoord, koppelen we deze aan onze speerpunten en schetsen we de haakjes voor verdere gesprekken met overheid en politiek.

1. Feitelijke analyse van de digitale en cybersecurity-relevante onderdelen

Digitale governance en de oprichting van de Nederlandse Digitale Dienst

Het coalitieakkoord introduceert een *Nederlandse Digitale Dienst (NDD)* die rijksbreed verantwoordelijk wordt voor digitalisering, kwaliteitsstandaarden en ontwerpkeuzes. Er komt géén minister of staatssecretaris voor Digitale Zaken. De departementale verantwoordelijkheden blijven ongewijzigd.

Dit betekent dat:

- de bestaande versnippering van cybersecurity-taken (NCSC, NCTV, politie, Defensie, vakdepartementen) grotendeels blijft bestaan;
- de NDD vooral een coördinerende en ondersteunende rol krijgt, zonder dat het stelsel fundamenteel wordt herzien;
- digitalisering binnen de rijksoverheid wel centraler wordt georganiseerd, maar cybersecurity als stelselvraagstuk niet wordt opgelost.

AVG-vereenvoudiging en relatie tot de Cyberbeveiligingswet

Het akkoord spreekt over vereenvoudiging van de AVG op Europees niveau en verbetering van de toepassing van de AVG in Nederland.

Tegelijkertijd staat Nederland aan de vooravond van implementatie van de Cyberbeveiligingswet (NIS2). De combinatie van “vereenvoudiging” en “verzwaring” van verplichtingen kan tot verwarring leiden bij organisaties. Harmonisatie van toezicht en definities wordt daarmee belangrijker.

Investeringen in Defensie en opsporing

De coalitie investeert in:

- offensieve en defensieve cybercapaciteiten bij Defensie;
- uitbreiding van cyberrecherche;
- digitalisering van het OM duurzaam op orde.

Er worden echter geen aanvullende investeringen aangekondigd voor de digitale weerbaarheid van vitale infrastructuur, terwijl deze cruciaal is voor nationale continuïteit.

Geïntegreerd inlichtingenbeeld met private data

Het kabinet wil toewerken naar een geïntegreerd inlichtingenbeeld op basis van data van private organisaties. Dit sluit aan bij bestaande publiek-private informatiedeling, maar vraagt om duidelijke juridische kaders, standaarden en governance.

Draghi-rapport en Europese investeringsagenda

Nederland wil een aanjagersrol spelen bij de implementatie van het Draghi-rapport over Europese concurrentiekracht. Dit rapport pleit voor grootschalige investeringen in digitale infrastructuur, AI, cloud, chips en defensie — domeinen waar cybersecurity een essentiële rol speelt.

Nederland koploper in een digitale wereld

Het akkoord benadrukt:

- versnelde implementatie van NIS2 in de Cyberbeveiligingswet
- digitale autonomie;
- investeren in sleuteltechnologieën (AI, quantum, chips, 5G/6G);
- versterking van de digitale economie.

Cybersecurity wordt niet expliciet als randvoorwaarde benoemd, maar is impliciet noodzakelijk om deze ambities te realiseren.

2. Wat betekent dit voor de cybersecuritysector?

- De digitale governance wordt versterkt, maar niet vereenvoudigd. De NDD kan kwaliteit verbeteren, maar lost versnippering niet op.
- De combinatie van AVG-vereenvoudiging en NIS2-implementatie vraagt om heldere communicatie richting organisaties.
- De focus op Defensie en opsporing is begrijpelijk, maar laat een gat vallen in investeringen in vitale infrastructuur.
- Publiek-private samenwerking wordt belangrijker, vooral rond dreigingsinformatie en inlichtingen.
- Europese investeringsprogramma's worden strategisch relevanter voor Nederlandse cybersecuritybedrijven.
- Digitale autonomie en sleuteltechnologieën bieden kansen, mits cybersecurity structureel wordt ingebed.

3. Aansluiting van CVNL-speerpunten op het coalitieakkoord

Koppeling regeerakkoord met de strategische agenda van Cyberveilig Nederland.

3.1 Kwaliteit & transparantie

- De NDD gaat standaarden en ontwerpkeuzes borgen.
  CVNL kan bijdragen met normenkaders, certificering en kwaliteitsrichtlijnen.

3.2 Publiek-private samenwerking & informatiedeling

- Het geïntegreerde inlichtingenbeeld vraagt om structurele samenwerking met private partijen.
  CVNL-leden leveren threat intelligence, incidentrespons en SOC-diensten. Daarnaast werken CVNL-leden al in verschillende vormen samen met overheid, denk aan project Melissa, Cyclotron en het nog op te richten cyberweerbaarheidsnetwerk. Ook het House of Cyber waar eerder over gesproken is zou hier een rol in kunnen spelen

3.3 OT-security en vitale infrastructuur

- Het akkoord investeert niet in de digitale weerbaarheid van de vitale infrastructuur. Wel wordt er gesproken over versnelde invoering van de NIS2.
  CVNL kan dit gat adresseren en pleiten voor een meerjarig investeringsprogramma.

3.4 Human capital

- De overheid wil minder externe inhuur en meer eigen IT-capaciteit.
  CVNL kan bijdragen met input geven op opleidingen, kennisoverdracht en beroepsprofielen.

3.5 Innovatie & sleuteltechnologieën

- Investeringen in AI, quantum en chips vragen om security-by-design.
  CVNL kan standaarden en best practices ontwikkelen.

3.6 Beleidsbeïnvloeding & stelselvorming

- De versnippering van cybersecurity blijft bestaan.
  CVNL kan pleiten voor een heldere stelselverantwoordelijkheid en één aanspreekpunt.

4. Boodschap voor leden van Cyberveilig Nederland

Het coalitieakkoord biedt kansen én uitdagingen voor de cybersecuritysector.
De oprichting van de Nederlandse Digitale Dienst kan leiden tot betere digitale standaarden binnen de overheid, maar lost de versnippering van cybersecurityverantwoordelijkheden niet op. De sector moet alert blijven op de impact van AVG-vereenvoudiging in combinatie met de Cyberbeveiligingswet.

De investeringen in Defensie en opsporing zijn positief, maar de afwezigheid van een vergelijkbaar programma voor vitale infrastructuur is zorgelijk. Tegelijkertijd ontstaan er nieuwe kansen in Europese investeringsprogramma's, sleuteltechnologieën en publiek-private informatiedeling.

Voor leden betekent dit: cybersecurity wordt strategischer, zichtbaarder en meer verweven met nationale en Europese ambities. De sector heeft een belangrijke rol om richting te geven aan standaarden, governance en praktische uitvoerbaarheid.

5. Haakjes voor verdere gesprekken van CVNL met overheid en politiek

5.1 Governance & stelsel

- Pleiten voor een duidelijke cybersecurity-stelselverantwoordelijkheid binnen het Rijk.
- Positioneren van CVNL als kennispartner van de Nederlandse Digitale Dienst.

5.2 Vitale infrastructuur

- Aandringen op een meerjarig investeringsprogramma voor digitale weerbaarheid van vitale en essentiële diensten.
- Voorstellen voor OT-security-normen en ondersteuning van MKB-ketenpartijen.

5.3 AVG & Cyberbeveiligingswet

- Pleiten voor harmonisatie van toezicht (AP, NIS2-autoriteiten).

5.4 Publiek-private informatiedeling

- Meedenken over juridische kaders voor het geïntegreerde inlichtingenbeeld.
- Standaardisatie van formats, taxonomieën en vertrouwelijkheidsniveaus.

5.5 Europese agenda & Draghi-rapport

- Bevorderen van deelname van Nederlandse cybersecuritybedrijven aan Europese programma's.
- Pleiten voor expliciete opname van cybersecurity in de Nederlandse inzet op Draghi-implementatie.

5.6 Human capital

- Voorstellen voor publiek-private opleidingsprogramma's en certificering.
- Aandacht voor de krapte op de arbeidsmarkt en de rol van de sector in kennis