

Oproep: het is tijd voor daadkracht, zichtbaarheid en toekomstgerichtheid in cyberveiligheid




CYBERVEILIG
NEDERLAND

Inleiding

28 april 2025 rond het middaguur.

Het begon met een plotselinge stilte. Verkeerslichten vielen uit, winkels sloten halsoverkop hun deuren en in woonwijken klonk verwarring – en soms zelfs paniek. In grote delen van Spanje en Portugal heerste plotselinge duisternis, niet alleen letterlijk, maar ook digitaal. Internetverbindingen vielen weg, pinautomaten werkten niet meer, treinen kwamen tot stilstand. In een samenleving die volledig leunt op digitale infrastructuur werd in één klap zichtbaar hoe kwetsbaar die afhankelijkheid is.

De storing legde niet alleen het elektriciteitsnet plat, maar ook het vertrouwen van burgers werd hiermee geraakt. Iedereen vroeg zich af of het een cyberaanval was. Bedrijven schakelden over op noodscenario's. Burgers zochten massaal naar informatie, maar werden van het kastje naar de muur gestuurd.

De storing gaf een voorproefje van wat er gebeurt als digitale voorzieningen uitvallen – en het gaf een krachtig signaal af: onze samenleving kan niet meer zonder digitale continuïteit, en daar hoort robuuste voorbereiding bij.

Met de verkiezingen, en later formatie, in aantocht hebben we een kans die we niet kunnen laten liggen: het fundamenteel versterken van onze digitale weerbaarheid en de daarbij horende soevereiniteit. In een wereld waarin geopolitieke spanningen toenemen en digitale dreigingen al lang geen fictie meer zijn, is er geen ruimte meer voor vrijblijvende adviezen, zachte maatregelen of enkel stimulerend beleid. Incidenten zoals recent in Spanje en Portugal maken pijnlijk duidelijk dat de eerste gedachte bij een crisis of incident tegenwoordig een cyberaanval is.

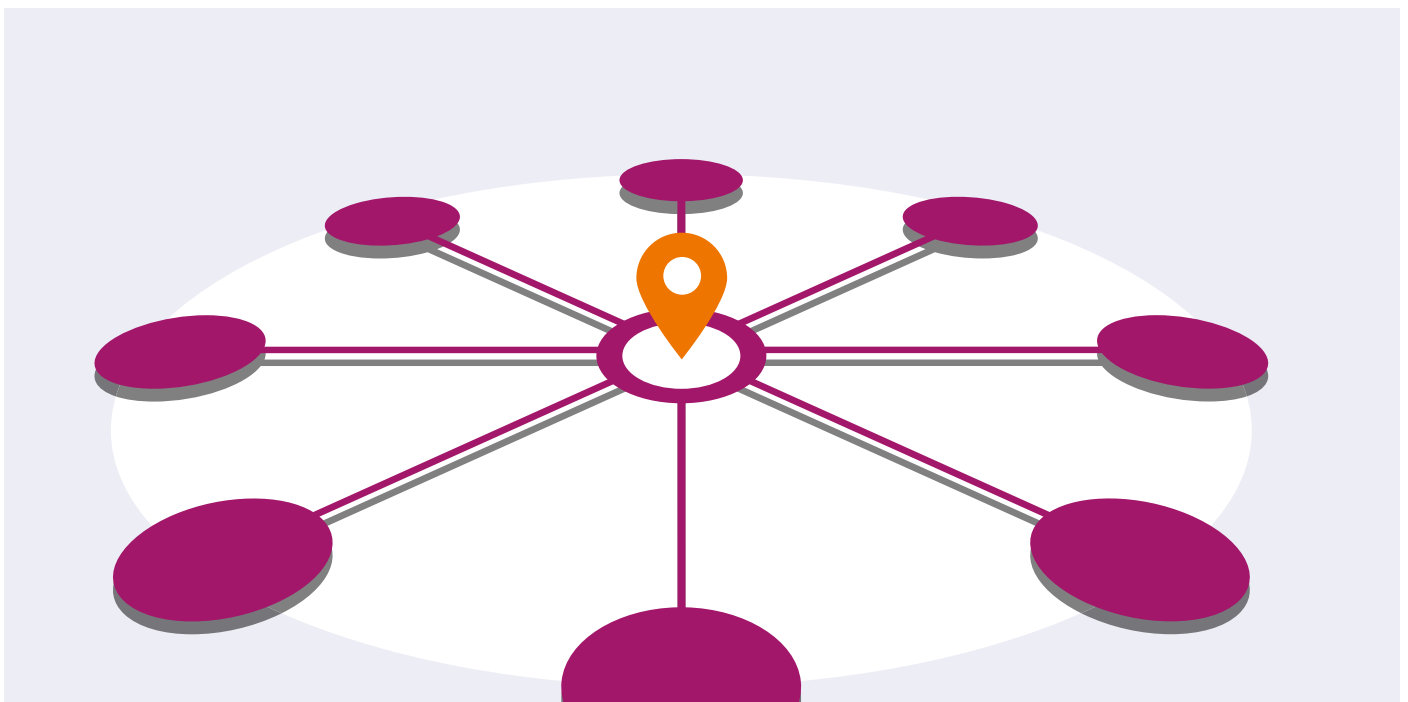
We kunnen het ons simpelweg niet meer veroorloven om weg te kijken of mondjesmaat actie te ondernemen. Deze onzekere tijd vraagt om daadkracht, centrale regie en structurele investeringen in uitvoering en toezicht.

Tegelijkertijd vraagt dit om opzichtig balanceren: de risico's nemen toe en dat vraagt om meer daadkracht vanuit de overheid en verantwoordelijkheden van individuele organisaties, anderzijds kan deze regeldruk

ook een remmende werking hebben op onze innovatie en wendbaarheid.

Die balans vereist scherpe keuzes en heldere afbakening van governance, van rollen en verantwoordelijkheden. Een Minister van Digitale Zaken kan zorgen voor meer centrale coördinatie, het tegengaan van versnippering en het duidelijk beleggen van verantwoordelijkheden, zowel binnen als buiten de overheid.

De huidige aanpak zet onvoldoende zoden aan de dijk. Investeren in onze digitale infrastructuur, inclusief onze OT-omgevingen. In talent, jong en oud en een leven lang leren. Digitale soevereiniteit moet bovenaan de agenda staan. De afhankelijkheid van buitenlandse techreuzen maakt ons nu te kwetsbaar – laten we dat met opkomende technologieën als AI en kwantum niet opnieuw laten gebeuren. Wet- en regelgeving zijn belangrijke stappen, maar moeten worden ingebed in een bredere, actieve strategie waarin Nederland optreedt als zijn eigen launching customer en innovatie en onderzoek stimuleert in publiek private samenwerkingsverbanden.



Cybersecurity is geen kostenpost, maar een voorwaarde voor welvaart. Elke grote ontwrichtende aanval kost het bedrijfsleven miljoenen. De NAVO norm voor infrastructuur en industrie van 1,5 % bbp opent de deur om een deel daarvan te alloceren aan digitale verdediging.

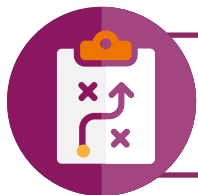
Investerings moeten voorspelbaar, transparant en doelgericht zijn, met een meerjareninvesteringsplan dat voorbij de kabinetsperiode kijkt.

Kortom, we staan op een kruispunt. Doorgaan op de huidige weg betekent achterlopen en kansen missen. Het is tijd om als overheid **daadkrachtig, zichtbaar en toekomstgericht** te handelen in samenwerking met het bedrijfsleven. Niet alleen met woorden, maar ook met concrete daden, investeringen en keuzes die onze digitale toekomst veiligstellen. En wij vanuit Cyberveilig Nederland reiken hierbij de helpende hand: want alleen ga je sneller maar samen kom je verder!

Speerpunten voor nu tot en met 2030

Daadkracht, Zichtbaar en Toekomstgericht

Zorg voor:



1. centrale overheidsregie voor samenhang en slagkracht



2. proactieve versnelling van de inbedding van wet- en regelgeving



3. verankering van digitale weerbaarheid in het onderwijs en een leven lang leren



4. regie op digitale soevereiniteit in tijden van geopolitieke spanningen



Zorg voor centrale overheidsregie voor samenhang en slagkracht

De versnipperde aansturing, mandaat en uitvoering van het Nederlandse cybersecuritybeleid en -aanpak vanuit de overheid vormt een structurele kwetsbaarheid. In een tijd waarin digitale dreigingen zich razendsnel ontwikkelen, kunnen we ons geen beleidspauzes of bestuurlijke ruis veroorloven. De coördinatielgtnuverspreidoververschillende departementen, agentschappen en programma's. Dit leidt tot veel afstemming, papierwerk, overlap, onduidelijkheid over rollen en verantwoordelijkheden, en onvoldoende uitvoering.

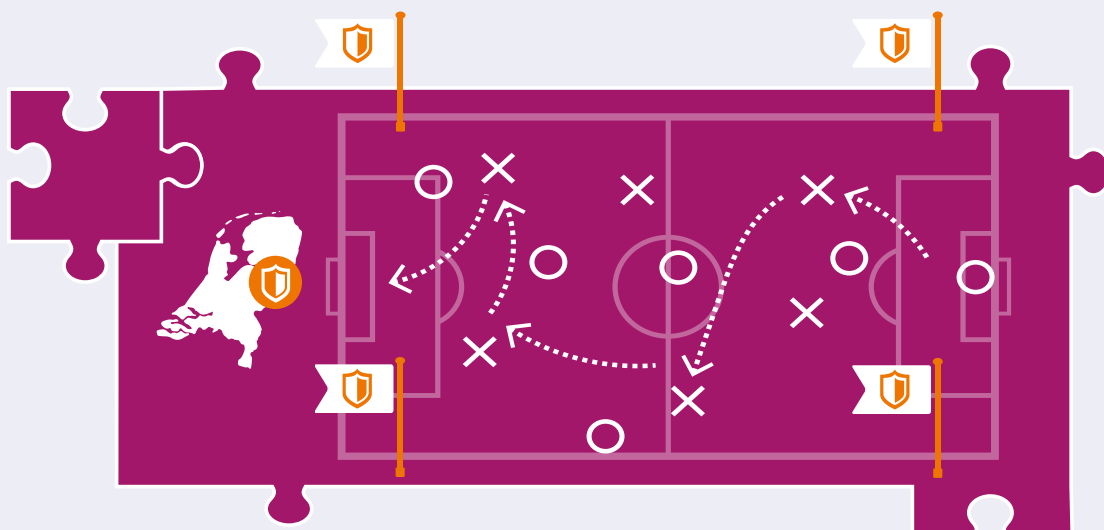
Deze versnippering zorgt momenteel voor trage besluitvorming en reactievermogen bij acute dreigingen of veranderende omstandigheden zoals geopolitieke spanningen, technische ontwikkelingen of wet- en regelgeving. Het zorgt ook voor een verlies van slagkracht bij de implementatie van beleid. De energie en financiering gaat naar het coördineren in plaats van naar de daadwerkelijke uitvoering. Ook het bedrijfsleven (vitale infrastructuur en diens keten) hebben last van deze versnippering doordat er onduidelijkheid is over regelgeving, communicatieberichten niet eenduidig zijn en ook het aanspreekpunt bij de overheid diffuus is, of tegenstrijdige antwoorden geeft.

Centrale regie is echter geen doel op zich, maar een noodzakelijke voorwaarde voor samenhang, tempo en doeltreffendheid. Zonder duidelijke sturing en gedeelde strategische richting blijven cybersecuritymaatregelen reactief, versnipperd en suboptimaal. Het aanstellen van een Minister van Digitale Zaken, met een helder mandaat, financiering en de regierol over cybersecurity, digitale infrastructuur en innovatie, is cruciaal.

Deze minister kan opereren als ankerpunt voor publiek-private samenwerking, verantwoordelijkheidsverdeling en interdepartementale afstemming of -verplichting. Alleen met een regieorgaan dat over alle relevante domeinen heen kijkt, kunnen we de snelheid en complexiteit van het digitale speelveld bijbenen.

OPROEP AAN DE POLITIEK:

- **BENOEM** een minister van Digitale Zaken gericht op alle digitale dossiers (cyber security, digitale infrastructuur, data, AI, digitale identiteit) vanuit één mandaat voor coördinatie van wet- en regelgeving, beleid, uitvoering en toezicht.
- **PAS** onder de verantwoordelijkheid van de minister van Digitale Zaken de huidige strategische cybersecurityagenda aan op basis van de huidige ontwikkelingen en draag zorg voor concrete doelstellingen en prestatie-indicatoren met jaarlijkse bijstellingsmomenten die door publiek en privaat ingebracht kan worden.
- **ZET** de inrichting van één centraal informatiepunt voor alle sectoren (Vitaal en MKB) voort door middel van het onderschrijven van de samenvoeging van het NCSC, DTC en CSIRT DSP en plaats deze onder de verantwoordelijkheid van de minister van Digitale Zaken.
- **RICHT** onder de minister van Digitale Zaken een centraal publiek-privaat-wetenschappelijke governance-structuur in, die sturing en feedback combineert met domeinexpertise en innovatiekracht.





Zorg voor proactieve versnelling van de inbedding van wet- en regelgeving

Wet- en regelgeving vormt onze uiterste digitale verdedigingslinie. Toch bungelt Nederland onderaan de EU ranglijst voor tijdige implementatie: de NIS2 en CER zijn al bijna twee jaar van kracht. De vertraging van de implementatie in nationale wetgeving schuift noodzakelijke maatregelen bij organisaties vooruit én vergroot het risico op sancties vanuit Brussel. Onduidelijke regels en laattijdige handhaving laten kwaadwillende vrij spel – én ondermijnen het vertrouwen van ondernemers.

Een toekomstbestendige cyberwet vraagt om tempo, helder taalgebruik en voorspelbare, zichtbare en effectieve handhaving. Wetgeving moet richting geven in plaats van verwarring zaaien, en de toezichthouder moet vanaf dag één mandaat, mensen en middelen hebben. En organisaties moeten zien en merken dat handhaving plaats vindt. Toezichthouders moeten in de praktijk staan door goede feedback te geven waar ondernemers echt beter van worden: geen vinkjes en checklist compliance.

Ook in het kader van digitale soevereiniteit is het van belang dat Nederland proactief een standpunt inneemt in het Europese debat. Het is van belang dat wet- en regelgeving voor nieuwe technologieën zoals AI en quantum wordt opgesteld vóórdat deze technologieën mainstream worden, om op deze manier publieke waarden, veiligheid, privacy en eigen controle te garanderen.

OPROEP AAN DE POLITIEK:

- **IMPLEMENTEER** de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke) en CER, uiterlijk Q2 2026 in werking en **HARMONISEER** deze met aanverwante wet- en regelgeving zoals de AI Act, AVG, DORA en CRA.
- **CREËER** één nationaal cyber-toezichthouder loket met heldere boete- en sanctie tabellen en draag zorg dat handhaving zichtbaar en effectief plaats vindt met oog voor de praktijk.
- **COMMUNICEER** door het oprichten van een centrale marketing en communicatie campagne zodat organisaties van groot tot klein aan kunnen op juistheid van de ontvangen informatie, toezichtkaders, handhaving, standaarden en normeringen, geaccrediteerde keurmerken, etc.
- **INTEGREER** evaluatiemomenten (één en driejaarlijks) om de wet adaptief bij te sturen.
- **ONTWIKKEL** proactief wet- en regelgeving voor nieuwe technologieën die een positieve bijdrage leveren aan de digitale soevereiniteit en de Europese normen en waarden positief beïnvloeden.





Zorg voor verankering van digitale weerbaarheid in het onderwijs en een leven lang leren

De digitale weerbaarheid van Nederland staat of valt met de beschikbaarheid van voldoende goed opgeleide professionals én digitaal vaardige burgers. Willen we in 2030 voorbereid zijn op de uitdagingen van de digitale samenleving, dan moet het onderwijssysteem nú structureel worden aangepast. Het is daarom noodzakelijk dat het Ministerie van Onderwijs, Cultuur en Wetenschap (OCW) de regie neemt in de ontwikkeling van toekomstbestendig onderwijs op het gebied van digitale veiligheid en cybersecurity in afstemming met de Minister van Digitale Zaken. De huidige versnippering in initiatieven, een gebrek aan structurele inbedding van cybersecurity in het curriculum, en een nog altijd te beperkte uitstroom van gekwalificeerde professionals leiden tot een structurele mismatch op de arbeidsmarkt. Dit vraagt om een nationaal gecoördineerde aanpak, waarin OCW duidelijke richtlijnen stelt, doorlopende leerlijnen ontwikkelt, en onderwijsinstellingen ondersteunt bij het integreren van cybersecurity in alle lagen van het onderwijs.

Digitalisering heeft een impact op alle levens en banen van de toekomst. Cybersecurity maakt deel uit van vaardigheden die essentieel zijn in elke moderne leeromgeving. Bij Leven Lang Leren hoort capaciteiten zoals het inzicht in cyberdreigingen, de vaardigheid in veilig online werken en het kritisch kunnen omgaan met informatie. Hier is een belangrijke voortrekkersrol weggelegd voor het Ministerie van Sociale Zaken en Werkgelegenheid in relatie met de Minister voor Digitale Zaken.

OPROEP AAN DE POLITIEK:

- **NEEM** regie op curriculum en aanbod door Ministerie van OCW en dit in samenhang met betreffende andere vakdepartementen in het vervullen en aanjagen van vakinhoudelijke leerlijnen en het vaststellen van sectorspecifieke competenties.
- **LEGWETTELIJKVAST** dat digitale geletterdheid vanaf schooljaar 2027/28 kernvak wordt in het primair en voortgezet onderwijs.
- **INTEGREER** digitale veiligheid in het gehele curriculum, van basisonderwijs tot universiteit
- **ONTWIKKEL** doorlopende leerlijnen waarin techniek, gedrag, ethiek en recht samenkomen. Daarbij opgemerkt dat kennis van organisaties en skills op het gebied van communicatie ook cruciaal zijn.
- **MAAK** praktijkgericht onderwijs de norm: real life casussen, hackathons, stageplaatsen.
- **ANTICIPEER** op toekomstige behoefte. Het onderwijsbeleid moet niet alleen aansluiten bij de huidige knelpunten, maar ook proactief sturen op wat er in 2030 nodig is.
- **ZORG** dat digitale vaardigheden een rol krijgt in het Leven Lang Leren





Zorg voor regie op digitale soevereiniteit in tijden van geopolitieke spanningen

Nederland is op dit moment in hoge mate afhankelijk van technologieën en infrastructuur buiten Europa. Onze data staan in Amerikaanse clouds, onze 5G-netwerken bevatten componenten uit China, en onze digitale economie draait op softwareplatforms waar Nederland nauwelijks grip op heeft.

Wat ontbreekt, is regie en daadkracht. Regie op de huidige situatie van de afhankelijkheid van buitenlandse grootmachten, maar ook regie op strategische technologieën zoals cryptografie, quantum computing en AI. Zonder eigen versleutelingstechnologie (encryptie), veilige segmentatie van netwerken en post-quantum-beveiligingsmaatregelen, lopen we ernstige risico's nu en in de toekomst. Als Nederland hier niet proactief en daadkrachtig op inzet, dreigt een herhaling van de fouten rondom cloud: te laat, te afhankelijk, te weinig soeverein.

Om dat te bereiken, is proactief beleid essentieel. De overheid moet vooruitkijken en strategische keuzes maken in plaats van reageren. Dat betekent ook dat de overheid optreedt als 'launching customer': investeert in nationale technologische oplossingen, consortia stimuleert waar MKB-ondernemers een plek vinden en deze toepast binnen overheidsorganisaties en zo innovatie stimuleert.

OPROEP AAN DE POLITIEK:

- **INVESTEER** in Nederlandse en Europese digitale infrastructuur, zoals onafhankelijke cloudvoorzieningen, eigen chipproductie, en veilige communicatienetwerken.
- **ONTWIKKEL EN IMPLEMENTEER** nationale crypto-grafische producten voor encryptie, netwerksegmentatie en post-quantum-beveiliging. Deze technologieën zijn essentieel voor veilige communicatie, bescherming van staatsgeheimen en het waarborgen van autonomie in het digitale domein.
- **MAAK** van de overheid een 'launching customer': stimuleer innovatie door actief in te kopen bij Nederlandse partijen op het gebied van AI, cybersecurity en cryptografie.
- **INTRODUCER** een verplicht soevereiniteits impactassessment voor alle vitale aanbestedingen (Q3 2026) met terugwerkende kracht op bestaande aanpassingen vanuit een risico gebaseerde aanpak.
- **VERANKER** in de Aanbestedingswet 2012 een voorkeursbehandeling voor veilige en soevereine – Nederlandse - oplossingen (pas toe of leg uit).

