

Consultatiereactie op het wetsvoorstel

Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten (Wbmv)

5-10-2026

Geachte heer/mevrouw,

Namens Cyberveilig Nederland, de brancheorganisatie voor cybersecuritybedrijven in Nederland, maken wij graag gebruik van de mogelijkheid om te reageren op het wetsvoorstel Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten (Wbmv).

Cyberveilig Nederland onderschrijft het belang van een effectieve en toekomstbestendige uitrusting van de AIVD en de MIVD en herkennen de noodzaak. Een groot deel van de dreigingen die dit wetsvoorstel beoogt te adresseren – statelijke actoren, sabotage, spionage, digitale ontwijking – vormen precies het domein waarin onze leden dagelijks actief zijn: het adviseren en beschermen van Nederlandse organisaties tegen diezelfde dreigingen.

En daar zit dan ook precies onze zorg. Ondanks dat we hetzelfde voor ogen hebben maakt het wetsvoorstel cybersecuritydienstverleners mogelijk tot geadresseerde van vergaande vorderingsbevoegdheden. Tevens hebben we vragen over het binnendringen en het treffen van voorbereidingen rondom de hackbevoegdheid. Dat lichten we graag toe.

Cybersecurity dienstverleners als vertrouwenspartner in het vergroten van de digitale veiligheid

Cybersecuritydienstverleners hebben kennis, of zijn beheerders van gevoelige gegevens van hun klanten: kwetsbaarheden, netwerkarchitecturen, incidentgegevens, logbestanden en soms zelfs broncodes. De vertrouwensrelaties tussen cybersecuritydienstverleners en de klant is cruciaal voor de uitvoering van de dienstverlening. Het wetsvoorstel voorziet, wat ons betreft, in onvoldoende waarborgen om deze vertrouwensrelatie te beschermen.

Cybersecuritydienstverleners vervullen een bijzondere functie binnen het Nederlandse digitale ecosysteem. Onze leden beschermen organisaties alleen effectief tegen cyberdreigingen wanneer deze hun beveiligingspartner volledig inzicht geven in kwetsbaarheden, incidenten, netwerkarchitecturen, loggegevens, forensische bevindingen en andere gevoelige (technische) informatie. Die openheid is uitsluitend mogelijk wanneer een hoge mate van vertrouwen bestaat in die relatie. Dat vertrouwen dient niet alleen een commercieel belang van de cybersecuritysector, maar juist ook een publiek belang. Effectieve detectie van cyberdreigingen, incidentrespons,

kwetsbaarhedenmanagement en de bestrijding van cybercriminaliteit zijn afhankelijk van de bereidheid van organisaties om volledige openheid van zaken te geven aan gespecialiseerde cybersecuritydienstverleners. Wanneer organisaties vrezen dat dergelijke informatie zonder hun medeweten onderwerp kan worden van geheime vorderingen, kan dat leiden tot terughoudendheid in het delen van informatie. Dat raakt niet alleen individuele ondernemingen, maar uiteindelijk ook de digitale weerbaarheid van Nederland als geheel en daarmee de belangen die dit wetsvoorstel juist beoogt te beschermen.

Cybersecuritybedrijven beheren vaak gecentraliseerd de gegevens van meerdere klanten. Vanuit het perspectief van de diensten kan dat een efficiënte informatiebron zijn. Een vordering bij de dienstverlener heeft niet tot gevolg dat de klant zelf – de primaire bron – van het onderzoek op de hoogte raakt. Naar onze overtuiging is aanvullende normering nodig om te voorkomen dat cybersecuritybedrijven in de praktijk structureel de kortste route worden, een “easy catch”, in plaats van uitsluitend te worden benaderd wanneer de primaire bron niet, niet tijdig of niet volledig kan leveren. Wij werken dit verderop, onder “Subsidiariteit: eerst de primaire bron benaderen”, uit in concrete vragen en een tekstvoorstel.

De reactie van Cyberveilig Nederland op het wetsvoorstel behandelt de volgende hoofdstukken:

- **1. Vorderingsbevoegdheden: reikwijdte, subsidiariteit en waarborgen.** De reikwijdte van artikel 87, eerste lid, onder c, en artikel 94, subsidiariteit bij vorderingen aan een derde, operationele waarborgen tijdens en na een vordering, en de gevolgen van publiek-private samenwerking voor de kans op een vordering.
- **2. Hackbevoegdheid: de grens tussen positioneren en uitwinnen.** Het risico dat handelingen zonder voorafgaande toets worden uitgevoerd.
- **3. Internationale gegevensdeling en economische veiligheid.** De weging van bedrijfsbelangen bij gegevensdeling met buitenlandse diensten.
- **4. Impactanalyse voor de cybersecuritysector.** Specifieke bedrijfseffectentoets en monitoring van de effecten in de praktijk.

Wij hebben het wetsvoorstel en de memorie van toelichting daarom artikel voor artikel bestudeerd en onze bevindingen vertaald naar concrete vragen met daar waar mogelijk tekstvoorstellen. **Wij verzoeken de regering deze vragen te beantwoorden in het verslag van de consultatie en in de memorie van toelichting bij indiening van het wetsvoorstel, en zo nodig schriftelijk tijdens de parlementaire behandeling.**

1. Vorderingsbevoegdheden: reikwijdte, subsidiariteit en waarborgen

Artikel 87: opgeslagen gegevens

Artikel 87, eerste lid, onder c, geeft de diensten de bevoegdheid gegevens te vorderen van “een persoon of instantie die in het kader van de uitoefening van een beroep of bedrijf de opslag verzorgt van door derden via geautomatiseerde werken verwerkte gegevens en waartoe voor die derde rechtstreeks geautomatiseerde toegang bestaat”. De toelichting noemt als voorbeeld de opslag bij een clouddienst. Ook de definitie van “aanbieder van een communicatiedienst” (artikel 1) is ruim: die omvat ook wie “gegevens verwerkt of opslaat voor een zodanige dienst of de gebruikers van die dienst”.

Deze bepaling kan, afhankelijk van de inrichting van de dienstverlening, ook cybersecuritydienstverleners treffen, waaronder managed hostingproviders, SOC-dienstverleners en bepaalde MDR-dienstverleners die log-, telemetrie- of incidentgegevens namens klanten opslaan en beschikbaar houden. Niet iedere MDR-dienstverlener verzorgt zelf de opslag; het enkele feit dat een partij MDR-diensten verleent betekent dus niet automatisch dat artikel 87, eerste lid, onder c, van toepassing is. De precieze reikwijdte is echter niet zonder meer duidelijk. Binnen de sector bestaan verschillende dienstverleningsmodellen: gegevens blijven soms bij de klant, worden soms door de dienstverlener zelf opgeslagen en soms in platformen van derde partijen, zoals Microsoft of CrowdStrike. Juist die onduidelijkheid vraagt om een expliciete verduidelijking van de positie van cybersecuritydienstverleners in de wet en/of de memorie van toelichting.

Daarnaast valt ons een technisch punt op. De toelichting bij artikel 87 zegt dat de medewerkingsplicht voor de in onderdeel c bedoelde persoon of instantie is neergelegd in artikel 91, derde lid. De tekst van dat lid spreekt echter alleen over “de aanbieder van een communicatiedienst of online platform”, en de strafbaarstelling in artikel 233 verwijst naar datzelfde lid. Naar de letter van de wet lijkt voor partijen onder onderdeel c daarom geen verplichting te bestaan, en dus ook geen strafbaarheid bij niet-nakoming. Of dat de bedoeling is, is niet duidelijk. Bedrijven moeten weten of zij aan een vordering moeten voldoen en wanneer zij zich strafbaar maken. Wij vragen daarom om verduidelijking van de bestaande tekst en nadrukkelijk niet om een uitbreiding van de plicht.

Onze vragen over artikel 87

1. Kan de regering tijdens de behandeling van het wetsvoorstel **schriftelijk bevestigen of artikel 87, eerste lid, onder c, van toepassing is op cybersecuritydienstverleners**, en zo ja onder welke omstandigheden? Wij vragen daarbij om onderscheid naar dienstverleningsmodel: opslag door de dienstverlener zelf, opslag bij een platform van een derde partij en opslag bij de klant zelf. Wij vragen daarbij ook om te verduidelijken wat moet worden verstaan onder “de opslag verzorgen” en onder “gegevens verwerkt of opslaat voor een zodanige dienst” (artikel 1), en of partijen die uitsluitend beveiligingsdiensten leveren (monitoring, detectie, respons, penetratietesten, advies) en niet zelfstandig als communicatiedienst of onlineplatform optreden, daaronder vallen.

2. De toelichting zegt dat artikel 87 overeenkomt met artikel 54 Wiv 2017, met onlineplatforms als enige nieuw element. Is de reikwijdte van onderdeel c en van de definitie van “aanbieder van een communicatiedienst” ten opzichte van de Wiv 2017 gewijzigd?
3. Artikel 87, derde lid, bepaalt dat een toestemming ook de bevoegdheid omvat zich te wenden tot een andere partij die “in de plaats treedt” van de geadresseerde of “naast” die partij wordt ingeschakeld. Wanneer is daarvan sprake bij cybersecuritydienstverleners, bijvoorbeeld bij een andere dienstverlener in de keten of een platform van een derde? Wordt de inzet tegen die andere partij afzonderlijk getoetst, of valt zij binnen de oorspronkelijke toestemming?
4. Gelden de medewerkingsplicht (artikel 91, derde lid) en de strafbaarstelling (artikel 233) ook voor de categorie in artikel 87, eerste lid, onder c, en zo ja op welke grondslag? Wij vragen uitdrukkelijk om verduidelijking van de bestaande tekst en niet om een verruiming van de plicht. Wij wijzen er daarbij op dat artikel 93, eerste lid, deze categorie voor de kostenvergoeding wél afzonderlijk noemt naast de aanbieders van een communicatiedienst of online platform; de wetgever heeft onderdeel c dus kennelijk niet over het hoofd gezien, wat het des te opvallender maakt dat deze categorie in artikel 91, derde lid, en artikel 233 ontbreekt.

Voorstel voor aangepaste tekst: wij geven in overweging artikel 91, derde lid, aan te vullen met een verwijzing naar de persoon of instantie, bedoeld in artikel 87, eerste lid, onder c, zodat de medewerkingsplicht – en daarmee ook de strafbaarstelling van artikel 233 – buiten twijfel ook voor deze categorie geldt. Artikel 93, eerste lid, laat zien dat dit geen theoretisch punt is: daar wordt dezelfde categorie voor de kostenvergoeding wel genoemd, wat onderstreept dat het ontbreken ervan in artikel 91 en artikel 233 eerder een omissie dan een bewuste keuze lijkt. Is dat uitdrukkelijk niet de bedoeling, dan vragen wij dat te bevestigen en artikel 87, eerste lid, onder c, van een eigen medewerkingsbepaling te voorzien.

Artikel 94: gegevens voor weerbaarheidsbelangen

Artikel 94 kent een nog bredere kring van geadresseerden: “bestuursorganen, ambtenaren en voorts een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken”. De toelichting (paragraaf 7.2.8) kiest er bewust voor de bevoegdheid niet af te bakenen naar sector of domein. Zij noemt als voorbeelden van te vorderen gegevens: logging- en netwerkgegevens, een overzicht van toeleveranciers, disk images en beveiligingsinformatie, en spreekt over vorderen “bij of over” een beoogd slachtoffer. Ook erkent de toelichting dat kwaadwillende actoren zich richten op niet-vitale aanbieders in de toeleveringsketen. Dit zijn typisch gegevens die cybersecuritybedrijven namens klanten beheren of analyseren.

De combinatie van een kring van adressanten die bestaat uit “een ieder die geacht wordt” gegevens te kunnen verstrekken, het ontbreken van een sectorale afbakening en het open begrip “weerbaarheidsbelangen” maakt dat de reikwijdte in de praktijk zeer ruim kan worden.

Onze vragen over artikel 94

5. Kan de regering tijdens de behandeling van het wetsvoorstel **schriftelijk bevestigen of artikel 94 van toepassing is op cybersecuritydienstverleners**, bijvoorbeeld als “anderen die beschikken over gegevens” waarmee de dreiging kan worden gemitigeerd, en zo ja onder welke voorwaarden zij adressant kunnen zijn voor gegevens die zij namens hun klanten beheren?
6. Welke objectieve grenzen gelden voor de toepassing van artikel 94, en welke waarborgen voorkomen dat de toepassing zich in de praktijk geleidelijk uitbreidt naar steeds meer categorieën bedrijven? Denk aan beleidsregels, publicatie van de toepassing en evaluatie.

Voorstel voor aangepaste tekst: *wij geven in overweging aan artikel 94 een lid toe te voegen dat de regering verplicht periodiek beleidsregels vast te stellen en te publiceren over de toepassing van artikel 94 op cybersecuritydienstverleners, met daarin ten minste objectieve criteria voor de afbakening van de kring van geadresseerden. De eis om te motiveren waarom niet rechtstreeks bij het beoogde slachtoffer wordt gevorderd, bespreken wij hieronder onder het kopje “Subsidiariteit: eerst de primaire bron benaderen”, omdat die eis naar ons oordeel evenzeer voor artikel 87 als voor artikel 94 zou moeten gelden.*

Subsidiariteit: eerst de primaire bron benaderen

Noch artikel 87, noch artikel 94 verplicht de diensten te motiveren waarom niet rechtstreeks bij de primaire bron – de betrokken organisatie zelf – wordt gevorderd, maar bij een derde die namens die organisatie gegevens beheert. Artikel 87, eerste lid, kent drie gelijkwaardige categorieën adressanten, die volgens de toelichting “separaat of in combinatie” kunnen worden toegepast.

Het principe “eerst de minst ingrijpende route” kent het wetsvoorstel elders wel. Bij binnendringen via een derde (artikel 76; paragraaf 7.2.2.4 van de toelichting) moet de toegang via een derde “afzonderlijk worden onderbouwd” in het toestemmingsverzoek, en moet worden afgezien van die route als dezelfde gegevens op een minder ingrijpende manier te verkrijgen zijn. Bij artikel 94 zegt de toelichting dat vrijwillige samenwerking de norm blijft en dat de bevoegdheid een ultimatum remedium is. Dat uitgangspunt staat niet in de wettekst; voor artikel 87 hebben wij het niet aangetroffen.

Artikel 16, derde lid, en artikel 41, onder I, vragen om de bevoegdheid met “het minste nadeel” voor de betrokkene en om een motivering waarom niet met een minder ingrijpende bevoegdheid kan worden volstaan. Dat gaat over de keuze tussen bevoegdheden, niet over de keuze tussen de primaire bron en een derde die voor die de bron gegevens beheert. Wij realiseren ons dat hacken via een derde en vorderen niet identiek zijn, maar het onderliggende principe – niet via een derde als het ook rechtstreeks kan – is hetzelfde.

Onze vragen aan de regering

7. Waarom geldt de eis van een afzonderlijke onderbouwing bij binnendringen via een derde (artikel 76) wel, maar niet bij vorderingen op grond van artikel 87, eerste lid, onder c, en artikel 94?
8. Geldt het uitgangspunt uit de toelichting bij artikel 94 (vrijwillige samenwerking als norm, vordering als ultimum remedium) ook wanneer de vordering is gericht aan een dienstverlener die gegevens namens het slachtoffer beheert? Waarom is dit niet in de wettekst opgenomen?
9. Kan de afdeling toetsing bij haar rechtmatigheidsoordeel beoordelen of dezelfde gegevens rechtstreeks bij de primaire bron te verkrijgen waren? Zo ja, waar in de wet volgt dat uit? Zo nee, is de regering bereid in artikel 41 te eisen dat het toestemmingsverzoek motiveert waarom niet rechtstreeks bij de primaire bron wordt gevorderd?
10. Is de regering bereid te eisen dat het toestemmingsverzoek bij vorderingen aan een derde partij ook motiveert welke gevolgen de vordering redelijkerwijs heeft voor de bedrijfsvoering en de klantrelaties van de geadresseerde?
11. Artikel 87, tweede lid, vereist een nauwkeurige omschrijving van de gegevens en de periode, en bij artikel 94 ontbreekt een vergelijkbare eis (wel geldt artikel 41). Hoe wordt voorkomen dat een vordering bij een dienstverlener ook gegevens raakt van klanten die geen onderwerp van onderzoek zijn, wanneer gegevens technisch niet te scheiden zijn? Welke regels gelden voor verdere verwerking en verwijdering van zulke gegevens?

Voorstel voor aangepaste tekst: *wij geven in overweging aan artikel 41 een onderdeel toe te voegen dat bepaalt dat het toestemmingsverzoek bij een vordering aan een derde partij die namens een ander gegevens beheert, mede bevat: (i) een motivering waarom niet rechtstreeks bij de primaire bron wordt gevorderd, en (ii) voor zover van toepassing, een motivering van de te verwachten gevolgen voor de bedrijfsvoering en de klantrelaties van die derde. Dit onderdeel zou moeten gelden voor vorderingen op grond van zowel artikel 87 als artikel 94, zodat de subsidiariteitseis niet afhankelijk is van welke grondslag de diensten kiezen.*

Waarborgen tijdens en na een vordering

Wij erkennen dat het wetsvoorstel voorziet in een voorafgaande rechtmatigheidstoets door de afdeling toetsing van een volledig onafhankelijk college (artikel 47, onder j en l, en artikel 160, vijfde lid). Die waarborg is waardevol. De toets kan echter alleen beoordelen wat de wet en het verzoek bevatten, en de wet kent geen criterium dat betrekking heeft op de positie van de geadresseerde.

Daarnaast zien wij een aantal praktische knelpunten. Notificatie achteraf (artikel 59) geldt alleen voor artikel 75, eerste lid, en artikel 79, eerste lid – niet voor vorderingen op grond van artikel 87 of 94.

Bezwaar en beroep staan voor de geadresseerde niet open (artikel 18, eerste lid, onder f); alleen een klachtrecht bestaat (artikel 189). Voor gedwongen verstrekking ontbreekt bovendien een bescherming van bedrijfsvertrouwelijke gegevens zoals artikel 156 die wel biedt bij inzageverzoeken, en blijft onduidelijk hoe een vordering zich verhoudt tot geheimhoudingsbedingen met klanten (artikel 91, vierde lid, jo. artikel 63, vierde lid). Deze knelpunten werken wij hieronder uit in concrete operationele waarborgen en vragen.

Operationele waarborgen bij een vordering

Deze zorgen vullen wij hieronder in met een aantal operationele waarborgen die wij als sector werkbaar achten. Wij zien ze als een uitvoerbare invulling van subsidiariteit en proportionaliteit:

- **Subsidiariteitstoets:** het toestemmingsverzoek motiveert waarom niet, niet tijdig of niet volledig rechtstreeks bij de primaire bron kan worden gevorderd.
- **Dataminimalisatie:** de vordering is beperkt tot de gegevens van de betrokken organisatie; is dat technisch niet mogelijk, dan wordt dat gemotiveerd, en worden gegevens van niet-betrokken klanten na filtering zo snel mogelijk vernietigd en niet verder gebruikt.
- **Eén vast, beveiligd aanspreekpunt:** een vast contactpunt bij de diensten voor de afhandeling van vorderingen aan cybersecuritydienstverleners, met een korte, vaste reactietermijn over de te volgen procedure.
- **Uitgestelde of geaggregeerde notificatie:** notificatie achteraf aan de geadresseerde dienstverlener, zo nodig vertraagd of in geaggregeerde vorm en zonder herleidbare bijzonderheden, zodra dat de lopende operatie niet meer schaadt.
- **Vrijwaring van contractuele aansprakelijkheid:** een wettelijke bepaling die uitsluit dat een dienstverlener die aan een rechtmatige vordering voldoet, daardoor niet door haar klanten aansprakelijk kan worden gesteld wegens schending van een geheimhoudingsbeding.
- **Gelijke kostenvergoeding:** de kostenvergoeding van artikel 93 geldt ook voor geadresseerden van artikel 94.
- **Bewaartermijn en vernietigingsplicht:** een maximale bewaartermijn voor gevorderde gegevens die niet relevant blijken, met een concrete vernietigingsplicht en verantwoording daarover.
- **Periodieke geaggregeerde rapportage:** jaarlijkse, geaggregeerde rapportage – bijvoorbeeld aan de Tweede Kamer of de CTIVD – over het aantal vorderingen aan cybersecuritydienstverleners op grond van artikel 87 en 94, zonder dat dit individuele vorderingen herleidbaar maakt.
- **Laagdrempelige escalatiemogelijkheid:** de mogelijkheid voor de geadresseerde om, zonder de uitvoering van de vordering op te schorten, een spoedig oordeel van de afdeling toetsing te vragen wanneer de geadresseerde meent dat de vordering breder is dan noodzakelijk.

Onze vragen

12. Artikel 63 staat verzoeken om gegevens toe zonder voorafgaande toestemming en zet wettelijke voorschriften opzij (vierde lid). Welke kaders gelden voor het gebruik van deze route richting cybersecuritydienstverleners, en hoe verhoudt die zich tot de waarborgen bij artikel 87 en 94?
13. Herkent de regering de hierboven genoemde operationele waarborgen als een werkbare invulling van de subsidiariteits- en proportionaliteitseisen bij vorderingen aan cybersecuritydienstverleners, en is zij bereid deze – of een gelijkwaardig alternatief – in de wet, de toelichting of de uitvoeringspraktijk te verankeren?

Publiek-private samenwerking

Cyberveilig Nederland is een groot voorstander van publiek-private samenwerking en van cybersecuritydienstverleners die zo veel mogelijk relevante informatie delen met de diensten, ten behoeve van de nationale veiligheid en de digitale weerbaarheid van Nederland. Juist omdat wij die actieve, vrijwillige informatiedeling willen aanmoedigen, willen wij voorkomen dat deze zich tegen de deelnemende dienstverlener keert.

Immers het wetsvoorstel positioneert de cybersecuritysector tegelijk als partner bij de nationale weerbaarheid en als potentiële bron van informatie en adressant van vorderingen: de artikelen 144 en 145 maken structurele publiek-private samenwerking mogelijk. Als de sector een cruciaal onderdeel is van de nationale cyberweerbaarheid, rechtvaardigt dat ook aandacht voor haar vertrouwenspositie binnen die samenwerking. Deze samenwerking omvat ook gegevensuitwisseling, gezamenlijke analyse en operationele ondersteuning.

Doordat de diensten via de samenwerking weten welke gegevens bij een dienstverlener voorhanden zijn, ontstaat het risico dat diezelfde kennis aanleiding is om die gegevens vervolgens te vorderen in plaats van verder vrijwillig te laten delen. Een dienstverlener die actief meewerkt aan publiek-private samenwerking zou daardoor per saldo niet slechter af moeten zijn dan een partij die dat niet doet; wij vragen de regering te verduidelijken wat de consequenties van deelname aan publiek-private samenwerking zijn in het licht van de vorderingsbevoegdheden.

De weging vooraf en de toestemming van de minister gelden bij structurele relaties waarbij de dienst persoonsgegevens verstrekt. De criteria voor bilaterale samenwerking (artikel 144, vierde lid: land van vestiging, doelstelling, professionaliteit en betrouwbaarheid, bijdrage aan de taakuitvoering) bieden weinig aanknopingspunt voor afspraken over de bescherming van bedrijfsvertrouwelijke informatie; bij multilaterale samenwerking noemt artikel 145, vierde lid, onder c, wel waarborgen over gegevensverwerking en informatiebeheer.

Voor een sector die draait op vertrouwen is het van belang dat samenwerking plaatsvindt op basis van vooraf kenbare en voorspelbare kaders, ontwikkelt in overleg met de sector zelf.

Onze vragen aan de regering

14. Is de regering bereid brancheorganisaties zoals Cyberveilig Nederland structureel te betrekken bij de generieke kaders en voorwaarden voor publiek-private samenwerking, vóór de vaststelling daarvan, en die generieke voorwaarden te publiceren?
15. Artikel 94 is volgens de toelichting bedoeld voor situaties waarin een mogelijk slachtoffer samenwerking weigert of niet tijdig levert. Hoe voorkomt de regering dat het weigeren van vrijwillige samenwerking (artikel 144 en 145) in de praktijk leidt tot een vordering, en dat de vrijwillige samenwerking daardoor onder druk komt te staan?
16. Kan de regering verduidelijken wat de consequenties zijn, in het licht van de vorderingsbevoegdheden van artikel 87 en 94, van deelname aan publiek-private samenwerking (artikel 144 en 145)? Is de regering bereid te bevestigen dat kennis die de diensten via zo'n samenwerking hebben verkregen over de bij een cybersecuritydienstverlener voorhanden gegevens, niet als zodanig aanleiding vormt voor een vordering, zodat vrijwillige deelname aan publiek-private samenwerking niet wordt ontmoedigd?

2. Hackbevoegdheid: de grens tussen positioneren en uitwinnen

Het binnendringen in geautomatiseerde werken (hacken) is geen nieuwe bevoegdheid; die bestond al onder artikel 45 Wiv 2017. Nieuw is de opdeling in drie fasen: binnendringen (artikel 76), positioneren en het treffen van voorbereidingen, ofwel het bestendigen van de toegang (artikel 77), en uitwinning, dat is het overnemen van gegevens en het aanbrengen van voorzieningen (artikel 78). De regering wil daarmee meer wendbaarheid in de eerste twee fasen, omdat de drempel voor toestemming onder de Wiv 2017 daarvoor te hoog werd bevonden.

Een voorafgaande toets door de afdeling toetsing van het college van toetsing en toezicht is alleen voorzien voor de derde fase (artikel 47, onder e). Voor binnendringen en positioneren volstaat toestemming van de minister; de toelichting zegt uitdrukkelijk dat de afdeling toetsing daar niet bij betrokken is. De gedachte is dat de inbreuk op de persoonlijke levenssfeer bij uitwinning het grootst is.

Ons punt is dat de grens tussen de tweede en de derde fase in de praktijk moeilijk te trekken is, terwijl van die grens afhangt of een voorafgaande toets plaatsvindt. Volgens de toelichting worden in de tweede fase geen gegevens ten behoeve van de inlichtingenanalyse verzameld, maar wel technische gegevens die nodig zijn om de positie te bestendigen. Artikel 77 staat verder toe dat het werk wordt onderzocht ten behoeve van de motivering van een verzoek om uitwinning; volgens de toelichting kan dat bestaan uit het inventariseren van de aanwezige gegevens. De toelichting erkent ook dat de fasen niet strikt na elkaar plaatsvinden en dat er gegevens kunnen worden verworven terwijl elders in het netwerk nog wordt gepositioneerd. Het onderscheid hangt daarmee sterk af van het doel van een handeling, en dat doel wordt door de dienst zelf gekwalificeerd. Wij vragen ons af hoe wordt voorkomen dat handelingen die in de kern neerkomen op het verzamelen van gegevens

onder de tweede fase worden geschaard, waarvoor geen voorafgaande toets nodig is. Wij erkennen dat de afdeling toezicht achteraf toezicht houdt op de rechtmatigheid (artikel 162), maar dat is een andere waarborg dan een voorafgaande toets.

Voor cybersecuritybedrijven speelt daarnaast een specifiek punt. Artikel 76 staat toe dat wordt binnengedrongen “door tussenkomst van het geautomatiseerd werk van een derde”. Onder een derde verstaat de toelichting onder meer een partij die een dienst, software of technische kennis levert, zoals een provider, tussenleverancier of dienstverlener. Ook een cybersecuritybedrijf kan zo’n derde partij zijn. Voor die route noemt de toelichting waarborgen: de derde is niet meer dan een doorgang, er mogen geen andere gegevens worden vergaard dan strikt noodzakelijk voor het binnendringen en de afdeling toezicht heeft een eigen oordeelsbevoegdheid (artikel 188, eerste lid, onder c). Die waarborgen worden genoemd bij artikel 76. Bij het positioneren (artikel 77), waartoe volgens de toelichting bijvoorbeeld het creëren van alternatieve toegangsroutes en het deactiveren van beveiligingsmaatregelen kan behoren, is niet duidelijk of dezelfde beperkingen gelden.

Onze vragen aan de regering

17. Op basis van welke objectieve criteria wordt bepaald of een handeling onder artikel 77 valt (bestendigen, onderzoeken, voorbereiden) of onder artikel 78, eerste lid, onder a (overnemen van gegevens)? Wie beoordeelt dat, en kan de afdeling toezicht of de afdeling toetsing dat onderscheid achteraf beoordelen?
18. Is de regering bereid ook het onderzoeken van een binnengedrongen werk ten behoeve van de motivering van een verzoek om uitwinning (artikel 77, eerste lid, onder b) aan een voorafgaande toets te onderwerpen, of anders te voorzien in een verplichte melding van de toepassing van artikel 77 aan de afdeling toezicht?
19. Is de regering bereid in de evaluatie (artikel 270) uitdrukkelijk te onderzoeken of het onderscheid tussen de fasen in de praktijk werkbaar is en niet leidt tot het verschuiven van handelingen naar fasen zonder voorafgaande toets?
20. Kan artikel 77 ook worden toegepast in het geautomatiseerd werk van de derde via wie is binnengedrongen, bijvoorbeeld bij een cybersecuritydienstverlener? Zo ja, gelden dan ook de beperkingen uit de toelichting bij artikel 76 (de derde is slechts een doorgang; geen andere gegevens dan strikt noodzakelijk) en de oordeelsbevoegdheid van de afdeling toezicht op grond van artikel 188, eerste lid, onder c?

Voorstel voor aangepaste tekst: wij geven in overweging aan artikel 77 een meldplicht aan de afdeling toezicht te verbinden voor de toepassing van deze bevoegdheid. Op deze manier is het gebruik ervan achteraf controleerbaar, ook als er geen aanleiding is voor een klacht. Dat biedt een waarborg die niet afhankelijk is van een sluitend afbakeningscriterium tussen de tweede en de derde fase, waarvan wij ons realiseren dat dit criterium – gelet op de door onszelf hierboven beschreven overlap tussen de fasen – lastig scherp te trekken zal zijn. Voor zover de regering toch een dergelijk

criterium wil vastleggen, geven wij in overweging dit in artikel 47 of de toelichting bij de artikelen 76 tot en met 78 te koppelen aan het feitelijk overnemen of raadplegen van de inhoud van gegevens.

3. Internationale gegevensdeling en economische veiligheid

Bij structurele samenwerking met buitenlandse diensten wegen de diensten onder meer de democratische inbedding, de mensenrechtensituatie, de professionaliteit en het niveau van gegevensbescherming van die dienst (artikel 138, derde lid). Dat is een waardevolle waarborg, maar zij gaat over de ontvangende dienst en niet over de belangen van de Nederlandse bedrijven van wie de gegevens oorspronkelijk afkomstig zijn. Artikel 141 staat bij een “zwaarwegende noodzaak” toe dat ook gegevens worden gedeeld met diensten waarmee geen samenwerkingsrelatie bestaat, of waarvoor de weging negatief uitviel. Voor die situatie gelden de criteria uit artikel 138 niet; vereist is toestemming van de minister, die niet kan worden gemandateerd (artikel 27, tweede lid, onder c). Overigens verwijst artikel 140, eerste lid, naar “artikel 140” zelf; bedoeld is vermoedelijk artikel 139.

De toelichting besteedt aandacht aan economische veiligheid en risicovolle strategische afhankelijkheden. Tegelijkertijd kan het wetsvoorstel ertoe leiden dat buitenlandse klanten terughoudender worden met het onderbrengen van gevoelige informatie bij Nederlandse cybersecuritybedrijven, dat Nederlandse aanbieders concurrentienadeel ondervinden ten opzichte van buitenlandse aanbieders en dat vragen ontstaan over internationale gegevensdeling en vertrouwelijkheid. Dat raakt ook de ambitie van Nederland om op het gebied van cybersecurity en digitale weerbaarheid een sterke positie te behouden.

Onze vragen aan de regering

21. Hoe worden bij internationale gegevensdeling de belangen van bedrijven meegewogen wanneer de gedeelde gegevens herleidbaar bedrijfsvertrouwelijke of technische beveiligingsinformatie bevatten, zowel binnen een samenwerkingsrelatie (artikel 140) als bij artikel 141? Welk toezicht is er specifiek op artikel 141?
22. Is onderzocht wat het wetsvoorstel betekent voor het vertrouwen van (buitenlandse) klanten in Nederlandse cybersecuritybedrijven en voor hun concurrentiepositie, gelet op de aandacht in de toelichting voor economische veiligheid?

4. Impactanalyse voor de cybersecuritysector

De bedrijfseffectentoets in hoofdstuk 16 van de toelichting is uitgevoerd voor onlineplatforms (artikel 87 tot en met 90), financiële ondernemingen (artikel 92) en de vorderingsbevoegdheid voor weerbaarheidsbelangen (artikel 94). Een specifieke analyse voor de categorie in artikel 87, eerste lid, onder c, waartoe cybersecuritydienstverleners kunnen behoren, ontbreekt. Voor artikel 94 verwacht de regering geen noemenswaardige effecten omdat het aantal vorderingen “zeer beperkt” zou blijven.

In de toets wijzen respondenten op reputatierisico's voor sectoren als geheel. De regering acht het niet voor de hand liggen dat reputatieschade zich voordoet, onder verwijzing naar de geheimhoudingsplicht en de strafbaarstelling van openbaarmaking. Ons punt is een ander: niet dat een individuele vordering openbaar wordt, maar dat de enkele wetenschap dat cybersecuritybedrijven onderworpen kunnen zijn aan geheime vorderingsplichten het klantvertrouwen structureel kan aantasten, ongeacht of een concreet geval ooit bekend wordt.

Onze vragen aan de regering

23. Is de regering bereid alsnog een specifieke bedrijfseffectentoets uit te voeren voor cybersecuritybedrijven en andere partijen onder artikel 87, eerste lid, onder c, en artikel 94, in overleg met de sector en voordat het wetsvoorstel bij de Tweede Kamer wordt ingediend?
24. Hoeveel vorderingen op grond van artikel 94 verwacht de regering, en hoe wordt dat gemonitord? Is zij bereid jaarlijks geaggregeerde, geanonimiseerde cijfers te publiceren over het aantal vorderingen op grond van artikel 87, eerste lid, onder c, en artikel 94, uitgesplitst naar sector, en over het aantal keer dat gegevens die mede afkomstig zijn van Nederlandse bedrijven internationaal zijn gedeeld (artikel 140 en 141)?
25. Is de regering bereid de effecten op het vertrouwen in en de concurrentiepositie van de Nederlandse cybersecuritysector als zelfstandig element op te nemen in de evaluatie op grond van artikel 270, en de sector daarbij te betrekken?

Samenvatting: waarop wij een reactie vragen

Cyberveilig Nederland onderschrijft de noodzaak van effectieve inlichtingen- en veiligheidsdiensten. Het wetsvoorstel maakt de Nederlandse cybersecuritysector echter mogelijk tot een voor de hand liggende geadresseerde van verstrekende vorderingsbevoegdheden, zonder dat het belang van de vertrouwensrelatie tussen organisaties en hun cybersecuritypartner in de wet of toelichting wordt erkend. Dat kan op termijn juist het vertrouwen ondermijnen waarop digitale weerbaarheid, en daarmee nationale veiligheid, is gebouwd. Onze belangrijkste vragen:

- **Reikwijdte:** vallen cybersecuritydienstverleners onder artikel 87, eerste lid, onder c, en artikel 94? Wij vragen om schriftelijke bevestiging tijdens de behandeling en om verduidelijking van artikel 91, derde lid, en artikel 233 (vragen 1 tot en met 6).
- **Primaire bron:** waarom geldt het principe “eerst de minst ingrijpende route” wel bij hacken via een derde, maar niet bij vorderingen aan derden (vragen 7 tot en met 11)?
- **Waarborgen:** herkent de regering de door ons voorgestelde operationele waarborgen tijdens en na een vordering als een werkbare invulling van subsidiariteit en proportionaliteit, en is zij bereid deze te verankeren, en hoe verhoudt de verzoekroute van artikel 63 zich daartoe (vragen 12 en 13)?

- **Samenwerking:** hoe worden brancheorganisaties betrokken bij publiek-private kaders, hoe wordt voorkomen dat weigering van vrijwillige samenwerking leidt tot een vordering, en hoe wordt voorkomen dat deelname aan publiek-private samenwerking cybersecuritydienstverleners eerder tot geadresseerde van een vordering maakt (vragen 14, 15 en 16)?
- **Hackbevoegdheid:** hoe wordt voorkomen dat handelingen in de tweede fase (positioneren) in de praktijk gegevens verzamelen zonder voorafgaande toets, ook in systemen van cybersecuritybedrijven als “derde” (vragen 17 tot en met 20)?
- **Internationaal:** hoe worden bedrijfsbelangen en economische veiligheid meegewogen bij gegevensdeling met buitenlandse diensten (vragen 21 en 22)?
- **Impact:** is de regering bereid alsnog een specifieke bedrijfseffectentoets uit te voeren, jaarlijks geaggregeerde cijfers te publiceren en sectorvertrouwen mee te nemen in de evaluatie (vragen 23 tot en met 25)?

Cyberveilig Nederland denkt graag actief mee over de beantwoording van deze vragen en is beschikbaar voor nadere toelichting, technische duiding vanuit de sector of overleg met de betrokken ministeries.