Internet Society
Netherlands Chapter

Reactie van Internet Society Nederland op de internetconsultatie over de Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten (Wbnv)

Aan: de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie
Datum: 11 oktober 2026
Betreft: internetconsultatie conceptwetsvoorstel Wbnv

Geachte heer/mevrouw,

Internet Society Nederland ("ISOC NL"), vereniging met volledige rechtsbevoegdheid en statutair gevestigd te Amsterdam, reageert hierbij op de internetconsultatie over het conceptwetsvoorstel Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten (Wbnv). I**SOC NL stemt in met openbare publicatie van deze reactie.**

Opbouw van deze reactie

Deze reactie bestaat uit drie delen:

- **Deel A — Samenvatting en aanbevelingen.** Hier staat in gewone taal wie wij zijn, wat onze boodschap is, wat goed is aan het voorstel en wat wij aanbevelen. Bij elke aanbeveling staat in welke paragraaf van Deel B de toelichting staat.
- **Deel B — Toelichting.** Hier lichten wij onze aanbevelingen uitgebreider toe:
  - In de paragrafen 1 tot en met 3 beschrijven wij wie wij zijn, welk toetsingskader wij gebruiken en wat wij eerder over dit onderwerp hebben gezegd.
  - In de paragrafen 4 tot en met 12 bespreken wij per onderwerp de artikelen van het wetsvoorstel. Het gaat om de onderbouwing van nieuwe bevoegdheden, versleuteling, hacken, aftappen en decentrale diensten, digitale onafhankelijkheid, bulkgegevens, AI, toezicht en een internettoets.
  - Paragraaf 13 bevat ons slot.
- **Referenties.** Aan het einde staan alle bronnen met hun webadres. In de tekst verwijzen wij daarnaar met een nummer tussen vierkante haken, zoals [1].

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

DEEL A — SAMENVATTING EN AANBEVELINGEN

Wie wij zijn

De Internet Society werd in 1992 opgericht door Vint Cerf en Bob Kahn, twee van de grondleggers van het internet. Zij is de moederorganisatie van de IETF, die de technische standaarden van het internet maakt. De Internet Society heeft wereldwijd ruim 187.000 leden en 126 afdelingen en themagroepen. Daarnaast zijn 82 organisaties lid.

Internet Society Nederland (ISOC NL) is sinds 1997 de Nederlandse afdeling. Wij zijn een zelfstandige vereniging met zo'n duizend leden. Zij komen uit de internetsector, het bedrijfsleven, de overheid, de wetenschap en maatschappelijke organisaties. Deze reactie geven wij namens ISOC NL, niet namens de wereldwijde Internet Society. Wel gebruiken wij haar internationale toetsingskader.

Onze boodschap in het kort

Nederland heeft sterke inlichtingen- en veiligheidsdiensten nodig. Daar zijn wij het mee eens. Maar een veilig Nederland heeft ook een veilig internet nodig. Het wetsvoorstel let daar te weinig op.

Wij hebben het voorstel getoetst met de *Internet Way of Networking*. Dat kader van de Internet Society is gebaseerd op tientallen jaren ervaring met de bouw van het internet. Ook hebben wij de officiële stukken bij de consultatie gelezen.

Onze conclusie: het voorstel kan het internet op een aantal punten onveiliger maken. Ook kan het Nederland afhankelijker maken van een paar grote buitenlandse techbedrijven. Dat is niet nodig. Met gerichte aanpassingen wordt de wet beter, zonder dat de diensten minder slagkracht krijgen.

Wat goed is

Er staan ook goede waarborgen in het voorstel:

- Bedrijven hoeven hun versleuteling niet zwakker te maken als de diensten hulp vragen bij het ontsleutelen (artikel 95).
- Bedrijven die moeten meewerken, hebben recht op vergoeding van hun kosten (artikel 93).
- De bewaartermijn voor gegevens uit grootschalig aftappen kan niet worden verlengd (artikel 108).
- De diensten starten geen onderzoek naar iemand alleen op basis van uitkomsten van een computer (artikel 36).

Op die waarborgen bouwen wij voort.

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

Onze aanbevelingen

1. **Verbied het verzwakken van versleuteling bij álle verplichtingen.** Artikel 95 regelt dit nu alleen bij hulp bij ontsleutelen. Laat het ook gelden bij hulp bij aftappen en bij het opvragen van gegevens. Sluit ook het scannen van berichten op apparaten uit. *(paragraaf 5)*
2. **Houd hacken controleerbaar.** Laat een onafhankelijke toezichthouder vooraf toetsen voordat de diensten via de computer van een ander binnendringen, of in apparatuur van het netwerk zelf. Laat de diensten weer opschrijven welke technische risico's zij nemen en of zij onbekende zwakke plekken gebruiken. *(paragraaf 6)*
3. **Zorg dat aftappen het internet niet onveiliger maakt.** Toets technische voorzieningen bij internetbedrijven vooraf op veiligheid. Maak duidelijk dat platforms niet zomaar nieuwe functies hoeven te bouwen om gebruikers live te volgen. *(paragraaf 7)*
4. **Houd ruimte voor kleine en decentrale diensten.** Onderzoek of kleine aanbieders, open source-projecten en het fediverse aan de eisen kunnen voldoen zonder hun techniek te veranderen. *(paragraaf 7)*
5. **Bescherm de digitale onafhankelijkheid van Nederland.** Kijk bij samenwerking met bedrijven ook naar de buitenlandse wetten die voor hen gelden. *(paragraaf 8)*
6. **Leg uit waarom elke nieuwe bevoegdheid nodig is.** Laat per bevoegdheid zien of die werkt en welke waarborgen veranderen. *(paragraaf 4)*
7. **Bewaar zo min mogelijk gegevens.** Stel een harde maximale bewaartermijn vast, ook voor versleutelde gegevens. *(paragraaf 9)*
8. **Toets AI op het gebruik, niet op hoe gewoon de techniek is.** *(paragraaf 10)*
9. **Zorg voor technisch sterk toezicht.** Leg in de wet vast dat de nieuwe toezichthouder eigen technische experts heeft. *(paragraaf 11)*
10. **Voer een internettoets in.** Kijk bij nieuwe technische bevoegdheden eerst kort naar de gevolgen voor het internet. Zijn er risico's, doe dan een volledige toets. *(paragraaf 12)*

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

DEEL B — TOELICHTING

Verwijzingen tussen vierkante haken verwijzen naar de referentielijst aan het einde. Artikelnummers verwijzen naar de consultatieversie van het wetsvoorstel [1]. Paginanummers bij de memorie van toelichting verwijzen naar de consultatieversie [2].

1. Over de Internet Society en ISOC NL

De Internet Society (ISOC) werd in 1992 opgericht door Vint Cerf en Bob Kahn, twee van de grondleggers van het internet [9]. ISOC is de moederorganisatie van de Internet Engineering Task Force (IETF), waar de open technische standaarden van het internet worden ontwikkeld, en van verwante organen zoals de Internet Architecture Board (IAB) [11][13]. De Internet Society telt wereldwijd 187.078 leden, 126 chapters en special interest groups (SIG's) en 82 organisatieleden [10]. In 2025 was zij actief in 150 landen en gebieden [12].

Internet Society Nederland is de Nederlandse afdeling ('chapter') van de Internet Society en daarmee onderdeel van deze internationale niet-gouvernementele organisatie [13]. ISOC NL is een zelfstandige vereniging, opgericht op 24 november 1997 [28]. Wie lid is van ISOC NL, is ook lid van de wereldwijde Internet Society [14].

ISOC NL brengt zo'n duizend leden samen uit onder meer de internetsector, het bedrijfsleven, de overheid, de wetenschap en het maatschappelijk middenveld [13]. Het werk krijgt mede vorm in werkgroepen, waaronder de Coalitie Eerlijk Digitaal Onderwijs (CEDO) en de ISOC NL ThinkTank [33].

Deze reactie is opgesteld door het bestuur van ISOC NL, met inbreng uit de werkgroepen. Zij is ingediend namens ISOC NL en niet namens de wereldwijde Internet Society, net als onze reactie op de Wiv in 2015 [29]. Wel baseren wij ons op de internationale kaders van de Internet Society.

ISOC NL onderschrijft dat Nederland slagvaardige inlichtingen- en veiligheidsdiensten nodig heeft, zeker gelet op de dreiging van statelijke actoren. De vraag is daarom niet óf de diensten bevoegdheden nodig hebben. De vraag is hoe de nationale veiligheid kan worden versterkt zonder de technische voorwaarden aan te tasten die het internet zelf veilig en betrouwbaar maken.

De rechtsstatelijke aspecten zijn uitvoerig belicht door onder meer de CTIVD en de TIB [7][8] en de Nederlandse orde van advocaten. Wij richten ons op de gevolgen voor het internet als technische infrastructuur. Daarvoor hebben wij de stukken bij de consultatie bestudeerd: het wetsvoorstel [1], de memorie van toelichting [2], de bedrijfseffectentoets [3], het beleidskompasformulier [4], de Engelstalige toelichting [5] en de infographic [6].

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

2. Beoordelingskader: de Internet Way of Networking

ISOC NL beoordeelt het wetsvoorstel aan de hand van de *Internet Way of Networking* (IWN) van de Internet Society [15]. De IWN is geen nieuwe theorie. Het kader vat de ontwerpprincipes samen waarop het internet vanaf het begin functioneert, en die de technische internetgemeenschap in tientallen jaren heeft ontwikkeld en beproefd [16].

Het kader bouwt voort op:

- het end-to-end-principe uit 1984 [16];
- de "Internet Invariants" die de Internet Society in 2012 formuleerde, waaronder *permissionless innovation*: vernieuwing zonder voorafgaande toestemming [18].

In 2020 zijn deze principes uitgewerkt tot vijf kritieke eigenschappen [16][17]:

1. een toegankelijke infrastructuur met een gemeenschappelijk protocol;
2. een open architectuur van interoperabele en herbruikbare bouwstenen;
3. decentraal beheer en één gedistribueerd routeringssysteem;
4. gemeenschappelijke, wereldwijd eenduidige identificatoren (IP-adressen en domeinnamen);
5. een technologieneutraal netwerk voor algemene doeleinden.

Daarnaast onderscheidt de Internet Society vier doelen: een internet dat open, wereldwijd verbonden, veilig en betrouwbaar is [15][19]. Met de bijbehorende *Internet Impact Assessment Toolkit* (IIAT) kan systematisch worden onderzocht of een maatregel deze eigenschappen en doelen ondersteunt of aantast [20].

Toegepast op de Wbnv zijn vooral de eigenschappen 1, 2, 3 en 5 en de doelen "veilig" en "betrouwbaar" in het geding. Wij stellen niet dat iedere bevoegdheid deze eigenschappen daadwerkelijk aantast. Wel stellen wij vast dat de gevolgen voor het internet niet afzonderlijk zijn onderzocht (zie paragraaf 12).

Lessen uit de praktijk

De principes achter de IWN hebben hun waarde in de praktijk bewezen, juist waar de nationale veiligheid op het spel stond:

- **Verenigde Staten (2024).** Bij de spionagecampagne Salt Typhoon drongen aan China gelieerde actoren binnen bij ten minste acht Amerikaanse telecombedrijven. Daarbij kregen zij ook toegang tot de systemen voor door de rechter bevolen interceptie. FBI en CISA adviseerden Amerikanen vervolgens versleutelde diensten te gebruiken [23]. De verplichte aftapvoorziening werd zelf het aanvalsoppervlak; versleuteling bood bescherming.

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

- **Oekraïne (sinds 2022).** Oekraïne had een ongewoon gedecentraliseerde internetarchitectuur, met relatief veel autonome netwerken [24]. Overheid en telecomsector noemen die decentralisatie een belangrijke reden dat het internet de oorlog heeft doorstaan [25].
- **Verenigd Koninkrijk (2025).** Na een bevel van de Britse overheid stopte Apple met zijn geavanceerde end-to-end-versleuteling van clouddata voor Britse gebruikers [26]. De maatregel leidde niet tot meer veiligheid, maar tot minder bescherming voor Britse burgers.
- **Nederland (2016).** Het kabinet stelde vast dat encryptie niet in algemene zin kan worden verzwakt zonder de veiligheid van digitale systemen te schaden. In 2021 bevestigde het kabinet dit standpunt en gaf het aan een verbod op encryptie niet te zullen steunen [27].

3. Continuïteit met eerdere standpunten van ISOC NL

- **Internetwitboek 2002–2006 [28].** Versleuteling hoort de norm te zijn, "zoals iedereen nu een envelop om een brief doet". ISOC NL wees sleutelbewaring (key escrow) en sleutelherstel (key recovery) door derden af.
- **Consultatiereactie Wiv, 28 augustus 2015 [29].** ISOC NL vroeg eerst de noodzaak en effectiviteit van ruimere bevoegdheden aan te tonen. Zij waarschuwde tegen het hacken via systemen van onschuldige derden en tegen het benutten van onbekende kwetsbaarheden. De categorie 'aanbieders van een communicatiedienst' noemde zij "in principe grenzeloos".
- **Oproep tot uitstel van de Wiv 2017, 18 oktober 2017 [30].** Samen met een brede coalitie vroeg ISOC NL de wet pas na het referendum in te voeren.
- **Open brief over client-side scanning, september 2024 [31].** ISOC NL waarschuwde dat het scannen van berichten op apparaten end-to-end-versleuteling ondermijnt.
- **Consultatiereactie Nota Frequentiebeleid, september 2026 [32].** ISOC NL stelde een gerichte internettoets voor bij belangrijke keuzes over digitale infrastructuur, uitdrukkelijk zonder zware nieuwe procedure voor elk besluit.

4. Van Wiv 2017 naar Wbnv: verantwoording van opeenvolgende verruimingen

Bij het raadgevend referendum van 21 maart 2018 stemden meer kiezers tegen de Wiv 2017 dan voor. Het kabinet kondigde daarop enkele aanscherpingen aan, waarna de wet per 1 mei 2018 in werking trad [34]. Sinds 1 juli 2024 geldt de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma [2, p. 13].

De Wbnv zet volgens de regering als "dreigingsgerichte" wet de koers van die tijdelijke wet voort. Zij noemt daarbij vooral de dreiging van landen als Rusland, China en Iran [5]. Volgens het beleidskompasformulier worden onder meer:

- de toestemmingstermijnen verlengd;

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

- de mogelijkheden voor mandaatverlening uitgebreid;
- de toets vooraf geschrapt bij "enkele lichte bevoegdheden (bijv. verkennen bij hacken)" [4].

De standaardtermijn voor toestemming gaat van in de meeste gevallen drie maanden onder de Wiv 2017 [2, p. 211] naar zes maanden, steeds verlengbaar (artikel 40).

Opvallend is dat de regering de koers van de Tijdelijke wet permanent maakt, terwijl de ministers zelf vaststellen dat er nog "geen compleet beeld" is van wat die wet in de praktijk betekent. Er kan volgens hen "nog geen sluitend antwoord" worden gegeven op de vraag of het doel is bereikt [2, p. 13].

ISOC NL neemt de dreigingen serieus. Een veranderend dreigingsbeeld vermindert echter niet de noodzaak van een zorgvuldige onderbouwing; het vergroot die. De CTIVD en de TIB constateerden op 9 september 2026 dat bevoegdheden worden verruimd, "terwijl de daarbij behorende waarborgen niet worden versterkt en op onderdelen juist worden verminderd" [7]. ISOC NL deelt die zorg.

Wij verzoeken de regering:

- per wezenlijke verruiming de noodzaak en de aangetoonde effectiviteit te onderbouwen, mede op basis van de ervaringen met de Tijdelijke wet;
- per bevoegdheid inzichtelijk te maken welke waarborgen behouden blijven, welke wijzigen en welke vervallen;
- toe te lichten hoe de lessen uit het referendum en de eerdere parlementaire behandeling zijn verwerkt;
- de kritiek van de CTIVD en de TIB afzonderlijk en inhoudelijk te beantwoorden.

5. Versleuteling (artikelen 70 en 95)

IWN: eigenschap 2. Doelen: veilig en betrouwbaar.

Sterke versleuteling beschermt overheid, bedrijven, onderwijs- en zorginstellingen, vitale infrastructuur en burgers tegen spionage en criminaliteit. Zij is daarmee zelf een voorwaarde voor nationale veiligheid. De Internet Society concludeerde in juni 2026 dat iedere opzettelijke verzwakking van versleuteling, ongeacht het doel, systemische kwetsbaarheden creëert die niet tot specifieke doelwitten kunnen worden beperkt [22].

ISOC NL waardeert dat het voorstel hierover een uitdrukkelijke waarborg bevat. Volgens artikel 95, eerste lid, ziet een opdracht tot medewerking bij ontsleutelen "niet op het inbouwen van het afzwakken van de versleuteling van de systemen of op het inbouwen van toegang tot de systemen om ontsleutelde gegevens te verkrijgen". De toelichting voegt toe dat er "geen enkele verplichting" is voor aanbieders om hun encryptie te verzwakken [2, p. 102 en 277].

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

Deze waarborg is echter beperkt:

- Zij geldt alleen voor ontsleutelopdrachten op grond van artikel 95. Zij geldt niet voor de medewerking bij interceptie en de daarvoor getroffen technische voorzieningen (artikel 86), het vorderen van opgeslagen of realtime gegevens (artikelen 87–90) en de nieuwe vorderingsbevoegdheid van artikel 94.
- Zij noemt het verzwakken van versleuteling en het inbouwen van toegang. Andere vormen van uitzonderlijke toegang noemt zij niet, zoals het scannen van berichten op het apparaat vóór versleuteling (client-side scanning), het ongemerkt toevoegen van een extra deelnemer aan versleutelde communicatie, of sleutelbewaring en -herstel door derden.

Wij verzoeken de wetgever:

- de waarborg uit artikel 95, eerste lid, op te nemen als algemene norm in hoofdstuk 3, die geldt voor alle verplichtingen en vorderingen op grond van deze wet;
- daarin ook client-side scanning, verborgen deelnemers en sleutelbewaring of -herstel door derden uit te sluiten;
- te verduidelijken dat ook publiek-private samenwerking (artikelen 144–145) niet mag leiden tot het verzwakken van versleuteling of het inbouwen van verborgen toegang.

Dit sluit aan bij het Internetwitboek [28] en bij onze open brief over client-side scanning [31]. Voor de bewaring van versleutelde gegevens: zie paragraaf 9.

6. Hacken en kwetsbaarheden (artikelen 76–78 en 80)

IWN: eigenschappen 2 en 3. Doelen: veilig en betrouwbaar.

De hackbevoegdheid omvat het binnendringen in een geautomatiseerd werk, "al dan niet door tussenkomst van het geautomatiseerd werk van een derde". Daaronder valt ook "het doorbreken van enige beveiliging" (artikel 76, eerste en tweede lid). Het begrip geautomatiseerd werk omvat volgens de toelichting onder meer servers, modems, routers, clouddiensten en industriële systemen [2, p. 72]. Het gaat dus ook om de infrastructuur waarop het internet zelf draait.

Twee wijzigingen baren ISOC NL zorgen.

Geen toets vooraf bij het binnendringen. Drie bevoegdheden vallen niet onder de bindende toets vooraf van artikel 47:

- het verkennen en binnendringen (artikel 76);
- het positioneren in een binnengedrongen systeem (artikel 77);
- het onderzoek aan communicatienetwerken (artikel 80).

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

Alleen de uitwinning van gegevens (artikel 78) wordt vooraf getoetst [2, p. 73]. Het binnendringen via het systeem van een derde valt wel onder bindend toezicht tijdens of na de inzet (artikel 188, eerste lid, onder c), maar niet onder de toets vooraf. In het nieuwe regime voor aangewezen organisaties vervalt bovendien de toets per inzet voor vrijwel alle bijzondere bevoegdheden; alleen de aanwijzing wordt vooraf getoetst (artikelen 57 en 58, vijfde lid) [4][5].

Geen uitdrukkelijke vermelding meer van technische risico's en onbekende kwetsbaarheden. Onder de Wiv 2017 moest een toestemmingsverzoek voor hacken de technische risico's vermelden. Dat vereiste vervalt, ook voor "het gebruik van onbekende kwetsbaarheden", omdat het "dubbelop" zou zijn met het algemene afwegingskader [2, p. 73–74].

Vanuit het perspectief van internetveiligheid is het binnendringen geen lichte bevoegdheid. Juist in die fase wordt beveiliging doorbroken, mogelijk via systemen van onschuldige derden. Er worden kwetsbaarheden benut die ook door criminelen en statelijke actoren kunnen worden misbruikt, zolang ze niet zijn gerepareerd. Schade aan systemen van derden en aan de netwerkveiligheid is achteraf vaak niet te herstellen.

ISOC NL waarschuwde hier in 2015 al voor [29]. De Internet Society rekent het gebruik van onbekende kwetsbaarheden tot de maatregelen die de technische fundamenten van het internet aantasten [22].

Wij verzoeken de wetgever:

- het binnendringen via systemen van derden en het binnendringen in netwerkinfrastructuur, zoals routers en servers van aanbieders, onder de bindende toets vooraf van artikel 47 te brengen;
- het vereiste te behouden dat een toestemmingsverzoek de technische risico's vermeldt, inclusief het gebruik van onbekende kwetsbaarheden, zodat het college deze kan beoordelen;
- een wettelijk kader op te nemen voor het melden van door de diensten ontdekte of gebruikte kwetsbaarheden, met melden als uitgangspunt en toezicht door het college.

7. Aftappen, medewerking van aanbieders en decentrale diensten (artikelen 81–93)

IWN: eigenschappen 1, 2, 3 en 5.

Een wezenlijke eigenschap van het internet is dat iedereen nieuwe diensten kan ontwikkelen zonder voorafgaande toestemming van een centrale partij [16][18]. Daardoor bestaan er alternatieven voor grote centrale platforms:

- het fediverse;
- open source-software;

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

- zelfbeheerde diensten;
- open en onafhankelijke digitale leeromgevingen in het onderwijs.

Reikwijdte. De medewerkingsplicht bij interceptie (artikel 86) geldt voor iedere "aanbieder van een communicatiedienst". Dat is iedereen die "in de uitoefening van een beroep of bedrijf" gebruikers laat communiceren via een geautomatiseerd werk, of gegevens verwerkt of opslaat voor zo'n dienst (artikel 1). Deze definitie is ongewijzigd overgenomen uit de Wiv 2017 [2, p. 212]. ISOC NL noemde deze categorie in 2015 al "in principe grenzeloos" [29].

De verstrekkingsplichten worden nu uitgebreid naar onlineplatforms (artikelen 87–91). Dat geldt ook voor realtime verkeers- en locatiegegevens, de zogeheten "stomme tap" (artikel 89) [2, p. 273]. De regering maakt daarbij bewust geen onderscheid naar bedrijfsgrootte, anders dan de Digital Services Act [2, p. 212]. Volgens de bedrijfseffectentoets is ongeveer vier op de vijf onlineplatforms in Nederland een microbedrijf met minder dan tien werkzame personen [3, p. 10].

Technische voorzieningen. Voor bulkinterceptie geldt een toestemming van maximaal een jaar die steeds kan worden verlengd (artikel 82, tweede lid). Aanbieders moeten de technische voorzieningen bovendien nog een jaar na afloop van de toestemming in stand houden (artikel 86, zesde lid).

Zulke voorzieningen kunnen een extra aanvalsoppervlak vormen. Hoe groot dat risico is, hangt af van ontwerp, toegangsbeveiliging en beheer. Dat het risico reëel is, bleek bij Salt Typhoon [23]. De toelichting op artikel 86 gaat niet in op de beveiliging van deze voorzieningen [2, p. 271]. Positief is dat de bevoegdheid pas wordt uitgeoefend na overleg met de aanbieder (artikel 86, vierde lid).

Realtime gegevens bij platforms. De bedrijfseffectentoets stelt vast dat onlineplatforms "momenteel niet [beschikken] over functionaliteiten om realtime gegevens te verzamelen", en dat handmatige afhandeling "buitenproportioneel veel tijd" vraagt. De kosten konden daarom niet worden gekwantificeerd [3, p. 36].

De toets waarschuwt dat een ongelijk speelveld kan ontstaan als sommige platforms "hun systemen en functionaliteiten moeten aanpassen" [3, p. 23]. Ook wijst zij op mogelijke markteffecten als "bedrijven nieuwe functionaliteiten moeten ontwikkelen zonder dat deze kosten volledig worden vergoed" [3, p. 38].

Het beleidskompasformulier concludeert dat de uitkomsten van de bedrijfseffectentoets "niet om aanpassingen van het wetsvoorstel" vragen [4]. ISOC NL ziet dat anders. Het inbouwen van nieuwe realtime volgfuncties in platforms is een ontwerpkeuze met gevolgen voor veiligheid en architectuur. Die keuze verdient een toets vooraf.

Kosten. ISOC NL waardeert dat aanbieders die moeten meewerken bij interceptie "naar redelijkheid" aanspraak hebben op vergoeding van investerings-, exploitatie- en onderhoudskosten (artikel 93,

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

tweede lid) [2, p. 276]. Een deel van de platforms geeft in de bedrijfseffectentoets echter aan dat een aanvraag "meer tijd kost dan het financieel oplevert" [3, p. 36]. Voor kleine aanbieders weegt dat zwaar.

Wij verzoeken de wetgever:

- vast te leggen dat technische voorzieningen de veiligheid en integriteit van netwerken en diensten niet mogen verminderen, en dat het overleg van artikel 86, vierde lid, ook de beveiliging van die voorzieningen omvat;
- te verduidelijken dat artikel 89 aanbieders niet verplicht om nieuwe realtime volgfuncties te bouwen, of zo'n verplichting alleen op te leggen na een internettoets (paragraaf 12) en met volledige kostenvergoeding;
- te onderzoeken of kleine, federatieve en decentrale aanbieders aan de verplichtingen kunnen voldoen zonder hun architectuur of beveiligingsmodel wezenlijk te wijzigen;
- eisen functioneel en technologieneutraal te formuleren;
- de kostenvergoeding van artikel 93 eenvoudig en volledig te maken, zodat zij ook voor kleine aanbieders werkt.

8. Digitale onafhankelijkheid (artikelen 87–91 en 144–145)

De regering stelt zelf dat "de afhankelijkheid van de private sector voor de instandhouding van publieke diensten" toeneemt. Samenwerking is volgens haar nodig om "de soevereiniteit van Europese digitale systemen te behouden" [2, p. 137–138]. De diensten richten zich bovendien op "het tegengaan van risicovolle strategische afhankelijkheden" [2, p. 17]. ISOC NL onderschrijft dat. Juist daarom moet de wet zelf geen nieuwe afhankelijkheden scheppen.

De grootste platforms, cloud- en communicatiediensten zijn overwegend in handen van niet-Europese bedrijven. De toelichting noemt als voorbeeld van publiek-private samenwerking het samen met Microsoft onderkennen van een Russische cyberactor [2, p. 138]. Zulke samenwerking kan waardevol zijn.

Kunnen alleen grote partijen aan zware technische eisen voldoen, dan kan de wet de afhankelijkheid van een klein aantal buitenlandse aanbieders vergroten. Dat risico bestaat ongeacht hun opstelling:

- **Werken zij mee?** Dan raakt de Nederlandse veiligheid verweven met bedrijven die onder buitenlandse jurisdictie vallen.
- **Weigeren zij?** Dan bepalen zij welk beveiligingsniveau Nederlandse gebruikers nog krijgen, zoals het Britse voorbeeld laat zien [26].

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

Hoe snel een buitenlands besluit doorwerkt, bleek in augustus 2026. Na een Amerikaanse sanctie tegen een Italiaanse internetaanbieder werd binnen twee dagen de domeinnaam geblokkeerd. Later beëindigde ook de bank de relatie. ISOC NL stuurde hierover op 17 september 2026 met 27 andere organisaties een brief aan de Tweede Kamer en het kabinet [33].

De weging voor structurele publiek-private samenwerking kijkt al naar "het land van vestiging" van de partij (artikel 144, vierde lid, onder a). Dat is een goed vertrekpunt. Maar ook een in Nederland gevestigde onderneming kan onder buitenlandse wetgeving met extraterritoriale werking vallen.

Wij verzoeken de wetgever:

- aan de wegingscriteria van artikel 144, vierde lid, toe te voegen: de toepasselijke buitenlandse wetgeving, waaronder wetgeving met extraterritoriale werking en sanctieregimes, en de afhankelijkheidsrisico's van de samenwerking;
- een herweging voor te schrijven wanneer die buitenlandse wetgeving wijzigt, naast het voorbeeld van een overname dat de toelichting al noemt [2, p. 140];
- te onderzoeken of de verplichtingen de afhankelijkheid van een klein aantal (buitenlandse) aanbieders vergroten, en of Europese en decentrale alternatieven aan de eisen kunnen voldoen.

Digitale onafhankelijkheid gaat niet alleen over eigendom van infrastructuur. Het gaat ook over de beschikbaarheid van alternatieven en de mogelijkheid om over te stappen [32].

9. Bulkgegevens en bewaartermijnen (artikelen 105–108)

Doelen: veilig en betrouwbaar.

De wet omschrijft bulkgegevens zelf als gegevens over "een zeer groot aantal personen waarvan het merendeel van de personen geen onderwerp van onderzoek van een dienst is en dat ook niet zal worden" (artikel 1). Zulke verzamelingen zijn bovendien een aantrekkelijk doelwit voor buitenlandse diensten en criminelen. Dataminimalisatie is daarom ook een veiligheidsvoorwaarde. De CTIVD en de TIB plaatsen eveneens vraagtekens bij de verwerking van bulkgegevens [7].

Het voorstel kent:

- een bewaartermijn van drie jaar, die "steeds" met ten hoogste drie jaar kan worden verlengd (artikel 105, eerste lid);
- voor versleutelde bulkgegevens drie jaar om de versleuteling te doorbreken, eveneens steeds verlengbaar (artikel 105, vierde lid) [2, p. 283];
- bij algemene maatregel van bestuur aangewezen categorieën die "geen specifieke bewaartermijn" kennen (artikel 107) [2, p. 284].

 | e-mail: bureau@isoc.nl . Koninklijke Bibliotheek, Prins Willem-Alexanderhof 5 (kamer i4.301) . 2595 BE Den Haag . Nederland |

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

Positief is:

- de bewaartermijn voor bijzondere bulkgegevens, waaronder gegevens uit bulkinterceptie, kan niet worden verlengd (artikel 108, tweede lid);
- bij elke verlenging moet worden beoordeeld of gegevens kunnen worden verwijderd (artikel 106);
- het college kan bindend oordelen over de toepassing van de artikelen 105 en 107 (artikel 188).

De regeling voor versleutelde gegevens verdient bijzondere aandacht. Zij maakt het mogelijk versleutelde communicatie langdurig te bewaren tot de versleuteling kan worden doorbroken ("nu verzamelen, later ontsleutelen"). Daarmee raakt de wet aan de vertrouwelijkheid van communicatie die vandaag als veilig geldt.

Wij verzoeken de wetgever:

- een absolute maximale bewaartermijn vast te leggen, ook voor versleutelde bulkgegevens;
- te verduidelijken of het verlengingsverbod van artikel 108, tweede lid, ook geldt voor de termijn van artikel 105, vierde lid;
- de aanwijzing van categorieën onder artikel 107 vooraf aan het college voor te leggen;
- een onafhankelijk controleerbare verwijderplicht op te nemen.

10. Algoritmen en AI (artikelen 32–37)

Doel: betrouwbaar.

ISOC NL waardeert dat het voorstel een eigen kader voor automatisering bevat, met een betrouwbaarheidsonderzoek vóór ingebruikname van risicotoepassingen (artikel 34) en een gedeeltelijk verbod op volledige automatisering (artikel 36).

Volgens artikel 33, tweede lid, is een toepassing echter "geen risicotoepassing" als het gebruik ervan "in het maatschappelijk verkeer gebruikelijk is". De toelichting noemt als voorbeelden zoekmachines, "ingeburgerde AI-toepassingen", routeplanners en een Large Language Model dat teksten vertaalt en samenvat. Zij verwacht dat dit "een levende categorie" wordt die groeit naarmate de technologie zich ontwikkelt [2, p. 42].

Daardoor kan een groeiend deel van de AI-toepassingen buiten de waarborgen vallen, zonder nieuwe wettelijke of onafhankelijke beoordeling. Ook de CTIVD en de TIB plaatsen vraagtekens bij het gebruik van automatisering, zoals AI [7].

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

Dat een techniek maatschappelijk gangbaar is, zegt weinig over haar betrouwbaarheid in een inlichtingencontext. Een taalmodel dat in het dagelijks leven een tekst samenvat, kan bij de analyse van onderschepte communicatie fouten maken met ingrijpende gevolgen voor betrokkenen.

Wij verzoeken de wetgever:

- de uitzondering van artikel 33, tweede lid, niet te laten gelden voor toepassingen op gegevens die met bijzondere bevoegdheden zijn verzameld of op bulkgegevens;
- het risico te laten bepalen door de inzet en de gevolgen, niet door de gangbaarheid van de techniek;
- de ingebruikname van risicotoepassingen (artikel 34, tweede lid) en de toepassing van artikel 33, tweede lid, onder het bindende toezicht van artikel 188 te brengen;
- de "levende categorie" van gebruikelijke toepassingen periodiek door het college te laten beoordelen.

11. Technisch deskundig toezicht (artikelen 47, 50 en 160–183)

Onafhankelijk toezicht op digitale bevoegdheden vraagt naast juridische ook technische deskundigheid. De toezichthouder moet zelfstandig kunnen beoordelen hoe systemen werken en welke risico's hun inzet meebrengt.

Het vertrek van Bert Hubert als technisch lid van de TIB per 9 september 2022 illustreert hoe kwetsbaar die deskundigheid is [35]. Hij verzette zich toen tegen het uitkleden van de toetsingscriteria en wees erop dat veel toezicht verschuift "van vooraf naar achteraf" [36].

Het voorstel voegt de CTIVD en de TIB samen tot het college van toetsing en toezicht op de inlichtingen- en veiligheidsdiensten (CTT), dat "volledig onafhankelijk" optreedt (artikel 160) [5]. ISOC NL constateert:

- **Alleen juridische benoemingseisen.** De wet eist ervaring als rechter voor ten minste één lid van de afdeling toetsing, en een juridische opleiding voor ten minste één lid van de afdeling toezicht en het lid klachtbehandeling (artikel 167). Een eis van technische deskundigheid ontbreekt.
- **Kleine afdeling toetsing.** De afdeling toetsing telt twee leden (artikel 161). Zaken worden in beginsel door één lid behandeld (artikel 50, eerste lid).
- **Geen deskundigen voor de toetsing.** Alleen de afdeling toezicht en de afdeling klachtbehandeling kunnen werk opdragen aan deskundigen (artikel 183). De afdeling toetsing wordt daarin niet genoemd.

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

- **Erkend knelpunt.** De regering erkent het belang van technische kennis. In de beroepsprocedure kunnen deskundigen worden ingeschakeld, "gelet op het geconstateerde knelpunt in de invoeringstoets", en die kennis "kan ook bij de afdeling toezicht aanwezig zijn" [2, p. 182]. Een wettelijke borging ontbreekt.
- **Minder toetsing vooraf.** Belangrijke technische bevoegdheden vallen buiten de toets vooraf (paragraaf 6).

De CTIVD en de TIB stellen dat onafhankelijke toetsing en toezicht "op belangrijke punten verminderd of naar een later moment verschoven" worden. Volgens hen biedt het voorstel "te weinig garanties" voor een onafhankelijk college "met voldoende bevoegdheden en middelen" [7][8]. ISOC NL deelt die zorg.

Wij verzoeken de wetgever:

- in artikel 167 vast te leggen dat ten minste één lid van de afdeling toetsing en één lid van de afdeling toezicht aantoonbare deskundigheid heeft op het gebied van informatiebeveiliging, netwerken en cryptografie;
- ook de afdeling toetsing de bevoegdheid te geven deskundigen in te schakelen (artikel 183);
- zaken met complexe technische aspecten in meervoudige samenstelling te behandelen, met een technisch deskundig lid (artikel 50);
- het college voldoende middelen te geven om interceptiesystemen, netwerkarchitecturen, versleuteling, kwetsbaarheden en AI-toepassingen zelfstandig te onderzoeken;
- technische risico's die achteraf niet herstelbaar zijn, altijd vooraf te laten toetsen.

12. Internettoets in twee stappen

De gebruikelijke toets op noodzaak en proportionaliteit beantwoordt niet de vraag wat een maatregel doet met het internet als infrastructuur.

Het beleidskompasformulier noemt de toetsen die vóór en tijdens de consultatie worden uitgevoerd, waaronder een uitvoeringstoets, de bedrijfseffectentoets, een toets gegevensbescherming en een grondrechtentoets. Een toets op de gevolgen voor de werking en veiligheid van het internet ontbreekt [4]. Als partijen buiten de overheid met relevante kennis noemt het formulier "wetenschappers en belangenorganisaties op het terrein van nationale veiligheid en privacy" [4]. De technische internetgemeenschap wordt niet genoemd. Ook in de memorie van toelichting hebben wij geen analyse aangetroffen van de gevolgen voor de internetinfrastructuur als geheel [2].

ISOC NL stelt daarom een Internet Impact Assessment (IIA) voor, vergelijkbaar met de toets gegevensbescherming:

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

- **Stap 1 — screening.** Bij technische bevoegdheden die gevolgen kunnen hebben voor de werking of veiligheid van het internet, wordt eerst kort beoordeeld of er relevante risico's zijn.
- **Stap 2 — volledige beoordeling.** Bij relevante risico's volgt een uitgebreide toets volgens de IIAT. Dat geldt in het bijzonder wanneer een maatregel raakt aan versleuteling, routering, DNS of IP-adressering.

Deze getrapte opzet volgt de methodiek van de IIAT zelf, die begint met een voorlopige analyse [21].

In elk geval verdienen een screening:

- het binnendringen in geautomatiseerde werken (artikelen 76–78);
- het onderzoek aan communicatienetwerken (artikel 80);
- bulkinterceptie (artikelen 81–82);
- de medewerking van aanbieders en de technische voorzieningen daarvoor (artikel 86);
- realtime gegevens bij platforms (artikel 89);
- ontsleutelopdrachten (artikel 95);
- verstorende maatregelen in het digitale domein (artikel 97) [2, p. 102].

Een IIA beantwoordt onder meer de volgende vragen:

- Brengt de maatregel de veiligheid van internetprotocollen en standaarden in gevaar?
- Ontstaan er nieuwe kwetsbaarheden of centrale faalpunten?
- Worden decentrale netwerken of sterke versleuteling ondermijnd?
- Kunnen nieuwe en kleine partijen blijven deelnemen?
- Wordt Nederland afhankelijker van een klein aantal buitenlandse aanbieders?
- Blijft het vertrouwen van gebruikers in het internet behouden?

De uitkomsten worden betrokken bij de besluitvorming en zijn toetsbaar voor het college. Waar geheimhouding dat vereist, kan worden gewerkt met een vertrouwelijke technische bijlage en een openbare samenvatting. Ook de voorziene invoeringstoets na één tot twee jaar en de wetsevaluatie na vijf jaar (artikel 270) moeten de gevolgen voor het internet uitdrukkelijk meenemen [4].

Het voorstel sluit aan bij onze reactie op de Nota Frequentiebeleid: een gerichte toets, geen zware nieuwe procedure [32]. ISOC NL draagt graag bij aan de uitwerking.

13. Slot

Nationale veiligheid vraagt niet alleen om effectieve inlichtingendiensten. Zij vraagt ook om bescherming van de digitale infrastructuur waarop economie, overheid en samenleving rusten. Beide

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

kunnen elkaar versterken, mits de wet de veiligheid van het internet even serieus neemt als de slagkracht van de diensten.

ISOC NL verzoekt de wetgever het wetsvoorstel op de genoemde punten aan te passen. Wij zijn graag bereid deze reactie mondeling toe te lichten. Voor vragen is de voorzitter van ISOC NL bereikbaar via voorzitter@isoc.nl.

Namens Internet Society Nederland,

Ruben Brave
Voorzitter Internet Society Nederland
voorzitter@isoc.nl

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

REFERENTIES

Officiële stukken bij de consultatie. Alle stukken zijn te vinden via https://www.internetconsultatie.nl/wbnv/b1

[1]Wetsvoorstel Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten, consultatieversie (28 augustus 2026).

[2]Memorie van toelichting Wbnv, consultatieversie. Paginanummers verwijzen naar deze versie.

[3]Sira Consulting (28 mei 2026), *BET herziening Wet op de inlichtingen- en veiligheidsdiensten 2017*, eindrapport. Let op: de BET gebruikt een eerdere artikelnummering. De BET-artikelen 78–81 komen overeen met de artikelen 87–90 van het wetsvoorstel; BET-artikel 83 komt overeen met artikel 94.

[4]Beleidskompasformulier voor internetconsultatie Wbnv.

[5]*Brief introduction* Wbnv (Engelstalige toelichting).

[6]Infographic Wet bescherming nationale veiligheid.

Toezichthouders

[7]CTIVD en TIB (9 september 2026), "Wetsvoorstel op de inlichtingen- en veiligheidsdiensten niet in balans; bevoegdheden uitgebreid, waarborgen verminderd". https://www.ctivd.nl/actueel/nieuws/2026/09/09/ctivd-en-tib-wetsvoorstel-op-de-inlichtingen-en-veiligheidsdiensten-niet-in-balans-bevoegdheden-uitgebreid-waarborgen-verminderd

[8]CTIVD en TIB (september 2026), volledige reactie op het concept-wetsvoorstel Wbnv. https://www.ctivd.nl/documenten/2026/09/09/reactie-ctivd-en-tib-op-het-concept-wetsvoorstel-wet-ter-bescherming-nationale-veiligheid-door-inlichtingen-en-veiligheids-diensten-wbnv-consultatieversie-28-augustus-2026

Internet Society en ISOC NL

[9]Internet Society (2012), "Internet Society Marks its 20-Year Anniversary". https://www.internetsociety.org/news/press-releases/2012/internet-society-marks-its-20-year-anniversary/

[10]Internet Society, homepage (geraadpleegd op 11 oktober 2026): 187.078 leden, 126 chapters en SIG's, 82 organisatieleden. https://www.internetsociety.org/

[11]Internet Society, "About Internet Society". https://www.internetsociety.org/about-internet-society/

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

[12]Internet Society (2026), "2025 Annual Report". https://www.internetsociety.org/resources/doc/2026/2025-annual-report/

[13]ISOC NL, "Over ons". https://isoc.nl/over-ons/

[14]ISOC NL, "Word lid van Internet Society Nederland". https://isoc.nl/word-lid-van-internet-society-nederland/

Internet Way of Networking en Internet Impact Assessment Toolkit

[15]Internet Society, "About the Internet Way of Networking". https://www.internetsociety.org/resources/internet-impact-assessment-toolkit/about-the-internet-way-of-networking/

[16]Internet Society (september 2020), "The Internet Way of Networking: Defining the critical properties of the Internet". https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-IIAT-Defining-the-critical-properties-of-the-Internet.pdf

[17]Internet Society, "The Internet's Five Critical Properties". https://www.internetsociety.org/resources/internet-impact-assessment-toolkit/the-internets-five-critical-properties/

[18]Internet Society (februari 2012), "Internet Invariants: What Really Matters". https://www.internetsociety.org/internet-invariants-what-really-matters/

[19]Internet Society, "Enablers of an Open, Globally Connected, Secure and Trustworthy Internet". https://www.internetsociety.org/wp-content/uploads/2021/11/Enablers-of-OGST-EN.pdf

[20]Internet Society, "Internet Impact Assessment Toolkit". https://www.internetsociety.org/resources/internet-impact-assessment-toolkit/

[21]Internet Society, "Internet Impact Assessment Toolkit: Do a Preliminary Analysis". https://www.internetsociety.org/resources/internet-impact-assessment-toolkit/do-a-preliminary-analysis/

[22]Internet Society (juni 2026), "Policy Brief: Solving Crime Without Breaking Encryption". https://www.internetsociety.org/resources/policybriefs/2026/solving-crime-without-breaking-encryption/

Praktijkvoorbeelden

[23]Help Net Security (5 december 2024), "8 US telcos compromised, FBI advises Americans to use encrypted communications". https://www.helpnetsecurity.com/2024/12/05/us-telcos-compromised-fbi-advises-use-of-encrypted-communications/

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

[24]Chatham House (augustus 2024), "Internet resilience in Ukraine". https://www.chathamhouse.org/2024/08/internet-under-attack/04-internet-resilience-ukraine

[25]Internews Ukraine, "Communications and Internet Resilience in War". https://internews.ua/en/opportunity/Press_Release_communications_and_internet_resilience_conference

[26]Associated Press (21 februari 2025), "Apple drops encryption feature for UK users after government reportedly demanded backdoor access". https://www.yahoo.com/news/apple-drops-encryption-feature-uk-163433609.html

[27]Kamerbrief over encryptie (2021), Kamerstukken II 26 643, nr. 729. https://zoek.officielebekendmakingen.nl/kst-26643-729.pdf

Eerdere standpunten van ISOC NL

[28]ISOC NL, "Internetwitboek 2002–2006". https://2014.isoc.nl/publ/witboek/internetwitboek.pdf

[29]ISOC NL (28 augustus 2015), "Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX: een respons van Internet Society Nederland". https://www.internetconsultatie.nl/wiv/reactie/40239/bestand

[30]Brief van een brede coalitie aan de minister-president (18 oktober 2017), "Uitstel inwerkingtreding Wet op de inlichtingen- en veiligheidsdiensten 2017". https://www.waag.org/sites/waag/files/brief-rutte-uitstel-inwerkingtreding-wiv-definitief.pdf

[31]ISOC NL (17 september 2024), "Brede maatschappelijke zorgen over impact EU-regelgeving op encryptie, privacy en digitale veiligheid". https://isoc.nl/nieuws/brede-maatschappelijke-zorgen-over-impact-eu-regelgeving-op-encryptie-privacy-en-digitale-veiligheid-lees-onze-open-brief/

[32]ISOC NL (23 september 2026), "Spectrum is digitale basisinfrastructuur: ISOC NL reageert op Nota Frequentiebeleid 2026". https://isoc.nl/nieuws/spectrum-is-digitale-basisinfrastructuur-isoc-nl-reageert-op-nota-frequentiebeleid-2026/

[33]ISOC NL (18 september 2026), "ISOC NL tekent oproep: bescherm Europese organisaties tegen de gevolgen van buitenlandse sancties". https://isoc.nl/nieuws/isoc-nl-tekent-oproep-bescherm-europese-organisaties-tegen-de-gevolgen-van-buitenlandse-sancties/

Geschiedenis en toezicht

[34]Rijksoverheid (6 april 2018), "Kabinet scherpt Wiv 2017 aan". https://www.rijksoverheid.nl/actueel/nieuws/2018/04/06/kabinet-scherpt-wiv-2017-aan

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.

[35]Kamerstukken II 2022/23, 36 214, nr. 1 (23 september 2022), ontslag van de heer A.W.R. Hubert als lid van de TIB per 9 september 2022.
https://zoek.officielebekendmakingen.nl/kst-36214-1.pdf

[36]Computable (september 2022), "Bert Hubert stapt op uit toetsingscommissie TIB".
https://www.computable.nl/?p=37658

Vereniging Internet Society Nederland is geregistreerd onder nummer 40539643 van de Kamer van Koophandel te Den Haag. Dit schrijven is bestemd voor de personen of entiteiten aan wie het gericht is en kan informatie bevatten die niet gedeeld of openbaar gemaakt mag worden krachtens de geldende wetgeving. Indien u dit schrijven per vergissing heeft ontvangen, verzoeken wij u om ons daarvan direct schriftelijk op de hoogte te stellen. Op al onze activiteiten zijn onverkort onze verenigingstatuten van toepassing. Dank voor uw medewerking.