Parlement en Wetenschap

Factsheet VOORGENOMEN WIJZIGINGEN IN DE WET OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN 2017

Deze factsheet is tot stand gekomen in het kader van de samenwerking van de Tweede Kamer met De Jonge Akademie, de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW), de Nederlandse Federatie van Universitair Medische Centra (NFU), de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), TNO en de Vereniging Universiteiten van Nederland (UNL).

6 september 2024

Prof. dr. Jan-Jaap Oerlemans, mr. Sophie Harleman (beiden Universiteit Utrecht)

Samenvatting

De wereld zag er in 2020 anders uit dan nu. In Nederland hebben we inmiddels een uitgebreid wetgevingsproces achter de rug op het gebied van inlichtingen en nationale veiligheid. Dit heeft geresulteerd in de 'Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma' (hierna: 'Tijdelijke cyberwet'). De hoofdlijnennotitie gaat echter hoofdzakelijk in op de aanbevelingen van de Commissie Jones-Bos, die in 2020 haar – wat premature – evaluatie uitvoerde en in 2021 publiceerde. Onze hoofdboodschap is dat de Tijdelijke cyberwet weliswaar enkele urgente knelpunten in de uitvoering van bijzondere bevoegdheden beoogt op te lossen, maar deze oplossingen niet altijd voldoende duidelijk regelt, met name met betrekking tot de reikwijdte van de rechtmatigheidstoets van de Toetsingscommissie Inzet Bevoegdheden (TIB). Het strekt daarom tot aanbeveling de ervaringen met deze nieuwe wet via een volgende evaluatie mee te nemen in een nieuw wetgevingsproces. Daarnaast is het dreigingsbeeld in de afgelopen jaren sterk veranderd. Nieuwe dreigingen in het cyberdomein en ondermijnende criminaliteit worden nu door de AIVD opgepakt. Het is echter maar de vraag in hoeverre al deze dreigingen in gelijke mate de nationale veiligheid raken, en daarmee tot het taakgebied van de dienst zijn te rekenen. De grijsgebieden die wij hierin signaleren zijn onwenselijk, gezien de vergaande bevoegdheden van de diensten.

Centrale vraagstelling

De Vaste commissie voor Binnenlandse Zaken vraagt de auteurs om een wetenschappelijke beoordeling te geven van de voorgenomen wijzigingen in de Wet op de inlichtingen- en veiligheidsdiensten 2017, zoals geschetst in de hoofdlijnennotitie. De vijf hoofdonderwerpen zijn:

1 - Verwerking van bulkdata
2 - Onderzoeksopdrachtgerichte interceptie (OOG-interceptie)
3 - Hacken
4 - Internationale samenwerking
5 - Stelsel toetsing, toezicht en klachtbehandeling

Als leidraad voor de beoordeling van de hoofdlijnennotitie zijn drie vragen geformuleerd:

1. Zijn de voorgenomen wijzigingen op de eerste vier onderwerpen effectief om het beoogde doel te bereiken? (Het doel is, volgens p. 11 van de notitie, herstel van de slagkracht van de diensten, 'mede door terugbrengen van de structurele administratieve lastenverzwaring die na inwerkingtreding van de Wiv 2017 heeft plaatsgevonden'.)
2. Zijn er in de voorgenomen wijzigingen op de eerste vier onderwerpen voldoende waarborgen voorzien voor het beschermen van de grondrechten (waaronder op het gebied van privacy)?
3. Kunt u een appreciatie geven van de scenario's voor het stelsel van toetsing, toezicht en klachtbehandeling? Heeft u een voorkeur voor een van de scenario's en zo ja, waarom?

1. Inleiding

De Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: Wiv 2017) is na veel controverse tot stand gekomen. De discussie ging destijds met name om een uitbreiding van de bijzondere bevoegdheid voor bulkinterceptie van de ether (zoals satellietcommunicatie en radio) naar de kabel (met internetverkeer).[1] Mede vanwege zorgen over een vergaande inbreuk op het recht op privacy en gegevensbescherming door de nieuwe Wiv 2017, is deze vervroegd geëvalueerd (binnen drie jaar in plaats van binnen vijf jaar). Uit de evaluatie van de Commissie Jones-Bos en het rapport van de Algemene Rekenkamer bleek dat de Wiv 2017 niet op alle onderdelen goed functioneert, en dat wijzigingen noodzakelijk zijn.[2] De hoofdlijnennotitie gaat met name in op de aanbevelingen naar aanleiding van deze evaluatie.

Wij beantwoorden de vragen van de commissie zo goed mogelijk door de voorgestelde aanpassingen omtrent bulkinterceptie, de hackbevoegdheid en bulkdatasets achtereenvolgens te bespreken en vervolgens in te gaan op de voorgestelde wijzigingen op het toezichtstelsel. Het is daarbij volgens ons noodzakelijk de ervaringen met de Tijdelijke cyberwet bij de wetswijziging te betrekken. Daarnaast benadrukken wij dat er meer aandacht moet zijn voor de gewijzigde dreigingen en voor nieuwe taken waarmee de AIVD en de MIVD zich klaarblijkelijk bezighouden.

2. Knelpunten bij de inzet van kabelinterceptie en de hackbevoegdheid

Zes jaar na de publicatie van de Wiv 2017 wordt bulkinterceptie op de kabel (ook wel 'kabelinterceptie' genoemd) nog 'beperkt' ingezet. In een brief van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (hierna: CTIVD) is te lezen dat tussen november 2022 en december 2023 een aantal toestemmingsaanvragen voor kabelinterceptie is goedgekeurd. Deze zagen op één specifiek thema, namelijk cyberdreiging, zoals is af te leiden uit een jaarverslag van de Toetsingscommissie Inzet Bevoegdheden (hierna: TIB).[3] Daarbij werden gegevens vooral gefilterd om *gekende*

[1] Zie ook J.J. Oerleman & M. Hagens, 'De wet op de inlichtingen- en veiligheidsdiensten 2017: een technologisch gedreven wet', *Computerrecht* 2018/111, p. 130-141.
[2] Zie ook J.J. Oerlemans & Q.A.M. Eijkman, 'Evaluatie Wiv 2017: betere uitvoerbaarheid, ten koste van privacy?', *Tijdschrift voor Internetrecht* 2021, nr. 3, p. 95-101.
[3] Brief CTIVD, 'Uitkomsten monitoring kabelinterceptie', 23 januari 2024 en *Jaarverslag* 2023, TIB, p. 16.

dreigingen te identificeren,[4] terwijl kabelinterceptie juist is bedoeld om ook *ongekende* dreigingen te identificeren.[5]

De ambities van het toenmalige kabinet om kabelinterceptie in te zetten voor alle taakgebieden van diensten evenals de voorziene uitbreiding van toegangslocaties zijn niet gerealiseerd. De oorzaak daarvan blijkt te liggen in de onrechtmatigheidsoordelen van de TIB, die plaatsvonden nadat door de verantwoordelijke ministers toestemming werd gegeven om kabelinterceptie breder in te zetten. De toestemming van de ministers werd door de toetsingscommissie onrechtmatig verklaard, omdat deze 'niet zo gericht mogelijk' en een bredere inzet disproportioneel zou zijn.[6] De voorziene uitbreiding van toegangslocaties had in januari 2024 nog geen doorgang gevonden. De verantwoordelijke ministers geven in een Kamerbrief aan dat de AIVD en de MIVD hierdoor niet kunnen overgaan tot een effectieve uitvoering van kabelinterceptie om met name de *ongekende* dreiging voor de nationale veiligheid van Nederland te onderzoeken.[7]

De problematiek bij deze bijzondere bevoegdheid wordt gekenmerkt door een verschil van mening over de reikwijdte van de toetsing door de TIB bij de inzet van bijzondere bevoegdheden.[8] Meer specifiek blijkt er bijvoorbeeld een verschil van inzicht te bestaan over het criterium van 'zo gericht mogelijk' in de verkenningsfase van kabelinterceptie (ook wel 'snapshotten' genoemd). Ook is er een verschil van inzicht over de mogelijkheid om gegevens uit deze verkenningsfase te delen met buitenlandse inlichtingen- en veiligheidsdiensten. De diensten benadrukken dat het delen van dergelijke gegevens van belang is voor de technische optimalisatie van kabelinterceptie; dat het omkleed is met waarborgen; een juridische grondslag kent onder de Wiv 2017, en onder toezicht staat van de CTIVD.[9] Toch strekt de toets van de TIB zich klaarblijkelijk ook uit over het delen van deze gegevens met buitenlandse inlichtingen- en veiligheidsdiensten.

De ministers hebben aangeven dat de problematiek betreffende de reikwijdte van de taakuitvoering en verschillen van mening over de wetsuitleg ook spelen bij de uitvoering van de hackbevoegdheid.[10] Door patstellingen tussen de TIB en de diensten over de wetsuitleg, kwamen hackoperaties volgens de minister in 2023 nog slechts 'hortend en stotend' op gang.[11] De evaluatiecommissie concludeerde eerder dat diensten een klein maar wezenlijk deel van hun onderzoeken niet (meer) kunnen uitvoeren en ook de Algemene Rekenkamer signaleerde problemen bij de uitvoering van de hackbevoegdheid. Ten slotte is ook uit het jaarverslag van de TIB over 2023 af te leiden dat de toetsingscommissie handelt op basis van een uitgebreide interpretatie van haar taakstelling, die bijvoorbeeld de verdere verwerking van gegevens uit bulkdatasets omvat, terwijl de CTIVD hier ook toezicht op houdt (tijdens en achteraf).

---

[4] Brief CTIVD, 'Uitkomsten monitoring kabelinterceptie', 23 januari 2024, p. 2.
[5] Zie Memorie van Toelichting Wiv 2017, *Kamerstukken II* 2016/17, 34588, 3, p. 93.
[6] *Jaarverslag* 2023, TIB, p. 16.
[7] Brief aan Tweede Kamer inzake brief CTIVD m.b.t. uitkomsten monitoring kabelinterceptie van 14 februari 2024.
[8] Zie ook: S.A.M. Harleman, 'Een tijdelijke Cyberwet maakt nog geen sleepwet', *NJB* 2022/2695, afl. 38, p. 3123; R.H.T. Jansen, 'Van accentverschuiving naar stelselwijziging', *NJB* 2022/2096, afl. 30, p. 2412.
[9] Brief aan Tweede Kamer inzake brief CTIVD m.b.t. uitkomsten monitoring kabelinterceptie van 14 februari 2024.
[10] Nota naar aanleiding van het verslag op de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, *Kamerstukken II* 2022/23, 36263, nr. 9, p. 4.
[11] Zie ook B.P.F. Jacobs & R.H.T. Jansen, 'Hoe hackers vastlopen', *Computerrecht* 2024/3, p. 10-21.

De Commissie Jones-Bos is overtuigd van de waarborgfunctie van de TIB, maar stelt voor om de toets van de TIB te beperken en deze niet uit te laten strekken over de verdere gegevensverwerking. De rapporten van de evaluatiecommissie en de Algemene Rekenkamer, en signalen van de diensten en de minister richting Tweede Kamer, hebben uiteindelijk geresulteerd in de Tijdelijke cyberwet. Deze heeft mede ten doel de slagkracht van de diensten te vergroten.[12] De zorgen over privacy en gegevensbescherming bij inwerkingtreding van de Wiv 2017 zijn inmiddels verworden tot zorgen over administratieve rompslomp en over de effectieve uitvoering van bulkinterceptie en de hackbevoegdheid. De Tijdelijke cyberwet verandert de toetsing door de TIB voor de bijzondere bevoegdheden van bulkinterceptie en de hackbevoegdheid waar het gaat om onderzoeken naar landen met een offensief cyberprogramma. Zo wordt de toets door de TIB in de eerdergenoemde verkenningsfase bij kabelinterceptie en de verkenningsfase bij hackbevoegdheid verlegd naar de CTIVD. Deze zou meer dynamisch toezicht kunnen houden *tijdens* de uitvoering van de bevoegdheden door de diensten. Eerder hebben wij ook betoogd dat dit een goede balans kan opleveren tussen voldoende slagkracht voor de diensten en voldoende waarborgen voor de bescherming van fundamentele rechten.[13]

Wel is het de vraag of deze Tijdelijke cyberwet de eerder gesignaleerde knelpunten geheel kan wegnemen. Er bestaat nog steeds onduidelijkheid over het criterium van 'zo gericht mogelijk' bij bulkinterceptie, evenals over de reikwijdte van de toetsing door de TIB bij – bijvoorbeeld – de toetsing van technische risico's bij de inzet van de hackbevoegdheid. Ook blijft onduidelijk of de TIB in het kader van de toets geclausuleerde toestemming mag geven: met voorwaarden voor de verdere gegevensverwerking, zoals bewaartermijnen voor bulkdatasets of het delen van gegevens met buitenlandse inlichtingen- en veiligheidsdiensten. Jacobs en Jansen wijzen in dit kader ook wel op het risico van 'micromanagen' door de TIB.[14] Voor de duidelijkheid: het gebrek aan een effectieve inzet van kabelinterceptie is ook voor een deel te verklaren door tekorten in IT-capaciteit en achterstanden bij de diensten zelf.[15] Uiteraard hoort hier ook voldoende huisvesting en capaciteit voor de toezichthouders bij.[16] Wij realiseren ons daarom dat met wetgeving niet alle problemen kunnen worden opgelost, en dat organisatorische knelpunten ook een rol spelen.

Antwoord op vraag 1 en vraag 2

De door de Commissie Jones-Bos en in de hoofdlijnennotitie voorgestelde wijzigingen om effectiviteit te vergroten en het beoogde doel te bereiken (Vraag 1) zijn deels opgepakt in de Tijdelijke cyberwet. Het is echter de vraag of de cyberwet alle knelpunten zodanig wegneemt dat de diensten daadwerkelijk hun taken effectiever kunnen uitoefenen. Tegelijkertijd lijkt het verleggen van toezicht op onderdelen van de uitvoering van bulkinterceptie en de hackbevoegdheid beter te passen bij de werkwijze van de diensten en de taken van de beide toezichthouders. Dit stelsel biedt naar onze mening in hoofdlijnen

[12] Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen, *Stb.* 2024, 155.
[13] Zie S.A.M. Harleman, 'Een tijdelijke Cyberwet maakt nog geen sleepwet', *NJB* 2022/2695, afl. 38, p. 3127 en J.J. Oerlemans, 'Inbreng rondetafelgesprek Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma', 5 april 2023.
[14] B.P.F. Jacobs & R.H.T. Jansen, 'Hoe hackers vastlopen', *Computerrecht* 2024/3, p. 10-21.
[15] Algemene Rekenkamer, *Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt*, 22 april 2021, p. 60, 61.
[16] In de media kwam de afgelopen maanden aan bod dat de huisvesting een knelpunt is, zie bijvoorbeeld: K. Versteegh, 'Invoering van nieuw toezicht op inlichtingen- en veiligheidsdiensten per 1 juli is "onverantwoord" door personeelstekort, waarschuwen toezichthouders', *NRC* 18 juni 2024.

voldoende adequate bescherming van de fundamentele rechten van burgers (vraag 2, zie ook paragraaf 4). Het is van belang dat ook de Tijdelijke cyberwet door een onafhankelijke commissie wordt geëvalueerd en dat de aanbevelingen worden meegenomen en verwerkt in een wetsvoorstel.

3. Bulkdatasets

Een bulkdataset is een verzameling van gegevens waarvan het merendeel betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek zijn en dat waarschijnlijk ook nooit zullen worden. Deze datasets bevatten vaak grote hoeveelheden persoonsgegevens die door inlichtingendiensten zoals de AIVD en MIVD worden verzameld voor hun taakuitvoering. Als een bulkdataset met een bijzondere bevoegdheid wordt verworven, dan moet deze binnen anderhalf jaar op relevantie worden beoordeeld. Het is echter niet op voorhand te bepalen welke gegevens uit die bulkdatasets relevant zijn voor een concreet inlichtingenonderzoek. Mogelijk zijn alle gegevens potentieel van waarde. Dit betekent dat de set als geheel bewaard moet worden, en dat pas achteraf zal blijken welke gegevens uit een bulkdataset daadwerkelijk gebruikt zijn bij het beantwoorden van concrete onderzoeksvragen.[17]

De CTIVD waarschuwt sinds 2019 dat – als de wet niet wordt aangepast – waardevolle bulkdatasets vernietigd moeten worden.[18] De Commissie Jones-Bos signaleerde de statische bewaartermijn van anderhalf jaar ook als knelpunt. Zij overwoog deze bewaartermijn langer te maken[19] en stelde ook een uniforme regeling voor de bewaartermijn van bulkdatasets voor.[20] Uiteindelijk is aan de Tijdelijke cyberwet een deel toegevoegd (hoofdstuk 3) dat een bewaartermijn regelt voor bulkdatasets die zijn verworven met bijzondere bevoegdheden (behalve kabelinterceptie). Gelet op de systematiek van de wet was een aparte regeling beter geweest. De reikwijdte van hoofdstuk 3 van de Tijdelijke cyberwet is namelijk groter dan geldt voor de rest van de wet: die ziet slechts op 'staten met een offensief cyberprogramma'. Bovendien geldt deze wetgeving alleen voor de verzameling van bulkdatasets met bijzondere bevoegdheden.

De regeling voor bulkdatasets zit zo in elkaar dat in de toestemmingsaanvraag bij de CTIVD om een bulkdataset langer te mogen bewaren, jaarlijks onderbouwd moet worden waarom de dataset nog steeds van belang is voor de onderzoeken van de diensten. Daarbij moet de opbrengst van de afgelopen periode gemeld worden en moet er vooruitgekeken worden naar wat deze bulkdataset nog kan opleveren in het komende jaar. In dit systeem is dus geen vooraf vastgestelde bewaartermijn voorzien. De CTIVD toetst deze motivering en houdt hier bindend toezicht op.

Antwoord op vraag 1 en vraag 2

In de hoofdlijnennotitie worden prima uitgangspunten benoemd voor de omgang met bulkdatasets. Daarbij geldt het devies: 'bulk is bulk', ongeacht hoe de data zijn verworven, en is het voornemen om een uniforme regeling voor bulkdatasets te creëren. Daarnaast wordt een stap aan het toestemmingsproces toegevoegd, waarbij de bulkbehoefte voorafgaand aan het toestemmingsverzoek wordt voorgelegd aan de minister. De

[17] Nota van wijziging, *Kamerstukken II* 2022/23, 36623, nr. 10, p. 21.
[18] Zie onder andere de CTIVD-voortgangsrapportages nrs. 66 (2019) en 69 (2020) en het toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid, nr. 70 (2020).
[19] Commissie Jones-Bos, *Evaluatie 2020: Wet op de inlichtingen en veiligheidsdiensten 2017,* p. 64, 65.
[20] Commissie Jones-Bos, *Evaluatie 2020: Wet op de inlichtingen en veiligheidsdiensten 2017,* p. 50, 51

hoofdlijnennotitie voorziet desondanks in een differentiatie voor bepaalde bulkdatasets die via de informantenbevoegdheid geraadpleegd kunnen worden. Zoals eerder is betoogd, is het noodzakelijk de informantenbevoegdheid te herzien en een duidelijke en voorzienbare regeling te creëren voor (al dan niet geautomatiseerde) toegang van de AIVD en de MIVD tot gegevens van andere (overheids)instanties.[21]

De regeling in de Tijdelijke cyberwet is onvoldoende, omdat bulkdatasets namelijk óók kunnen worden verzameld met *algemene* bevoegdheden, zoals de informantenbevoegdheid, en uit OSINT[22]. Daarnaast kunnen bulkdatasets worden verkregen van buitenlandse inlichtingen- en veiligheidsdiensten in het kader van internationale samenwerking. De Tijdelijke cyberwet is hierop niet van toepassing. Het is goed dat de diensten een eigen tussentijdse regeling aanhouden, maar dit onderwerp zou bij wet geregeld moeten worden.

Ten aanzien van internationale samenwerking liggen er nog tal van andere voorstellen met een verzoek daar een appreciatie van te geven. Aangezien er al geruime tijd geen toezichtrapporten van de CTIVD zijn gepubliceerd over internationale samenwerking, is niet goed in te schatten of het huidige systeem effectief is en of er tegelijkertijd voldoende waarborgen bestaan. Het is daardoor onduidelijk hoe het huidige systeem functioneert en welke effecten een gewijzigde regeling met zich meebrengen.

4. Het toezichtstelsel

De hoofdlijnennotitie biedt verschillende scenario's met betrekking tot het toezichtstelsel. Gezien de discussies en ontwikkelingen in aanloop naar de Tijdelijke cyberwet lijken deze scenario's al enigszins achterhaald. Met de Tijdelijke cyberwet heeft de wetgever duidelijk gekozen voor meer dynamisch toezicht, met name om de knelpunten van de statische voorafgaande toets tegen te gaan (zie paragraaf 2). Duidelijk is ook dat voor bepaalde bevoegdheden, zoals bulkinterceptie en de hackbevoegdheid, voorafgaande onafhankelijke toetsing noodzakelijk is. De verdere gegevensverwerking en de naleving van andere artikelen in de Wiv 2017 moeten door een onafhankelijk orgaan getoetst worden. Betrokkenen moeten de mogelijkheid hebben een klacht in te dienen, die vervolgens door een onafhankelijk orgaan dient te worden behandeld, en waar bindende beslissingen op kunnen volgen.

Antwoord op vraag 3

Volgens ons wijzen alle pijlen naar het creëren van één toezichthouder die – in aparte kamers - zowel een voorafgaande toets uitvoert, als achteraf toezicht houdt (scenario 3 uit de hoofdlijnennotitie). De voortdurende discussies over kwesties als het gerichtheidsvereiste, klaarblijkelijk ook tussen de TIB en de CTIVD onderling, moeten ophouden. De Tijdelijke wet laat zien dat de uitvoering van toezicht met 'end-to-end safeguards'[23] ook afstemming vereist tussen de TIB en de CTIVD. De beide toezichthouders hebben zelf in jaarverslagen te kennen gegeven op te willen gaan in één 'Autoriteit Nationale Veiligheid'.[24]

---

[21] Zie J.J. Oerlemans, *Grenzen stellen aan datahonger* (oratie Utrecht), 16 november 2020.
[22] OSINT staat voor 'Open Source Intelligence': het verzamelen gegevens uit publiek toegankelijke bronnen.
[23] Zoals ook vereist door het Europees Hof voor de Rechten van de Mens, zie: EHRM (GK) 25 mei 2021, *Big Brother Watch e.a. t. het Verenigd Koninkrijk*, (nrs. 58170/13, 62322/14 en 24960/15), §350.
[24] *Jaarverslag* 2023, CTIVD, p. 4; *Jaarverslag* 2023, TIB, p. 33.

De beroepsmogelijkheid op beslissingen van de TIB en bindende oordelen van de CTIVD bij de afdeling bestuursrechtspraak van de Raad van State verwelkomen wij. In een systeem van 'checks & balances' is het een welkome aanvulling. Het is echter te vroeg om een appreciatie van dit nieuwe systeem in het kader van de Tijdelijke wet te geven, aangezien er nog geen jurisprudentie ligt.

5. Grijsgebieden

In de afgelopen jaren is duidelijk geworden dat het taak- en werkveld van de AIVD en de MIVD ingrijpend is veranderd. Wij laten het appreciëren van deze dreiging door het Rusland-Oekraïne conflict en wat dit betekent voor (met name) de MIVD graag aan anderen over. Wij gaan verder in op de grijsgebieden bij de dreigingen op het gebied van cybersecurity en ondermijnende criminaliteit. Het terugkerende punt is dat veel onduidelijkheid bestaat over de rollen en verantwoordelijkheden van de diensten bij deze nieuwe dreigingen.

Eerder hebben wij al gewaarschuwd voor de dreiging voor de nationale veiligheid op cybersecuritygebied.[25] Het is ons bijvoorbeeld onvoldoende duidelijk in hoeverre de AIVD, het Nationaal Cyber Security Centrum en andere onderdelen van het ministerie van Justitie en Veiligheid gegevens met elkaar mogen uitwisselen over de (cyber)dreigingen die de nationale veiligheid raken. Afgelopen zomer hebben de AIVD en de MIVD in samenwerking met de Nationale Politie bijvoorbeeld een 'Russische offensieve cybercampagne verstoord'.[26] Maar daarbij komen vragen op, zoals: welke bevoegdheden zijn daarvoor ingezet, welke gegevensuitwisseling heeft plaatsgevonden, is dat volgens de regels gegaan, wie is daar verantwoordelijk voor, en hoe wordt daar onafhankelijk en effectief toezicht op gehouden? Dit zijn vragen die niet tot een noemenswaardig parlementair debat hebben geleid, en onzes inziens opheldering verdienen.

Wij signaleren overigens soortgelijke grijsgebieden waar het gaat om criminaliteit die de democratische rechtsorde ondermijnt, wat wel als taakgebied op de website van de AIVD wordt vermeld, maar niet is terug te vinden in de openbare versie van de Geïntegreerde Aanwijzing van 2023-2026.[27] Het begrip 'ondermijnende criminaliteit' is op zichzelf al problematisch, omdat uit onderzoek blijkt dat niet duidelijk is wat met het begrip wordt bedoeld.[28]

Kortom, meer duidelijkheid over de rollen en verantwoordelijkheden van de diensten bij deze nieuwe dreigingen is noodzakelijk. Daarbij moet ook antwoord komen op de vraag of de diensten actief gegevens verzamelen over deze dreigingen door de inzet van bijzondere bevoegdheden, om ook niet-traditionele afnemers, zoals bedrijven, handelingsperspectief te bieden. Mogelijk leidt een debat – en nopen de antwoorden op deze vragen – tot aanpassingen van een nieuwe Wet op de inlichtingen- en veiligheidsdiensten.

---

[25] Zie S.A.M. Harleman, 'Een tijdelijke Cyberwet maakt nog geen sleepwet', *Nederlands Juristenblad* 2022, p. 3120-3127 en J.J. Oerlemans, 'Inbreng rondetafelgesprek Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma', 5 april 2023.
[26] Zie ook Kamerbrief 'Verstoringsactie van een Russische offensieve cybercampagne' van 9 juli 2024.
[27] Zie 'Criminele ondermijning', AIVD.nl, 2 september 2024. Beschikbaar op: Criminele ondermijning van de democratische rechtsorde | AIVD.
[28] Zie bijvoorbeeld H. Nelen, R. Moerland & K. van Wingerde e.a., 'De aanpak van ondermijning ondermijnd', *Tijdschrift over Cultuur & Criminaliteit* 2023, p. 53-68 en W. Huisman, 'De aanpak van ondermijnende criminaliteit: oude wijn in nieuwe zakken?', *Delikt en Delinkwent* 2017, p. 331-443.

Bronnenlijst

- S.A.M. Harleman, 'Een tijdelijke Cyberwet maakt nog geen sleepwet', *NJB* 2022/2695, afl. 38, p. 3120-3127.
- W. Huisman, 'De aanpak van ondermijnende criminaliteit: oude wijn in nieuwe zakken?', *Delikt en Delinkwent* 2017, p. 331-443.
- B.P.F. Jacobs & R.H.T. Jansen, 'Hoe hackers vastlopen', *Computerrecht* 2024/3, p. 10-21.
- R.H.T. Jansen, 'Toezicht onder de Wet op de inlichtingen- en veiligheidsdiensten 2017: een Tour de Force', *Nederlands Tijdschrift voor de Mensenrechten. NJCM Bulletin* 2021/46, p. 419-443.
- R.H.T. Jansen, 'Van accentverschuiving naar stelselwijziging', *NJB* 2022/2096, afl. 30, p. 2406-2416.
- H. Nelen, R. Moerland & K. van Wingerde e.a., 'De aanpak van ondermijning ondermijnd', *Tijdschrift over Cultuur & Criminaliteit* 2023, p. 53-68
- J.J. Oerlemans & M. Hagens, 'De wet op de inlichtingen- en veiligheidsdiensten 2017: een technologisch gedreven wet', *Computerrecht* 2018/111, p. 130-141.
- J.J. Oerlemans, *Grenzen stellen aan datahonger* (oratie Utrecht), 16 november 2020.
- J.J. Oerlemans & Q.A.M. Eijkman, 'Evaluatie Wiv 2017: betere uitvoerbaarheid, ten koste van privacy?', *Tijdschrift voor Internetrecht* 2021, nr. 3, p. 95-101.

Overig

- Commissie Jones-Bos, *Evaluatie 2020: Wet op de inlichtingen- en veiligheidsdiensten 2017*, 20 januari 2021.
- Algemene Rekenkamer, *Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt*, 22 april 2021.
- J.J. Oerlemans, 'Inbreng rondetafelgesprek Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma', 5 april 2023.
- Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, *Jaarverslag* 2023, 24 april 2024.
- Toetsingscommissie Inzet Bevoegdheden, *Jaarverslag* 2023, 30 april 2024.