Een tijdelijke Cyberwet maakt nog geen sleepwet

Sophie Harleman[1]

Het voorstel Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma zal naar alle waarschijnlijkheid binnenkort naar de Tweede Kamer gaan. Het wetsvoorstel beoogt de inlichtingen- en veiligheidsdiensten meer slagkracht te geven in hun onderzoek naar landen met een offensief cyberprogramma. Dit artikel gaat in op de verwachte effectiviteit van deze 'Cyberwet', en met name die van de voorgestelde wijzigingen rondom de inzet van bijzondere bevoegdheden. Het gaat hierbij vooral om de hackbevoegdheid en de bevoegdheid tot kabelinterceptie. Het kabinet wil de inzet van deze bevoegdheden in de context van offensieve cyberprogramma's dynamischer maken. Hiermee doet het kabinet een goede poging om het juridisch kader beter te laten aansluiten op de praktijk. Hoewel de Cyberwet sommige drempels voorafgaand aan de inzet van bevoegdheden verlaagt, kan het voorgestelde toezicht tijdens de inzet van bevoegdheden een goede balans opleveren tussen voldoende slagkracht en voldoende waarborgen.

1. Inleiding

Het conceptwetsvoorstel Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma (hierna: Cyberwet) beoogt de inlichting- en veiligheidsdiensten meer armslag te geven tegen offensieve cyberprogramma's van staten. Tegelijkertijd beoogt het voorstel de waarborgen tegen misbruik van de vergaande bevoegdheden van de inlichtingen- en veiligheidsdiensten (hierna: diensten) op peil te houden. De Cyberwet staat los van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) en is bedoeld als aanvulling op deze wet. De Wiv 2017 belemmert volgens de wetgever het onderzoek naar landen met een offensief cyberprogramma, zoals Rusland en China. Hierdoor kan Nederland zich niet voldoende verdedigen tegen cyberaanvallen.[2]

De belemmering ligt vooral in het spanningsveld tussen het toezicht aan de voorkant zoals dat in de Wiv 2017 is neergelegd, en hoe de diensten in de praktijk moeten handelen om effectief te opereren in het cyberdomein. Hierdoor kan een dynamische inzet van bevoegdheden, met name kabelinterceptie en de hackbevoegdheid, niet worden gerealiseerd.[3] Hoewel een grote wijziging van de Wiv 2017 ophanden is, acht de wetgever het noodzakelijk met de Cyberwet een oplossing op korte termijn te bieden.[4] De voorgestelde wijzigingen hebben reeds stof doen opwaaien,[5] waarbij zelfs gesproken wordt van een 'Sleepwet 2.0'.[6]

Het voorstel brengt wijzigingen aan omtrent de inzet van bijzondere bevoegdheden zoals hacken en kabelinterceptie. Ook verlegt het voorstel het toezicht deels van toezicht vooraf (*ex ante*) naar toezicht tijdens en achteraf (*ex durante* en *ex post*). Rowin Jansen heeft daar eerder in dit blad een uitgebreide analyse over geschreven.[7] De wijzigingen met betrekking tot het toezichtstelsel worden daarom in dit artikel grotendeels buiten beschouwing gelaten. De vraag rijst of het wetsvoorstel voorziet in meer slagkracht voor de inlichtingen- en veiligheidsdiensten in onderzoeken naar offensieve cyberprogramma's. Deze bijdrage analyseert de (verwachte) effectiviteit van de wijzigingen met betrekking tot de hackbevoegdheid en kabelinterceptie.

Deze bijdrage gaat eerst nader in op de aanleiding van het wetsvoorstel (par. 2) Vervolgens wordt het huidig juridisch kader besproken waarbinnen de Nederlandse

De vraag rijst of het wetsvoorstel voorziet in meer slagkracht voor de inlichtingen- en veiligheidsdiensten in onderzoeken naar offensieve cyberprogramma's

diensten opereren (par. 3). Daarna volgt een uiteenzetting van de wijzigingen omtrent de hackbevoegdheid (par. 4), gevolgd door de wijzigingen omtrent kabelinterceptie (par. 5). De reflectie en antwoord op de onderzoeksvraag volgen in par. 6.

2. Aanleiding

De Cyberwet is tot stand gekomen in een tijd waarin de dreiging die uitgaat van statelijke actoren alsmaar toeneemt. Deze ontwikkeling kan worden geplaatst tegen de achtergrond van verschuivende politieke verhoudingen, onder andere als gevolg van de assertievere opstelling van Rusland en China en het veranderend Amerikaans leiderschap.[8] De Nederlandse inlichtingen- en veiligheidsdiensten dienen onderzoek te verrichten naar staten met een offensief cyberprogramma, omdat dit voortvloeit uit de Geïntegreerde Aanwijzing.[9] Deze aanwijzing wordt vastgesteld door de regering en bepaalt welke onderzoeksopdrachten door de regering noodzakelijk worden geacht in het kader van nationale veiligheid.[10]

De toegenomen 'cyberdreiging' resulteert niet enkel in grote internationale incidenten zoals 'Solarwinds', waarbij Russische hackers via Solarwinds Orion software binnendrongen bij Amerikaanse overheidsdiensten.[11] Ook Nederland is regelmatig doelwit. Dit wordt door jaarlijkse Cybersecuritybeelden en het 'Dreigingsbeeld statelijke actoren' onderstreept.[12] Zo werd industrieconcerngroep VDL, een belangrijke toeleverancier van zowel ASML als Philips, in oktober 2021 getroffen door een digitale aanval. Dit had wekenlang invloed op de productie van essentiële leveringen.[13] In februari 2022 werd duidelijk dat Nederlandse digitale infrastructuur werd gebruikt voor digitale aanvallen op Oekraïne.[14] Daaruit blijkt wederom dat cyberaanvallen door staten gebruikt worden voor kwestieuze politieke doeleinden of zelfs in het kader van oorlogsvoering. In diezelfde maand bleek dat de Russische hackgroep Sandworm, gelieerd aan de Russische militaire inlichtingendienst (GRU), Nederlandse routers had gehackt teneinde ze onderdeel te maken van een Russisch botnet.[15] Dientengevolge konden de routers misbruikt worden voor cyberaanvallen.[16]

Offensieve cyberprogramma's kunnen echter ook resulteren in meer ongrijpbare vormen van gevaar. Cyber*spionage,* het met digitale middelen verwerven van gevoelige of vertrouwelijke informatie van een andere staat voor het behalen van eigen strategische doelen,[17] is een groeiend probleem. Dit geldt ook voor economische cyberspionage, waarmee economisch en strategisch voordeel kan worden behaald ten behoeve van nationale stabiliteit en welvaart en ten koste van een andere staat.[18] De Britse veiligheidsdienst MI5 waarschuwde onlangs wederom voor de grote dreiging die uitgaat van China in dit opzicht.[19] Hoewel minder evident, bedreigt ook deze vorm van spionage de nationale veiligheid.[20]

Bovendien draagt de geëscaleerde oorlog in Oekraïne bij aan het gevoel van urgentie om adequaat tegen offensieve cyberprogramma's van staten te kunnen optreden. In de toelichting bij de Cyberwet wordt dit benadrukt ter onderbouwing van de noodzaak van het voorstel.[21] Het voorstel is evenwel niet in het leven geroepen *vanwege* de oorlog in Oekraïne; plannen voor het wetsvoorstel lagen er al in november 2021,[22] en sluiten aan bij eerder genoemde dreigingsbeelden.

3. Het huidige juridisch kader voor de diensten

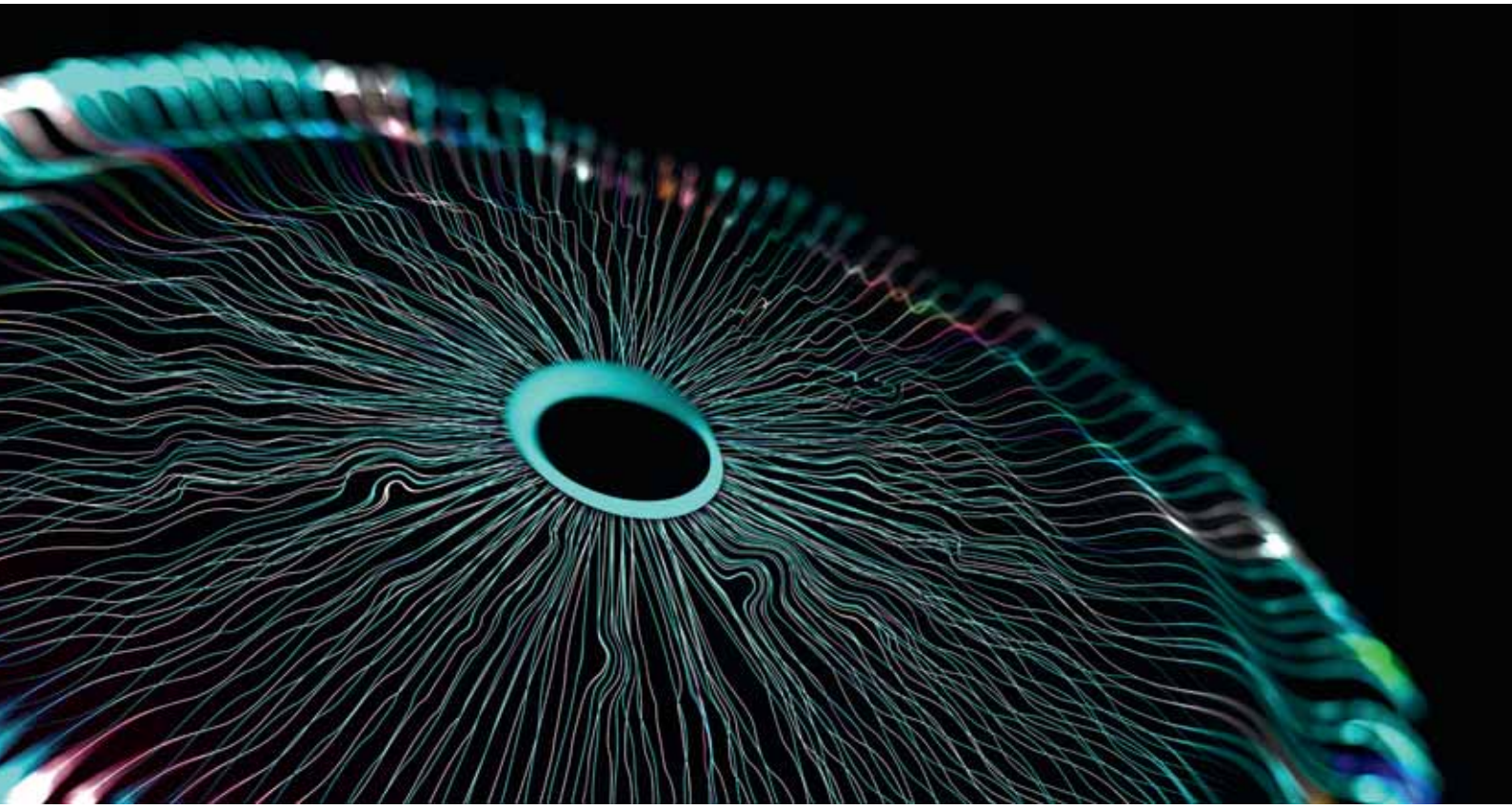
Het voorstel voor de tijdelijke Cyberwet bouwt voort op verscheidene rapporten die zijn uitgebracht naar aanleiding van de implementatie van de Wiv 2017.[23] De Wiv 2017 vormt het juridisch kader voor de AIVD en de MIVD. Deze diensten zijn dus gebonden aan de normen die voortvloeien uit de wet, zoals regels op het gebied van gegevensverwerking en de inzet van bijzondere bevoegdheden. De Wiv 2017 bevat een groot aantal wijzigingen

Auteur

1. Mr. S.A.M. Harleman is als promovenda verbonden aan het Montaigne Instituut voor Rechtsstaat en Rechtspleging en het Willem Pompe Instituut voor Strafrechtwetenschappen van de Universiteit Utrecht.

Noten

2. S. Derix & K. Berkhout, 'Een cyberaanval is nu niet te stoppen, waarschuw defensieminister Kamp', *NRC* 3 januari 2022.
3. Concept MvT bij het Wetsvoorstel Tijdelijke Wet Cyberoperaties, versie september 2022 (hierna: MvT Cyberwet), p. 16.
4. *Kamerstukken I* 2010/21, 34588, O.
5. Zo stapte er bij de Toetsingscommissie Inzet Bevoegdheden (TIB) een toezichthouder op. Zie: R. Wassens, 'Toezichthouder geheime diensten stopt ermee wegens nieuwe inlichtingenwet: "Ze willen gewoon minder pottenkijkers"', *NRC* 9 september 2022; J. Daalder & S. Brommersma, 'Geheime diensten forceren nieuwe inlichtingenwet, toezichthouder stapt op', *Follow the Money* 9 september 2022.
6. Onderzoeksplatform Argos maakte een podcastaflevering getiteld: 'Komt er een sleepwet 2.0?', vpro.nl, 24 september 2022.
7. R. Jansen, 'Van accentverschuiving naar stelselwijziging', *NJB* 2022/2096, afl. 30.
8. Evaluatiecommissie Wiv 2017 (commissie Jones-Bos), *Evaluatie 2020 - Wet op de inlichtingen- en veiligheidsdiensten 2017*, 20 januari 2021 (hierna: Evaluatierapport), p. 21.
9. Geïntegreerde Aanwijzing Inlichtingen en Veiligheid 2021-2022, art. 1, lid 2 (*Stcrt.* 2020, 61506).
10. Voor de AIVD en de MIVD respectievelijk neergelegd in art. 8, lid 2, onder a en d, en in art. 10, lid 2, onder a, c en e.
11. D.E. Sanger, N. Perlroth & J.E. Barnes, 'As understanding of Russian hacking grows, so does alarm', *The New York Times* 29 mei 2021.
12. Het Nationaal Cyber Security Centrum (NCSC) publiceert ieder jaar een nationaal Cybersecuritybeeld. Het Dreigingsbeeld statelijke actoren is in februari 2021 gepubliceerd en in samenwerking tussen de AIVD, de MIVD en de NCTV tot stand gekomen. Zie ook: NCTV, *Nederlandse Cybersecuritystrategie 2022-2028,* oktober 2022.
13. 'Industrieconcern VDL Groep getroffen door digitale aanval', *NOS Nieuws* 7 oktober 2021.
14. Cybersecuritybeeld 2022, p. 39.
15. H. Modderkolk, 'MIVD verstoort Russische digitale aanval op routers van Nederlandse burgers', *de Volkskrant* 3 maart 2022. Een botnet is een netwerk van geïnfecteerde computers die door een derde worden aangestuurd.
16. Zie ook: L. Grustniy, 'De verborgen gevaren van routermalware', *Kaspersky* 20 juni 2022.
17. Dit is de definitie die wordt gehanteerd door de AIVD.
18. Dreigingsbeeld statelijke actoren, p. 24-27. Zie ook: W.C. Banks, 'Cyber espionage and electronic surveillance: Beyond the media coverage', *Emory Law Journal* 2017/66.
19. 'Joint address by MI5 and FBI Heads', www.mi5.gov.uk/news/speech-by-mi5-and-fbi. Zie ook: S. Eikelenboom e.a., 'De grote sprong voorwaarts van Chinese bedrijven in Nederland', *Follow the Money* 29 september 2022.
20. AIVD, *Jaarverslag 2021,* april 2022, p. 16, 18, 20. Ook is economische veiligheid een van de zes pijlers van nationale veiligheid (Cybersecuritybeeld 2022).
21. Concept-memorie van toelichting Cyberwet, p. 11.
22. Zie de geannoteerde besluitenlijst van de ministerraad van 26 november 2021.
23. Evaluatierapport; Algemene Rekenkamer, *Slagkracht AIVD en MIVD: De wet dwingt, de tijd dringt, de praktijk wringt',* 22 april 2021 (hierna: Algemene Rekenkamer 2021).



© Shutterstock

ten opzichte van zijn voorganger uit 2002, omdat de wetgever vond dat technologische en maatschappelijke ontwikkelingen noopten tot modernisering van de bevoegdheden van de diensten.[24] De Wiv 2002 voorzag bijvoorbeeld slechts in niet-kabelgebonden interceptie, terwijl een groot deel van de telecommunicatie en het gegevensverkeer vandaag de dag plaatsvindt via het internet.[25] Omdat het internet grotendeels over een kabelinfrastructuur verloopt, manifesteren gegevens over dreigingen voor de nationale veiligheid (en dus potentiële inlichtingen) zich voor een groot deel op dit wereldwijde kabelgebonden netwerk.[26]

De totstandkoming van de Wiv 2017 ging vervolgens niet zonder slag of stoot. Zowel NGO's als wetenschappers uitten grote zorgen over de waarborgen die de wet bood voor privacy en gegevensbescherming.[27] Na het aannemen van de motie-Recourt werd in de wet opgenomen dat de inzet van bevoegdheden 'zo gericht mogelijk' moest zijn, als uitvloeisel van de wettelijke eisen van noodzakelijkheid, proportionaliteit en subsidiariteit.[28] De maatschappelijke commotie rondom de wet mondde uit in een raadgevend referendum, waarbij 49,44% tegen de wet stemde en 46,53% vóór. De tegenstand was vooral te verklaren door controverse over de mogelijkheid tot kabelinterceptie, waarbij data in bulk worden vergaard en waardoor de wet door tegenstanders al gauw tot 'sleepwet' werd gedoopt. Als tegenhanger van de geuite bezwaren werd een spoedige evaluatie van de wet beloofd. De Commissie Jones-Bos constateerde in 2020 dat de wet de waarborgen aanzienlijk heeft versterkt, vooral door introductie van de Toetsingscommissie Inzet Bevoegdheden (TIB).[29] De TIB toetst vóóraf de toestemming (gegeven door de minister) voor de inzet van bijzondere bevoegdheden (zoals de hackbevoegdheid en kabelinterceptie) op rechtmatigheid. Deze toets komt in feite neer op een toets aan het proportionaliteits-, noodzakelijkheids-, subsidiariteits- en gerichtheidsvereiste, plus de vereisten uit de desbetreffende bevoegdheden zelf.[30]

Gegevens over dreigingen voor de nationale veiligheid (en dus potentiële inlichtingen) manifesteren zich voor een groot deel op dit wereldwijde kabelgebonden netwerk

Tegelijkertijd zijn er sinds de implementatie van de Wiv 2017 de nodige zorgen gerezen over de slagkracht van de diensten.[31] De Commissie Jones-Bos constateert in haar evaluatierapport dat de wet onvoldoende aansluit bij wat het werk van de diensten inhoudt als het gaat om het tegengaan van cyberdreigingen.[32] Ook de Algemene Rekenkamer concludeert dat sommige waarborgen uit de Wiv 2017 de inzet van bepaalde bijzondere bevoegdheden beperken, vooral in onderzoek naar nieuwe of verborgen dreigingen en in het verkrijgen van strategische posities.[33] Twee jaar na inwerkingtreding van de Wiv 2017 (mei 2020) was de felbegeerde bijzondere bevoegdheid tot kabelinterceptie bijvoorbeeld nog niet gerealiseerd. Daarnaast constateert de Algemene Rekenkamer dat er sprake

is van een toename van administratieve handelingen, waardoor er minder capaciteit overblijft voor inhoudelijk onderzoek.[34]

Vooral de huidige invulling van de rechtmatigheidstoets door de TIB lijkt een heikel punt te zijn. Zo concludeert de Commissie Jones-Bos dat de TIB soms via haar *ex ante* toets voorwaarden stelt aan de inzet van bijzondere bevoegdheden.[35] Dit uit zich in het op detailniveau verzoeken om informatie over hoe een bevoegdheid wordt uitgevoerd en hoe de gegevens verwerkt zullen worden (bijvoorbeeld de vraag of gegevens gedeeld zullen worden met buitenlandse partners).[36] Dergelijke 'geclausuleerde toestemming' is niet in de Wiv 2017 voorzien. De Commissie Jones-Bos benadrukt dat het aan de minister is om voorwaarden te stellen, aan de hand waarvan de TIB slechts zou moeten toetsen of de toestemming rechtmatig is: 'Óf de slagboom blijft naar beneden, en de auto kan niet verder, of de slagboom gaat omhoog (...)'.[37]

Het duwen en trekken tussen toezichthouder en de diensten vindt zijn oorsprong in de Wiv 2017, die helaas niet voldoende aansluit bij de praktijk

De invulling van de rechtmatigheidstoets door de TIB lijkt aldus in ieder geval ten dele te verschillen van die van de diensten en de evaluatiecommissie. Het duwen en trekken tussen toezichthouder en de diensten als gevolg daarvan, vindt zijn oorsprong in de Wiv 2017, die helaas niet voldoende aansluit bij de praktijk.[38] De wetgever tracht met de Cyberwet de patstelling die is ontstaan op te lossen, onder meer via aanpassingen van de hackbevoegdheid en kabelinterceptie.

4. De hackbevoegdheid in de Tijdelijke wet

De hackbevoegdheid betreft de bijzondere bevoegdheid tot het binnendringen van een geautomatiseerd werk door de diensten. In de Wiv 2017 valt zowel *verkennen* als het *binnendringen* van een geautomatiseerd werk onder de algemene hackbevoegdheid.[39] Bij het verkennen van een geautomatiseerd werk kunnen de diensten bijvoorbeeld te weten komen op welke software een geautomatiseerd werk draait. Zulke informatie kan vervolgens worden gebruikt bij het binnendringen (hacken) van dat werk.[40] Hieronder worden een paar belangrijke wijzigingen toegelicht die de Cyberwet aanbrengt omtrent de inzet van de hackbevoegdheid. Ook wordt vooruitlopend op de reflectie vast kort de verwachte effectiviteit van deze wijzigingen besproken.

4.1. Toestemming voor verkennen

Ten eerste regelt de Cyberwet dat het verlenen van toestemming voor het *verkennen* van geautomatiseerde werken wordt belegd bij het hoofd van de dienst in plaats van bij de TIB.[41] Het verkennen heeft in de Wiv 2017 hetzelfde waarborgenregime gekregen als het binnendringen van een geautomatiseerd werk. Door de TIB-toets te laten vallen voor wat betreft het verkennen, wordt de drempel aan de voorkant verlaagd. Daarmee beoogt de Cyberwet de snelheid en effectiviteit van de inzet van de bevoegdheid tot het *binnendringen* van een werk te verhogen. De *ex ante* toets van de TIB wordt vervangen door bindend *ex durante* toezicht door de CTIVD. Dit is een stap ten faveure van een meer dynamische inzet van de hackbevoegdheid. Een toets voor verkennen die even zwaar is als de toets voor binnendringen, lijkt uit verhouding. Op deze wijziging is tot nu toe dan ook relatief weinig kritiek geweest. Wel moet in het oog worden gehouden dat het niet altijd makkelijk is te bepalen waar verkennen eindigt en binnendringen begint. Bij functionerend *ex durante* toezicht kan er op worden toegezien dat verkennen blijft bij verkennen; het toezicht van de CTIVD zal immers zien op elke stap van de hackbevoegdheid. In 'real-time' kan aan de rem getrokken worden als een verkenning te ver gaat.

4.2. Bijschrijven

Ten tweede wordt door het conceptwetsvoorstel het 'exclusiviteitsvereiste van de bijschrijfmogelijkheid' losgelaten. De bijschrijfmogelijkheid houdt in dat verleende toestemming voor hacken ook de bevoegdheid omvat om een ander geautomatiseerd werk te hacken *van* dezelfde persoon of organisatie.[42] Het idee dat computers exclusief in het bezit en gebruik zijn van één bepaalde partij is volgens de wetgever echter wat er wringt. De wijziging die de Cyberwet aanbrengt, houdt dan ook kort en goed in dat waar in de Wiv 2017 wordt gesproken over 'een ander

24. Zie ook: J.J. Oerlemans & M. Hagens, 'De wet op de inlichtingen- en veiligheidsdiensten 2017: een technologisch gedreven wet', *Computerrecht* 2018/111, p. 130-141.
25. Evaluatiecommissie Wiv 2002 (Commissie Dessens), *Wet op de inlichtingen- en veiligheidsdiensten 2002: Naar een nieuwe balans tussen bevoegdheden en waarborgen*, 2 december 2013.
26. *Kamerstukken II* 2016/17, 34588, nr. 3, p. 105 (hierna: MvT Wiv 2017).
27. Zie: Bijlagen 'Externe adviezen' bij *Kamerstukken II* 2016/17, 35488, nr. 3.
28. *Kamerstukken II* 2016/17, 34588, nr. 66 (motie-Recourt). Dit vereiste is daarna als wettelijke norm geïmplementeerd middels de Wet van 16 juni 2021 tot wijziging van de Wiv 2017, *Stb.* 2021, 300.
29. Evaluatierapport, p. 4.
30. Art. 26 Wiv 2017.
31. Zie ook: J.J. Oerlemans & Q.A.M. Eijkman, 'Evaluatie Wiv 2017: betere uitvoerbaarheid, ten koste van privacy?', *Tijdschrift voor Internetrecht* 2021/3, p. 95-101.
32. Evaluatierapport, p. 83, 156.
33. Algemene Rekenkamer 2021, p. 63.
34. Algemene Rekenkamer 2021, p. 64.
35. Evaluatierapport, p. 126, 127. Voorbeelden: TIB, *Jaarverslag 2018/2019*, p. 14; TIB, *Jaarverslag 2019/2020*, p. 10. Zie ook: 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.
36. Evaluatierapport, p. 126. Vgl. Y. Buruma, 'Wettelijke hackbevoegdheden', *NJB* 2022/2545, afl. 36.
37. Evaluatierapport, p. 127.
38. Zie ook: H. Vijver, 'Overdaad aan toezicht schaadt inlichtingenwerk', *NRC* 25 april 2022.
39. Art. 45 Wiv 2017
40. MvT Wiv 2017, p. 77.
41. Voorgesteld art. 4 lid 1.
42. Art. 45 lid 8 Wiv 2017.

geautomatiseerd werk van die persoon of organisatie', het voorstel spreekt van 'een ander geautomatiseerd werk dat door de desbetreffende persoon of organisatie *in gebruik* is'. Het eigendomsbegrip dat wordt geïmpliceerd door het woord 'van' wordt hierbij dus losgelaten.

Hierdoor maakt de Cyberwet het bijschrijven van gedeelde systemen mogelijk.[43] De CTIVD houdt hier bindend toezicht op. Gedeelde systemen houden in deze context in dat een *target* bijvoorbeeld gebruik blijkt te maken van nog een ander geautomatiseerd werk dan wat in eerste instantie door de diensten gehackt wordt. Zoals reeds benoemd willen de diensten meebewegen met actoren die potentieel een bedreiging vormen. Als de andere computer van een actor dan niet gehackt mag worden, verliezen de diensten het zicht op de actor. Bovendien gaat de Wiv 2017 uit van *fysieke* systemen, terwijl computers vaak *virtueel* zijn op gedeelde servers.[44] Met de wijziging in de Cyberwet komen de diensten dus niet voor een figuurlijk dichte deur te staan bij het volgen van bedreigende actoren. Ook deze wijziging komt ten gunste van een dynamische inzet van de hackbevoegdheid die aansluit bij de digitale realiteit.

Als de andere computer van een actor dan niet gehackt mag worden verliezen de diensten het zicht op de actor

4.3. Technische risico's

Ten derde stelt de Cyberwet voor de technische toets door de TIB los te laten. Onder de Wiv 2017 is het zo dat de TIB vóóraf de technische risico's toetst die verbonden zijn aan de inzet van de hackbevoegdheid. Deze toets wordt vervangen door *ex durante* toetsing door de CTIVD. De toelichting bij het wetsvoorstel geeft aan dat technische risico's moeilijk zijn in te schatten of te beschrijven als de hackbevoegdheid nog niet is ingezet.[45] Dat onder de Wiv 2017 deze risico's toch uitgebreid in de aanvraag voor toestemming moeten worden opgenomen, zorgt volgens de toelichting bij de Cyberwet voor vertraging bij de inzet van de hackbevoegdheid.

Het buiten toepassing laten van het beschrijven van alle technische risico's is vooral van belang als het gaat om het gebruik van onbekende kwetsbaarheden bij de hack.[46] Deze kwetsbaarheden (fouten in hard- of software) kunnen door de diensten worden gebruikt om beveiliging te doorbreken.[47] Hiervoor geldt des te meer dat het vaak pas tijdens een hackoperatie duidelijk wordt of een onbekende kwetsbaarheid daadwerkelijk moet worden ingezet en zo ja, welke.[48] Onbekende kwetsbaarheden die onbekend blijven, brengen de nodige maatschappelijke risico's met zich mee. Eenieder kan ze immers in potentie gebruiken om te hacken. De diensten hebben daarom als uitgangspunt dat onbekende kwetsbaarheden gemeld moeten worden, tenzij er zwaarwegende belangen zijn voor de nationale veiligheid.[49]

Het is niet zo dat het toezicht op technische risico's verdwijnt: het wordt slechts belegd bij de CTIVD in plaats van bij de TIB. De CTIVD krijgt dan de mogelijkheid om onbekende kwetsbaarheden casuïstisch te benaderen. Dit sluit beter aan bij het feit dat het per kwetsbaarheid sterk verschilt hoeveel maatschappelijk risico de kwetsbaarheid met zich meebrengt.[50] Juist omdat technische risico's pas bekend zijn kort voordat zij zich in de loop van de hackoperatie manifesteren, sluit het *ex durante* toezicht van de CTIVD hier goed bij aan. Overigens moet worden opgemerkt dat de TIB de *voorzienbare* technische risico's nog wel bij de proportionaliteitstoets voor de inzet van de hackbevoegdheid mag betrekken. In het wetsvoorstel blijft echter in het midden wanneer technische risico's precies voorzienbaar zijn. Waarschijnlijk kan de TIB alleen evident ontwrichtende technische risico's als voorzienbaar bestempelen en meenemen in de proportionaliteitstoets. Een hackoperatie die met zulke risico's gepaard gaat, zal met het oog op bestaand beleid van de diensten en het belang dat zij zelf hebben bij 'operational security' (de diensten willen niet ontdekt worden tijdens een hackoperatie)[51] niet snel worden uitgevoerd. Het is daarnaast niet wenselijk dat de TIB het begrip 'voorzienbaar' te ruim invult, nu dat niet strookt met de insteek van het gewijzigde toezichtstelsel, waarbij juist de CTIVD toeziet op de technische risico's.

4.4. Strategische operaties

De toelichting bij het wetsvoorstel gaat ook in op de 'strategische inzet van bevoegdheden'. Een zogenoemde 'strategische operatie', gaat niet over het inzetten van nieuwe bevoegdheden maar over de inzet van bevoegdheden (vaak de hackbevoegdheid) met een strategisch doel.[52] Strategische operaties kunnen gericht zijn op het verkrijgen van kennis over hard- en software of over specifieke locaties van apparatuur.[53] Een dergelijke operatie kan ook plaatsvinden omdat de diensten een informatiepositie willen verkrijgen, bijvoorbeeld als het gaat over nieuwe technologieën. Een technologie is immers per definitie geen *target*, terwijl het inwinnen van informatie erover wel een onderzoeksopdracht kan zijn uit de Geïntegreerde Aanwijzing. De diensten hebben onder de Wiv 2017 meermaals verzocht de hackbevoegdheid in te zetten op basis van een strategische onderbouwing, wat soms als rechtmatig werd beoordeeld.[54] Desalniettemin bestaat er onder andere bij de TIB onduidelijkheid over hoe een dergelijke inzet zich verhoudt tot een goede taakuitvoering van de diensten.[55]

De TIB heeft meermaals benadrukt dat zij moeite ondervindt bij het beoordelen van de hackbevoegdheid in het kader van strategische operaties.[56] Ook de Evaluatiecommissie drong eerder aan op verduidelijking op dit punt. Het wetsvoorstel poogt daarom uitgebreider toe te lichten wanneer een strategische operatie aan de orde kan zijn, maar slaagde daar in eerste instantie slechts deels in, zoals bleek uit de reacties op de consultatieversie van het wetsvoorstel.[57] Daarom zijn in de meest recente versie van het voorstel (september 2022) meer voorbeelden opgenomen.[58] Het kabinet doet met de Cyberwet een goede poging om de strategische inzet van

bevoegdheden verder te duiden en om de TIB handvatten te geven in haar beoordeling daarvan. Het concept van een strategische operatie lijkt echter dusdanig breed invulbaar te zijn (deze kan in theorie betrekking hebben op zowel het hacken van een telecomprovider als het verzamelen van concrete informatie over een bepaalde technologie) dat de proportionaliteitstoets een lastige opgave zal blijven.

5. Kabelinterceptie in de Tijdelijke wet

5.1. Waarom is kabelinterceptie nodig?

In het wetsvoorstel wordt ten opzichte van de inzet van onderzoeksopdrachtgerichte interceptie (artikel 48 Wiv 2017) een aantal wijzigingen voorgesteld. De tijdelijke wet maakt, beter dan de Wiv 2017, in heldere bewoordingen duidelijk wat kabelinterceptie is: bulkinterceptie. Dit kan uit de ether, maar belangrijker: ook op de internetkabel. In het kader van cybersecurity willen de diensten zicht hebben op bekende, maar ook op onbekende dreigingen die zich manifesteren op de ICT-infrastructuur. Deze dreigingen veranderen en verspringen continu.

De toelichting bij het wetsvoorstel geeft aan, net zoals de memorie van toelichting bij de Wiv 2017, dat dit is waar de noodzaak van kabelinterceptie ligt: in het onderkennen van ongekende dreigingen. Dit 'ongekende' element zorgt voor spanning met het gerichtheidsvereiste: er moet een bepaalde mate van ongerichtheid zijn om dreigingen te vinden die (nog) niet evident zijn, maar uit de wet vloeit voort dat wél onderbouwd moet worden dat de inzet voldoet aan het gerichtheidsvereiste. Waar bij bulkinterceptie uit de ether sprake was van uitgebreide kennis bij de diensten over welke specifieke satelliet nodig was voor welke specifieke gegevensstromen, is bij interceptie op een internetkabel vaak moeilijk te voorspellen door welke *fiber* van een internetkabel de benodigde informatie precies zal lopen. Dientengevolge is de *status quo* dat de terminologie en opzet van de Wiv 2017 het lastig maken om bepaalde bijzondere bevoegdheden (tijdig) in te zetten wanneer dit door de diensten noodzakelijk wordt geacht.[59] Het gerichtheidsvereiste waarop de TIB volgens de wet dient te toetsen, leidt bij bulkinterceptie op de kabel tot een paradox; bulkinterceptie is per definitie ongericht.[60]

Het gerichtheidsvereiste waarop de TIB volgens de wet dient te toetsen leidt bij bulkinterceptie op de kabel tot een paradox; bulkinterceptie is per definitie ongericht

Cybersecurity was een van de redenen waarom bulkinterceptie op de kabel in de Wiv 2017 noodzakelijk werd geacht. Door bulkinterceptie kan internetverkeer namelijk aan onderzoek worden onderworpen. Daardoor kunnen bijvoorbeeld bepaalde kenmerken van malware worden ontdekt, of kan afwijkend verkeer worden opgemerkt om zo ook aanvallen te detecteren.[61] Dit stelt de diensten in staat om informatie met handelingsperspectief te bieden aan betrokken partijen.[62] Gezien de enorme hoeveelheid gegevens die dagelijks via internetkabels over de wereld wordt gestuurd, leidt geen zicht hebben op internetkabels inherent tot een beperkte inlichtingenpositie. Dat door de Wiv 2017 de inzet van kabelinterceptie vaak niet kan worden goedgekeurd, is vanuit nationaal veiligheidsperspectief dan ook geen goede zaak. De AIVD en de MIVD zijn niet in het leven geroepen om achter incidenten aan te hollen, maar om dreigingen voor de nationale veiligheid in kaart te brengen en waar nodig aan te pakken.[63] Ze moeten dus *inspelen* op de onbekende en ongekende dreigingen.[64] In de praktijk komt dit erop neer dat de diensten flexibel moeten kunnen zijn om operationeel effectief te zijn. De Cyberwet poogt de diensten in dit kader meer armslag te geven.

5.2. Verkennen op de kabel

De bestaande spanning tussen kabelinterceptie en het gerichtheidsvereiste tracht de wetgever in de Cyberwet aan te pakken. Zo wordt er een aparte, zelfstandige regeling gegeven voor de verkenning van gegevensstromen op de kabel, met als doel de daadwerkelijke kabelinterceptie zo goed mogelijk te kunnen omschrijven. Dit wordt 'snapshotten' genoemd, oftewel: 'verkenningsinter-

43. Concept-memorie van toelichting Cyberwet, onder 3.2.5.
44. Evaluatierapport, p. 93.
45. Zie ook: CTIVD, Toezichtsrapport nr. 70 over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD, 19 augustus 2020 (hierna: CTIVD-rapport nr. 70).
46. Zie ook: Advies Raad van State over de consultatieversie van de Cyberwet, W04.22.0073/I, 22 juni 2022, p. 19-20.
47. Zie ook: CTIVD Toezichtsrapport nr. 53 over de inzet van de hackbevoegdheid door de AIVD en de MIVD in 2015, 8 maart 2017.
48. CTIVD-rapport nr. 70.
49. AIVD, *Beleid omgang onbekende kwetsbaarheden* (aivd.nl/documenten/publicaties/2018/05/01/beleid-omgang-met-onbekende-kwetsbaarheden).
50. AIVD, *Beleid omgang onbekende kwetsbaarheden*.
51. CTIVD-rapport nr. 70, p. 17.
52. Zie ook: TIB Jaarverslag 2021, p. 15; Memorie van toelichting bij het Wetsvoorstel Tijdelijke Wet Cyberoperaties, versie september 2022, onder 2.2.2.
53. Concept-memorie van toelichting Cyberwet, onder 2.2.2.
54. Toetsingscommissie Inzet Bevoegdheden, Jaarverslag 2021 (hierna: TIB Jaarverslag 2021), p. 10.
55. TIB Jaarverslag 2021, p. 15. Een goede taakuitvoering van de diensten is neergelegd in art. 28 Wiv 2017.
56. TIB jaarverslag 2020; TIB jaarverslag 2021.
57. Zie ook de reactie van J.J. Oerlemans en mijzelf bij het voorstel: internetconsultatie.nl/tijdelijkewetcyber/reactie/28f40004-3100-42a9-a309-b4bd7b92b42e (hierna: Reactie Cyberwet Oerlemans & Harleman).
58. Concept-memorie van toelichting Cyberwet, onder 2.2.2.
59. Algemene Rekenkamer 2021, p. 63-64.
60. CTIVD, *Toezichtsrapport nr. 75 over de inzet van kabelinterceptie door de AIVD en de MIVD*, 26 januari 2022 (hierna: CTIVD rapport nr. 75), p. 5, 6, 12 e.v. Zie verder par. 4.2 over kabelinterceptie.
61. MvT Wiv 2017, p. 105. Zie ook: T. Steffens, *Attribution of Advanced Persistent Threats: How to identify the actors behind cyber-espionage*, Berlijn: Springer 2020.
62. *Kamerstukken II* 2021/22, 30977, nr. 161, p. 1.
63. Zie ook: P.H.A.M. Abels, *Per undas adversas? Geheime diensten in de maalstroom van politiek en beleid* (oratie Leiden), 16 februari 2018.
64. Algemene Rekenkamer 2021, p. 38, 39.

ceptie', om de gegevensstromen te verkennen en te bezien of men de juiste stromen te pakken heeft om antwoord te kunnen geven op de onderzoeksvragen.[65] Aan de hand van deze voorfase van kabelinterceptie kan bij de opvolgende aanvraag tot kabelinterceptie worden onderbouwd of er wordt voldaan aan het gerichtheidsvereiste, door aan te geven over welke *fiber* veel potentieel relevant verkeer loopt. Nu snapshotten klaarblijkelijk als doel heeft bij te dragen aan de *onderbouwing* van het gerichtheidsvereiste, wordt door de wetgever in de Cyberwet het gerichtheidsvereiste buiten werking gesteld bij het snapshotten zelf.[66]

Het produceren van inlichtingen voor afnemers (zoals het Ministerie van Justitie en Veiligheid of Defensie) is niet het doel van de gegevens die door snapshotten worden verzameld.[67] Dientengevolge komt er met het wetsvoorstel niet 'alsnog een sleepnet',[68] maar wordt juist gepoogd de kabelinterceptie *gerichter* te kunnen inzetten. In die zin tracht de wetgever met de verkenningsbevoegdheid een extra waarborg in het leven te roepen.

Dientengevolge komt er met het wetsvoorstel niet 'alsnog een sleepnet', maar wordt juist gepoogd de kabelinterceptie *gerichter* te kunnen inzetten

5.3. 'Nederland-Nederland-verkeer'

De TIB geeft in zijn reactie op het conceptwetsvoorstel aan dat de bevoegdheid voor kabelinterceptie wordt uitgebreid als het gaat om verkeer van en naar streamingdiensten en verkeer van en naar Nederland ('Nederland-Nederland-verkeer'). Dit was eerder door de ministers uitgesloten.[69] Bij de totstandkoming van de Wiv 2017 is echter reeds benoemd dat voor 'cyber defence' een uitzondering moet worden gemaakt.[70]

Bij digitale aanvallen kan immers misbruik worden gemaakt van de Nederlandse digitale infrastructuur. Zonder zicht op deze infrastructuur (door middel van kabelinterceptie) kan dit misbruik niet worden ontdekt.[71] De geografische locatie waar een dreiging zich manifesteert, en de locatie van de actor *achter* de dreiging, komen in het huidige digitale tijdperk vaak niet overeen. Het standpunt van de ministers paste derhalve op voorhand niet bij de infrastructuur van het internet. Nederland-Nederland-verkeer kan feitelijk slaan op gehuurde of gehackte routers die in Nederland staan, en van waaruit er gegevensverkeer wordt verstuurd naar een ander router in Nederland. Dit verkeer heeft in dat geval niet uitsluitend betrekking op Nederlandse burgers. De MIVD zag bijvoorbeeld in 2021 dat de Russische militaire inlichtingendienst (GRU) Nederlandse routers had gehackt van het midden- en kleinbedrijf en privépersonen.[72] Op deze manier kon de GRU cyberoperaties uitvoeren via routers van onwetende burgers en bedrijven in Nederland. Als de diensten Nederland-Nederland verkeer niet mogen onderscheppen, lopen ze een significante achterstand op statelijke actoren die dat wel doen, om het vervolgens te gebruiken voor spionage- of sabotagedoeleinden.

Ook een verbod op het intercepteren van gegevens van streamingsdiensten en BitTorent-verkeer lijkt niet reëel.[73] Ten eerste kan er, los van de inhoud van de streaminggegevens, sprake zijn van relevante metadata in het kader van 'cyber defence' (bijvoorbeeld om te bezien vanuit waar verbinding wordt gemaakt met een bepaald netwerk). Ten tweede worden streamingdiensten allang niet meer enkel gebruikt voor een avondje film, maar ook voor livestreaming van gebeurtenissen van uiteenlopende aard en als discussie- en communicatieplatform (hierbij valt te denken aan YouTubekanalen waar middels reacties of livechat op wordt gecommuniceerd). Het is daarom goed dat de Cyberwet afstand doet van de belofte om voor Nederland-Nederland-verkeer en streamingdiensten een uitzondering te maken. Deze uitzondering sluit immers niet aan bij de feitelijke werking van het internet en de bijbehorende infrastructuur.

6. Slot

In deze bijdrage zijn enkele wijzigingen rondom de inzet van bevoegdheden besproken, die volgens het wetsvoorstel moeten voorzien in meer slagkracht voor de inlichtingen- en veiligheidsdiensten in onderzoeken naar offensieve cyberprogramma's. Evident is dat de vraag hoe effectief het wetsvoorstel zal zijn lastig op voorhand te beantwoorden is. Desalniettemin zijn er enkele belangrijke wijzigingen die mijns inziens de effectiviteit voor een groot deel zullen beïnvloeden.

In de kern zullen de huidige patstellingen tussen de TIB en de diensten doorbroken moeten worden. Het voorstel doet daartoe een poging en probeert vooral enkele knelpunten rondom de inzet van bulkinterceptie en de hackbevoegdheid op te lossen. Daarmee is het wetsvoorstel, voor zover in de praktijk het toezicht zal functioneren, op het eerste gezicht een effectief middel om het door het kabinet gestelde doel te bereiken. Daarnaast wordt voorgesteld om het toezicht met waarborgen op niveau te houden. De 'bottom line' is dat bulkinterceptie en de hackbevoegdheid tegenwoordig van essentieel belang zijn voor de nationale veiligheid van Nederland. De inlichtingen- en veiligheidsdiensten hebben te maken met offensieve cyberprogramma's van statelijke actoren die erop gebrand zijn met steeds geavanceerdere middelen steeds grotere strategische voordelen te behalen, met alle risico's van dien. Dit wordt door Cybersecuritybeelden al jaren benadrukt.

De hackbevoegdheid geeft de diensten de mogelijkheid om statelijke actoren te volgen en cyberaanvallen te attribueren aan buitenlandse inlichtingen- en veiligheidsdiensten. Hierbij is van belang dat de diensten kunnen meebewegen en dat de bevoegdheid dynamisch kan worden ingezet tijdens de periode waarvoor toestemming is gegeven. Met dit doel in het achterhoofd zet het wetsvoorstel met het verlagen van de verkenningsdrempel een goede stap. Ook het loslaten van het exclusiviteitsvereiste

bij de hackbevoegdheid sluit aan bij wat het meebewegen op het internet bij de inzet van hackbevoegdheid in de praktijk inhoudt.

Met kabelinterceptie kunnen bulkdata verzameld worden. Dit is gezien de verborgen en verspringende aard van cyberdreigingen van essentieel belang om zicht te kunnen houden op welke dreigingen er zijn en hoe zij zich zullen manifesteren. In het huidige tijdperk is nu eenmaal geen sprake meer van enkel vastomlijnde targets in het cyberdomein, in de vorm van personen of organisaties. Deze zitten wellicht *achter* de dreiging, maar door gebruik te maken van digitale infrastructuur wordt de dreiging zelf (deels) anoniem, diffuus en sluipend. Er is, kort gezegd, meer informatie nodig om een dreiging tastbaar te kunnen maken en handelingsperspectief te bieden aan afnemers van inlichtingenproducten.

Het is desalniettemin begrijpelijk dat aspecten van het wetsvoorstel het nodige stof doen opwaaien. Verkennen ten behoeve van kabelinterceptie is zelf immers ook bulkinterceptie én mag ongericht. Met de huidige beperkingen en waarborgen (de gegevens mogen niet worden meegenomen in het inlichtingenproces en er blijft bindend toezicht middels het *ex durante* toezicht van de CTIVD) is er echter geen sprake van ongerichte datahonger. Dat met verkenning op de kabel gepoogd wordt om gerichter te intercepteren, lijkt in theorie geen extra privacy-inbreuk, maar een extra waarborg.

Hoe effectief het wetsvoorstel is zal voor een groot deel afhangen van hoe het toezichtstelsel in de praktijk zal werken. Het veranderde toezicht brengt de nodige onzekerheid met zich mee. Niet is van tevoren precies te voorspellen hoe *ex durante* en *ex post* toezicht in de praktijk zal functioneren. Wel kan toezicht *tijdens* een operatie een goede balans zijn tussen voldoende dynamiek in de inzet van bevoegdheden en voldoende waarborgen. Aangescherpt bindend toezicht tijdens de inzet van een bevoegdheid kan bovendien ten opzichte van slechts voorafgoedkeuren ook een extra waarborg zijn, omdat dan de daadwerkelijke uitvoering van bevoegdheden door de diensten onder de loep ligt. Gezien de onzekerheid omtrent het nieuwe toezichtstelsel is het noodzakelijk het functioneren van het wetsvoorstel, en in het verlengde daarvan ook van de uitwerking van het toezicht in de praktijk, tijdig te evalueren.

Tot slot rijst de vraag hoe het wetsvoorstel bijdraagt aan het in een vroeg stadium vaststellen of achter een cyberaanval een statelijke actor of een criminele organisatie zit. Deze vraag is relevant gezien de reikwijdte van het wetsvoorstel, die beperkt is tot offensieve cyberprogramma's van staten. Wat als er sprake blijkt te zijn van cybercrime? En wat als er sprake is van cybercrime die de nationale veiligheid bedreigt, zoals volgens het meest recente 'Cybersecuritybeeld Nederland' bij ransomware het geval is? Door de dreiging die (voor de nationale veiligheid) uitgaat van cybercrime buiten beschouwing te laten, is de wetgeving smaller gemaakt dan het vraagstuk feitelijk is. Daarmee lijkt de effectiviteit voor wat betreft het tegengaan van ransomware in ieder geval beperkt.

Door de dreiging die (voor de nationale veiligheid) uitgaat van cybercrime buiten beschouwing te laten, is de wetgeving smaller gemaakt dan het vraagstuk feitelijk is

Dit doet er echter niet aan af dat het wetsvoorstel op het eerste gezicht bijdraagt aan een goede balans tussen waarborgen en effectieve inzet van bevoegdheden. Alles overwegende concludeer ik dat de Cyberwet voorziet in meer dynamische bevoegdheden die in potentie de diensten meer armslag geven in het tegengaan van offensieve cyberprogramma's van statelijke actoren. •

65. CTIVD-rapport nr. 75.
66. Concept-art. 7 lid 4.
67. Zie ook: CTIVD-rapport nr. 75.
68. Zie: Huib Modderkolk, 'Nederland stemde tegen de "sleepwet" en toch staat nu alles klaar voor grootschalig aftappen', *de Volkskrant* 16 mei 2022.
69. Brief van de Ministers van BZK en van Defensie van 6 april 2018 (*Kamerstukken I* 2017/18, 34588, G).
70. *Kamerstukken I* 2017/18, 34588, G, p. 3.
71. MvT Wiv 2017, p. 224.
72. H. Modderkolk, 'MIVD verstoort Russische digitale aanval op routers van Nederlandse burgers', *de Volkskrant* 3 maart 2022.
73. Dit verbod blijkt uit de bijlage bij 'Brief minister BZK aan Tweede Kamer over Wiv 2017 en het regeerakkoord', 15 december 2017, *Kamerstukken II* 2017/18, 34588, nr. 69, p. 3.