Cyber agent technology en de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV)

Bart Custers

Onderzoek uitgevoerd door
eLaw, centrum voor recht en digitale technologie
Universiteit Leiden
in opdracht van
Tracks Inspector
Den Haag

30 september 2017

Inhoud

1. Inleiding

1.1 Aanleiding en context

Tracks Inspector is een bedrijf dat innovatieve software ontwikkelt die het voor gebruikers mogelijk maakt samen te werken bij onderzoek van grote hoeveelheden digitaal bewijs. In de afgelopen jaren heeft Tracks Inspector software ontwikkeld die gekenschetst kan worden als *cyber agent technology*. Dit is technologie die cyber agents (online actoren) ondersteunt in een online omgeving door bepaalde taken te automatiseren. De technologie kan onder meer interacties aangaan met anderen in dynamische en open omgevingen. De cyber agent technology van Tracks Inspector werd onder meer ontwikkeld voor het Sweetie 2.0 project van Terre des Hommes.[1] Op basis van eerder onderzoek werd deze technologie zodanig vormgegeven dat zeer realistisch een 10-jarig meisje kon worden gesimuleerd dat op internet conversaties kan aangaan met verdachte personen die seksuele interesse tonen voor kinderen, met als doel deze verdachte personen te identificeren en te waarschuwen.

Eerder is reeds onderzoek gedaan naar de juridische aspecten van deze software voor de strafrechtelijke opsporing,[2] maar nog niet voor inlichtingen- en veiligheidsdiensten. Mogelijk is deze cyber agent technology ook bruikbaar voor inlichtingen- en veiligheidsdiensten in Nederland. Daarom heeft Tracks Inspector gevraagd aan eLaw, het centrum voor recht en digitale technologie van de Universiteit Leiden, uit te zoeken hoe de ontwikkelde software zich verhoudt tot het kader van de Wet op de inlichten- en veiligheidsdiensten (WIV), teneinde inzicht te krijgen enerzijds in hoeverre deze software inzetbaar is onder de nieuwe WIV-bevoegdheden en anderzijds in hoeverre deze software inlichtingen- en veiligheidsdiensten kan helpen bij het invullen van nieuwe WIV-verplichtingen omtrent gegevensbeheer, bijvoorbeeld als het gaat om betrouwbaarheid en volledigheid van gegevens of om het bewaren en vernietigen van informatie.

1.2 Probleemstelling

De centrale vraagstelling van dit onderzoek is:

Hoe verhoudt het gebruik van de cyber agent technology door inlichtingen- en veiligheidsdiensten zich tot het juridisch kader van de nieuwe WIV, in het bijzonder ten aanzien van:

a) De inzetbaarheid van de software onder de nieuwe WIV-bevoegdheden?
b) De bruikbaarheid van de software bij het invullen van WIV-verplichtingen?

Het onderzoek dat is beschreven in dit rapport is verkennend van karakter. Het onderzoek is juridisch van aard en richt zich op de 'nieuwe' WIV, de WIV 2017. Het juridisch kader voor de inlichtingen- en veiligheidsdiensten in Nederland wordt ten tijde van uitvoering van dit onderzoek (najaar 2017) herzien. Het 'oude' kader is de WIV uit 2002. Het kabinet heeft op 15 april 2016 ingestemd met een

[1] https://www.terredeshommes.nl/programmas/sweetie-20-webcamseks-met-kinderen-de-wereld-uit. Zie ook Wal, C. van der (2016) Sweetie 2.0: nieuw virtueel meisje gaat op pedojacht, *Algemeen Dagblad*, 13 februari 2016. https://www.ad.nl/binnenland/sweetie-2-0-nieuw-virtueel-meisje-gaat-op-pedojacht~ad3739ca/

[2] Schermer, B.W., Georgieva, I., Van der Hof, S., Koops, B.J. (2016) *Legal Aspects of Sweetie 2.0*. Leiden University & Tilburg University.
Zie https://www.terredeshommes.nl/sites/tdh/files/uploads/2016_10_03_sweetie_legal_aspects_report.pdf.

wetsvoorstel[3] voor een nieuwe WIV van de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie. Het wetsvoorstel wijziging Wet op de inlichtingen- en veiligheidsdiensten is in het najaar van 2016 naar de Tweede Kamer gestuurd. Op 14 februari 2017 ging de Tweede Kamer akkoord. De Eerste Kamer is op 11 juli 2017 akkoord gegaan. Het is niet bekend wanneer de nieuwe wet in werking treedt.[4] Omdat het wetsvoorstel reeds door beide kamers der Staten-Generaal is goedgekeurd, zal de nieuwe WIV het uitgangspunt vormen voor dit onderzoek.

Bij deelvraag a is het doel van het onderzoek een lijst met knelpunten (aandachtspunten) te produceren ten aanzien van de inzetbaarheid van de software binnen de WIV-bevoegdheden van inlichten- en veiligheidsdiensten. Daartoe wordt eerst in kaart gebracht binnen welke bevoegdheden de inzet van de cyber agent technology toegelaten is. Daarna wordt nagegaan aan welke vereisten waaraan zou moeten worden voldaan of waaraan aandacht zou moeten worden besteed in de context van de nieuwe WIV. Waar mogelijk wordt ook gesuggereerd hoe dat aangepakt kan worden, maar het onderzoek is niet zo opgezet dat gedetailleerd advies wordt geboden over hoe de cyber agent technology WIV-compliant zou kunnen worden gemaakt – daarvoor zou een uitgebreider onderzoek nodig zijn.

Bij deelvraag b is het doel van het onderzoek een overzicht van kansen te produceren voor de bruikbaarheid van de software bij het (verder/beter) invullen van verplichtingen die inlichtingen- en veiligheidsdiensten onder de nieuwe WIV hebben ten aanzien van het verzamelen, verwerken en vernietigen van informatie. Daarbij kan in het bijzonder worden gedacht aan termijnen voor het bewaren en vernietigen van informatie, maar aan verslaglegging, notificatieplichten, verbeteren van betrouwbaarheid en volledigheid van de gegevens en geheimhoudingsplichten.

1.3 Methodologie

Dit onderzoek is vrijwel geheel gebaseerd op desk research, waarbij onder meer (a) de bevoegdheden van de inlichtingen- en veiligheidsdiensten en (b) de verplichtingen met betrekking tot verzamelen, verwerken en vernietigen van informatie zoals genoemd in de nieuwe WIV stapsgewijs zijn nagelopen met het oog op mogelijke toepassingen van de door Tracks Inspector ontwikkelde cyber agent technology. Ter verheldering van de werking van de software is in het kader van dit project een interview uitgevoerd (d.d. woensdag 13 september 2017) met de opdrachtgever, met de heer dr. ir. Hans Henseler en de heer ir. Rens van der Wolf CISSP CISA CISM. Tijdens dit interview stond de werking van de ontwikkelde software centraal, teneinde dit goed te kunnen kaderen in de context van de WIV en de beperkingen c.q. wettelijke vereisten te kunnen signaleren. Er zijn geen interviews gehouden met medewerkers van inlichtingen- en veiligheidsdiensten.

Het onderzoek is uitgevoerd in de periode 28 augustus – 1 oktober 2017. Ontwikkelingen na deze periode zijn niet meegenomen in dit onderzoek. Gelet op de geringe omvang van het onderzoek is geen begeleidingscommissie opgezet.

1.4 Structuur van dit rapport

Dit rapport is als volgt opgebouwd. In hoofdstuk 2 wordt een korte beschrijving gegeven van de door Tracks Inspector ontwikkelde cyber agent technology. Daarbij wordt ingegaan op de verschillende

[3] Voorstel van wet houdende regels met betrekking tot de inlichten- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..). *Kamerstukken II* Vergaderjaar 2016/2017, 34 588, nrs. 1 t/m 3.

[4] https://www.rijksoverheid.nl/onderwerpen/bevoegdheden-inlichtingendiensten-en-veiligheidsdiensten/wet-op-de-inlichtingen-en-veiligheidsdiensten-wiv

technische elementen van de software, waaronder het online platform dat beschikbaar is en de optionele inzet van een chatbot functionaliteit en de 3-dimensionale uitbeelding van personen.

In hoofdstuk 3 wordt kort ingegaan op enkele mogelijke toepassingen van de cyber agent technology voor inlichtingen- en veiligheidsdiensten. Eerst worden de taken van de AIVD en de MIVD beschreven. Daarna komen verschillende toepassingen van cyber agent technology aan bod die meerwaarde kunnen bieden bij de uitvoering van verschillende van deze taken.

In hoofdstuk 4 wordt een korte introductie tot de nieuwe wet op de inlichtingen- en veiligheidsdiensten (WIV 2017) gegeven. Daarbij wordt kort de geschiedenis en totstandkoming van de nieuwe WIV beschreven. Daarna wordt dieper ingegaan op de voor dit onderzoek relevante onderdelen van de WIV, te weten de informatiebevoegdheden in hoofdstuk 3 (de verwerking van gegevens) en hoofdstuk 4 (overige bijzondere bevoegdheden) van de WIV en de informatieverplichtingen in onder meer paragraaf 3.4 (de verstrekking van gegevens) en hoofdstuk 5 (kennisneming van verwerkte gegevens) van de WIV.

In hoofdstuk 5 wordt antwoord gegeven op deelvraag a (de inzetbaarheid van de cyber agent technology onder de nieuwe WIV-bevoegdheden). Daarbij worden wettelijke bevoegdheden (interceptie, observatie, afluisteren, werken onder dekmantel, infiltratie, etc.) nagelopen om te zien welke van deze bevoegdheden (het beste) ruimte bieden voor de inzet van cyber agent technology. Vervolgens wordt onderzocht welke knelpunten er zijn en welke eisen (onder meer met betrekking tot proportionaliteit en subsidiariteit) gesteld worden aan de inzet van cyber agent technology.

In hoofdstuk 6 wordt antwoord gegeven op deelvraag b (de bruikbaarheid van de cyber agent technology bij het invullen van WIV-verplichtingen). De verplichtingen die in hoofdstuk 4 van dit rapport in kaart zijn gebracht, worden nagelopen. Deze verplichtingen worden nader onderzocht evenals de kansen die de cyber agent technology kan bieden.

In hoofdstuk 7 wordt de centrale vraagstelling van dit onderzoek beantwoord en worden conclusies getrokken ten aanzien van de inzetbaarheid en bruikbaarheid van de cyber agent technology onder de nieuwe WIV. Daarbij worden enkele aandachtspunten benoemd voor de verdere ontwikkeling van de onderzocht cyber agent technology.

2. Cyber agent technology

In dit hoofdstuk wordt een korte beschrijving gegeven van de door Tracks Inspector ontwikkelde cyber agent technology. Eerst wordt enige gebruikte terminologie verduidelijkt (paragraaf 2.1), vervolgens wordt de functionaliteit van de cyber agent technology geschetst (paragraaf 2.2).

2.1 Terminologie

Dit onderzoek gaat over *cyber agent technology*. Daarmee wordt technologie bedoeld die cyber agents (online actoren) ondersteunt. De door Tracks Inspector ontwikkelde technologie betreft een online omgeving die bepaalde taken automatiseert, zodat medewerkers zich meer kunnen richten op hun kerntaken, bijvoorbeeld het selecteren van relevante informatie of zogeheten *persons of interest*. Deze cyber agent technology kan naast het systematisch en gestructureerd vastleggen van gegevens bovendien interacties aangaan met andere personen die online zijn (zie hieronder). Cyber agent technology kan een bepaalde autonomie bevatten en daarmee zelfstandig handelen, waarmee de technologie een zelfstandige online actor wordt. Hiervoor worden ook wel de termen *software agents*[5] (als het gaat om de actoren) en *agent technology*[6] (als het gaat om de onderliggende technologie) gebruikt. Dit zijn intelligente programma's die zonder directe tussenkomst van de mens kunnen handelen.[7] Het zijn technieken en algoritmen die interacties met anderen kunnen aangaan in dynamische en open omgevingen.[8] Als zodanig kunnen software agents worden beschouwd als een vorm van kunstmatige intelligentie (*artificial intelligence*, AI).[9]

De *cyber agents* zijn online actoren. Dat kunnen natuurlijke personen zijn of software agents. De natuurlijke personen in de context van inlichtingen- en veiligheidsdiensten zijn de medewerkers (ambtenaren) van deze diensten. De software agents worden ook wel aangeduid als *bots* (als afkorting van robots, al hoeven ze geen fysieke verschijningsvorm te hebben). Afhankelijk van hun functionaliteit kunnen specifieke vormen worden onderscheiden, zoals chatbots (programma's die kunnen communiceren in natuurlijke taal), web crawlers (programma's die het internet in kaart brengen), spambots (programma's die geautomatiseerd spam rondsturen) en Twitterbots (programma's die geautomatiseerd berichten op Twitter plaatsen). De bots kunnen meerdere verschillende *virtuele identiteiten* aannemen. Een chatbot kan bijvoorbeeld gelijktijdig chats voeren onder de namen John, Tracey en Mike, die elk converseren op hun eigen accounts, met hun eigen jargon en op basis van hun eigen karakteristieken.

De mate waarin software agents zelfstandig kunnen handelen, kan verschillen van ondersteunend tot volledig autonoom. Wanneer de software agents de natuurlijke personen ondersteunen, wordt gesproken van een hybride aanpak. In dat geval kan de natuurlijke persoon handmatig ingrijpen, in beginsel zonder dat degenen met wie interacties zijn aangegaan dat kunnen zien.

---

[5] Nwana, H. S. (1996) Software Agents: An Overview. *Knowledge Engineering Review*. 21 (3): 205–244.

[6] Luck, M., McBurney, P., and Preist, C. (2004) A Manifesto for Agent Technology: Towards Next Generation Computing, *Autonomous Agents and Multi-Agent Systems*, 9, 203-252.

[7] Schermer, B.W. (2007) *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance*, Leiden: Leiden University Press.

[8] Boccara, N. (2004) *Modeling Complex Systems, Graduate Texts in Contemporary Physics*, Springer: New York, NY, USA.

[9] Kurzweil, R. (1990) *The Age of Intelligent Machines*, Cambridge MA: MIT Press.

2.2 Functionaliteit

De door Tracks Inspector ontwikkelde cyber agent technology is in de eerste plaats een online platform (het software framework), waarbij optioneel ook chatbot en videostreaming functionaliteiten zijn in te zetten. Het platform biedt gebruikers virtuele identiteiten van cyber agents en instrumenten als chatbots, visuele avatars, het verwerken van communicatie, methoden voor data-analyse en identiteitsmanagement, takenplanning en gerichte berichtgeving en communicatie.

Het software framework is een online omgeving die werkt als een soort (real-time) dashboard, waarin gebruikers een overzicht wordt geboden van de verschillende functionaliteiten van de cyber agent technology. Zo zijn er overzichten van de verschillende chatrooms waarin de cyber agents zich begeven en overzichten van de gesprekken die daar worden gevoerd (inclusief uiteraard met wie wordt gesproken, wanneer en hoe lang). Ook zijn er overzichten van de verschillende identiteiten en karakters van de verschillende software agents.

In het platform kunnen personen met wie de cyber agent technology interacteert, worden gemarkeerd als '*person of interest*' en worden voorzien van verdere typeringen en markeringen (bijvoorbeeld gegevens met betrekking tot de identiteit en het karakter van deze personen). Ook in de gesprekken kunnen onderdelen en passages worden getypeerd, gecategoriseerd en gemarkeerd. Alle gesprekken worden via vooraf vastgestelde formats opgeslagen, inclusief schermopnames. Wanneer gebruik wordt gemaakt van andere kanalen (bijvoorbeeld skype, e-mail, etc.) en andere communicatievormen (bijvoorbeeld videoverbinding), wordt dit ook in vaste formats opgeslagen. Het gebruik van algemeen geaccepteerde standaarden voor de opslag van gegevens faciliteert de uitwisseling van gegevens en de mogelijkheden tot het matchen en combineren van gegevens, inclusief gegevens van andere organisaties. In termen van bewijsvoering bevorderen de vaste formats ook de transparantie van de wijze van bewijsvergaring.

Het is mogelijk om een hele range van digitale identiteiten aan te maken. Voor de cyber agents worden identiteiten met specifieke karakters aangemaakt, bestaande uit onder meer een persoonlijk profiel met naam, vrienden, locatie, etc. Daaraan worden verschillende accounts (e-mail, skype, etc.) toegevoegd waarmee de cyber agent ook buiten de chatroom 1-op-1 kan communiceren met anderen.

De 1-op-1 communicatie (bijvoorbeeld via e-mail) kan naast een bericht ook één of meer specifieke links (zogenaamde clickbait URL's) of bijlagen bevatten die gericht zijn op het verzamelen van aanvullende informatie over bijvoorbeeld de locatie, de gebruikte computer of identificatie van een *person of interest*. Bijlagen kunnen daarnaast een bepaalde "payload" bevatten die de gebruikte computer kan infecteren, commando's kan uitvoeren en/of heimelijke toegang op afstand kan verschaffen.

De chatbot functionaliteit is technisch gezien een traditionele vorm van artificial intelligence die rule-based is (met "als-dan"-redeneringen: "als iemand a zegt, dan is de reactie b"), al kan wel worden gekozen uit meerdere antwoorden, om de geloofwaardigheid van de persoon te vergroten. Onder de chatbot functionaliteit ligt een uitgebreid geteste database met vraag-antwoord structuren, die verder kunnen worden toegespitst op de identiteit en het karakter van de cyber agent.

Wanneer een cyber agent zich begeeft in een chatroom, zijn er verschillende strategieën mogelijk. De eerste optie is dat de cyber agent niet uit zichzelf begint te communiceren, maar (passief) afwacht.[10]

[10] Er kunnen meerdere cyber agents in een chatroom zijn, maar door de passieve instelling zullen ze niet met elkaar communiceren. Niet uitgesloten is uiteraard dat andere inlichtingendiensten eveneens (hun eigen) cyber agents hebben ingezet.

Uiteraard kunnen anderen in de chatroom wel zien dat de cyber agent is toegetreden tot de chatroom. Zodra er iemand tegen de cyber agent begint te chatten, geeft deze antwoorden die passen bij het ingegeven profiel. De tweede optie betreft een actieve cyber agent, die contact zoekt met anderen in de chatroom, eventueel op basis van vooraf bepaalde criteria.

De chatbot functionaliteit is zodanig vormgegeven dat de cyber agent zo realistisch mogelijk overkomt als een echt, natuurlijk persoon met de ingegeven eigenschappen. Reacties worden daarop aangepast, bijvoorbeeld door te wachten, te aarzelen of antwoorden te variëren. Bovendien is de chatbot functionaliteit zo geprogrammeerd dat conversaties worden gestuurd richting bruikbare informatie. Teneinde alles zo echt mogelijk te laten lijken, is de cyber agent technology eerst getest in chatrooms onder menselijke supervisie, om te zien of het bedoelde publiek de cyber agents ook als echte personen accepteert.

Vanuit het hierboven beschreven software framework kunnen de medewerkers van inlichtingen- en veiligheidsdiensten meekijken met de communicatie van de cyber agents en waar nodig de communicatie overnemen. Voor de andere personen in de chatroom is dit niet waarneembaar. Deze hybride oplossing stelt de medewerkers in staat handmatig antwoorden te geven op vragen die de chatbot niet kan beantwoorden. Dit kan de geloofwaardigheid van de cyber agent verder vergroten.

Tot slot is er ook een 3D imaging functionaliteit, waarmee realistische animaties van de cyber agent kunnen worden getoond via bijvoorbeeld een virtuele webcam. Deze animaties zijn vooraf opgenomen en de hoeveelheid beeldmateriaal is beperkt. Vandaar dat met behulp van de chatbot functionaliteit zoveel mogelijk wordt getracht conversaties op te rekken, teneinde meer informatie te vergaren, alvorens het beeldmateriaal wordt getoond.

3. Mogelijke toepassingen van cyber agent technology voor inlichtingen- en veiligheidsdiensten

3.1 Taken van de AIVD en de MIVD

Een inventarisatie van de mogelijke meerwaarde die cyber agent technology heeft voor inlichtingen- en veiligheidsdiensten start bij de taken van de diensten, omdat daar bezien kan worden of en waaraan de software een bijdrage kan leveren. Er zijn in Nederland twee inlichtingen- en veiligheidsdiensten, de AIVD en de MIVD. De taken van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) zijn beschreven in art. 8 lid 2 WIV 2017. Deze taken zijn opgesomd onder a t/m f en zodoende wordt er ook wel naar verwezen als de a-taak, de b-taak, etc. De taken van de AIVD zijn:[11]

- onderzoek doen naar organisaties en personen die aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor de democratische rechtsorde en/of de nationale veiligheid. Onder deze taak valt onder meer terrorismebestrijding en bestrijding van radicalisering en extremisme (a-taak);
- veiligheidsonderzoeken uitvoeren (b-taak);
- veiligheidsmaatregelen bevorderen (c-taak);
- inlichtingen over het buitenland inwinnen. Onder deze taak valt onder meer (cyber)spionage (d-taak);
- dreigings- en risicoanalyses opstellen (e-taak);[12]
- op verzoek mededeling doen omtrent verwerkte gegevens (f-taak).[13]

De taken van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) zijn beschreven in art. 10 lid 2 WIV 2017. De taken van de MIVD zijn:

- inlichtingen verzamelen over het militaire potentieel van andere landen, om het eigen leger beter te kunnen inrichten en benutten (a-taak);
- veiligheidsonderzoeken uitvoeren (b-taak);
- informatie verzamelen ter preventie van activiteiten die de veiligheid of de paraatheid van de krijgsmacht schaden (ook wel aangeduid als de veiligheids- of contra-inlichtingentaak) (c-taak);
- maatregelen nemen ter beveiliging van geheime militaire informatie (d-taak);
- (militaire) inlichtingen over het buitenland inwinnen (e-taak);
- dreigingsanalyses opstellen met betrekking tot personen, zaken en plaatsen die van militair belang zijn (f-taak);
- op verzoek mededeling doen omtrent verwerkte gegevens (g-taak).[14]

Het mag duidelijk zijn dat de AIVD en de MIVD voor een groot deel vergelijkbare taken hebben. De onderlinge afbakening volgt doorgaans de scheidslijn tussen (overwegend) militaire en (overwegend)

[11] https://www.aivd.nl/onderwerpen/het-werk-van-de-aivd/de-taken-van-de-aivd
[12] Deze taak is in 2006 aan de WIV toegevoegd.
[13] Deze taak was niet opgenomen in de WIV 2002.
[14] Deze taak was niet opgenomen in de WIV 2002.

niet-militaire aangelegenheden. Een beschrijving van wanneer zaken onder de AIVD danwel de MIVD vallen, ligt buiten de reikwijdte van dit onderzoek.[15]

3.2 Cyber agent technology toepassingen

Er zijn op het internet zeer veel chatrooms en platforms voor instant messaging, met honderden miljoenen gebruikers en voor zeer uiteenlopende doeleinden. Veel communicatie is onschuldig, maar er kunnen ook illegale activiteiten en personen met kwaadaardige bedoelingen tussen zitten. Privécommunicatie in chatrooms en op platforms voor instant messaging kunnen niet voortdurend worden gemonitord om deze personen en activiteiten uit de massa te filteren – er zijn te veel gegevens. Een persoonlijke aanpak, via werken onder dekmantel, kost zeer veel mankracht en is onderworpen aan juridische beperkingen (die in het strafrecht, voor opsporingsinstanties, overigens anders zijn dan voor inlichtingen- en veiligheidsdiensten).[16]

De meerwaarde van cyber agent technology is vooral gelegen in een aantal voordelen op het vlak van enerzijds effectiviteit, met name op het vlak van doelgerichtheid, transparantie, objectivering en (complete en juiste) registratie, en anderzijds efficiency, met name op het vlak van automatisering, schaalvergroting en kostenbesparing.

Om met de effectiviteit te beginnen, biedt cyber agent technology de mogelijkheid om veel gerichter grotere hoeveelheden communicatie te verwerken. Door de **gerichte aanpak**, waarbij *persons of interest* in een vroeg stadium worden geïdentificeerd en verder worden uitgevraagd via de doorlopende communicatie, kan snel duidelijk worden welke personen verdere aandacht verdienen. Tegelijkertijd hoeven geen grote hoeveelheden informatie van onschuldige personen te worden verzameld en verwerkt. Zo kan gericht resultaat worden geboekt en gaan relevante gegevens niet ten onder in massale gegevensstromen. Zoals in de volgende hoofdstukken aan bod zal komen, vergroot dit ook de juridische haalbaarheid en maatschappelijke acceptatie van de inzet van cyber agent technology.

Een ander voordeel gerelateerd aan effectiviteit is dat van **transparantie** en **objectivering**. Doordat het systeem werkt ‘op afstand’, waardoor geen fysiek contact is tussen degenen die observeren en degenen die geobserveerd worden, is het risico op (te) grote emotionele persoonlijke betrokkenheid kleiner. Waar fysiek werken onder dekmantel risico’s met betrekking tot veiligheid en emotionele betrokkenheid kent, is bij online werken onder dekmantel sprake van meer afstand, waarbij de ambtenaar met meer kritische distantie de gegevens kan analyseren.[17] Tot op zekere hoogte kan dit ook persoonlijke vooroordelen van de ambtenaar uitschakelen en kan de cyber agent technology zelfs nieuwe inzichten verschaffen doordat op punten conversaties anders worden gevoerd dan de ambtenaar zelf zou hebben gedaan. Bovendien kan een ambtenaar een *person of interest* met behulp van meerdere virtuele identiteiten op verschillende manieren, gebruikmakend van verschillende strategieën, benaderen.

Doordat de cyber agent technology taken uitvoert in een digitale omgeving, kunnen ook zaken als conversaties en observaties geautomatiseerd worden vastgelegd. Dit kan enerzijds **registraties**

[15] Voor meer gedetailleerde informatie, zie Graaf, B.A. de, Muller, E.R., & Reijn, J.A. van (2010) *Inlichtingen- en veiligheidsdiensten*, Deventer: Kluwer.

[16] Zie ook: Bronitt, S. (2004) The law in undercover policing: A comparative study of entrapment and covert interviewing in Australia, Canada and Europe, *Common Law World Review*, *33*(1), pp. 35-80.

[17] Uiteraard kan de architectuur van de technologie wel bepalend zijn voor welk soort gegevens wordt verzameld, inclusief ruis en onnauwkeurigheden. Cf. Lessig, L. (2006) *Code Version 2.0*, New York: Basic Books.

verbeteren in termen van volledigheid en juistheid en anderzijds (zoals hierboven genoemd) verder objectiveren.

Wat betreft efficiency is het helder dat de cyber agent technology verschillende voordelen biedt op het terrein van **automatisering** en **schaalvergroting**. De technologie kan grote hoeveelheden gegevens en datastromen verwerken, waardoor het bereik van chatrooms en online platforms en de personen die zich daarop begeven aanzienlijk groter wordt, al kan dat wel jurisdictieproblemen met zich meebrengen.[18]

Hoewel de technologie zodanig schaalbaar is dat zeer grote hoeveelheden virtuele identiteiten kunnen worden ingezet, zal steeds een natuurlijk persoon nodig zijn om in de conversaties zaken te markeren en om te beoordelen of en welke interventies nodig zijn.[19] Daardoor zit er een limiet aan het aantal virtuele identiteiten dat een ambtenaar kan ´aansturen´. Niettemin zijn dat veel meer cyber agents dan een natuurlijk persoon zelf zou kunnen verwerken. Daardoor neemt de hoeveelheid werk die een ambtenaar kan verzetten enorm toe wanneer gebruik wordt gemaakt van cyber agent technology. Door het automatiseren van saaie, repetitieve en vervelende onderdelen (zoals verslaglegging, confrontatie met onwenselijk beeldmateriaal),[20] wordt het werk bovendien interessanter. Doordat de cyber agent technology doelgericht wordt ingezet, wordt meer resultaat geboekt, waardoor het werk bovendien meer voldoening geeft. Meer succesverhalen kunnen bovendien de legitimiteit van de werkzaamheden van de diensten (inclusief bijbehorende bevoegdheden en beschikbare budgetten) verder vergroten.[21] Automatisering vergroot ook de doorzoekbaarheid van de vastgelegde informatie, hetgeen enerzijds een efficiency voordeel is (informatie kan sneller worden teruggevonden en/of gecombineerd) en anderzijds een effectiviteitsvoordeel (omdat sommige informatie zonder automatisering helemaal niet meer teruggevonden of gecombineerd zou zijn).

De constatering dat een medewerker aanzienlijk meer werk kan verzetten als hij of zij wordt ondersteund met cyber agent technology kan ook omgekeerd worden: dezelfde hoeveelheid werk kan dus met minder mensen worden verzet wanneer cyber agent technology wordt ingezet. In dat geval wordt het een punt van **kostenbesparing**. Bovendien kunnen kostbare experts met hoogwaardige expertise efficiënter worden ingezet, hetgeen een tweede punt van kostenbesparing is. Een derde punt van kostenbesparing is dat van (samen)werken op afstand, waardoor reis- en verblijfskosten van medewerkers worden bespaard.

Bovenstaande meerwaarde van cyber agent technology is breed geformuleerd en in beginsel van toepassing voor zowel opsporingsinstanties als inlichtingen- en veiligheidsdiensten. Wanneer de taken van de AIVD en de MIVD, zoals beschreven in de vorige paragraaf, erbij worden genomen, wordt duidelijk hoe cyber agent technology concreet door deze diensten kan worden ingezet. Gelet op de overlap in taken, wordt dit hieronder enkel uitgewerkt voor de AIVD:

---

[18] Voor meer achtergrond, zie Brenner, S.W. & Koops, B.J. (2004) Approaches to Cybercrime Jurisdiction, *Journal of High Technology Law*, *4*(1), pp. 189-202; Koops, B.J. and Goodwin, M. (2014) *Cyberspace, the cloud, and cross-border investigation: The limits of international law.* Tilburg Law School Research Paper No. 5/2016.

[19] De verwachting is dat op termijn ook dit aspect (gedeeltelijk) geautomatiseerd kan worden door middel van classificatie op basis van machine learning technologie. Als voldoende data beschikbaar is die betrouwbaar is gemarkeerd door natuurlijke personen, dan kan deze data gebruikt worden om een machine learning model te maken voor de ondersteuning bij de classificatie.

[20] In de context van Sweetie 2.0 betrof dit bijvoorbeeld kinderpornografie. In de context van inlichtingen- en veiligheidsdiensten kan gedacht worden aan bijvoorbeeld video's van onthoofdingen.

[21] Zie ook: Tyler, T.R. (2004) Enhancing Police Legitimacy, *The Annals of the American Academy of Political and Social Science*, 593, 84e99; Custers B.H.M. (2012), Technology in Policing: Experiences, Obstacles and Police Needs, *Computer law & security report* (1): 62-68.

- a-taak: de AIVD verricht onderzoek naar organisaties en personen die een bedreiging kunnen vormen voor de nationale veiligheid. Daarbij gaat het onder meer om terrorisme, radicalisering, extremisme en (cyber)spionage. Met behulp van cyber agent technology kunnen kwaadwillende personen online benaderd worden en kunnen inlichtingen over hen worden verzameld.
- b-taak: de AIVD voert veiligheidsonderzoeken uit naar kandidaten voor vertrouwensfuncties. Cyber agent technology zou kunnen worden ingezet om de achtergrond van deze personen verder te onderzoeken en eventuele verborgen bedoelingen te achterhalen. Echter, een belangrijk punt is dat de personen naar wie een veiligheidsonderzoek wordt ingesteld, daarover altijd van tevoren worden ingelicht en dat bijzondere bevoegdheden niet voor deze taak kunnen worden ingezet (zie volgende hoofdstuk).
- c- en e-taak: de AIVD heeft tot taak dreigings- en risicoanalyses op te stellen en te bevorderen dat de verantwoordelijke autoriteiten en instanties zorgen voor een adequate beveiliging. Cyber agent technology kan hieraan bijdragen door inlichtingen te verzamelen over dreigingen en risico's. Echter, ook hier geldt dat bijzondere bevoegdheden niet voor deze taak kunnen worden ingezet (zie volgende hoofdstuk).
- d-taak: de AIVD verricht onderzoek over en naar andere landen. Dit betreft het inlichtingen inwinnen over het buitenland, een taak die onder meer (cyber)spionage omvat. Cyber agent technology kan hieraan bijdragen, net als bij de a-taak, door bepaalde personen online te benaderen en inlichtingen over hen of via hen te verzamelen.
- f-taak: de AIVD doet op verzoek mededeling omtrent verwerkte gegevens. Cyber agent technology kan hieraan bijdragen door op geautomatiseerde manier vast te stellen welke gegevens wel en niet mogen worden verstrekt en door geautomatiseerde verstrekking (of inzage) van die gegevens. De geautomatiseerde vastlegging van gegevens zorgt bovendien voor volledige overzichten en tijdige verwijdering van de verwerkte gegevens (zie ook hoofdstuk 6).

Dit overzicht laat zien dat in de context van inlichtingen- en veiligheidsdiensten de meerwaarde van cyber agent technology vooral ligt op de a-taak (bestrijding van terrorisme, radicalisering, extremisme en spionage, inclusief cyberspionage), de d-taak (inlichtingen over het buitenland inwinnen, inclusief spionage en cyberspionage) en de f-taak (op verzoek mededeling doen omtrent verwerkte gegevens).

4. Wet op de inlichtingen- en veiligheidsdiensten (WIV 2017)

In dit hoofdstuk wordt een korte introductie op de 'nieuwe' Wet op de inlichtingen- en veiligheidsdiensten (WIV 2017) gegeven. Daarbij wordt kort de geschiedenis en totstandkoming van de nieuwe WIV beschreven. Daarna wordt dieper ingegaan op de voor dit onderzoek relevante onderdelen van de WIV, te weten de informatiebevoegdheden in hoofdstuk 3 van de WIV (de verwerking van gegevens) en hoofdstuk 4 van de WIV (overige bijzondere bevoegdheden) en de informatieverplichtingen in onder meer paragraaf 3.4 van de WIV (de verstrekking van gegevens), hoofdstuk 5 van de WIV (kennisneming van verwerkte gegevens).

4.1 Een nieuwe wet

De huidige (tot najaar 2017) Wet op de inlichtingen- en veiligheidsdiensten (WIV) dateert van 2002. Deze wet is in zekere zin achterhaald door de realiteit, met name door nieuwe veiligheidsbedreigingen.[22] Sinds 2002 hebben verschillende terroristische aanslagen plaatsgevonden in Europese steden, waaronder in Madrid (2004), Londen (2005), Parijs (2015), Nice (2016), Brussel (2016), Berlijn (2016), Londen (2017), Manchester (2017) en Barcelona (2017). Een andere belangrijke ontwikkeling sinds 2002 is technologisch van aard. Toen de WIV 2002 werd opgesteld, verliep de meeste communicatie nog via de ether en relatief weinig communicatie via de kabel, terwijl in 2016 de situatie juist omgekeerd is: de meeste communicatie is anno 2017 kabelgebonden. Dit maakt een belangrijk verschil voor de interceptie van communicatie (en de daarvoor benodigde bevoegdheden).

Met het oog op deze veranderingen wordt het juridisch kader voor de inlichtingen- en veiligheidsdiensten in Nederland momenteel herzien. Het kabinet heeft op 15 april 2016 ingestemd met een wetsvoorstel voor een nieuwe WIV van de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie. Het wetsvoorstel wijziging Wet op de inlichtingen- en veiligheidsdiensten is in het najaar van 2016 naar de Tweede Kamer gestuurd. Op 14 februari 2017 ging de Tweede Kamer akkoord. De Eerste Kamer is op 11 juli 2017 akkoord gegaan. Het is ten tijde van het opstellen van dit rapport niet bekend wanneer de nieuwe wet in werking treedt, maar waarschijnlijk is dat nog in 2017. Omdat het wetsvoorstel reeds door beide kamers der Staten-Generaal is goedgekeurd, zal de nieuwe WIV (aangeduid als de WIV 2017) het uitgangspunt vormen voor dit onderzoek.

De WIV 2017 regelt de instelling van de AIVD en de MIVD, stelt vast wat hun taken zijn, regelt hoe de diensten gegevens mogen verzamelen en verwerken, regelt bijzondere bevoegdheden van de diensten, bepaalt wanneer en aan wie gegevens mogen worden verstrekt, biedt burgers recht op kennisneming, regelt samenwerkingsverbanden en organiseert toezicht op het handelen van de diensten. Een uitgebreide beschrijving van de WIV valt buiten het bestek van dit rapport.[23]

De belangrijkste wijziging in de WIV 2017 ten opzichte van de WIV 2002 is wellicht de toegang tot de kabel, d.w.z. een nieuwe bevoegdheid van de diensten om al het communicatieverkeer (in het

[22] Zie Muller, E.R. (2017) Commentaar op aanhef WIV 2017, in: Brainich, E. en Brouwer, J. (red.) *Tekst en Commentaar Openbare Orde en Veiligheid*, Alphen a/d Rijn: Wolters Kluwer.

[23] Voor meer informatie, zie Graaf, B.A. de, Muller, E.R., & Reijn, J.A. van (2010) *Inlichtingen- en veiligheidsdiensten*, Deventer: Kluwer.

bijzonder via de kabel) te onderscheppen.[24] Hiervoor is een nieuw interceptiestelsel ingericht, bestaande uit drie fasen (verwerving, voorbewerking en verwerking).[25] Op dit onderdeel is veel kritiek: onder meer een groep studenten is een handtekeningenactie gestart voor een correctief referendum.[26] Veel van de kritiek richt zich op de ruime bevoegdheden, die enerzijds burgerrechten schenden[27] en anderzijds mogelijk weinig meerwaarde opleveren.[28]

Andere nieuwe onderdelen van de wet zijn onder meer de bevoegdheid tot binnendringen van geautomatiseerde werken ('hacken'), de bevoegdheid gegevens op te vragen (i.v.m. cloud computing en file sharing), de bevoegdheid DNA-sporen veilig te stellen en te analyseren, en strengere controle en toezicht.[29] De nieuwe wet is zoveel mogelijk technologie-neutraal geformuleerd, hetgeen inhoudt dat de wetsartikelen ook bij nieuwe technologische ontwikkelingen waarschijnlijk toepasbaar zullen zijn en blijven.[30] In de volgende paragrafen wordt nader ingegaan op de bevoegdheden en de informatiebeheerverplichtingen van de diensten onder de nieuwe WIV.

4.2 Bevoegdheden

De WIV kent algemene bevoegdheden en (meer ingrijpende) bijzondere bevoegdheden toe aan de diensten. Al het handelen van de diensten, inclusief de inzet van technologie, dient te passen binnen (een van) deze bevoegdheden, anders is het niet toegestaan. De algemene bevoegdheden zijn te vinden in paragraaf 3.2 van de WIV 2017. Krachtens artikel 25 zijn de diensten onder meer bevoegd tot het (stelselmatig) verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen (open source), via raadpleging van informanten en in het kader van samenwerking met andere inlichtingen- en veiligheidsdiensten en met andere instanties. De bijzondere bevoegdheden zijn geregeld in paragraaf 3.2.5 van de WIV 2017 en betreffen:

- Het observeren en volgen van personen, al dan niet met behulp van apparatuur (art. 40)
- Het onder een dekmantel verzamelen van informatie en het beschermen van nationale belangen (art. 41)
- Het doorzoeken van besloten plaatsen en gesloten voorwerpen, al dan niet met behulp van technische hulpmiddelen (art. 42)
- DNA-onderzoek (art. 43)
- Het heimelijk openen van brieven en andere geadresseerde zendingen (art. 44)[31]
- Het binnendringen in een "geautomatiseerd werk", al dan niet met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheid (art. 45)[32]

---

[24] Tokmetzis, D. (2015) Wat staat er in de nieuwe Nederlandse surveillancewet? *De Correspondent*. https://decorrespondent.nl/3070/wat-staat-er-in-de-nieuwe-nederlandse-surveillancewet/149499790-e7e03df9

[25] Jacobs, B. (2016) Select while you collect; over de voorgestelde interceptiebevoegdheden voor inlichtingen- en veiligheidsdiensten, *Nederlands Juristenblad*, afl. 4, 29 januari 2016.

[26] Jongejan, D. (2017) Referendum over aftapwet stap dichterbij, *Algemeen Dagblad*, 1 september 2017. https://www.ad.nl/politiek/referendum-over-aftapwet-stap-dichterbij~aafb9761/

[27] Martijn, M. (2017) Vier redenen waarom de nieuwe aftapwet een slecht idee is. De Correspondent, https://decorrespondent.nl/7054/vier-redenen-waarom-de-nieuwe-aftapwet-een-slecht-idee-is/216952824-74addb25

[28] Custers, B.H.M. (2017) Nederlandse Patriot Act gaat weinig opleveren. *Nederlands Juristenblad*, Vol. 92, afl. 2, p. 110-111.

[29] https://www.aivd.nl/onderwerpen/nieuwe-wet-op-de-inlichtingen--en-veiligheidsdiensten/andere-aspecten-van-de-wiv

[30] Muller, E. & Voermans, W. (2017) Nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten: een nieuw evenwicht tussen veiligheid en waarborgen. *Nederlands Juristenblad*, Vol. 92, afl. 2, p. 102-109.

[31] Dit is inclusief e-mail, zie Memorie van Toelichting op de WIV 2002, p. 37.

- Het gericht aftappen, ontvangen, opnemen en afluisteren van elke vorm van gesprek of telecommunicatie (art. 47)
- Het ('ongericht')[33] afluisteren van niet-kabelgebonden telecommunicatie die zijn oorsprong of bestemming in andere landen heeft (art. 48), inclusief het toepassen van geautomatiseerde data-analyse (art. 50)
- Het bij aanbieders van (tele)communicatiediensten opvragen van gegevens, bijvoorbeeld over een gebruiker (art. 52-65), inclusief ontsleuteling van de communicatie (art. 57)
- Toegang tot elke plaats, inclusief plaatsen om volg- en observatieapparatuur te installeren (art. 58).

Met betrekking tot geautomatiseerde data-analyse is ook de bepaling in art. 60 relevant. Hier wordt gesteld dat de diensten bevoegd zijn om geautomatiseerde data-analyse toe te passen op onder meer eigen gegevensbestanden en open source informatiebronnen. Daarbij mogen de gegevens geautomatiseerd met elkaar worden vergeleken, mag worden gezocht aan de hand van profielen en mogen gegevens worden vergeleken teneinde bepaalde patronen op te sporen.

Het uitoefenen van al deze bevoegdheden is gebonden aan voorwaarden die in de wet nader worden genoemd. Bij de bijzondere opsporingsbevoegdheden, die meer ingrijpend zijn, gelden strengere eisen. Zo zijn de bijzondere bevoegdheden niet inzetbaar bij veiligheidsonderzoeken en veiligheidsmaatregelen (de b- resp. c-taak van de AIVD en de b- resp. d-taak van de MIVD, zie paragraaf 3.1). Bovendien is de uitoefening van deze bijzondere bevoegdheden alleen geoorloofd als de benodigde gegevens niet of niet tijdig via openbare informatiebronnen verzameld kunnen worden. Wanneer een onderzoek plaatsvindt naar bepaalde gegevens, moeten de diensten bovendien toestemming krijgen van de beheerder van die gegevens, tenzij het gaat om politie, justitie, douane en telecomaanbieders (die zijn tot medewerking verplicht). De belangrijkste eisen die gelden bij de inzet van (bijzondere) bevoegdheden zijn:

- Noodzakelijkheid (de methode is nodig voor de inlichtingen- of veiligheidstaak)[34]
- Proportionaliteit (de middelen staan in verhouding tot het te bereiken doel)[35]
- Subsidiariteit (het doel kan niet met minder zware middelen bereikt worden)[36]

Als hieraan niet wordt voldaan, kan de toezichthouder of de rechter de diensten terugfluiten. Een ander belangrijk punt is dat medewerkers van de diensten geen bevoegdheid hebben tot het opsporen van strafbare feiten. Ze dragen bijvoorbeeld ook geen wapens. Er is een strikte scheiding tussen het WIV-regime en het strafrechtelijke regime. De AIVD en de MIVD zijn géén opsporingsinstanties. De diensten kunnen wel relevante informatie verstrekken aan andere (overheids)organisaties, die op basis van die informatie maatregelen kunnen treffen.

4.3 Informatiebeheerverplichtingen

De nieuwe WIV kent ook verschillende verplichtingen ten aanzien van hoe gegevens moeten worden verwerkt, mede als tegenwicht voor de relatief ruime bevoegdheden voor het verzamelen van deze gegevens. Deze verplichtingen duiden we hier aan als informatiebeheerverplichtingen. Het gaat onder meer om verplichtingen met betrekking tot de gegevens zelf (doelbinding, betrouwbaarheid, juistheid, volledigheid, etc.) en met betrekking tot de verstrekking van de gegevens (beveiliging,

[32] Met deze bevoegdheid wordt in feite computervredebreuk gelegitimeerd voor de diensten.
[33] De bepaling stelt dat er onderzoeksopdrachtgericht moet worden gewerkt, maar gelet op de brede interpretatie die hieraan kan worden gegeven, wordt dit ook wel geduid als 'ongericht'.
[34] Art. 18 lid 1 WIV 2017.
[35] Art. 26 lid 2 en 3 WIV 2017.
[36] Art. 26 lid 1 WIV 2017.

need-to-know toegang, notificatieplichten, bewaartermijnen, etc.). Deze verplichtingen worden hieronder besproken.

In de eerste plaats mogen gegevens slechts worden verwerkt voor zover noodzakelijk voor de goede uitvoering van de wet (art. 18 lid 1 WIV 2017). Deze noodzakelijkheidseis komt uitgebreid aan bod in paragraaf 5.2. In het bijzonder mogen geen gevoelige gegevens (d.w.z. godsdienst, levensovertuiging, ras, vakbondslidmaatschap, gezondheid en seksleven) worden verwerkt – dit is verboden teneinde discriminatie te voorkomen (art. 19 lid 3 WIV 2017). Voorts moeten de gegevens op behoorlijke en zorgvuldige wijze worden verwerkt (art. 18 lid 2 WIV 2017) en moeten de gegevens worden voorzien van een aanduiding omtrent de mate van betrouwbaarheid, danwel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend (art. 18 lid 3 WIV 2017). Onder de WIV 2002 bestonden reeds soortgelijke verplichtingen. Deze verplichtingen worden gezamenlijk ook wel aangeduid als een **zorgverplichting**.

Gegevens die geen of niet langer betekenis hebben voor het doel waarvoor ze worden verwerkt, dienen te worden verwijderd en vernietigd. Deze **verwijderingsplicht** is opgenomen in art. 20 WIV 2017. Ook gegevens die onjuist zijn of ten onrechte worden verwerkt dienen te worden verwijderd en vernietigd. De WIV 2017 kent geen algemene bewaartermijnen, al worden in art. 21 WIV 2017 gegevens ouder dan 20 jaar aangemerkt als gegevens die in beginsel (als er geen beperkingen aan de openbaarheid zijn) dienen te worden gearchiveerd als ze onder de Archiefwet vallen. Voor bepaalde bijzondere bevoegdheden zijn er specifieke bewaartermijnen. Zo kent art. 48 WIV 2017 (ongericht aftappen) een maximale bewaartermijn van drie jaar. De notificatieplicht (art. 59 WIV 2017, zie hieronder), kent een termijn van vijf jaar. Dit kan echter eerder als een minimum- dan een maximumtermijn worden beschouwd, omdat het bedoeld is om burgers te informeren en dus in het algemeen wordt gezien als een bepaling in het belang van die burgers en hun (informatie)rechten.

Op grond van art. 23 WIV 2017 dient gezorgd te worden voor geheimhouding van de gegevens en de bronnen waaruit de gegevens afkomstig zijn (zogeheten bronbescherming). Uiteraard geldt deze **geheimhoudingsplicht** niet voor informatie afkomstig uit open bronnen. Bronbescherming is vooral relevant ingeval gegevens worden verstrekt aan andere inlichtingen- en veiligheidsdiensten en/of aan andere organisaties. Verstrekking van persoonsgegevens waarvan de juistheid redelijkerwijs niet kan worden vastgesteld of die meer dan 10 jaar geleden zijn verwerkt, is verboden (art. 69 lid 1 WIV). In het kader van cyber agent technology is bovendien relevant dat bronbescherming niet alleen menselijke bronnen betreft, maar ook technische bronnen. De bescherming is absoluut, er zijn geen uitzonderingen.[37] Op grond van art 61 WIV 2017 mogen gegevens alleen worden ingezien door medewerkers voor wie het voor hun taakuitvoering noodzakelijk is (zogeheten need-to-know of role-based access). Hiertoe moeten ook technische maatregelen zijn genomen (zogeheten role-based access controls, RBAC's), zie art. 24 lid 2 sub c WIV 2017.

Ook ten aanzien van de inhoud van de gegevens zijn er verplichtingen. Deze **kwaliteitsverplichtingen** zien met name op de juistheid en volledigheid van de gegevens (art. 24 lid 2 sub a WIV 2017). Uiteraard kan niet worden vereist dat alle gegevens juist en volledig zijn, dat laat de aard van de gegevens en de werkzaamheden van de diensten niet toe. De juistheid en volledigheid van de verzamelde informatie dient wel zoveel mogelijk bevorderd te worden. Verder dienen, zoals hierboven aangegeven, de gegevens te worden voorzien van metadata die de mate van betrouwbaarheid aanduiden, danwel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend (art. 18 lid 3 WIV 2017).

[37] Dielemans, R.J.I. (2010) *Lexplicatie, Wet op de inlichtingen- en veiligheidsdiensten 2002*, Alphen a/d Rijn: Kluwer, p. 82.

Op grond van art. 31 WIV 2017 zijn de diensten verplicht om van de uitoefening van een (bijzondere) bevoegdheid aantekening te houden. Dit is een **verslagleggingsverplichting**. Hiermee worden de activiteiten van de diensten controleerbaar, zowel intern (door de diensten zelf) als extern (door de commissie van toezicht).

Tot slot is er nog de zogeheten **notificatieplicht**, in art. 59 WIV 2017. Deze verplichting houdt in dat de diensten vijf jaar na beëindiging van de uitoefening van een bijzondere bevoegdheid de persoon ten aanzien van wie deze bevoegdheid is uitgeoefend (en daarvan mogelijk dus nadeel heeft ondervonden, bewust of onbewust) daarvan op de hoogte stellen. Indien dit mogelijk is (er zijn verschillende uitzonderingen), dan dient dit schriftelijk en zo spoedig mogelijk te gebeuren.

5. Cyber agent technology en WIV-bevoegdheden

In dit hoofdstuk wordt onderzocht onder welke van de WIV-bevoegdheden (zoals beschreven in paragraaf 4.2) de inzet van cyber agent technology denkbaar is. De technologie dient immers binnen een of meer bevoegdheden te passen, anders is de inzet ervan verboden. De wetgever geeft nergens expliciet aan waar dit het geval is – in de Memorie van Toelichting op de WIV 2017 wordt nergens gesproken over cyber agent technology en daaraan verwante technologie.[38] De bijzondere bevoegdheden zijn echter zodanig geformuleerd, dat ze tot op zekere hoogte technologie-neutraal zijn. Zodoende moet per technologie worden bezien onder welke bevoegdheden deze inzetbaar is, hetgeen hieronder is uitgewerkt voor de cyber agent technology, zoals die beschreven is in hoofdstuk 2. Eerst wordt de toepasbaarheid onder de verschillende bevoegdheden besproken (paragraaf 5.1) en daarna komt het afwegingskader aan bod (paragraaf 5.2). Daarmee wordt deelvraag a van dit onderzoek (is de cyber agent technology inzetbaar onder de nieuwe WIV-bevoegdheden?) beantwoord.

5.1 Toepasbaarheid

De algemene bevoegdheden in art. 25 van de WIV zien onder meer op het (stelselmatig) verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen (open source), via raadpleging van informanten en in het kader van samenwerking met andere inlichtingen- en veiligheidsdiensten en met andere instanties. Onder deze bevoegdheden is de beschreven cyber agent technology *niet* inzetbaar, omdat het (in beginsel) niet gaat om open source informatie,[39] informanten en samenwerkingsverbanden met andere diensten en instanties. Het gaat immers om een interactieve technologie, die meer doet dan interceptie van gegevens. De gegevens zijn bovendien niet altijd gegevens in open bronnen, omdat sommige communicatie privé is en sommige chatrooms en platforms niet openbaar toegankelijk zijn. De virtuele identiteiten kunnen evenmin als informanten worden gezien: de Memorie van Toelichting geeft expliciet aan dat informanten natuurlijke personen zijn. Uiteraard kan de beschreven cyber agent technology wel worden gebruikt om informanten te benaderen en met hen te communiceren (art. 39 WIV 2017). Het voordeel is dan dat de cyber agent technology op afstand wordt ingezet, hetgeen gevaar voor onthulling en ontmaskering (van zowel de informant als de medewerkers van de diensten) verkleint. Enerzijds wordt de kans verkleind, omdat de kans op herkenning/identificatie kleiner is, en anderzijds wordt de impact verkleind, omdat fysieke dreiging kleiner of afwezig is.

De eerste bijzondere bevoegdheid in de WIV 2017 is die tot het observeren en volgen van personen, al dan niet met behulp van apparatuur (art. 40 WIV). Onder deze bevoegdheid is de beschreven cyber agent technology inzetbaar. De technologie kan dan worden gezien als apparatuur waarmee *persons of interest* worden geobserveerd en hun online activiteiten worden gevolgd, bijvoorbeeld door hun aanwezigheid online bij te houden. Personen die zich via meerdere identiteiten voordoen en/of op verschillende platforms en media actief zijn, kunnen worden gevolgd. Zowel statische (vanuit één vaste positie) als dynamische observatie (waarbij de observant en/of de

[38] Dit is evenmin het geval voor de Memorie van Toelichting op de WIV 2002.

[39] In de praktijk is het wel mogelijk om (open source) publieke informatie te verzamelen via de cyber agent technology. Een voorbeeld is de publieke ruimte van een chatroom of chatserver, waar iedereen berichten kan plaatsen die leesbaar zijn voor iedereen is aangemeld (ook als gast, niet noodzakelijkerwijs als lid). Een ander voorbeeld is het aanmelden op een publiek kanaal op Telegram. Om deze (semi-)publieke informatie te kunnen verzamelen is een account nodig, maar een account is eenvoudig aan te maken zonder verdere belemmeringen of goedkeuringen.

observatieapparatuur meebeweegt) is toegestaan.[40] De inzet van deze bijzondere bevoegdheid schept echter enkel ruimte voor passieve, non-interactieve verzameling van inlichtingen: gegevens kunnen worden vastgelegd, maar er is geen ruimte voor de inzet van de interactiemogelijkheden die de cyber agent technology biedt.

De volgende bijzondere bevoegdheid in de lijst is het onder een dekmantel verzamelen van informatie (art. 41 WIV 2017). Deze bevoegdheid biedt ruimte voor natuurlijke personen om, al dan niet onder dekmantel van een aangenomen identiteit of hoedanigheid, gegevens te verzamelen.[41] De bevoegdheid is in zekere zin technologie-neutraal geformuleerd: het gebruik van cyber agent technologie lijkt zeker denkbaar om een dekmantel te verschaffen. In zoverre biedt deze bevoegdheid dus een bepaalde ruimte tot de inzetbaarheid van cyber agent technology. Echter, de bepaling dat het moet gaan om natuurlijke personen, maakt dat volledig zelfstandig handelende software agents niet onder de reikwijdte van deze bepaling vallen. Zolang er dus een natuurlijk persoon betrokken is die toezicht houdt op de cyber agent technology zodra deze wordt ingezet en eventueel ingrijpt, kan de technologie worden ingezet onder deze bevoegdheid. De werking van de cyber agent technology zoals beschreven in hoofdstuk 2 is hiermee in lijn en kan dus worden ingezet onder art. 41 WIV 2017.

De bijzondere bevoegdheden betreffende het doorzoeken van plaatsen (art. 42 WIV 2017) en toegang tot plaatsen, inclusief plaatsen om volg- en observatieapparatuur te installeren (art. 58 WIV 2017), zijn volgens de Memorie van Toelichting expliciet gericht op fysieke plaatsen. Het doorzoeken van online plaatsen valt hier niet onder, dat is geregeld in art. 45 WIV 2017 (binnendringen van geautomatiseerd werk). De aard van de cyber agent technology maakt toegang tot plaatsen om de technologie te installeren onnodig. Onder deze bevoegdheden kan cyber agent technology dus niet worden ingezet. Ook de inzet van DNA-onderzoek (art. 43 WIV 2017) lijkt in dit opzicht geen relevante bijzondere bevoegdheid.

De bijzondere bevoegdheid tot het heimelijk openen van brieven en andere geadresseerde zendingen (art. 44 WIV 2017), omvat ook de bevoegdheid tot het heimelijk openen van e-mail, aldus de Memorie van Toelichting.[42] Deze bijzondere bevoegdheid heeft dus ook een online bereik. Aannemelijk is dat ook communicatie via chatrooms, Skype en dergelijke binnen het bereik van deze bevoegdheid vallen, al hebben de wetgever noch de rechter zich hierover (tot dusver) uitgesproken. Hoewel bij de inzet van cyber agent technology weliswaar e-mail kan worden gebruikt, bijvoorbeeld voor 1-op-1 communicatie met *persons of interest*, is niet noodzakelijkerwijs sprake van heimelijke inzage. Immers, het gaat om inzage door verzender en ontvanger van de communicatie, niet om inzage door een derde die meekijkt. In gevallen van twijfel over de toelaatbaarheid van het gebruik van informatie in e-mail, chatrooms, Skype, etc., kan een beroep op deze bepaling worden gedaan. Dat moet dan uiteraard wel gebeuren met voorafgaande toestemming voor de inzet van deze bevoegdheid. De bevoegdheid in art. 44 van de WIV 2017 kan dus vooral als ondersteunend worden gezien.

Voor de bijzondere bevoegdheid betreffende het binnendringen in een "geautomatiseerd werk", al dan niet met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheid (art. 45 WIV 2017)[43] en de bevoegdheid tot het gericht aftappen, ontvangen, opnemen en afluisteren van elke vorm van gesprek of telecommunicatie (art. 47 WIV 2017) geldt ongeveer hetzelfde als voor het heimelijk openen van e-mail en andere communicatie. De bevoegdheid tot het

[40] Memorie van Toelichting op de WIV 2002, p. 30.
[41] Zie ook art. 15 lid 2 WIV 2017, waarin wordt bepaald dat een dekmantel ook is toegestaan met het oog op de persoonlijke veiligheid van medewerkers.
[42] Zie Memorie van Toelichting op de WIV 2002, p. 37.
[43] Met deze bevoegdheid wordt in feite computervredebreuk gelegitimeerd voor de diensten.

binnendringen van geautomatiseerde werken kan nodig zijn om toegang te krijgen tot bepaalde fora op het darkweb om de cyber agent technology daar te kunnen inzetten. De cyber agent technology zoals beschreven in hoofdstuk 2 kan bovendien via de communicatie met *persons of interest* worden ingezet voor de aflevering van zogenaamde payloads. Deze kunnen, indien ze worden geopend of uitgevoerd op een geautomatiseerd werk van de *person of interest* het systeem binnendringen en eventueel overnemen. Hoewel de cyber agent technology vooral gericht is op de interactie met *persons of interest*, kan deze dus ook worden ingezet als technisch hulpmiddel bij het inzetten bij hacken of aftappen van deze personen.

De bijzondere bevoegdheid tot ('ongericht')[44] afluisteren van niet-kabelgebonden telecommunicatie die zijn oorsprong of bestemming in andere landen heeft (art. 48), inclusief het toepassen van geautomatiseerde data-analyse (art. 50) is ook primair een interceptiebevoegdheid en daarmee niet gericht op interactie met degenen die worden afgeluisterd. Ook bij de inzet van deze bevoegdheid, net als bij de gerichte interceptie- en aftapbevoegdheden, zijn de diensten afhankelijk van hetgeen *persons of interest* communiceren. Gericht inlichtingen inwinnen door de interactie met deze personen aan te gaan is er niet bij. Wel kan de bepaling met betrekking tot geautomatiseerde data-analyse in art. 60 WIV 2017 nog relevant zijn in deze context. Hier wordt gesteld dat de diensten bevoegd zijn om geautomatiseerde data-analyse toe te passen op onder meer eigen gegevensbestanden en open source informatiebronnen. Daarbij mogen de gegevens geautomatiseerd met elkaar worden vergeleken, mag worden gezocht aan de hand van profielen en mogen gegevens worden vergeleken teneinde bepaalde patronen op te sporen. Los van de bevoegdheden tot interceptie en aftappen, kunnen dus ook inlichtingen die worden vergaard via cyber agent technology verder (geautomatiseerd) worden geanalyseerd.

De laatste bijzondere bevoegdheid betreft het bij aanbieders van (tele)communicatiediensten opvragen van gegevens, bijvoorbeeld over een gebruiker (art. 52-65), inclusief ontsleuteling van de communicatie (art. 57). Deze bevoegdheid is zeer relevant in het kader van de beschreven cyber agent technology, omdat het kan bijdragen aan het vaststellen van de werkelijke identiteit van personen die verborgen gaan achter de schuilnamen die ze online gebruiken. Door het opvragen van gegevens bij Internet Service Providers kan duidelijk worden wie er werkelijk zit achter gebruikersnamen als "Dread Pirate Roberts" en "Frosty", al zijn er uiteraard beperkingen met betrekking tot jurisdictie. Niettemin kan worden vastgesteld dat ook hier geldt dat deze bevoegdheid niet zozeer de inzet van cyber agent technology toelaat, als wel dat deze bevoegdheid de inzet van deze technologie verder ondersteunt.

Samengevat kan worden gesteld dat de cyber agent technology zeker inzetbaar lijkt te zijn onder de bevoegdheden van de WIV 2017. Het gaat dan vooral om art. 42 (werken onder dekmantel), al biedt ook art. 41 (volgen, observeren) enige ruimte, zij het voor de meer passieve (non-interactieve) onderdelen van de cyber agent technology en niet voor de interactieve onderdelen. Andere bevoegdheden, zoals genoemd in art. 44 (openen van communicatie), art. 45 (hacken), art. 46 (gericht aftappen), art. 47/50 (ongericht aftappen) en art. 52-65 (opvragen van gegevens) zijn meer ondersteunend. Niet onbelangrijk is dat op basis van art. 60 WIV 2017 bovendien geautomatiseerde data-analyse is toegestaan.

5.2 Afwegingskader

In de vorige paragraaf is onderzocht onder welke (bijzondere) bevoegdheden cyber agent technology mogelijk inzetbaar is. Echter, naast het punt dat de technologie binnen de beschrijving van de

[44] De bepaling stelt dat er onderzoeksopdrachtgericht moet worden gewerkt, maar gelet op de brede interpretatie die hieraan kan worden gegeven, wordt dit ook wel geduid als 'ongericht'.

bevoegdheden moet passen, is er nog een belangrijk punt en dat is de toelaatbaarheid van de uitoefening van de bijzondere bevoegdheid. Hiertoe moet worden voldaan aan de criteria van noodzakelijkheid, proportionaliteit en subsidiariteit. Omdat het een interactieve werkwijze betreft, mag bovendien geen sprake zijn van uitlokking. Op deze eisen wordt hieronder nader ingegaan.

De eerste eis is die van noodzakelijkheid (de methode is noodzakelijk voor de inlichtingen- of veiligheidstaak).[45] De inzet van bijzondere bevoegdheden, inclusief de inzet van cyber agent technology kan niet gebaseerd worden op argumenten van efficiency, omdat er in dat geval kennelijk ook alternatieven (al zijn die minder efficiënt) voorhanden zijn. De eis van noodzakelijkheid schrijft voor dat enerzijds met de in te zetten middelen het doel kan worden bereikt en anderzijds dat het doel niet met andere middelen kan worden bereikt. De inzet van cyber agent technology kan zeker bijdragen aan het inwinnen van inlichtingen die anders niet verkregen zouden kunnen worden. Bijvoorbeeld in het geval van zogeheten 'lone wolfs', geheel zelfstandig opererende terroristen of extremisten, is er vaak weinig of geen communicatie die afgetapt kan worden, terwijl via interactieve cyber agent technology mogelijk wel meer te weten kan worden gekomen van/over deze personen. Zoals eerder aangegeven, bij interceptie zijn de diensten afhankelijk van wat er wordt gecommuniceerd, terwijl bij interactieve cyber agent technology gericht doorgevraagd kan worden.

De tweede eis is die van proportionaliteit (de inbreuken op grondrechten staan in verhouding tot het te bereiken doel).[46] Interactieve cyber agent technology biedt de mogelijkheid reeds in een vroeg stadium te identificeren wie mogelijke *persons of interest* zijn en deze verder uit te vragen via de doorlopende communicatie. Met relatief weinig informatie kan reeds worden nagegaan welke personen verdere aandacht verdienen.[47] Daarmee is de uitoefening van de bevoegdheden evenredig aan het beoogde doel (art. 26 lid 3 WIV 2017). Tegelijkertijd hoeven geen grote hoeveelheden informatie van onschuldige personen te worden verzameld en verwerkt. Hierdoor wordt geen onevenredig nadeel gecreëerd voor betrokken personen. In het bijzonder worden geen onnodige gegevens verzameld over onschuldige burgers en is geen sprake van grootschalig aftappen en/of mass surveillance. Bovendien is ook het nadeel voor de betrokken *person of interest* niet snel onevenredig, omdat per fase wordt bezien of verdere aandacht nodig is.

De derde eis betreft subsidiariteit (het doel kan niet met minder zware middelen bereikt worden).[48] Om te beoordelen of aan deze eis is voldaan, moeten alternatieven worden vergeleken.[49] Voor de passieve kant van de beschreven cyber agent technology zijn dat vooral de genoemde interceptie- en aftapbevoegdheden. Echter, deze bevoegdheden zijn gericht op massale gegevensstromen en kunnen snel stuiten op bovenstaande proportionaliteitseis. Voor de interactieve kant van de beschreven cyber agent technology is het enige echte alternatief de inzet van natuurlijke personen onder dekmantel. Hoewel betwist kan worden hoeveel nadeel deze bevoegdheid oplevert voor betrokkenen, kan gesteld worden dat de inzet van cyber agent technology zeker niet meer nadeel oplevert voor betrokkenen. Daarmee levert de subsidiariteitseis waarschijnlijk dus geen probleem op.

[45] Art. 18 lid 1 WIV 2017.
[46] Art. 26 lid 2 en 3 WIV 2017.
[47] Zie ook: Taslitz, A.E. (2013) Cybersurveillance without Restraint: The Meaning and Social Value of the Probable Cause and Reasonable Suspicion Standards in Governmental Access to Third-Party Electronic Records, *Journal of Criminal Law & Criminology*, *103*, pp.839-905.
[48] Art. 26 lid 1 WIV 2017.
[49] Pool R.L.D & Custers B.H.M. (2017), The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime, *European journal of crime, criminal law and criminal justice* 2017(25): 123-144.

Tot slot is van belang dat geen sprake is van uitlokking. Dit is vastgelegd in het zogeheten Tallon-criterium.[50] Dit criterium is in de WIV 2002 en de WIV 2017 vastgelegd en geformuleerd als: "[de agent mag] door zijn optreden een persoon niet brengen tot ander handelen betreffende het beramen of plegen van strafbare feiten, dan waarop diens opzet reeds tevoren was gericht".[51] Daarbij is niet van belang of de uitlokking gericht of ongericht is, het gaat erom dat van de inzet van de cyber agent technology objectief gezien geen uitlokkende werking uitgaat.[52] In beginsel vormt het feit dat een chatbot zich begeeft in een chatroom of op een (instant) messaging platform geen uitlokking. Het feit dat de chatbot passief afwacht, niet actief personen aanspreekt en pas reageert indien aangesproken, maakt dat waarschijnlijk geen sprake is van schending van het Tallon-criterium. Echter, een passieve houding van een cyber agent maakt nog niet dat geen sprake is van uitlokking.[53] Bovendien is het mogelijk dat de cyber agent uitspraken doet die evenwel als uitlokking kunnen worden aangemerkt. Een zorgvuldige screening van de scripts van de chatbots is derhalve noodzakelijk, evenals zorgvuldige formuleringen van de medewerkers indien ze conversaties overnemen van de chatbots. Doordat alle communicatie wordt vastgelegd in het systeem kan in alle gevallen achteraf getoetst worden in hoeverre er sprake is geweest van uitlokking. Bij de inzet van de chatbot functionaliteit zou bovendien vooraf al getoetst kunnen worden (bijvoorbeeld door de minister, de commissie van toezicht of een rechter) welke gedragingen/teksten te veel neigen naar uitlokking.

Samengevat voldoet de cyber agent technology wat betreft opzet en doelstellingen in grote lijnen aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit en ook aan het Tallon-criterium dat uitlokking verbiedt. Echter, de specifieke wijze waarop de cyber agent technology wordt ingezet in een bepaalde casus is uiteindelijk bepalend hiervoor.

[50] HR 4 december 1979, NJ 1980, 356. ECLI:NL:HR:1979:AB7429 (*Tallon-arrest*).
[51] Zie onder meer art. 41 lid 5 WIV 2017.
[52] HR 28 oktober 2008, ECLI:NL:HR:2008:BE9817
[53] Teixeira de Castro tegen Portugal, EHRM 9 juni 1998, *NJ* 2001, 471.

6. Cyber agent technology en WIV-informatiebeheerverplichtingen

In dit hoofdstuk wordt onderzocht in hoeverre de in hoofdstuk 2 beschreven cyber agent technology kan bijdragen aan het (verder/beter) invullen van verplichtingen die inlichtingen- en veiligheidsdiensten onder de WIV 2017 hebben ten aanzien van het verzamelen, verwerken en vernietigen van informatie. Deze informatiebeheerverplichtingen zijn beschreven in paragraaf 4.3. Het gaat in het bijzonder om zorgverplichtingen, verwijderingsplichten, geheimhoudingsplichten, kwaliteitsverplichtingen, verslagleggingsverplichtingen en notificatieplichten. In dit hoofdstuk wordt deelvraag b van dit onderzoek (is de cyber agent technology bruikbaar bij het invullen van WIV-verplichtingen?) beantwoord.

De zorgverplichtingen in art. 18 en 19 van de WIV 2017 schrijven voor dat gegevens slechts mogen worden verwerkt voor zover noodzakelijk, dat geen gevoelige gegevens mogen worden verwerkt, dat gegevens op behoorlijke en zorgvuldige wijze moeten worden verwerkt en dat de gegevens moeten worden voorzien van een indicatie omtrent betrouwbaarheid danwel bronvermelding. Het gebruik van cyber agent technology kan hier op verschillende manieren aan bijdragen. Ten eerste biedt de cyber agent technology zoals beschreven in paragraaf 2.2 een gerichte aanpak, waardoor niet snel gegevens worden verwerkt die niet noodzakelijk zijn (zie ook de analyse in paragraaf 5.2). Ten tweede biedt de cyber agent technology vaste formats, waardoor de vergaarde informatie steeds op dezelfde manier wordt vastgelegd, hetgeen de transparantie en doorzoekbaarheid bevordert. Ten derde is er de mogelijkheid om markeringen aan te brengen in het bronmateriaal, waardoor herleidbaarheid wordt bevorderd.

In de cyber agent technology ontbreekt echter een filter dat de vastlegging van gevoelige gegevens blokkeert. Ook is het vastleggen van indicaties omtrent de betrouwbaarheid van de vergaarde gegevens niet standaard ingebouwd in de cyber agent technology. Herleidbaarheid is wel een ingebouwde functionaliteit.

De WIV 2017 kent geen algemene bewaartermijn, maar schrijft voor dat gegevens moeten worden verwijderd en vernietigd die geen of niet langer betekenis hebben voor het doel waarvoor ze worden verwerkt (art. 20 WIV 2017). Deze regeling is lastig te automatiseren en de cyber agent technology voorziet hier niet direct in. Echter, op indirecte wijze wordt wel bijgedragen, aangezien gericht gegevens worden verzameld en dus minder gegevens moeten worden beoordeeld op hun betekenis. De verzamelde gegevens zijn sterk gekoppeld aan *persons of interest*, waardoor ze ook snel kunnen worden geïdentificeerd en verwijderd wanneer blijkt dat de betreffende persoon geen verdere aandacht van de diensten behoeft. De cyber agent technology volgt in grote lijnen reeds het adagium ‘select while you collect’,[54] hetgeen aanzienlijk beter tegemoetkomt aan art. 20 WIV 2017.[55] Dit zou nog verder kunnen worden verstevigd door het inbouwen van zogeheten *rolling buffers*, waarmee onder meer de NSA werkt. Daarbij worden de verzamelde gegevens na enige tijd automatisch overschreven door wat nieuw binnenkomt. Binnen een vastgestelde periode moet de relevantie worden vastgesteld, anders zijn de gegevens weg.

[54] Jacobs, B. (2016) Select while you collect; over de voorgestelde interceptiebevoegdheden voor inlichtingen- en veiligheidsdiensten, *Nederlands Juristenblad*, afl. 4, 29 januari 2016.

[55] Merk op dat de alternatieven problematisch kunnen zijn: ‘select before you collect’ heeft als groot nadeel dat het lastig is vooraf in te schatten welke informatie relevant is, terwijl ‘select after you collect’ als groot nadeel heeft dat heel veel informatie wordt verzameld, waardoor selectie lastiger wordt en bovendien massaal gegevens van onschuldige burgers worden vastgelegd.

Daarnaast zijn er wel specifieke bewaartermijnen voor bepaalde categorieën gegevens, bijvoorbeeld voor ongericht aftappen. In beginsel zou de cyber agent technology metadata kunnen vastleggen en voorzien in geautomatiseerde vernietiging van gegevens na het aflopen van bewaartermijnen, ware het niet dat dit nu niet is ingebouwd in de software. De vraag is echter of dit van toegevoegde waarde is, omdat de cyber agent technology niet is bedoeld voor ongericht aftappen. Het vastleggen van metadata is vooral van belang om de betrouwbaarheid van de gegevens beter te kunnen indiceren (zie de zorgverplichting hierboven).[56]

Wat betreft de geheimhoudingsplicht is er onderscheid te maken tussen intern en externe veiligheidsrisico's (hier kortweg aangeduid als resp. 'hacken' en 'lekken') en tussen bewuste en onbewuste veiligheidsrisico's (waarbij informatie doelbewust danwel per ongeluk naar buiten komt).[57] Door de gerichte aanpak slaat de cyber agent technology minder gegevens op dan in gevallen van mass surveillance. In zijn algemeenheid kan worden gesteld dat wanneer er minder gegevens worden opgeslagen, databases minder interessant zijn voor hackers en dat er ook simpelweg minder te hacken en te lekken valt. Als gegevens niet zijn opgeslagen, kunnen ze ook niet op straat komen te liggen. De cyber agent technology voorziet weliswaar in audit trails via een database, maar er is (nog) geen user interface om deze informatie op te vragen. Audit trails voorkomen wellicht niet elke vorm van ongeautoriseerde toegang, maar kunnen wel bijdragen in het achterhalen ervan, waarna maatregelen kunnen worden getroffen. Autorisatie voor enkel die medewerkers die gegevens moeten inzien voor de uitoefening van hun taak (need-to-know, role-based access) is niet in de cyber agent technology ingebouwd, maar kan wel worden georganiseerd via het beperkt verstrekken van accounts die toegang verschaffen tot de cyber agent technology.

De kwaliteitsverplichtingen in art. 24 van de WIV 2017 zijn met name gericht op het bevorderen van de juistheid en volledigheid van de gegevens. Doordat de cyber agent technology op afstand werkt, waardoor geen fysiek contact is tussen degenen die observeren en degenen die geobserveerd worden, is het risico op (te) grote emotionele persoonlijke betrokkenheid kleiner, hetgeen de objectivering van de gegevens kan bevorderen. Tegelijkertijd zou ook een zekere mate van onthechting kunnen ontstaan, waarbij de personen onder observatie niet of verminderd als echte mensen worden gezien, maar meer als digitale personen of spelfiguren.[58] De wijze waarop de cyber agent technology verder kan bijdragen aan art. 18 en 19 van de WIV 2017 (onder meer bronvermelding en aanduiding omtrent de mate van betrouwbaarheid van gegevens) is hierboven reeds beschreven. Doordat de gegevens in vaste formats worden vastgelegd, worden bovendien audits, inzagerechten en de afhandeling van klachten en meldingen gefaciliteerd.

De verslagleggingsplicht in art. 31 WIV 2017 ziet op het aantekening houden van de uitoefening van een (bijzondere) bevoegdheid, waardoor de activiteiten van de diensten controleerbaar worden. De cyber agent technology kan hieraan bijdragen doordat, bijvoorbeeld in tegenstelling tot het handelen van fysieke informanten en infiltranten, alle handelingen transparant en doorzoekbaar worden vastgelegd. Deze activiteit is daardoor minder afhankelijk van het geheugen van personen en de wijze waarop zij (verschillend) verslagleggen.

[56] Voor houdbaarheidsdata, zie ook: Custers B.H.M. (2016), Click here to consent forever; Expiry dates for informed consent, *Big Data & Society,* pp. 1-6.

[57] In termen van veiligheidsrisico's kan de cyber agent technology ook bijdragen aan persoonlijke veiligheid, omdat op afstand wordt gewerkt. (zie bijvoorbeeld het reisverbod in art 14 WIV 2017).

[58] Dit fenomeen doet zich bijvoorbeeld voor bij het gebruik van drones, waarbij de observanten enkel via beeldschermen (en dus op fysieke afstand) observeren, en wordt ook wel aangeduid als de 'playstation mentality'. Zie ook: Custers B.H.M. (2016) *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives.* Heidelberg: Springer.

Hetzelfde geldt voor de notificatieplicht zoals genoemd in art. 59 van de WIV 2017, die stelt dat (waar mogelijk) personen ten aanzien van wie een bijzondere bevoegdheid is uitgeoefend 5 jaar na beëindiging daarvan op de hoogte moeten worden gesteld. De cyber agent technology kan hierin faciliteren door de termijnen bij te houden via metadata (al zou dit nog in de software moeten worden ingebouwd) en door geautomatiseerd notificaties te verstrekken na afloop van de termijnen (al zou dit eveneens nog in de software moeten worden ingebouwd).

Samengevat kan de cyber agent technology inderdaad een bijdrage leveren aan het (verder/beter) invullen van de informatiebeheerverplichtingen in de WIV 2017. Door het gericht verzamelen van gegevens worden veiligheidsrisico's verkleind en doorzoekbaarheid en transparantie vergroot. Tegelijkertijd wordt daarmee de controleerbaarheid van de activiteiten van de diensten verstevigd. Wanneer het systeem ook metadata zou bijhouden over bewaartermijnen, kan nog verder tegemoet worden gekomen aan de verwijderingsplichten, de geheimhoudingsplichten en notificatieplichten. Het bijhouden van metadata over de betrouwbaarheid van de gegevens zou nog verder bijdragen aan de zorgverplichtingen en de kwaliteitsverplichtingen. Daarbij moet worden aangetekend dat het systeem reeds voorziet in het bijhouden van bronvermeldingen.

7. Conclusies

De centrale vraagstelling in dit onderzoek valt uiteen in twee deelvragen, die hieronder beantwoord worden. Ter herinnering wordt de centrale vraagstelling eerst herhaald:

Hoe verhoudt het gebruik van de cyber agent technology door inlichtingen- en veiligheidsdiensten zich tot het juridisch kader van de nieuwe WIV, in het bijzonder ten aanzien van:

a) De inzetbaarheid van de software onder de nieuwe WIV-bevoegdheden?
b) De bruikbaarheid van de software bij het invullen van WIV-verplichtingen?

Antwoord op deelvraag a

Op basis van de analyse in hoofdstuk 5 kan worden gesteld dat de cyber agent technology zeker inzetbaar lijkt onder de bevoegdheden van de WIV 2017. Het gaat dan vooral om art. 42 (werken onder dekmantel), al biedt ook art. 41 (volgen, observeren) enige ruimte, zij het voor de meer passieve (non-interactieve) onderdelen van de cyber agent technology en niet voor de interactieve onderdelen. Andere bevoegdheden, zoals genoemd in art. 44 (openen communicatie), art. 45 (hacken), art. 46 (gericht aftappen), art. 47/50 (ongericht aftappen) en art. 52-65 (opvragen van gegevens) zijn meer ondersteunend. Niet onbelangrijk is dat op basis van art. 60 WIV 2017 bovendien geautomatiseerde data-analyse is toegestaan.

Naast een analyse van de vraag onder welke bevoegdheden de cyber agent technology mogelijk inzetbaar is, is ook nagegaan in hoeverre de cyber agent technology wat betreft opzet en doelstellingen voldoet aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit en aan het Tallon-criterium dat uitlokking verbiedt. In grote lijnen voldoet de cyber agent technology hieraan, met name omdat het een gerichte inzet van bevoegdheden betreft. Echter, de specifieke wijze waarop de cyber agent technology wordt ingezet in een bepaalde casus is uiteindelijk bepalend hiervoor.

Antwoord op deelvraag b

Op basis van de analyse in hoofdstuk 6 kan worden gesteld dat de cyber agent technology inderdaad een bijdrage kan leveren aan het (verder/beter) invullen van de informatiebeheerverplichtingen in de WIV 2017. Door het gericht verzamelen van gegevens worden veiligheidsrisico's verkleind en doorzoekbaarheid en transparantie vergroot. Tegelijkertijd wordt daarmee de controleerbaarheid van de activiteiten van de diensten verstevigd. Wanneer het systeem ook metadata zou bijhouden over bewaartermijnen, kan nog verder tegemoet worden gekomen aan de verwijderingsplichten, de geheimhoudingsplichten en notificatieplichten. Het bijhouden van metadata over de betrouwbaarheid van de gegevens zou nog verder bijdragen aan de zorgverplichtingen en de kwaliteitsverplichtingen. Daarbij moet worden aangetekend dat het systeem reeds voorziet in het bijhouden van bronvermeldingen.

De antwoorden op beide deelvragen leveren enkele aandachtspunten op voor de verdere ontwikkeling van de cyber agent technology. Wat betreft de bevoegdheden en inzetbaarheid is het van belang in de gaten te houden dat de cyber agent technology steeds een hulpmiddel is dat ondersteuning biedt aan de medewerkers van de diensten. Wanneer de technologie zodanig wordt doorontwikkeld dat deze te autonoom zou werken, kan het buiten de reikwijdte van de bevoegdheden van de diensten vallen.

Wat betreft de informatiebeheerverplichtingen en de bruikbaarheid is het verder ontwikkelen van functionaliteit die metadata kan bijhouden omtrent zowel bewaartermijnen als betrouwbaarheid van gegevens van grote meerwaarde. Dit is functionaliteit die relatief eenvoudig toe te voegen is en waarmee aanzienlijk verder wordt tegemoet gekomen aan de verplichtingen in de WIV 2017.

Literatuur

Boccara, N. (2004) *Modeling Complex Systems, Graduate Texts in Contemporary Physics*, Springer: New York, NY, USA.

Bronitt, S. (2004) The law in undercover policing: A comparative study of entrapment and covert interviewing in Australia, Canada and Europe, *Common Law World Review*, *33*(1), pp. 35-80.

Brenner, S.W. & Koops, B.J. (2004) Approaches to Cybercrime Jurisdiction, *Journal of High Technology Law*, *4*(1), pp. 189-202.

Custers, B.H.M. (2017) Nederlandse Patriot Act gaat weinig opleveren. *Nederlands Juristenblad*, Vol. 92, afl. 2, p. 110-111.

Custers B.H.M. (2016) Click here to consent forever; Expiry dates for informed consent, *Big Data & Society,* pp. 1-6.

Custers B.H.M. (2016) *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives.* Heidelberg: Springer.

Custers B.H.M. (2012), Technology in Policing: Experiences, Obstacles and Police Needs, *Computer law & security report* (1): 62-68.

Dielemans, R.J.I. (2010) *Lexplicatie, Wet op de inlichtingen- en veiligheidsdiensten 2002*, Alphen a/d Rijn: Kluwer.

Graaf, B.A. de, Muller, E.R., & Reijn, J.A. van (2010) *Inlichtingen- en veiligheidsdiensten*, Deventer: Kluwer.

Jacobs, B. (2016) Select while you collect; over de voorgestelde interceptiebevoegdheden voor inlichtingen- en veiligheidsdiensten, *Nederlands Juristenblad*, afl. 4, 29 januari 2016.

Johnson, D.R. and Post, D. (1996) Law and borders: The rise of law in cyberspace, *Stanford Law Review*, pp. 1367-1402.

Jongejan, D. (2017) Referendum over aftapwet stap dichterbij, *Algemeen Dagblad*, 1 september 2017. https://www.ad.nl/politiek/referendum-over-aftapwet-stap-dichterbij~aafb9761/

Koops, B.J. (2013) Police investigations in Internet open sources: Procedural-law issues, *Computer Law & Security Review*, *29*(6), pp. 654-665.

Koops, B.J. and Goodwin, M. (2014) *Cyberspace, the cloud, and cross-border investigation: The limits of international law.* Tilburg Law School Research Paper No. 5/2016.

Kurzweil, R. (1990) *The Age of Intelligent Machines*, Cambridge MA: MIT Press.

Lessig, L. (2006) *Code Version 2.0*, New York: Basic Books.

Luck, M., McBurney, P., and Preist, C. (2004) A Manifesto for Agent Technology: Towards Next Generation Computing, *Autonomous Agents and Multi-Agent Systems*, 9, 203-252.

Martijn, M. (2017) Vier redenen waarom de nieuwe aftapwet een slecht idee is. De Correspondent, https://decorrespondent.nl/7054/vier-redenen-waarom-de-nieuwe-aftapwet-een-slecht-idee-is/216952824-74addb25

Muller, E. & Voermans, W. (2017) Nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten: een nieuw evenwicht tussen veiligheid en waarborgen. *Nederlands Juristenblad*, Vol. 92, afl. 2, p. 102-109.

Nwana, H. S. (1996) Software Agents: An Overview. *Knowledge Engineering Review*. 21 (3): 205–244.

Pool R.L.D & Custers B.H.M. (2017), The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime, *European journal of crime, criminal law and criminal justice* 2017(25): 123-144.

Schermer, B.W. (2007) *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance*, Leiden: Leiden University Press.

Schermer, B.W., Georgieva, I., Van der Hof, S., Koops, B.J. (2016) Legal Aspects of Sweetie 2.0. Leiden University & Tilburg University. https://www.terredeshommes.nl/sites/tdh/files/uploads/2016_10_03_sweetie_legal_aspects_report.pdf

Taslitz, A.E. (2013) Cybersurveillance without Restraint: The Meaning and Social Value of the Probable Cause and Reasonable Suspicion Standards in Governmental Access to Third-Party Electronic Records, *Journal of Criminal Law & Criminology*, *103*, pp.839-905.

Tokmetzis, D. (2015) Wat staat er in de nieuwe Nederlandse surveillancewet? *De Correspondent*. https://decorrespondent.nl/3070/wat-staat-er-in-de-nieuwe-nederlandse-surveillancewet/149499790-e7e03df9

Tyler, T.R. (2004) Enhancing Police Legitimacy, *The Annals of the American Academy of Political and Social Science*, 593, 84e99;

Wal, C. van der (2016) Sweetie 2.0: nieuw virtueel meisje gaat op pedojacht, Algemeen Dagblad, 13 februari 2016. https://www.ad.nl/binnenland/sweetie-2-0-nieuw-virtueel-meisje-gaat-op-pedojacht~ad3739ca/

Over de auteur

Dit onderzoek is uitgevoerd door mr. dr. ir. B.H.M. (Bart) Custers, associate professor en hoofd onderzoek van eLaw, het centrum voor recht en digitale technologie van de Universiteit Leiden. De heer Custers heeft een achtergrond in zowel rechten als technische natuurkunde. Zijn onderzoek is gericht op het snijvlak van recht en digitale technologie, onder meer op onderwerpen als cybercrime, opsporingsbevoegdheden, big data, privacy en kunstmatige intelligentie. Hij is een ervaren onderzoeker die onder meer in opdracht van de Europese Commissie, NWO en verschillende ministeries en bedrijven contractonderzoek uitvoerde. Hij presenteert zijn werk regelmatig op internationale congressen, onder meer in de Verenigde Staten, China, Japan, het Midden-Oosten en Europa. Hij publiceerde zes boeken en meer dan honderd publicaties in wetenschappelijke tijdschriften, vakbladen en kranten.