11 Inlichtingen– en veiligheidsdiensten in de weerbare rechtsstaat

Rowin Jansen[1]

1 INLEIDING

De democratische rechtsstaat is een groot goed. De grondgedachte ervan is dat burgers moeten worden beschermd tegen willekeur en machtsmisbruik. Echter, niet alleen de burgers behoeven bescherming. Soms moet de democratische rechtsstaat zélf worden verdedigd. Er zijn nu eenmaal personen, organisaties en staten die zijn voorbestaan ondermijnen. Die zullen er ook altijd zijn. Het huidige dreigingsspectrum varieert van radicalisering, terrorisme en spionage tot sabotage, desinformatie en ondermijning. Het thema van deze bundel, 'de weerbare rechtsstaat', veronderstelt dat een democratische rechtsstaat moet beschikken over arrangementen waarmee hij zich kan wapenen tegen zulke subversieve krachten. In mijn bijdrage staan overheidsorganisaties centraal die bij uitstek die weerbaarheidsgedachte representeren: de inlichtingen– en veiligheidsdiensten.

In ons staatsbestel is de positie van zulke diensten delicaat. Zij worden geacht aan *early warning* te doen. Daartoe speuren zij naar onbekende en ongekende dreigingen voor de nationale veiligheid, de democratische rechtsorde en andere gewichtige staatsbelangen. In die zoektocht is veel toegestaan. De diensten beschikken over bevoegdheden die diep kunnen ingrijpen op grondrechten van burgers. In de volksmond spreekt men ook wel over 'geheime diensten'. Zelf omschrijven zij zich liever als 'diensten met geheimen', die 'niet geheimzinnig, maar zinnig geheim' zijn.[2] Onderzoeksprioriteiten, *modus operandi* en actuele kennisniveaus worden voor de buitenwereld afgeschermd om lopende (en toekomstige) operaties niet in gevaar te brengen.[3] Die geheimhouding is noodzakelijk, maar belemmert het afleggen van publieke verantwoording. Van *carte blance* mag evenwel geen sprake zijn. In de woorden van Frissen: 'De rechtsstaat is de hoogste norm en begrenzing tegelijkertijd'.[4] Anno

---

1 Mr. drs. R.H.T. Jansen is als docent en promovendus verbonden aan het Onderzoekcentrum voor Staat en Recht alsook aan de Interdisciplinary Hub for Digitalization and Society van de Radboud Universiteit. De kopij is afgerond op 1 november 2021.

2 *Jaarverslag AIVD 2018*, Den Haag 2019, p. 3; *Jaarverslag MIVD 2014*, Den Haag 2015, p. 5.

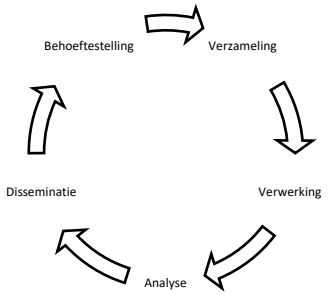
3 Art. 12 lid 3 en lid 5 Wiv 2017.

4 P.H.A. Frissen, *Het geheim van de laatste staat. Kritiek van de transparantie*, Amsterdam: Boom 2016, p. 215.

2021 zijn de diensten dan ook stevig wettelijk ingesnoerd, omgeven met *checks and balances* en onderworpen aan een speciaal toezichtregime.

Er zit een spanningsveld tussen slagkracht en insnoering van inlichtingen– en veiligheidsdiensten. Men kan zelfs spreken van een paradox: ter bescherming van de democratische rechtsstaat mogen de diensten activiteiten ontplooien die op gespannen voet staan met rechtsstatelijke uitgangspunten.[5] In deze bijdrage staat die paradox centraal. Specifieker: ik laat hier zien hoe de wetgever omspringt met dit spanningsveld en hoe hij de diensten juridisch heeft ingebed.

De opbouw van deze bijdrage is als volgt. Ik start met een korte karakterschets van de diensten (§ 2) en een beknopte beschrijving van het toepasselijke wettelijke kader (§ 3). Vervolgens staan de werkzaamheden van de diensten centraal. Daarbij hanteer ik, zij het losjes, het *intelligence cycle*–model.[6] Eerst bespreek ik de sturingsrelaties en behoeftestelling: wie is ministerieel verantwoordelijk en wie bepaalt de onderzoeksagenda's (§ 4)? Daarna ga ik in op het verzamelen, verwerken en analyseren van gegevens door de diensten (§ 5) en het dissemineren van de inlichtingen (§ 6). Tot slot analyseer ik de verschillende controle– en toezichtmechanismen (§ 7) en maak ik de balans op (§ 8).



Figuur 1: Inlichtingencyclus [7]

---

5 Vgl.: Y. Buruma, 'De AIVD en de grenzen van de democratische rechtsstaat' (toespraak 'Symposium Vrijheid versus veiligheid: 60 jaar AIVD', Ridderzaal, 1 september 2005), Den Haag 2005; R.K. Visser, 'Geheim en gecontroleerd: een paradox', in: B.A. de Graaf e.a. (red.), *Inlichtingen- en veiligheidsdiensten,* Deventer: Kluwer 2010, p. 23-35.

6 Binnen de inlichtingenstudies klinkt weliswaar kritiek op dit model, maar conceptueel is het onverminderd relevant. De *intelligence web*-theorie is een veelzijdiger alternatief. Zie: M. Phythian (red.), *Understanding the Intelligence Cycle*, Londen: Routledge 2015. Vgl.: B.A. de Graaf, 'De intelligence cycle als functie van de nationale veiligheid', in: B.A. de Graaf e.a. (red.), *Inlichtingen- en veiligheidsdiensten,* Deventer: Kluwer 2010, p. 349-376; D. Omand, 'The cycle of intelligence', in: R. Dover e.a. (red.), *Routledge Companion to Intelligence Studies*, Oxfordshire: Routledge 2014, p. 59-70.

7 Van dit model zijn talloze varianten in omloop. Deze weergave is gebaseerd op: CIA, *A Consumer's Handbook to Intelligence*, Langly: CIA 1993.

2 ALGEMENE KARAKTERISERING

2.1 Soorten geheime diensten

Geheime diensten zijn er in aller soorten en maten. Voor een goed begrip van dit type overheidsorganisaties, is het behulpzaam enkele karakteristieken te schetsen. In de eerste plaats dient er te worden gedifferentieerd tussen militaire en civiele diensten. Militaire diensten verzamelen strategische en tactische inlichtingen voor de krijgsmacht om sabotage en ondermijning te voorkomen. Civiele diensten zijn doorgaans gericht op politieke, economische of andersoortige gegevens. In de tweede plaats verschilt een inlichtingendienst van een veiligheidsdienst. Door de bank genomen is een inlichtingendienst offensief ingesteld en actief in het buitenland. Zij houdt zich bezig met wat in de wandelgangen 'spioneren' heet. Waar een inlichtingendienst ook handelt zonder dat de nationale veiligheid direct in het geding is, heeft een veiligheidsdienst primair een defensieve taak: het bestrijden van bedreigingen voor de nationale veiligheid op eigen bodem.[8]

2.2 Nederlandse diensten

In veel democratische rechtsstaten zijn de inlichtingentaak en de veiligheidstaak ondergebracht in afzonderlijke organisaties, niet zelden met eigen juridische kaders.[9] Nederland heeft dat strikte onderscheid ook jarenlang gehanteerd, maar rond de millenniumwisseling losgelaten. Voorheen kende het staatsbestel een Binnenlandse Veiligheidsdienst (BVD), een Inlichtingendienst Buitenland[10] en drie militaire inlichtingendiensten – voor elk krijgsmachtonderdeel één.[11] Parallel daaraan functioneerde de tweeledige *stay behind*–organisatie Inlichtingen en Operatiën.[12]

---

8 Zie o.a.: C.W. Hijzen, *Vijandbeelden. De veiligheidsdiensten en democratie, 1912-1922*, Amsterdam: Boom 2016, p. 11; C.W. Hijzen & W.J.M. Aerdts, 'Vóór de aanslag: terrorismebestrijding door inlichtingen- en veiligheidsdiensten', in E. Bakker e.a. (red.), *Terrorisme. Studies over terrorisme en terrorismebestrijding*, Deventer: Wolters Kluwer 2017, p. 521-554, aldaar p. 525; B.G.J. de Graaff, *Data en dreiging. Stap in de wereld van intelligence*, Amsterdam: Boom 2019, p. 29.

9 MI5 en het Bundesamt für Verfassungsschutz zijn voorbeelden van veiligheidsdiensten; MI6 en Bundesnachrichtendienst van inlichtingendiensten.

10 Tot 1972 de Buitenlandse Inlichtingendienst geheten. De dienst is opgeheven in 1994. Zie: B.G.J. de Graaff & C. Wiebes, *Villa Maarheeze. De geschiedenis van de inlichtingendienst buitenland*, Den Haag: Sdu Uitgevers 1998.

11 In 1987 zijn de drie diensten samengevoegd tot één Militaire Inlichtingendienst. Zie: D. Engelen, *De Militaire Inlichtingen Dienst 1913-2000*, Den Haag: Sdu Uitgevers 2000.

12 Zie o.a.: D. Engelen, 'Lessons learned. De Nederlandse 'stay behind'-organisatie in de Koude Oorlog', *Militaire Spectator* 2005, afl. 10, p. 415-420; W. Kuijl, 'Warmlopen voor de Koude Oorlog. De Nederlandse stay-behind-organisatie Inlichtingen en Operatiën, 1950-1980', *Militaire Spectator* 2020, afl. 1, p. 28-39.

Tegenwoordig zijn er twee 'combidiensten': de Algemene Inlichtingen– en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen– en Veiligheidsdienst (MIVD). Het voordeel van zulke combidiensten is, zo lezen wij althans op de AIVD–website, dat de onderlinge lijnen korter zijn en dat het leidt tot 'integrale en slagvaardige analyses'.[13] Aanvankelijk leek de AIVD in de praktijk vooral een veiligheidsdienst te zijn – dat wil zeggen: gericht op de binnenlandse veiligheid – en de MIVD primair een inlichtingendienst.[14] Maar de afgelopen jaren zijn 'inlichtingen' en 'veiligheid' steeds verder verknoopt geraakt. Dat is het gevolg van globalisering en de groeiende verwevenheid van interne en externe veiligheidsdreigingen.[15] De diensten werken bovendien intensiever samen. Momenteel krijgt de civiel–militaire samenwerking vooral gestalte in gemeenschappelijke teams en de *Joint Sigint and Cyber Unit*.[16]

2.3 Inlichtingen en opsporing

Bij de bestudering van de inlichtingen– en veiligheidsdiensten moet men in het achterhoofd houden dat inlichtingenwerk en opsporingsactiviteiten in Nederland strikt van elkaar zijn gescheiden.[17] Opsporingsactiviteiten richten zich op gepleegde strafbare feiten. Inlichtingenwerk daarentegen draagt bij aan het onderkennen van dreigingen. Soms is dat ter voorkoming van misdrijven, maar vaak ook niet, al was het maar omdat het handelen van een tegenstander niet altijd strafbaar is of omdat het niet in alle gevallen hard te maken is. Anders gesteld: politie en justitie werken vooral *ex post factum*, de diensten *ex ante factum*.[18] Voor het opstarten van een inlichtingenonderzoek is ook géén verdenking in de zin van artikel 27 Wetboek van Strafvordering vereist. Een aanwijzing dat een persoon of organisatie de nationale veiligheid – in de ruime

13 Zie de AIVD-infopagina 'Waarom is de AIVD een gecombineerde dienst' (online).

14 C.W. Hijzen & A. Tjepkema, 'De toekomst van de inlichtingendiensten', *S&D* 2014, afl. 4, p. 73-79, aldaar p. 76-77; J.J. Oerlemans, *Grenzen stellen aan datahonger. De bescherming van de nationale veiligheid in een democratische rechtsstaat* (oratie), Utrecht: Universiteit Utrecht 2020, p. 4.

15 De Graaff 2019, p. 30 (noot 8).

16 De *Joint Signal and Cyber Unit* ondersteunt operaties van de AIVD en de MIVD in technische zin en valt met enige goede wil te beschouwen als pendant van het GCHQ (Verenigd Koninkrijk) of de NSA (Verenigde Staten).

17 Dit is sinds de Tweede Wereldoorlog het geval. In andere landen worden inlichtingen en opsporing soms gecombineerd. Denk bijvoorbeeld aan het Amerikaanse FBI, de Britse Special Branch of het voormalige Franse DTS.

18 Zie o.a.: Y. Buruma, 'Terrorisme en de weerbare rechtsstaat', *DD* 2001, afl. 10, p. 1025-1033; P.D. van Hees, 'De AIVD en het strafrecht', *AA* 2007, afl. 3, p. 210-217; E.R. Muller, 'Inlichtingendiensten in Nederland', in: C.J.C.F. Fijnaut e.a. (red.), *Politie. Studies over haar werking en organisatie*, Deventer: Kluwer 2007; Y. Buruma, 'Geheime diensten en het afluisteren van advocaten', in: Th.O.M. Dieben, J.I.M.G. Jahae & P.T.C. van Kampen (red.), *Advocaat(-generaal). Liber amicorum Taru Spronken*, Deventer: Wolters Kluwer 2015, p. 55-73, aldaar p. 58-59; Anonieme AIVD-medewerkers, 'De AIVD ontrafelt', *Strafblad* 2016, afl. 4, p. 277-282, aldaar p. 277-278.

zin des woords – bedreigt, is daarvoor voldoende. De diensten spreken daarom niet over een 'verdachte', maar over een 'target'. Institutioneel staan de diensten bovendien los van de justitiële keten. Zij hebben uitdrukkelijk géén opsporingstaak. Het ontbreekt dienstmedewerkers daarom aan executieve justitiële bevoegdheden.[19] Zij mogen dus geen burgers aanhouden, verhoren, gevangennemen of uitzetten. AIVD'ers en MIVD'ers beschikken ook zeker niet over wat in James Bond–films een *license to kill* heet.[20]

3 WETTELIJK KADER

In een democratische rechtsstaat speelt het legaliteitsbeginsel een cruciale rol. De wetgever hecht tegenwoordig dan ook veel belang aan de wettelijke inkadering van de diensten. De wet is, zoals de diensten plegen te zeggen, hun *license to operate*.[21] Dat was vroeger wel anders. Decennialang ontbrak elke formeel–wettelijke grondslag voor het inlichtingen– en veiligheidsbedrijf. De werkzaamheden van de eerste naoorlogse diensten berustten op Koninklijke Besluiten, die als staatsgeheim waren gerubriceerd. De regering wilde namelijk niet dat uit de *Staatscourant* zou blijken dat Nederland in het buitenland spioneerde.[22]

Pas in 1972 ging de regering, na stevige parlementaire druk, overstag. Zij gaf de bedoelde besluiten vrij.[23] Het parlement bleef nadien aandringen op een ordentelijke, *wettelijke* regeling. De regering boog uiteindelijk mee. Eind jaren tachtig trad 's lands eerste Wet op de inlichtingen– en veiligheidsdiensten (Wiv) in werking. Maar deze wet had weinig om het lijf. Het was in feite niet meer dan een takenlijst. Een opsomming van bevoegdheden en de voorwaarden waaronder deze mochten worden ingezet, trof men daarin immers niet aan. De regeling stond dan ook op gespannen voet met het legaliteitsbeginsel en het rechtszekerheidsbeginsel.[24]

In 1994 oordeelde de Afdeling bestuursrechtspraak van de Raad van State dat de inlichtingenwet op belangrijke punten tekortschoot.[25] Er was nu geen ontkomen aan: de wet moest worden herzien. Een langdurig wetgevingstraject

---

19 Art. 13 Wiv 2017.

20 Vgl.: Oerlemans 2020, p. 5 (noot 14).

21 *Jaarverslag AIVD 2020*, Den Haag 2021, p. 18.

22 D. Engelen, *Geschiedenis van de Binnenlandse Veiligheidsdienst*, Den Haag: Sdu Uitgeverij 1995, p. 93-95, 10-105 en 367-368.

23 *Stb*. 1972, 437. Zie uitgebreid: Hijzen 2016, p. 237-245 (noot 8).

24 A.J. Nieuwenhuis, 'Tussen geheimhouding en controle: de AIVD in de democratische rechtsstaat', *TvCR* 2016, afl. 2, p. 79-98, p. 81-82.

25 Het betreft de zaken Van Baggum en Valkenier. Laatstgenoemde zaak is niet gepubliceerd en verwijst voor de motivering naar Van Baggum. Zie: ABRvS 9 juni 1994, ECLI:NL:RVS:1994:AN4196, *AB* 1995, 238 m.nt. A.A.L. Beers.

ving aan. Uiteindelijk resulteerde dit in de Wiv 2002.[26] Deze inlichtingenwet overtrof haar voorloper ruimschoots in omvang en detailniveau. Waar de oude wet slechts 26 artikelen kende en een toelichting van 17 pagina's had, had de nieuwe 106 artikelen en ruim honderd pagina's toelichting. De Wiv 2002 bevatte enkele noviteiten, waaronder – daarover later meer – de instelling van de Commissie van Toezicht op de Inlichtingen– en Veiligheidsdiensten (CTIVD). Toch betrof het hier vooral een codificatie van verschillende onderzoekshandelingen die de diensten allang toepasten bij de uitoefening van hun wettelijke taken.[27]

Aanvankelijk voldeed de Wiv 2002. Naarmate de jaren vorderden, kwamen er echter steeds meer knelpunten aan het licht. De uit het pre–digitale tijdperk afkomstige inlichtingenwet bleek onvoldoende toegesneden op de digitalisering van overheid en samenleving, die met steeds rassere schreden vorderde. In de praktijk troffen de diensten in toenemende mate maatregelen – zoals het binnendringen van geautomatiseerde werken, oftewel 'hacken' – die een specifieke wettelijke basis ontbeerden, maar die zij noodzakelijk achtten voor de bescherming van de nationale veiligheid.[28]

De Commissie–Dessens evalueerde in 2013 het inlichtingen– en veiligheidsbestel. Haar rapport toonde aan dat de vigerende inlichtingenwetgeving inderdaad was verouderd.[29] De wetgever was opnieuw aan zet. Ditmaal gooide hij het over een andere boeg. Uitgangspunt was dat de nieuwe wet 'technologieneutraal' én 'EVRM–proof' moest zijn. Bevoegdheden werden daarom niet, zoals voorheen, gekoppeld aan specifieke technologische toepassingen. Zo zouden diensten technologische ontwikkelingen beter kunnen bijbenen. Tegelijkertijd verruimde de wetgever de mogelijkheden om digitale communicatie te intercepteren en geautomatiseerde data–analyse toe te passen.[30] Ter compensatie verzwaarde de wetgever de wettelijke waarborgen voor een bevoegdhedeninzet en herschikte hij het stelsel van controle– en toezichtmechanismen.

---

26 Zie voor enige context: C.J.C.F. Fijnaut, 'Inlichtingendiensten in Europa en Amerika: de heroriëntering sinds de val van de Muur en 11 september 2001', *JV* 2004, afl. 3, p. 10-43; B.G.J. de Graaff, 'Het contraterrorismebeleid in Nederland', in: F. Osinga e.a. (red.), *Nine eleven. Tien jaar later*, Amsterdam: Boom 2011, p. 144-162.

27 R.J.I. Dielemans, 'De Wiv 2002 en Wiv 2017 op enkele hoofdlijnen vergeleken', *JV* 2018, afl. 1, p. 68-84, aldaar p. 69.

28 Nieuwenhuis, *TvCR* 2016, afl. 2, p. 83 (noot 24); Dielemans, *JV* 2018, afl. 1, p. 70 (noot 27); E.R. Muller & W.J.M. Voermans, 'Nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten. Een nieuw evenwicht tussen veiligheid en waarborgen', *NJB* 2017, afl. 2, p. 102-109, aldaar p. 105.

29 Commissie Evaluatie Wet op de Inlichtingen- en Veiligheidsdiensten (hierna: Commissie-Dessens), *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002: naar een nieuwe balans tussen bevoegdheden en waarborgen*, Den Haag 2013.

30 Zie J.J. Oerlemans & M. Hagens, 'De Wet op de inlichtingen- en veiligheidsdiensten 2017: Een technologisch gedreven wet', *Computerrecht* 2018, afl. 3, p. 130-141; J.J. Oerlemans & M. Hagens, 'Privacy en bulkinterceptie in de Wiv 2017', *AA* 2017, afl. 7/8, p. 560-568.

Nadat de nieuwe wet, de Wiv 2017, door het parlement was aangenomen, ontstond commotie over wat in de volksmond 'de sleepnetwet' is gaan heten. Het een en ander mondde uit in een raadgevend referendum, waarin een nipte meerderheid van de kiesgerechtigden zich kantte tegen de Wiv 2017. De regering deed enkele concessies, maar zette wel door: de wet trad op 1 mei 2018 volledig in werking. De resultante is een nogal complexe wet met veel specialistische termen en welgeteld 283 pagina's aan toelichting.[31]

4 STURING EN BEHOEFTESTELLING

Na de algemene karakterisering van de diensten en het relevante wettelijk kader ziet deze paragraaf op de sturingsrelaties en, meer in het bijzonder, op wat in de *intelligence cycle* de behoeftestelling heet.

4.1 Sturing

Vanouds eist de Wiv dat de diensten hun taken verrichten 'in gebondenheid aan de wet' en 'in ondergeschiktheid aan Onze betrokken Minister'.[32] Dat lijkt misschien vanzelfsprekend, maar blijkbaar vond (en vindt) de wetgever het noodzakelijk dit nog eens uitdrukkelijk in de wet te benoemen. Hiermee wil hij benadrukken dat de diensten niet boven de wet staan en tevens de centrale rol van de ministeriële verantwoordelijkheid in dit domein onderstrepen.

De AIVD ressorteert onder de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK); de MIVD onder de minister van Defensie.[33] De bewindslieden zijn de spilfiguren tussen parlement en dienst.[34] Zij leggen verantwoording af voor het totale beleid (prioriteiten én posterioriteiten), de aansturing van de diensten, waaronder de bedrijfsvoering, en de interne controle.[35] Voorts zijn zij betrokken bij diverse autorisatiesprocessen. Vanzelfsprekend zijn zij voor de door hun verstrekte machtiging tot een inzet van bijzondere bevoegdheden – de lastgeving – volledig ministerieel verantwoordelijk.[36]

Op het eerste oog lijkt de sturing eenduidig geregeld. De praktijk is wat complexer. De diensten presenteren zich graag als reguliere uitvoeringsorganisaties. Vanwege hun taken, werkwijzen en verantwoordelijkheden zijn zij

---

31 Zie uitgebreid over de turbulente wetsgeschiedenis: R.H.T. Jansen, 'Toezicht onder de Wet op de inlichtingen- en veiligheidsdiensten 2017: een tour de force', *NTM/NJCM-Bulletin* 2021, afl. 4, p. 419-443.

32 Art. 2 Wiv 2017.

33 Met dien verstande dat de AIVD als directoraat-generaal is ondergebracht bij BZK, terwijl de MIVD integraal onderdeel is van het defensieapparaat.

34 Nieuwenhuis, *TvCR* 2016, afl. 2, p. 84 (noot 24).

35 Opsomming uit Commissie-Dessens 2013, p. 46 (noot 29).

36 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 197.

echter moeilijk te beschouwen als 'gewone' departementsonderdelen. Hun positie is van oudsher betrekkelijk eigenstandig. Dat laat zich als volgt verklaren. De ultieme opdrachtgever van de diensten is niet zozeer de zittende regeringscoalitie, maar de Staat der Nederlanden, zo luidt althans de geldende consensus.[37] Hiermee wordt bedoeld dat de diensten er niet zijn om politieke (coalitie) belangen te behartigen, maar om de nationale veiligheid, de democratische rechtsorde en andere gewichtige staatsbelangen te beschermen. De diensten zien 'speaking thruth to power' dan ook als hun plicht.[38]

Het is van groot belang dat de diensten geen speelbal worden van politieke wisselvalligheid. Niet alleen zou dat de legitimiteit en de continuïteit van hun optreden schaden, maar ook kan dat ervoor zorgen dat hun inlichtingenpositie internationaal verslechtert. Oud–diensthoofd Docters van Leeuwen, die in de vroege jaren negentig leiding gaf aan de BVD, schreef daarover: 'Niemand [wil] een gepolitiseerde geheime dienst. De minister van Binnenlandse Zaken gaat erover en mag bevelen geven, maar terughoudendheid is geboden; zo gauw de minister iets doet dat kan worden uitgelegd als politieke sturing, kan dat het einde betekenen van de minister en van de veiligheidsdienst zelf'.[39] Dat is, zo meen ik, vandaag de dag niet anders.

4.2 Behoeftestelling

Aansturen is één ding, het bepalen van prioriteiten en posterioriteiten is iets anders. Wie bepaalt eigenlijk de onderzoeksagenda's van de diensten? Of in inlichtingenjargon: wie stelt de behoeften? Traditioneel hadden de Nederlandse diensten op dit punt grote zelfstandigheid. Vanuit de *early warning*–taak geredeneerd pleit daar ook wel het nodige voor.[40] Het risico ervan is dat een dienst zich loszingt van de politiek–ambtelijke top, wat zich niet goed verdraagt met de ministeriële verantwoordelijkheid. Derhalve adviseerde de Commissie–Dessens in 2013 de *governance*–structuren te herzien en de betrokkenheid van 'behoeftestellers c.q. veiligheidspartners' te versterken.[41] De regering heeft daarop de zogeheten 'Geïntegreerde Aanwijzing' geïntroduceerd: volgens een vaste procedure onderhandelen afgevaardigden van verschillende ministeries[42] en van de diensten over, kort samengevat, de gewenste

---

37 Frissen 2016, p. 206-207 (noot 4); De Graaff 2019, p. 31 (noot 8).

38 Vgl.: P. Bindt, 'Taken, bevoegdheden en waarborgen Wiv in balans', *iBestuur* 26 februari 2018, www.ibestuur.nl.

39 A.W.H. Docters van Leeuwen, *Een spoor van vernieuwing*, Amsterdam: Prometheus 2020, p. 250.

40 Vgl.: De Graaff 2019, p. 34 (noot 8).

41 Commissie-Dessens 2013, p. 56-57 (noot 29).

42 Vertegenwoordigers van de ministeries van Algemene Zaken, BZK, Defensie, Buitenlandse Zaken en Justitie & Veiligheid onderhandelen eerst in een ambtelijk voorportaal, de zogenoemde 'Commissie Veiligheids- en Inlichtingendiensten Nederland'. Afstemming vindt vervolgens plaats in de ministeriële onderraad Veiligheid en Inlichtingen en

scope en dekkingsgraad van onderzoeken, de onderzoeksprioritering en de taakverdeling tussen de diensten.[43] Inmiddels heeft de wetgever deze figuur geformaliseerd.[44]

4.3 Politisering

Ogenschijnlijk heeft 'Politiek Den Haag' de afgelopen decennia de teugels wat aangetrokken. Niet alleen hebben de ministers hun grip op de diensten verstevigd, ook hebben andere departementen formeel (iets) meer in de pap te brokkelen gekregen bij de behoeftestelling. Hoe nu deze koerswijziging te beoordelen? De Algemene Rekenkamer ziet laatstgenoemde ontwikkeling als een vooruitgang. Hierdoor zouden 'elementen van verzakelijking en meerjarige sturing binnentreden in de relatie tussen het kabinet en de beide inlichtingen– en veiligheidsdiensten'.[45]

Critici waarschuwen weleens voor wat in de Angelsaksische literatuur *politicisation of intelligence* heet.[46] Meer concreet: de figuur van de Geïntegreerde Aanwijzing zou het gevaar in zich bergen van een verkeerde *mindset*. 'Niet de behoefte van de afnemers moet immers centraal staan bij de diensten, maar de inschatting van de dreigingen voor de nationale veiligheid', aldus inlichtingenhistoricus Abels.[47] Zijn vrees is, als ik het goed zie, dat de diensten te veel aan de leiband van de politiek zouden gaan lopen.

Men kan ook anders redeneren. Mijns inziens draagt dit instrument eraan bij dat de diensten niet verworden tot een soort staat–in–een–staat. Het dwingt de afnemers van inlichtingen (lees: de andere departementen) na te denken over hun inlichtingenbehoeften en in samenspraak met de diensten een realistische afweging te maken van de mensen en middelen die daarvoor nodig zijn.

---

daarna in de ministerraad. Uiteindelijk stellen de minister-president, de minister van BZK en de minister van Defensie de Geïntegreerde Aanwijzing vast.

43 Onder het regime van de Wiv 2002 werd jaarlijks een 'Aanwijzingsbesluit voor de inlichtingentaak van de AIVD' en een 'Inlichtingen- en Veiligheidsbehoefte voor Defensie' vastgesteld. De Geïntegreerde Aanwijzing ziet op bijna alle terreinen van inlichtingen én veiligheid. Alleen zaken als veiligheids- of betrouwbaarheidsonderzoeken en de dreigings- en risicoanalyses ten behoeve van het stelsel bewaken en beveiligen vallen erbuiten. Zie: *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 24.

44 Art. 5-6 Wiv 2017.

45 Algemene Rekenkamer, Bezuinigingen en intensiveringen bij de AIVD. Gevolgen van de budgettaire turbulentie in de periode 2012-2015, Den Haag 2015, p. 55.

46 P.H.A.M. Abels, *Per undas adversas? Geheime diensten in de maalstroom van politiek en beleid*, (oratie), Leiden: Universiteit Leiden 2018, p. 6-11; P.H.A.M. Abels, *Spionkoppen. Inlichtingenleiderschap in elf portretten*, Amsterdam: Prometheus 2020, p. 265-266 en 317; Vgl.: Frissen 2016, p. 207 en 222-223 (noot 4).

47 Abels 2018, p. 9-10 (noot 46).

5 TAKEN EN BEVOEGDHEDEN

Nu verandert de invalshoek van deze bijdrage. Waar de vorige paragrafen zijn opgesteld vanuit een meer extern perspectief, ziet deze paragraaf op interne processen bij de diensten. In inlichtingencyclustermen gaat het hier om verzameling, verwerking en analyse. Omwille van de omvang van deze bijdrage neem ik deze aspecten samen.

5.1 Taken

Welnu, waartoe zijn de AIVD en de MIVD precies op aard? Hun taken zijn limitatief opgesomd in de Wiv 2017.[48] In de kern komt het erop neer dat de diensten activiteiten verrichten in het belang van de 'nationale veiligheid'.[49] Juridisch is dat een moeilijk begrip. De wetgever heeft dit begrip ontleend aan artikel 8 EVRM en de jurisprudentie daarover, maar nagelaten het te definieren in de Wiv 2002 of in de Wiv 2017.[50] In feite is het een containerbegrip, waaronder diverse veiligheidsbelangen te scharen zijn.

Als men het begrip 'nationale veiligheid' nader wil inkleuren, moeten de taakstellingsbepalingen worden bekeken. Daaruit volgt dat de diensten handelen ter bescherming van de 'democratische rechtsorde', 'veiligheid van de staat', 'andere gewichtige belangen van de staat' en, in het geval van de MIVD, 'veiligheid en paraatheid van de krijgsmacht'.[51] Een verdere concretisering treft men in aan het openbare meerjarenplan *Nationale Veiligheid Strategie*, het jaarlijkse *Cybersecuritybeeld Nederland* en het informatierijke *Dreigingsbeeld Statelijke Actoren*. Het blijkt dan te gaan om onderzoeken naar onder meer extremisme, activisme, terrorisme, (digitale) spionage, proliferatie, statelijke actoren, heimelijke politieke beïnvloeding, cyberaanvallen[52] en desinformatie.[53]

---

48 Art. 8 respectievelijk 10 Wiv 2017.

49 *Kamerstukken II* 1999/00, 25 877, nr. 8, p. 18-19; *Kamerstukken II* 2000/01, 25 877, nr. 59, p. 1-2.

50 M. Hagens & E.R. Muller, 'Inlichtingen- en veiligheidsdiensten', in: E.R. Muller e.a. (red.), *Instituten van de staat*, Deventer: Kluwer 2020, p. 435-459, aldaar p. 439-442.

51 Zie specifiek over de militaire context: O. Eichelsheim & M.V. Metselaar, 'Inlichtingen en veiligheid', in: E.R. Muller e.a. (red.), *Krijgsmacht. Studies over de organisatie en het optreden*, Deventer: Wolters Kluwer 2017, p. 379-416.

52 Zie voor meer achtergrondinformatie de AIVD-publicatie *Offensief cyberprogramma: een ideaal businessmodel voor staten*, Den Haag 2019; alsook de AIVD/MIVD-publicatie *Cyberaanvallen door statelijke actoren: zeven momenten om een aanval te stoppen*, Den Haag 2021.

53 *Jaarverslag AIVD 2020*, Den Haag 2021, m.n. p. 4-11; *Jaarverslag MIVD 2020*, Den Haag 2021, m.n. 7-16.

5.2 Vergaren

In feite zijn de diensten, zoals een AIVD–medewerker het in een podcastaflevering eens treffend verwoordde, informatieraffinaderijen.[54] Hun doel is *early warning*. Preciezer: door allerhande gegevens te verzamelen, te analyseren en te duiden, pogen zij veiligheidsrisico's te signaleren en – in samenwerking met ketenpartners – te mitigeren. Om die gegevens te verkrijgen, mogen de diensten menselijke bronnen inschakelen, technische hulpmiddelen inzetten, buitenlandse diensten contacteren en open bronnen onderzoeken.[55]

De wet kent twee soorten bevoegdheden. Ten eerste hebben de diensten 'algemene bevoegdheden' om gegevens uit open en bepaalde gesloten informatiebronnen te verzamelen, en om gegevens op te vragen bij andere instanties.[56] Ten tweede beschikken zij over 'bijzondere bevoegdheden', ook wel 'bijzondere inlichtingenmiddelen' geheten. Laatstgenoemde bevoegdheden hebben een ingrijpender karakter, omdat inzet ervan doorgaans tot een grotere privacy–inbreuk leidt.[57] De diensten mogen vanouds personen observeren, infiltranten en agenten[58] runnen, besloten plaatsen doorzoeken, brieven openen, DNA–onderzoek verrichten en telefoontaps inzetten. De huidige wet voorziet bovendien in ruime(re) bevoegdheden in het digitale domein. Onder voorwaarden is het de diensten bijvoorbeeld toegestaan – in bulk – dataverkeer uit de ether of via de kabel te onderscheppen, alsook computers en andere devices binnen te dringen, oftewel te 'hacken'.

Algemene bevoegdheden mogen worden aangewend ten behoeve van *alle* wettelijke taken van de diensten. Het gebruik van bijzondere bevoegdheden is daarentegen beperkt tot de inlichtingentaken. De bijzondere bevoegdheden mogen dus niet worden aangewend in het kader van veiligheidstaken, zoals het verrichten van veiligheidsonderzoeken en het opstellen van dreigings– en risicoanalyses.[59] Voorts geldt dat de bevoegdhedeninzet altijd in tijd is begrensd en steeds dient te voldoen aan de beginselen van noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid.[60]

---

54 '# 2- Wat tref je aan als de poort opengaat (min. 33:50)', *Podcastserie Dossier AIVD* 12 november 2020.

55 Vgl.: Eichelsheim & Metselaar 2017, p. 385-387 (noot 51).

56 Art. 25, 38, 39, 86-87, 62, 88-90, 91-95 Wiv 2017.

57 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 60. Zie uitgebreid: Oerlemans 2020 (noot 14).

58 Een agent verzamelt onder instructie van een dienst gericht gegevens over personen en organisaties. Als hij online wordt ingezet, heet hij een 'virtueel agent'.

59 Vgl. Hagens & Muller 2020, p. 443-445 (noot 50).

60 Zie art. 26 en 29-30 Wiv 2017. Het gerichtheidscriterium is naar aanleiding van de motie-Recourt toegevoegd aan de toetsingscriteria voor de inzet van bijzondere bevoegdheden. Zie: *Kamerstukken II* 2016/17, 34 588, nr. 66. Dit criterium was neergelegd in art. 5 Beleidsregel Wiv 2017, maar heeft via de Wijzigingswet Wiv 2017 een wettelijke basis gekregen en geldt sindsdien voor de inzet van *alle* bevoegdheden.

5.3 Verwerken

Als de ruwe gegevens eenmaal zijn vergaard, moeten zij worden verwerkt tot bruikbare inlichtingenproducten. In de verwekingfase draait het erom dat dienstmedewerkers de gegevens analyseren, duiden en in verbinding brengen met andere gegevens om zo een steeds completer beeld van een dreiging te verkrijgen. Hierbij dienen de algemene bepalingen omtrent gegevensverwerking uit de Wiv 2017 in acht te worden genomen.[61]

Voor het verwerken van persoonsgegevens gelden enkele beperkende voorschriften. Gegevensverwerking is slechts toelaatbaar ten aanzien van personen die een ernstig vermoeden oproepen dat zij een gevaar vormen voor 'de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat', tenzij de gegevens een 'onlosmakelijk onderdeel vormen van door de diensten te verwerven gegevensbestanden'.[62] Voorts mag persoonsgegevensverwerking niet plaatsvinden op grond van godsdienst of levensbeschouwing, ras, vakverenigingslidmaatschap, gezondheid of seksuele geaardheid, behalve als dat geschiedt 'in aanvulling op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is'.[63] Tot slot gelden er algemene bewaarnormen[64] en zorgplichtvereisten,[65] die onder meer de juistheid en volledigheid van de gegevens en de kwaliteit van de gegevensverwerking normeren.

Overigens worden op de werkvloer ook praktische maatregelen genomen om de privacy–impact van een bevoegdhedeninzet te beperken. Neem het *need–to–know*–principe: dienstmedewerkers mogen slechts kennisnemen van die gegevens die noodzakelijk zijn voor de uitvoering van hun taken. Hier hangt ook functie– en taakscheiding mee samen. Slechts aan bepaalde medewerkers wordt de bevoegdheid toegekend inhoudelijk kennis te nemen van bepaalde gegevens en zij moeten ook steeds specifieke taken verrichten.[66] Zomaar grasduinen in datasets is er dus niet bij. Voorts is er binnen de diensten aandacht voor compartimentalisering: zij kennen – ook fysiek – afgescheiden onderdelen, met verschillende niveaus van geheimhouding. Wie welke informatie(dragers) mag raadplegen, op welk moment en op welke locatie, is bovendien strikt gereglementeerd.[67] Dat is maar goed ook, want de diensten werken met hooggerubriceerde informatie, oftewel 'staatsgeheimen'.

---

61 Hoofdstuk 3 Wiv 2017.
62 Art. 19 lid 1 en lid 5 Wiv 2017.
63 Art. 19 lid 3 en lid 4 Wiv 2017.
64 Art. 20 Wiv 2017.
65 Art. 24 Wiv 2017.
66 In de vier voortgangsrapportages over de werking van de Wiv 2017 onderkent de CTIVD dat functie- en taakscheiding, hoewel wettelijk niet vereist, een waarborg kan vormen bij de toepassing van metadata-analyse.
67 Zie het lezenswaardige hoofdstuk 'Kleine antropologie van het staatsgeheim' in: Frissen 2016 (noot 4).

5.4 Verstoren

Als gezegd, het ontbreekt de diensten aan executieve justitiële bevoegdheden. Minder bekend, maar met het oog op de weerbaarheidsgedachte niet minder interessant, is dat de diensten incidenteel preventief operationeel mogen optreden. Er is een specifieke procedure om bepaalde voorgenomen acties te verstoren van personen en of organisaties die de nationale veiligheid acuut bedreigen.[68] Dit type handelen is slechts in beperkte mate juridisch geregeld.[69] De wetgever heeft – op aanbeveling van de Commissie Bestuurlijke Evaluatie AIVD[70] – een afwegingskader neergelegd in de wet, maar dat is tamelijk beknopt.[71] Formeel–juridisch betreft het hier 'maatregelen' om subversieve activiteiten 'te ontmoedigen of in de kiem te smoren'.[72] 'Maatregelen in de preventieve sfeer kunnen echter ook voorwaardenscheppend zijn voor het op een adequate wijze onder controle krijgen en houden van targets, of dat bijzondere bevoegdheden die op de verzameling van gegevens zijn gericht op een (nog) effectieve(re) manier kunnen worden toegepast', aldus de wetgever.[73]

Over concrete verstoringsacties door de inlichtingen– en veiligheidsdiensten is maar weinig bekend. Te denken valt aan het hinderlijk opvallend volgen of het aanspreken van targets, het verspreiden van desinformatie of het frustreren van voorgenomen gewelddadige acties. De AIVD zou 'met enige regelmaat' de verstoringsbevoegdheid inzetten, 'waarbij kleine vormen van verstoring redelijk frequent worden gehanteerd, terwijl ingrijpende maatregelen slechts sporadisch worden getroffen'.[74]

De diensten mogen ook verstoren in het cyberdomein.[75] Gezien de toenemende digitale dreiging zullen dergelijke acties vermoedelijk nog aan belang winnen.[76] Om evidente redenen komt over concrete cyberoperaties zelden informatie naar buiten. Publiekelijk bekend is de verstoringsactie waarmee de MIVD de OPCW–hack door de Russische militaire inlichtingendienst voorkwam.[77] Dergelijke acties dienen een belangrijk operationeel doel, maar

---

68 Commissie Bestuurlijke Evaluatie Algemene Inlichtingen- en Veiligheidsdienst (hierna: Commissie-Havermans), *De AIVD in verandering*, Den Haag 2004, p. 50.

69 E.R. Muller, 'Bijzondere bevoegdheden van inlichtingen- en veiligheidsdiensten', in: P.H.P.H.M.C. van Kempen e.a. (red.), *Levend strafrecht. Strafrechtelijke vernieuwingen in een maatschappelijke context. Liber amicorum Ybo Buruma*, Deventer: Kluwer 2011, p. 419-435, aldaar p, 430-434.

70 Commissie-Havermans 2004, p. 126 (noot 68).

71 Art. 73 Wiv 2017. Vgl. *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 145.

72 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 145.

73 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 145-146.

74 E.R. Muller, 'De geheime dienst gecontroleerd', *AA* 2009, afl. 4, p. 223-232, aldaar p. 225.

75 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 146.

76 Vgl. L. Bomers & B. de Waal, 'AIVD-topman ziet dreiging toenemen en wil meer kunnen doen tegen cyberaanvallen: 'We moeten sneller, slimmer en beter zijn'', *EenVandaag* 29 juli 2021, eenvandaag.avrotros.nl.

77 H. Modderkolk, *Het is oorlog maar niemand die het ziet*, Amsterdam: Uitgeverij Podium 2019, p. 219-221; Evaluatiecommissie Wiv 2017 (hierna: Commissie-Jones-Bos), *Wet op de*

roepen ook de vraag op hoe ver diensten in de nog weinig gereguleerde cyberspace mogen gaan.[78]

De huidige inlichtingenwet sluit trouwens niet uit dat bij verstoringsacties onder verantwoordelijkheid van de dienst strafbare feiten worden begaan. Een dergelijke actie behoeft voorafgaande interne toestemming en is gebonden aan strikte voorwaarden.[79] Welke strafbare feiten medewerkers of agenten al dan niet mogen plegen, staat niet moet zoveel woorden in de wet. Wel blijkt uit de wetsgeschiedenis van de Wiv 2002 dat 'bijvoorbeeld het (verlenen van medewerking bij het) plegen van moord' onder geen beding is toegestaan.[80] Aanvankelijk overwoog de wetgever een negatieve lijst met strafbare feiten (wat dus zeker niet mag), dan wel een positieve (wat alleen zou mogen), of een 'meer categoriale aanduiding van een bepaald soort delicten' wettelijk te verankeren.[81] Uiteindelijk heeft hij daarvan afgezien en slechts een algemeen kader in de wet neergelegd.

6 DISSEMINATIE

We zetten nu een stap verder in de inlichtingencyclus. De laatste fase, de disseminatie, betreft de inlichtingenverspreiding. Rechtsstatelijk is dit een belangrijk, maar ook een precair proces. Hierin krijgt namelijk de concretisering naar het individuele geval gestalte, waarna ketenpartners mogelijk overgaan tot een interventie.

6.1 Risico's

Wat gebeurt er met door de diensten vergaarde en verwerkte gegevens? Een flink deel ervan verlaat de dienst niet, omdat het ten bate komt van eigen

inlichtingen- en veiligheidsdiensten 2017. Evaluatie 2020, p. 41, bijlage bij *Kamerstukken II* 2020/21, 34588 nr. 88. Beluister voor een nadere duiding door een MIVD'er ook aflevering 19 van de podcastserie 'Cyberhelden'. Zie over recentere cyberverstoringsoperaties ook: *Kamerstukken II* 2020/21, 30 977, nr. 157.

78 Vgl. Y. Buruma, 'International Law and Cyberspace. Issues of Sovereignty and the Common Good', in: *International Law for a Digitalised World*, Den Haag: KNVIR/Asser Press 2020, p. 69-111; Commissie-Jones-Bos 2021, p. 23 (noot 77).

79 Art. 41 lid 3 tot en met lid 7 Wiv 2017. Het in lid 5 verankerde Tallon-criterium is afkomstig uit HR 4 december 1979, ECLI:NL:HR:1979:AB7429, *NJ* 1980, 356. Zie over het plegen van strafbare feiten door agenten: *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 147; CTIVD, *Toezichtsrapport Inzake het onderzoek van de Commissie van Toezicht naar de rechtmatigheid van de uitvoering van een contra-terrorisme operatie van de AIVD* (nr. 7), Den Haag 2006, p. 3-7; Van Hees, *AA* 2007, afl. 3, p. 214-216 (noot 17); Commissie-Dessens 2013, p. 127-128 (noot 29).

80 *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 34.

81 *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 34.

operationele doeleinden.[82] Inlichtingen kunnen bijvoorbeeld behulpzaam zijn bij de rekrutering van nieuwe menselijke bronnen, het initiëren van *covert action* en het verwerven van contra–inlichtingen.[83] Pas in de laatste plaats komt de vraag aan de orde of interventie nodig is en, zo ja, op welke wijze.[84]

Als het noodzakelijk wordt geacht om handelend op te treden, dan moet de dienst andere actoren uit de veiligheidsketen benaderen. Of preciezer: de dienst moet in contact treden met partijen die wél bevoegd zijn om maatregelen jegens personen of organisaties te nemen. De dienst geeft het onderzoek dan uit handen. Vaak is daarmee de inlichtingenoperatie 'kapot'.[85] Essentieel is dan ook dat de inlichtingenproducten op het juiste tijdstip, op de juiste wijze, in de juiste vorm en rubricering bij de juiste afnemer terechtkomen.[86]

Aan disseminatie kleven risico's.[87] In de eerste plaats kan een vroegtijdige informatieoverdracht afbreuk doen aan de kwaliteit en doelmatigheid van het eigenlijke inlichtingen– en veiligheidswerk.[88] In de tweede plaats neemt het risico van compromittering van vertrouwelijke informatie toe, zodra informatie in bredere kring wordt gedeeld. In de derde plaats kan het zijn dat afnemers de dreigingsinformatie niet op waarde weten te schatten en daarom niet of onvoldoende acteren.

Het mag dan wel risicovol zijn, vanuit rechtsstatelijk perspectief bezien heeft disseminatie van inlichtingen een belangrijke meerwaarde. Eerst en vooral omdat het laat zien dat er geen sprake is van machtsopeenhoping bij de diensten, maar dat er een duidelijke taakverdeling geldt tussen verschillende overheidsorganisaties. Het naar buiten treden met informatie draagt bovendien bij aan multiperspectiviteit – er wordt van meer kanten tegen een probleem aangekeken – en is zo bezien een vorm van *checks and balances*.[89]

6.2 Gesloten verstrekkingsregime

De diensten mogen informatie niet lukraak delen met andere overheidsorganisaties, laat staan met buitenlandse diensten. De inlichtingenwetgeving voorziet van oudsher in een gesloten verstrekkingsregime. Gegevensverstrekking is uitsluitend toegestaan in de gevallen waarin de Wiv 2017 voorziet en onder

---

82 De Graaff stelt dat 'slechts een beperkt deel' van de inlichtingen naar externe afnemers gaat. Dat deel is in internationale literatuur geschat op tien procent, maar hij vermoedt dat dat percentage aan de hoge kant is. Zie: De Graaff 2019, p. 129 (noot 8).

83 De Graaff 2019, p. 117 (noot 8).

84 Buruma 2015, p. 58 (noot 18).

85 Frissen 2016, p. 189 (noot 4).

86 Eichelsheim & Metselaar 2017, 389 (noot 51).

87 Zie: De Graaff 2019, p. 118-129 (noot 8). Vgl.: J.G.M. Rademaker en E.J. Frinking, 'Disseminatie en feedback', in: B.A. de Graaf e.a. (red.), *Inlichtingen- en veiligheidsdiensten,* Deventer: Kluwer 2010, p. 535-550.

88 Vgl.: *Jaarverslag CTIVD 2004-2005*, Den Haag 2005, p. 6.

89 Buruma 2005, p. 7 (noot 5).

de daaraan gestelde voorwaarden.[90] Op nationaal niveau mogen de diensten informatie verstrekken aan onder meer politie en justitie, burgermeesters, de Immigratie– en Naturalisatiedienst en de NCTV.

De informatieverstrekking kan op verschillende manieren gestalte krijgen. In de eerste plaats kan het gaan om een 'ten behoeve van zogeheten belangendragers opgestelde specifieke analyse', oftewel een (staatsgeheim) inlichtingenrapport.[91] Veel vaker betreft het een zogenoemd 'ambtsbericht'.[92] Dat is een formele melding over onderzochte personen, organisaties en activiteiten die mogelijk opsporing en vervolging rechtvaardigen. Zo'n bericht heeft in principe een open karakter, want daarin staat – uitzonderingen daargelaten[93] – geen staatsgeheime informatie. Een impressie: in 2020 bracht de AIVD 500 inlichtingenrapporten uit (waarvan 134 tezamen met de MIVD), 63 ambtsberichten en 76 'schriftelijke dreigingsproducten'.[94]

6.3 Vervolging en opsporing

Een ambtsbericht kan de aanzet geven tot opsporing en vervolging,[95] en mag bijdragen aan het bewijs in een strafzaak.[96] Aan het gebruik van ambtsberichten kleven evenwel nadelen. Niet alleen kan de daarin vervatte informatie onbetrouwbaar zijn of onrechtmatig zijn verkregen, ook tasten de procesdeelnemers in het duister over de achtergronden van het ambtsbericht. Zelfs de strafrechter kan de onderliggende gegevens slechts in beperkte mate toetsen op rechtmatigheid en betrouwbaarheid. Omdat dit op gespannen voet staat met het in artikel 6 EVRM verankerde recht op een eerlijk proces,[97] zijn er enkele *checks and balances* ingesteld.

---

90 Paragraaf 3.4.2. Wiv 2017.

91 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 135.

92 Verstrekking geschiedt in beginsel schriftelijk, maar in spoedgevallen mondeling. Opschriftstelling volgt dan later. Zie art. 66 lid 2 en 68 lid 2 Wiv 2017.

93 Bijvoorbeeld: mededelingen van de AIVD aan het ministerie van Buitenlandse Zaken inzake aanvragen voor bepaalde exportvergunningen. Zie: *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 135.

94 *Jaarverslag AIVD 2020*, Den Haag 2021, p. 12-14. De MIVD maakt soortgelijke gegevens niet bekend.

95 Zie over de verstrekking van informatie over strafbaar gedrag aan justitie ook de informatierijke masterscriptie: P.S.M. Rademakers, *Misdaad, inlichtingen, en straf? Waarom de AIVD en de MIVD strafbaar gedrag niet geheim houden voor het Openbaar Ministerie*, Leiden: Universiteit Leiden 2020.

96 Zie uitgebreid: F. Krips, 'Over de bruikbaarheid van AIVD-informatie in strafzaken', *Preadviezen Vereniging voor de vergelijkende studie van het recht* 2009, afl. 1, p. 129-194.

97 Zie o.a.: Brinkhoff, 'Ambtsberichten van de AIVD. Belangrijke maar wel met risico's omgeven schakel in de strafrechtelijke aanpak van jihadisme', *NJB* 2014, afl. 37, p. 2633-2639; M. Hirsch Ballin, 'Informationele solidariteit bij terrorismebestrijding', *NJB* 2016, afl. 27, p. 1900-1909, aldaar p. 1907; Hagens & Muller 2020, p. 436 (noot 50).

Vóórdat een dienst een ambtsbericht aan het Openbaar Ministerie verstrekt, moet eerst een uitgebreide interne procedure worden doorlopen.[98] Vervolgens mag de Landelijk Officier van Justitie Terrorismebestrijding *alle* documenten inzien, dus ook de staatsgeheime documenten.[99] In een later stadium mag de rechter(–commissaris) desgewenst dienstmedewerkers horen.[100] Voorts oefent de CTIVD, zo zullen wij hierna nog zien, rechtmatigheidstoezicht uit. Volgens de regering is dit samenstel aan waarborgen voldoende om het strafrechtelijk gebruik van geheime informatie mogelijk te maken.[101] In de juridische literatuur klinken met enige regelmaat tegengeluiden, maar vooralsnog bestaat er geen consensus over mogelijke oplossingen.[102]

7 CONTROLE EN TOEZICHT

Het *intelligence cycle*–model laat ik nu verder voor wat het is. In deze paragraaf staan de controle– en toezichtmechanismen centraal. Die mechanismen moeten ervoor zorgen dat de diensten rechtmatig opereren. Zij hebben ook een legitimerende functie: een robuust stelsel van controle en toezicht draagt bij aan het maatschappelijk en politiek vertrouwen in de diensten.[103]

---

98 De CTIVD verrichte meermaals onderzoek naar en behandelde verschillende klachten over ambtsberichten. Zie o.a.: CTIVD, *Toezichtsrapport inzake het onderzoek van de Commissie van Toezicht naar de door de AIVD uitgebrachte ambtsberichten in de periode van januari 2004 tot oktober 2005* (nr. 9a), Den Haag 2006; CTIVD, *Toezichtsrapport inzake het onderzoek van de Commissie van Toezicht naar de door de MIVD uitgebrachte ambtsberichten in de periode van januari 2004 tot januari 2006* (nr. 9b), Den Haag 2006; CTIVD, *Toezichtsrapport inzake de door de AIVD uitgebrachte ambtsberichten in de periode van oktober 2005 tot en met mei 2010* (nr. 29), Den Haag 2011; CTIVD, *Toezichtsrapport inzake de door de MIVD uitgebrachte ambtsberichten in de periode van januari 2006 tot en met juni 2011* (nr. 32), Den Haag 2012; CTIVD, *Toezichtsrapport inzake het vervolgonderzoek naar de door de AIVD uitgebrachte ambtsberichten betreffende (kandidaat) politieke ambtsdragers en potentiële leden van de koninklijke familie* (nr. 36), Den Haag 2013.

99 Art. 66 Wiv 2017; *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 140-141.

100 Art. 226m e.v. Sv (Wet afgeschermde getuigen).

101 *Kamerstukken II* 2015/16, 29 279, nr. 309.

102 Brinkhoff, *NJB* 2014, afl. 37 (noot 96); Hirsch Ballin, *NJB* 2016, afl. 27, m.n. p. 1907-1909 (noot 96). Vgl.: Commissie-Dessens 2013, p. 157-158 (noot 29).

103 Zie uitgebreid: N. Verhoeven, 'Toezicht op inlichtingen- en veiligheidsdiensten', in: B.A. de Graaf e.a. (red.), *Inlichtingen- en veiligheidsdiensten,* Deventer: Kluwer 2010, p. 143-160; M. Hagens, 'Toezicht op de inlichtingen- en veiligheidsdiensten in het kader van terrorismebestrijding', *Strafblad* 2016, afl. 4, p. 283-292; M. Hagens, 'Toezicht op de inlichtingen- en veiligheidsdiensten: een blik op het heden, het verleden en de toekomst', in E. Bakker e.a. (red.), *Terrorisme. Studies over terrorisme en terrorismebestrijding*, Deventer: Wolters Kluwer 2017, p. 555-594; M. Hagens, 'Toezicht in de Wiv 2017. Kansen en uitdagingen voor een effectief en sterk toezichtstelsel', *JV* 2018, afl. 3, p. 85-98.

7.1 Intern en extern

Eerst een kanttekening: het is niet precies duidelijk wat te gelden heeft als 'controle' en wat als 'toezicht'. In parlementaire stukken worden de begrippen door elkaar heen gebruikt.[104] Misschien doet dit conceptuele onderscheid er ook weinig toe. Het komt erop neer dat verschillende personen en instanties over de schouders van de diensten meekijken, opdat onrechtmatigheden worden gesignaleerd, beëindigd en voorkomen. In de inlichtingenstudies is het gebruikelijk te differentiëren tussen 'intern toezicht' en 'extern toezicht'.[105] Intern toezicht betreft toezicht door de betrokken ministers en de ambtelijke dienstleiding op basis van interne, op schrift gestelde richtlijnen.[106] Hoe dit toezicht in de huidige praktijk precies functioneert, is voor een buitenstaander waarschijnlijk lastig te achterhalen maar beslist de moeite van het nader onderzoeken waard.[107]

7.2 Externe mechanismen

Over het extern toezicht beduidend méér bekend, al zal een niet–ingewijde wegens de geheimhoudingsnoodzaak ook hiervan nooit alle *ins* en *outs* kennen. Het valt onder te verdelen in parlementair toezicht, rekenkamertoezicht, toezicht door gespecialiseerde toezichthouders, rechterlijk toezicht en klachtregelingen.[108] Dit totaalbeeld wijkt af van toezichtstelsels in andere domeinen. Niet alleen is dit stelsel zeer gefragmenteerd, ook moet binnen elk afzonderlijk mechanisme de geheimhouding gewaarborgd zijn. Dat laatste vergt afwijkende procedures, met als gevolg dat het toezicht op de diensten zich grotendeels achter gesloten deuren voltrekt. Uiteraard heeft dat alles te maken met de bijzondere aard en context van het inlichtingen– en veiligheidswerk.

Het voorgaande is duidelijk terug te zien in de parlementaire controle op de diensten. De openbare parlementaire controle verloopt via de vaste commissie van de Tweede Kamer, in dit geval die voor BZK en Defensie. Om evidente redenen kunnen daar niet alle *faits et gestes* van de dienstactiviteiten aan bod komen. Er is daarom een geïnstitutionaliseerde vorm van vertrouwelijke informatievoorziening opgetuigd. De besloten controle op de diensten vindt plaats in de Commissie voor de Inlichtingen– en Veiligheidsdiensten (CIVD), in de volksmond bekend als de 'Commissie–Stiekem'. Deze bijzondere

104 Vgl. Commissie-Jones-Bos 2021, p. 117 (noot 77).

105 Zie ook de rechtsvergelijkende studie: I. Leigh & N. Wegge (red.), *Intelligence oversight in the twenty-first century. Accountability in a changing world*, Oxfordshire: Routledge 2019.

106 *Kamerstukken II* 1997/98, 25 877, nr. 3 p. 78; Vgl.: Buruma 2015, p. 59-60 (noot 18).

107 Zie het wat oudere, maar op hoofdlijnen nog relevante CTIVD-Toezichtsrapport nr. 31 over de inzet van de afluisterbevoegdheid en de bevoegdheid tot Sigint-selectie: CTIVD, *Toezichtsrapport inzake de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van Sigint door de AIVD* (nr. 31), Den Haag 2012.

108 Vgl. *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 77-78.

commissie wordt bemenst door de voorzitters van de vijf grootste fracties[109] en ziet toe op de operationele taakuitvoering door de diensten.[110] De CIVD is trouwens niet onomstreden: volgens critici ontbreekt het fractievoorzitters aan tijd, expertise en affiniteit met dit beleidsterrein. Zij betwijfelen dan ook of sprake is van volwaardige en betekenisvolle parlementaire controle op de diensten.[111]

Ook de Algemene Rekenkamer vervult een rol. Het rekenkamertoezicht is drieledig.[112] Ten eerste buigt de Algemene Rekenkamer zich over de financiële en administratieve organisatie van de AIVD en de MIVD. Zij neemt de diensten dan als 'normale' organisaties' mee in het verantwoordingsonderzoek.[113] Ten tweede onderzoekt zij de besteding van de zogeheten 'geheime uitgaven en ontvangsten'.[114] Ten derde rapporteert zij incidenteel over specifieke aangelegenheden inzake het inlichtingen– en veiligheidsbedrijf.[115] Met name de tweede taak vraagt om afwijkende procedures en bijzondere controlebevoegdheden. De Algemene Rekenkamer kan immers in de kluis van de diensten kijken. Om te voorkomen dat vervolgens te gedetailleerd inzicht wordt gegeven in de geldstromen van de diensten, worden rapporten over de geheime budgetten in beginsel als staatsgeheim aangemerkt.[116]

Ter compensatie van de gebrekkige openbare controle op de diensten heeft de wetgever twee onafhankelijke, gespecialiseerde toezichthouders ingesteld. De Toetsingscommissie Inzet Bevoegdheden (TIB) – de nieuwste loot aan de stam – is nadrukkelijk gepositioneerd in de autorisatiefase. Zij toetst de door een minister verleende toestemming voor de inzet van bepaalde bijzondere bevoegdheden op rechtmatigheid (*ex ante*).[117] Als de TIB concludeert dat de

---

109 Conform art. 22 lid 2 van dat reglement kan de commissie worden uitgebreid met hoogstens twee leden.

110 *Kamerstukken II* 2009/10, 29 924, nr. 25; Zie: R.H.T. Jansen, 'Parlementaire controle op de inlichtingen- en veiligheidsdiensten in Nederland', *RM Themis* 2019, afl. 5, p. 179-194.

111 Jansen, *RM Themis 2019*, afl. 5, par. 5 (noot 110).

112 Anders dan de wetgever veronderstelt, meent de Algemene Rekenkamer géén deel uit te maken van het toezichtstelsel; zij oefent naar eigen zeggen *controle* uit op de financiële huishouding van de diensten. Althans, zo lezen wij in het rapport van de commissie-Dessens. Opvallend is het rapport even verderop wel spreekt van 'toezicht door de Algemene Rekenkamer'. Zie: Commissie-Dessens 2013, p. 47, vn. 92 (noot 29).

113 C.J.C.F. Fijnaut, *Het toezicht op de inlichtingen- en veiligheidsdiensten: de noodzaak van krachtiger samenspel. De vertrekpunten en uitkomsten van een gespreksronde*, Den Haag: CTIVD 2012, m.n. p. 41 en 84.

114 Art. 7.20 Comptabiliteitswet 2016. Zie uitgebreid R.H.T. Jansen, 'Geheime uitgaven en ontvangsten van de Staat: known unknowns? Een staatsrechtelijke analyse van de begrotingsartikelen met de omschrijving geheim', *TvCR* 2020, afl. 4, p. 340-363.

115 Belangwekkende voorbeelden zijn de rapporten: Algemene Rekenkamer, *Bezuinigingen en intensiveringen bij de AIVD. Gevolgen van de budgettaire turbulentie in de periode 2012-2015*, Den Haag 2015; Algemene Rekenkamer, *Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt,* Den Haag 2021. Zie enkele oudere voorbeelden in Commissie-Havermans 2004, par. 4.2.3 (noot 68).

116 Jansen 2020, *TvCR* 2020, afl. 4, par. 6 (noot 114).

117 Art. 32 Wiv 2017.

ministeriële toestemming ten onrechte is verleend, vervalt de toestemming van rechtswege.[118] De bevoegdheid mag dan dus niet worden ingezet. Vooralsnog is beroep bij de rechter tegen zo'n afwijzing niet mogelijk.

Daarnaast is er de CTIVD. Zij is operationeel sinds de inwerkingtreding van de Wiv 2002, en bestaat tegenwoordig uit twee gescheiden afdelingen: een afdeling toezicht en een afdeling klachtbehandeling.[119] De eerstgenoemde afdeling houdt gedurende een bevoegdhedeninzet (*ex nunc*) of na afloop daarvan (*ex post*) toezicht op naleving van zowel de Wiv 2017 als de Wet Veiligheidsonderzoeken. Let wel: de wetgever ziet dit toezicht graag beperkt tot rechtmatigheidstoezicht. Doelmatigheidstoezicht zou namelijk te zeer interfereren met de ministeriële verantwoordelijkheid.[120] Bij de afdeling klachtbehandeling zijn de klachtprocedure[121] en de klokkenluidersregeling[122] neergelegd.

Tot slot vervult de rechter verschillende taken. In de eerste plaats moet de rechtbank Den Haag de inzet autoriseren van sommige inlichtingenmiddelen, zoals het openen van poststukken[123] en het afluisteren van journalisten of advocaten.[124] Feitelijk vervult de rechter dan dezelfde *ex ante*–rol als de TIB. In de tweede plaats vervult de rechter 'klassiek' *ex post*–toezicht.[125] Zo kan de strafrechter zich geconfronteerd zien met een tot vervolging leidend ambtsbericht of een dienstmedewerker die als getuige is opgeroepen. De bestuursrechter moet soms oordelen over verzoeken om inzage in c.q. openbaarheid van dossiers of veiligheidsonderzoeken. De burgerlijke rechter kan in beeld komen als de diensten een onrechtmatige daad zouden hebben begaan.

---

118 Het staat de diensten vrij om later een nieuw, aangepast verzoek in te dienen. Dat komt in de praktijk ook regelmatig voor. Zie: *Jaarverslag TIB 2020*, Den Haag 2021, p. 14.

119 Art. 97 Wiv 2017.

120 *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 81. Vgl.: Frissen 2016, p. 217-218 (noot 4).

121 Voorheen behandelde de Nationale Ombudsman klachten over het optreden van de diensten. Zie over de vigerende klachtenprocedure: A.H. toe Laer, 'Klachtbehandeling in de WIV 2017. Een belangrijke waarborg tegen onrechtmatig handelen van de inlichtingen- en veiligheidsdiensten', *NJB* 2019, afl. 11, p. 734-738.

122 Paragraaf 7.2.4. Wiv 2017. Zie ook: *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 178-180.

123 Art. 23 Wiv 2002. Thans art. 44 Wiv 2017.

124 Art. 30 lid 2 en lid 3 Wiv 2017. De diensten moeten hierbij grote terughoudendheid betrachten. Dit is pas geoorloofd als sprake is van zwaarwegende operationele belangen, zoals het bestaan van een direct gevaar voor de nationale veiligheid. De rechterlijke toestemming geldt voor hoogstens vier weken. Een en ander komt voort uit: Rb. Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436; Hof Den Haag 27 oktober 2015, ECLI:NL:2015:2881. Zie: *Kamerstukken II* 2014/15, 29 279, nr. 268; *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 47-50; Oerlemans & Hagens 2018, *Computerrecht* 2018, afl. 3, p. 139 (noot 30). Vgl.: Buruma 2015 (noot 18); M.J. Kroon-van Zweeden, 'Het afluisteren van advocaten door de AIVD. Waar ligt de grens?', *NJB* 2015, afl. 18, p. 1219-1226.

125 Vgl.: Fijnaut 2012, p. 53-64 (noot 113).

7.3 Toezichtbevoegdheden

Ik zoom nog iets verder in. De voorgenoemde instanties hebben zeer uiteenlopende toezichtbevoegdheden. De CTIVD bezit de meest vergaande. Zij heeft toegang tot alle staatsgeheime informatie, kan de systemen van de diensten inzien, mag medewerkers onder ede horen en is bevoegd om desgewenst bijna elke plek te betreden.[126] Zulke royale onderzoeksbevoegdheden hebben de andere toezichthouders niet. Zelfs de rechter moet het met minder doen. Waar de CIVD en de Algemene Rekenkamer op gezette tijden kennisnemen van staatsgeheime informatie, krijgt de rechter daar lang niet altijd inzage in.[127] Ook voor de TIB geldt dat zij goeddeels afhankelijk is van de mededeelzaamheid van de diensten.[128] Daartegenover staat dat de rechter vonnis wijst – dat vanzelfsprekend een bindend karakter heeft – en de TIB bindende rechtmatigheidsoordelen velt. De afdeling toezicht van de CTIVD mag daarentegen slechts rapporteren en adviseren.[129] Uitsluitend een oordeel van de afdeling klachtbehandeling behoeft opvolging door een minister.[130]

7.4 Toekomstbestendigheid

Sinds de millenniumwisseling is het toezichtstelsel uitgedijd. Het is ook gefragmenteerd geraakt. Dat laatste brengt risico's met zich. Toezichthiaten en –doublures zijn niet ondenkbaar. Tijdens de recente wetsevaluatie door 'Evaluatiecommissie Wiv 2017', kortweg 'Commissie–Jones–Bos', kwamen een aantal knelpunten in het huidige toezichtstelsel aan het licht. Zo blijkt de wetgever de relatie tussen het *ex ante*– en het *ex post*–toezicht onvoldoende te hebben doordacht.[131] Daardoor zijn mettertijd patstellingen ontstaan tussen de diensten enerzijds en de toezichthouders anderzijds. Als het aan de evaluatiecommissie ligt, wijst de Afdeling bestuursrechtspraak van de Raad van State voortaan in eerste en enige instantie 'richtinggevende uitspraken' over de uitleg van wettelijke normen en begrippen.[132] Zo hoopt de commissie de balans (terug) te brengen in het toezichtstelsel. Zo'n gang naar de rechter is een interessante

126 Paragraaf 7.2 Wiv 2017.
127 Fijnaut 2012, p. 53-64 (noot 113); Vgl.: Oerlemans 2020, p. 11 (noot 14).
128 Dat leidt weleens tot frictie, omdat de TIB naar eigen zeggen meermaals onjuist is geïnformeerd door de diensten. Zie: *Jaarverslag TIB 2019/2020*, Den Haag 2020, p. 14-15; *Jaarverslag TIB 2020*, Den Haag 2021, p. 12-13.
129 De CTIVD pleit al enige tijd voor bindende toezichtsbevoegdheden. Zie o.a. brieven van de CTIVD aan Evaluatiecommissie Wiv 2017 met kenmerken 2020/0096, d.d. 11 augustus 2020, en 2020/0157, d.d. 2 december 2020 (online). Vgl. R.H.T. Jansen & M.D. Reijneveld, 'Conventie 108+ en (het toezicht op) gegevensverwerkingen in het nationale veiligheidsdomein', *Computerrecht* 2021, afl. 4, p. 411-422, aldaar par. 5.2.
130 Art. 124 Wiv 2017.
131 Commissie-Jones-Bos 2021, p. 126 (noot 77).
132 Commissie-Jones-Bos 2021, p. 135-140 (noot 77).

oplossing, waar ook het nodige voor pleit, maar zal een toch al ingewikkeld toezichtstelsel verder compliceren.

Het kabinet heeft de analyse, de conclusies en de aanbevelingen uit het evaluatierapport inmiddels 'omarmd'.[133] Op het moment dat deze bijdrage ter perse gaat is nog onduidelijk of en, zo ja, hoe de aanbevelingen wetstechnisch worden geïmplementeerd. Wel is duidelijk dat de discussie over het toezicht de laatste tijd is verhard. Vanuit de toezichthouders klinkt, vaak onder verwijzing naar de jurisprudentie van de Europese hoven, een steeds luidere roep om verregaande, bindende mechanismen over de volle breedte van het toezichtspectrum.[134] Een moderne toezichthouder zou niet alleen moeten kunnen informeren en rapporteren, maar ook zelfstandig moeten kunnen intervenieren, zo is de gedachte.

Als een dergelijke maximalisering van het toezicht er inderdaad komt, zal dat een *gamechanger* zijn. Vanuit privacyrechtelijk perspectief is die ontwikkeling misschien aan te moedigen. Onduidelijk is echter hoe dit alles de informatiepositie en de slagkracht van de diensten zal beïnvloeden en ook – vanuit staatsrechtelijk perspectief zeker niet onbelangrijk – of de ministeriële verantwoordelijkheid voor de diensten erdoor niet (te zeer) zou worden uitgehold.[135]

8 BESLUIT

BVD–huishistoricus Engelen stelde ooit: inlichtingen– en veiligheidsdiensten zijn gewone ambtelijke diensten én diensten met een bijzonder karakter.[136] En zo is het. Zulke diensten zijn bureaucratische organisaties, met deels dezelfde en soortgelijke problemen als andere uitvoeringsinstanties. Tegelijkertijd zijn het instituties met speciale karakteristieken. In feite tasten zij de grenzen af van wat in een democratische rechtsstaat vermag. Ter bescherming van de nationale veiligheid en de democratische rechtsorde mogen zij zeer verstrekkende bevoegdheden aanwenden. Doorgaans geschiedt de bevoegdhedeninzet bovendien in het geheim: inlichtingen– en veiligheidsoperaties gedijen nu eenmaal het best bij een vergaande mate van geslotenheid.

Lastig is dat de geheimhoudingsnoodzaak vaak het afleggen van verantwoording aan het parlement en de rechter bemoeilijkt. In een democratische rechtsstaat, waarin controleerbaarheid en voorspelbaarheid van het overheidsoptreden voorop staan, is dat soms ongemakkelijk. Reguliere verantwoordingsregimes volstaan hier dan ook niet. Voor inlichtingen– en veiligheidsdiensten dienen speciale verantwoordingsprocedures te worden

133 *Kamerstukken II* 2020/21, 34 588, nr. 89, p. 2.

134 J.J. Oerlemans & Q.A.M. Eijkman, 'Evaluatie Wiv 2017: betere uitvoerbaarheid, ten koste van privacy?', *IR* 2021, afl. 3, p. 95-101; Jansen *NTM/NJCM-Bulletin* 2021, afl. 4 (noot 31).

135 Vgl. *Kamerstukken II* 2018/19, 29 924, nr. 179.

136 D. Engelen, *Frontdienst. De BVD in de Koude Oorlog,* Amsterdam: Boom 2007, p. 282-283.

opgetuigd. Hoe ver men daarin zou moeten gaan, is moeilijk in algemene zin te zeggen. In feite is het een constante evenwichtsoefening voor de wetgever, waarbij de dreigingscontext en het tijdsgewricht van doorslaggevend belang zijn. Steeds opnieuw zal hij een verantwoord evenwicht moeten zoeken tussen het belang van bescherming van de nationale veiligheid enerzijds en dat van grondrechten van burgers anderzijds. Slaat de balans door naar slagvaardigheid, dan brengt dat potentieel ongebreidelde en onrechtmatige machtsuitoefening met zich. Slaat de balans te zeer de andere kant op, dan tast dat mogelijk de informatiepositie van de diensten en daarmee de nationale veiligheid aan.

Op dit moment mogen de Nederlandse diensten al vrij veel. Hun bevoegdhedenarsenaal is rijkgeschakeerd. Er zijn bijna geen bevoegdheden te verzinnen waarin de vigerende wetgeving niet al op de een of andere manier voorziet. Dat lijkt mij, gezien de huidige dreigingscomplexiteit, zeer wel verdedigbaar. De diensten zijn ook nadrukkelijker actief in het digitale domein.[137] Dat is evengoed te billijken. Samenleving en overheid digitaliseren in rap tempo; de diensten mogen niet achterblijven. Wel lijken de regels van het spel door de voortschrijdende digitalisering en dataficatie te veranderen. Voor de diensten wordt het steeds eenvoudiger om nog grotere hoeveelheden data binnen te halen, op te slaan en te analyseren. Het risico dat zij ook informatie verwerven en verwerken van burgers die geen onderwerp zijn van een inlichtingenonderzoek, de *non–targets*, neemt daardoor toe. Des te belangrijker is het om ferme *checks and balances* op te tuigen.

Als substituut voor volledig openbare verantwoording heeft de wetgever externe toezichtmechanismen opgetuigd. De afgelopen twee decennia is het toezichtveld flink uitgedijd. De diensten zijn daardoor strakker rechtsstatelijk ingesnoerd. Het stelsel is ook gefragmenteerd geraakt. Er zijn thans verschillende instituties die fungeren als grens– en scheidsrechters. Dat maakt het geheel onoverzichtelijk. Verdere versplintering van het toezichtstelsel is geen ondenkbaar scenario. Om hiaten en leemtes in het toezicht te voorkomen en tegelijkertijd de rechtseenheid te borgen, is nu al veel onderlinge afstemming vereist. Ministers, diensten en toezichthouders moeten steeds opnieuw een werkbare *modus vivendi* zien te vinden. Ongetwijfeld brengt een en ander een zekere bureaucratische ballast met zich. Dat zij dan zo. Toezicht schuurt en wringt soms. In een democratische rechtsstaat hoort dat er nu eenmaal erbij. Als niemand volkomen tevreden is, is dat wellicht een signaal dat een stelsel – en daarmee de rechtsstaat – naar behoren functioneert.

---

137 Zie: S. van Schendel, *Het gebruik van Big Data door de MIVD en de AIVD*, Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid 2016.