AIVD / MIVD 2018-2023

Verslag van het functioneren van de diensten

Inleiding

Dit verslag bespreekt hoe de AIVD en de MIVD tussen 2018 en 2023 hebben gefunctioneerd. Het was een periode waarin de diensten voor een reeks uitzonderlijke opgaven stonden. Voor de AIVD bleef de dreiging van het mondiaal jihadisme de volledige aandacht vragen, ook toen de zwarte vlaggen van ISIS niet langer boven Mosul wapperden. Tegelijkertijd eisten, in een tijd van polarisatie, nieuwe vormen van extremisme en terrorisme de aandacht op. Het nieuwe dreigingsbeeld werd gekenmerkt door meerdere dominante dreigingen op hetzelfde moment, of in snelle afwisseling.

De laatste Nederlandse militairen vertrokken in juni 2021 uit Afghanistan, na twintig jaar inzet. Dat was het einde van een tijdperk voor de krijgsmacht. De MIVD heeft tot 2021 bijgedragen aan het inlichtingenbeeld van de missie in Afghanistan, naast de aandacht voor andere missies en dreigingen zoals in Syrië, Irak, Iran, Mali en breder in de Sahel. Daarbij ging het niet alleen om terroristische- en jihadistische groeperingen maar ook om aandacht voor chemische wapens, zoals in Syrië of de capaciteiten van de Iraanse marine en kustverdediging in de Perzische Golf. De militaire activiteiten van Rusland en China in de diverse regio's, en leveranties ook aan Venezuela een buurland van het Koninkrijk, zijn intensief gevolgd, dat geldt ook voor de militaire (niet) conventionele capaciteitsopbouw in de klassieke domeinen maar ook in de ruimte en het cyber- en informatiedomein.

Voor beide diensten kreeg de dreiging uit Rusland en China hoge prioriteit. In 2014 schond Rusland door de inval in de Krim de soevereiniteit van Oekraïne. Sinds 24 februari 2021 woedt aan de grenzen van het NAVO-grondgebied de grootste oorlog in Europa sinds de Tweede Wereldoorlog. Een militair conflict tussen Rusland en de Navo is voorstelbaar geworden. Rusland voert oorlog in Oekraïne en is actief in het hybride domein. Het probeert de Oekraïne en de cohesie van de NAVO en de EU te verzwakken, ook door chantage met graan, gas en olie. Verhogingen van de prijzen zorgen voor hogere lasten voor burgers en bedrijven. Wekelijks varen Russische marineschepen op de Noordzee, waar belangrijke onderzeese kabels lopen. Dagelijks zijn Russische en Chinese (militaire) hackers actief.

Het heeft er onder meer voor gezorgd dat de MIVD en AIVD in de voorhoede zijn komen te staan van een digitaal front. Autocratische landen als Rusland, China, Iran en Noord-Korea voeren voortdurend cyberaanvallen uit op het Westen, ook op Nederland. Ook terroristen vinden elkaar online en extremisten bouwen er hun podium. Het tegengaan van digitale dreigingen, en het steeds meer hybride worden van dreigingen, vraagt om een heel andere manier van werken van de diensten. Eén die draait om technologie en data.

De grootste uitdaging voor de AIVD en de MIVD was dat tussen 2018 en 2023 al die ontwikkelingen samenvielen. En dat kort na de invoering van de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017), die zorgde voor ingrijpende veranderingen in de werkwijze van de diensten. Toetsing, toezicht en gegevensverwerking

[1] Algemene Rekenkamer, 2021, Slagkracht AIVD en MIVD, de wet dwingt, de tijd dringt, de praktijk wringt.

veranderden zo ingrijpend, dat het ten koste ging van de slagkracht1. Juist in zulke beproevende jaren.

De volgende hoofdstukken beschrijven hoe de AIVD en de MIVD die situatie het hoofd hebben geboden. Het is een gezamenlijk verslag. De diensten opereren onder dezelfde wet, stonden (grotendeels) voor dezelfde opgaven en konden daarbij rekenen op elkaar. Samenwerking is een rode draad in dit stuk, zonder dat er voorbij wordt gegaan aan verschillen die de diensten elk kenmerken. Dit verslag is een nieuw soort verslag. Het wijkt in twee opzichten af van de openbare jaarverslagen en de geheime verantwoordingsproducten die de diensten uitbrengen. In de eerste plaats beslaat het een periode van vijf jaar – de wet vraagt dat van de diensten (Wiv 2017 artikel 167 lid 2). In de tweede plaats staat in dit verslag het functioneren van de diensten centraal, níet de dreigingen tegen Nederland of de Nederlandse krijgsmacht. Dat functioneren wordt besproken aan de hand van de zes ontwikkelingen die daarop het meest van invloed waren, en met een openheid die bij de diensten past.

Thema 1:
Een veranderd nationaal dreigingsbeeld …

Vanaf 11 september 2001 was dé prioriteit voor de AIVD het onderzoek naar het mondiaal jihadisme. Dat veranderde gaandeweg na 2018. Niet omdat jihadisme minder belangrijk werd, of minder gevaarlijk – aanslagen, arrestaties en recent toegenomen aanslagdreiging illustreren dat. Maar omdat er dreigingen tegen Nederland bijkwamen die evenzeer prioriteit vroegen. Het dreigingsbeeld ontwikkelde van één dominante dreiging, naar meerdere dominante dreigingen die elkaar in korte tijd afwisselden, of op hetzelfde moment kwamen. Elk vroegen die uitbreiding van het onderzoek.

De dreiging van statelijke actoren speelde daarin een grote rol, cyberdreigingen en Ruslands oorlog tegen Oekraïne in het bijzonder (meer daarover bij thema's 2 en 3). En verder de dreiging van nieuwe vormen van extremisme en terrorisme in Nederland. In 2018 typeert de AIVD de acties van rechts-extremisten nog als 'geweldloos of licht verstorend'. In 2021 stelt de AIVD vast dat er rechts-terrorisme in Nederland aanwezig is. Aanslagen door eenlingen of groepjes zijn dan voorstelbaar, en dat zijn ze nog steeds.
In dezelfde periode groeit een relatief nieuwe vorm van extremisme, gericht tegen de overheid, journalisten, juristen, wetenschappers en bestuurders. In 2022 lijkt dat 'anti-institutioneel-extremisme een dreiging voor de lange termijn geworden.

…een breder takenpakket, hogere druk, meer flexibiliteit

Met het aantal aandachtsgebieden, groeien de diensten. Ook bij de MIVD breidt het takenpakket drastisch uit. Vooral vanwege de toegenomen dreiging van China en Rusland. Omdat die hybride is – de militaire doelen en capaciteiten van de landen zijn niet los te zien van wat ze op economisch vlak en op gebied van cyber doen – vraagt dat uitbreiding van onderzoek. (Thema 2 gaat daar dieper op in, ook op de nog intensiever samenwerking die ervan het gevolg is.)

De diensten investeerden een groot deel van het toegenomen budget in personeel. Beide diensten waren in 2013 sterk gekrompen na ingrijpende kabinetsbezuinigingen. De AIVD kreeg daarbij een derde minder budget. Voor de MIVD kwam de bezuiniging bovenop eerdere kortingen op het budget. Het effect daarvan was bij de diensten in 2018 nog voelbaar.

De groei van de diensten kan de indruk wekken dat inlichtingenteams tussen 2018 en 2023 functioneerden met meer armslag. Dat was niet altijd het geval, om twee redenen. In 2018 werd de nieuwe Wiv (2017) van kracht (thema 5). Die had gevolgen voor de operationele slagkracht van de diensten. Inlichtingenteams moesten extra administratieve handelingen verrichten dat er minder tijd overbleef voor onderzoek naar dreigingen. Ook werd onder meer de inzet van hackoperaties, het gebruik van bulkdatasets en onderzoeksopdrachtgerichte interceptie (op de ether) minder effectief[2].
Het kabinet gaf de diensten daarna het budget om slagkracht te herstellen. Maar nieuwe collega's kunnen pas na langere tijd de druk op zittende collega's verlichten – werving op een competitieve arbeidsmarkt, een grondig veiligheidsonderzoek en interne opleiding (nodig voor taken die nergens anders te leren zijn) kosten tijd.

Het heeft veel veerkracht van de diensten gevraagd om binnen kort tijdsbestek om te gaan met verlies aan slagkracht, pogingen die slagkracht weer te herstellen en om sturing en overzicht te houden bij groei.
De verandering in dreigingsbeeld heeft ook veel flexibiliteit gevraagd van de organisaties. De aandacht verdelen tussen meer dreigingen betekent in de praktijk vaak: de ervaren mensen verdelen over onderzoeken. De aandacht verleggen naar een nieuwe prioriteit, vraagt soms op korte termijn uitbreiding van het ene team ten koste van het andere.

De diensten staan bij het huidige dreigingsbeeld ook voor de opgave verbanden te leggen tussen

[2] Algemene Rekenkamer, 2021, Slagkracht AIVD en MIVD, de wet dwingt, de tijd dringt, de praktijk wringt.

verschillende onderzoeken. Bij statelijke dreigingen omdat die vaker hybride zijn. Maar ook omdat dreigingen effect kunnen hebben op elkaar. Zowel extremisten, terroristen als georganiseerde misdaad bedreigen momenteel bijvoorbeeld de democratische rechtsorde. De optelsom daarvan kan ondermijning zijn, in een mate die één onderzoek alleen niet boven tafel zou brengen. Dat risico wordt nog groter als andere landen zulke ondermijning aanmoedigen of uitbuiten.

Thema 2:
De dreiging van grootmachten …

Voor zowel de MIVD als de AIVD komt tussen 2018 en 2023 het accent te liggen op cyberdreigingen en statelijk conflict – dreigingen die dan al lang de aandacht hebben van de diensten. De voornaamste statelijke dreiging tegen het Westen kwam van Rusland en China. Beide stelden zich assertiever op toen de Verenigde Staten zich onder president Trump leken terug te trekken van het wereldtoneel. De dreiging die van de twee landen uitgaat, verschilt. China vormt de belangrijkste economische dreiging tegen Nederland, concluderen de AIVD, de MIVD en de NCTV in 2021 in het eerste Dreigingsbeeld Statelijke Actoren. Dat de diensten en de NCTV juist over dat onderwerp een gezamenlijke publicatie uitbrengen, is illustratief voor de mate van dreiging. De diensten waarschuwen al langer dat China het verdienvermogen van het Nederlands bedrijfsleven aantast, door cyberaanvallen, gebruik van spionage, insiders, heimelijke investeringen en illegale export. Door Chinese bedrijfsovernames kan Nederland op strategisch gebied afhankelijk worden, en kwetsbaar voor sabotage. Ook lijkt het land, met Rusland, bezig de internationale rechtsorde uit te hollen. Maar China is behalve een dreiging, op veel vlakken ook een partner van Nederland. Daartussen blijft het balans zoeken.

Tussen Rusland en Nederland verslechteren de verhoudingen dan al jaren. President Poetin geeft in 2007 een speech in München, waaruit blijkt dat hij het Westen als dreiging is gaan zien. In de jaren erna gebruikt het land steeds meer geweld om invloed te houden in de directe omgeving: critici worden geliquideerd, Georgië wordt binnengevallen, de Krim wordt geannexeerd, MH17 wordt neergehaald. Rusland mengt zich ook in conflicten in Syrië en Afrika. Het land zet daarvoor vaak huurlingen in, zoals de Wagner Group, zodat het formele betrokkenheid kan ontkennen.

Tegelijk probeert Rusland clandestien het Westen te verzwakken. In het bijzonder de Westerse veiligheidsarchitectuur die het moet hebben van samenwerking. Dat doet het land met cyberaanvallen, spionage, desinformatie en beïnvloedingscampagnes die tweespalt in Westerse samenlevingen aanwakkeren. Op 24 februari 2022 valt het Russische leger met 160 duizend militairen Oekraïne binnen. Een enorme escalatie van het geweld, en een openlijke confrontatie met het Westen.

… krachtenbundeling bij de diensten op een nieuwe schaal

Veel westerse landen bereiken tussen 2018 en 2023 in hun relaties met Rusland en China een kantelpunt. Het wordt duidelijk dat de assertieve opstelling van deze staten in de diverse regio's onvermijdelijk ten koste gaat van de internationale rechtsorde, en de veiligheid van de EU en de NAVO. Beide diensten besteden in nauwe onderlinge samenwerking vanzelfsprekend in die periode met internationale partners veel aandacht aan de militaire activiteiten, de opbouw van (niet) conventionele capaciteiten en de intenties van beide landen.

In 2049 wenst China een militaire en economische grootmacht te zijn. Om die doelstelling te bereiken schuwt China grootschalige spionage niet. En beide landen maken gebruik van strategische afhankelijkheden. Dergelijke methoden gaan ten koste van een eerlijk economisch speelveld en het westerse economische verdienmodel. Daarom investeert het kabinet in een betere inlichtingenpositie op dreigingen uit Rusland en China. Economische veiligheid wordt een aandachtsgebied voor beide diensten. De MIVD kijkt daarbij vooral naar in Nederland aanwezige technische kennis, die door andere landen ook militair kan

worden gebruikt. Dat de dienst al een sterk netwerk heeft in Nederlandse defensie-industrie, helpt daarbij. De MIVD gaat zich ook meer bezighouden met veiligheid op de Noordzee – een belangrijke doorvaartroute voor de Russische marine. Die vaart momenteel vaker dan gemiddeld door Nederlands exclusieve economische zone (elke week met zo'n twee schepen). Dat is zorgelijk, onder meer omdat door de Noordzee internet- en elektriciteitskabels lopen. Ook heeft een Russisch schip geprobeerd de infrastructuur van windmolenparken voor de Nederlandse kust in kaart te brengen.

Het lag voor de diensten voor de hand om hun onderzoekscapaciteit naar dreigingen uit China en Rusland te bundelen. In 2018 werkten de diensten in veel opzichten al nauw samen, en hadden ze al diverse gezamenlijke teams. Maar in het onderzoek naar statelijke dreigingen intensiveerden ze hun samenwerking op een nieuwe schaal. Ze vormen vanaf 2019 gezamenlijke 'huizen', afdelingen waar hun expertise, middelen en onderzoek naar Rusland en China samenkomen. De steeds inniger samenwerking krijgt in de jaren erna ook vorm in gezamenlijke huisvesting, nieuwe units, en het meer gelijktrekken van werkprocessen. Veel van de samenwerking komt onder tijdsdruk tot stand, en er is veel learning by doing. Het vraagt een voortdurende inspanning van beide diensten om personeel, organisatie en middelen op elkaar te laten aansluiten.

In reactie op de statelijke dreiging legden de diensten kortere lijnen met diverse ministeries. Onder meer door het (onderling) plaatsen van contactpersonen en het uitwisselen van meer informatie. De betere aansluiting maakt dat er sneller kan worden ingegrepen op basis van inlichtingen. Een voorbeeld daarvan is de invoering van een veiligheidstoets op investeringen en overnames die een risico kunnen zijn voor de nationale veiligheid. Op 1 juni 2023 trad die in werking.

Thema 3:
Cyberdreigingen ...

China en Rusland spelen een grote rol in de toegenomen cyberdreiging in de wereld. In 2018 hoefde niemand nog naïef te zijn over de risico's daarvan. Het jaar ervoor was er een cyberaanval uitgevoerd die bekend kwam te staan als 'NotPetya'. Het Amerikaanse techblad Wired omschreef die later als 'the most devastating cyberattack in history'. Het voornaamste doelwit van de gebruikte malware was Oekraïne. Maar websites en werkprocessen liepen vast tot in (onder meer) Duitsland, Frankrijk, Italië, Polen, Groot-Brittannië en de Verenigde Staten. In de haven van Rotterdam kwam een containerterminal stil te liggen. Het was het soort cyberaanval dat Westerse landen al jaren vreesden. De CIA en het Britse ministerie van Defensie schrijven 'NotPetya' toe aan Rusland.

Net zo reëel als het risico op zulke op grote, ontwrichtende aanvallen, is het gevaar van death by a thousand cuts: de opgetelde schade van een voortdurend offensief van kleinschaliger hacks, phishing-campagnes, innesteling in digitale systemen, het uitbuiten van kwetsbaarheden en diefstal van data. Nederlandse bedrijven, universiteiten en de overheid werden daardoor de afgelopen jaren dagelijks bedreigd of beschadigd. Landen zijn daarvoor vaak de opdrachtgever. Duizenden hackers van autoritaire regimes zoeken elke dag doelen in andere landen en vallen die aan. De MIVD en de AIVD maakten in de loop van de jaren bekend dat naast Rusland en China, ook Noord-Korea en Iran cyberaanvalsprogramma's hebben opgezet. Cyberaanvallen werden de afgelopen jaren geavanceerder en beter verborgen. Het risico op succesvolle aanvallen nam toe, omdat er meer kwam om aan te vallen: steeds meer van ons maatschappelijk leven speelt zich digitaal af, en steeds meer computersystemen zijn met elkaar verknoopt.
(Communicatie)technologie en digitalisering spelen niet alleen een rol bij cyberaanvallen, maar bij vrijwel alle dreigingen. Een voorbeeld is het accelerationisme, een vrij nieuwe rechts-terroristische stroming. De AIVD heeft al diverse keren een concrete dreiging daarvan voorkomen. De beweging bestaat vooral uit (soms heel) jonge mannen

die zijn opgegroeid met het internet, en elkaar bij uitstek daar ontmoeten. Ze verheerlijken extreem geweld, delen streams van aanslagen en bespreken het maken van bommen en het kopen van wapens om een rassenoorlog te kunnen voeren. De broedkamer van de beweging is een online wereld van gesloten communities.

… technologie en data in het hart van het inlichtingenonderzoek

Dat technologie een rol is gaan spelen in bijna elke dreiging (voor communicatie, inspiratie of actie) maakt dat technologie ook een rol is gaan spelen in elk inlichtingenonderzoek. Teams moeten vaker gebruik maken van virtual agents, hackoperaties en interceptie op de kabel. Ze moeten aanwijzingen over dreigingen kunnen vinden in de groeiende hoeveelheid gegevens, teksten, video's, geluidsopnames en beelden – data kortom – in de wereld. Dat heeft gevolgen voor de bedrijfsvoering van de diensten.
Het vraagt nieuwe hardware, software en applicaties. En de mensen die daarmee kunnen werken. De nadruk op techniek in de onderzoeken vertaalt zich dan ook in een nadruk op technische vaardigheden in het personeelsbestand. Soms vraagt dat nieuwe mensen, veelal met een bèta-profiel. Maar waar dat relevant is, wordt van alle medewerkers digitale vaardigheden verwacht. De diensten hebben (mede) daarom geïnvesteerd in de ontwikkeling en verdere opleiding van de medewerkers. Veel data is beveiligd en versleuteld, onbetrouwbaar of onvolledig, het vraagt nieuwe werkwijzen om daarvan bruikbare inlichtingen te maken. Ook het vastleggen van hoe data wordt verwerkt vraagt om nieuwe werkprocessen en soms om nieuwe wettelijke kaders.

Niet voor niets krijgt de Joint Sigint Cyber Unit van de AIVD en de MIVD in steeds meer onderzoeken een cruciaal aandeel. De unit is in 2014 formeel door beide diensten opgericht, maar is juist de afgelopen vijf jaar een onlosmakelijk onderdeel van het inlichtingenproces geworden. Door de oprichting van de JSCU ontstond een krachtige eenheid die veel cybertalent aantrok en afleverde.

Op digitaal vlak kenden de diensten ook tegenslagen. De meest in het oog springende was dat het intercepteren van communicatie via glasvezelkabels amper van de grond kwam. De meeste mobiele- en onlinecommunicatie verloopt via zulke kabels. In de praktijk bleek het onduidelijk onder welke voorwaarden zulke interceptie mag worden ingezet (meer daarover bij thema 5). Ook legde de invoering van de Wiv 2017 zo'n beslag op de ICT-capaciteit van de dienst, dat het innovatie heeft geremd. Tenslotte bleek de toetsing vooraf van met name de digitale middelen in de praktijk te knellen. In de Wiv 2017 staan normen en begrippen die niet duidelijk worden uitgelegd. Dat komt omdat de wet techniekneutraal bedoeld is. Een onbedoeld gevolg was echter dat de diensten en de toezichthouders over begrippen soms verschilden van inzicht. Hierdoor konden inlichtingenmiddelen soms niet worden ingezet of voortgezet. Een goede inlichtingenpositie wordt pas bereikt door een optelsom van factoren: internationale samenwerking, onderzoekscapaciteit en een optimale mix van inlichtingenmiddelen – daarbij is de afgelopen jaren gebleken dat elk middel op zichzelf nodig is, maar dat ze juist in samenhang het effectiefst zijn.

Thema 4:
Verwachtingen en vragen uit de samenleving …

Technologie en data hebben tussen 2018 en 2023 invloed gehad op het beeld dat een deel van de samenleving heeft van de AIVD en MIVD. Nederlanders verwachten van de diensten dat zij waken over de nationale veiligheid en bijdragen aan de bescherming van de krijgsmacht. Tegelijk zijn sommige Nederlanders bezorgd dat bij uitstek digitaal inlichtingenonderzoek ten koste kan gaan van privacy. In de samenleving groeit al lang het onbehagen over hoe privé-gegevens van burgers worden opgeslagen en over hoe online gedrag door bedrijven wordt geregistreerd. Dat onbehagen richtte zich op de diensten rond de introductie van de Wiv 2017. Die wet moest de diensten meer toekomstbestendige bevoegdheden geven. Bij een raadgevend referendum, in maart 2018, stemden

3,3 miljoen Nederlanders tegen de wet (3,1 miljoen stemden vóór). Zorgen over privacy speelden bij de tegenstem een grote rol. In het maatschappelijk debat kwamen bedenkingen en beelden ('sleepwet') op, die een reactie vroegen van de diensten.

Rond het referendum ging toenmalig directeur-generaal AIVD Rob Bertholee daarom publiekelijk in op vragen, onduidelijkheden of zorgen over hoe de dienst werkt. Hij deed dat ook live op televisie – in veel landen ondenkbaar voor het hoofd van een inlichtingen- of veiligheidsdienst. Geregeld trad hij samen op met het toenmalig hoofd van de MIVD, Onno Eichelsheim. De huidige diensthoofden – Erik Akerboom (AIVD) en Jan Swillens (MIVD) – zijn dat blijven doen. Dat bleek mede nodig omdat bij uitvoering van de wet in de praktijk bleek dat deze op punten tekort schoot. Het kabinet heeft beoordeeld dat het noodzakelijk is die punten te repareren met (tijdelijke) wetgeving. Tijdens het maken van die wetgeving bleef een maatschappelijk debat spelen over de diensten, dat uitleg, inbreng of weerwoord van de diensten vroeg.

Dat gebeurde tegen de achtergrond van een breder debat over vertrouwen in de overheid, dat op gang kwam na het toeslagenschandaal. Het bracht bij de Rijksoverheid bezinning op gang over openheid en transparantie. Daar werden later nieuwe vereisten aan verbonden, ook voor de diensten.

… nieuwe manieren om open te zijn waar dat kan

De diensten zijn meer dan voorheen naar buiten getreden tussen 2018 en 2023. Openheid draagt bij aan legitimiteit. Ook bevordert het de weerbaarheid van maatschappij, bestuur, bedrijven en burgers. Maar openheid is niet nieuw voor de diensten. 'Open waar het kan (gesloten waar het moet)', is een gevleugelde uitspraak van Arthur Docters van Leeuwen, tussen 1989 en 1995 directeur-generaal van de Binnenlandse Veiligheidsdienst – de voorloper van de AIVD. Sindsdien zoekt de dienst steeds naar bijtijdse manieren om publiekelijk verantwoording af te leggen. Zo hoorde de AIVD (inclusief voorlopers) bij de eerste inlichtingen- en veiligheidsdiensten in de wereld met een openbaar jaarverslag en een website. In 2021 was het een van de eerste I&V-diensten met een podcast.

Tussen 2018 en 2023 heeft de AIVD hernieuwde invulling gegeven aan open waar het kan. Het aantal AIVD'ers dat in open of semi-open setting over het werk mag spreken, is uitgebreid: behalve de dienstleiding, doen inmiddels alle leden van het MT en een enkel unithoofd dat. Technisch deskundigen spreken bij openbare hoorzittingen, zodat Kamerleden hen rechtstreeks kunnen bevragen, desgevraagd wordt de Kamer ook in vertrouwen geïnformeerd. De AIVD communiceert meer online, ook via sociale kanalen, en bereikt daar meer Nederlanders. Ook bevatten de openbare jaarverslagen elk jaar meer informatie.
In november 2018 organiseerde de MIVD (met Britse en Amerikaanse autoriteiten) een grote persconferentie, en gaf daar een openheid van zaken die op dat moment ongekend was. Het zou de toon zetten voor de komende jaren. Het toenmalig diensthoofd vertelde in detail hoe de Russische militaire inlichtingendienst GRU had geprobeerd een hackoperatie uit te voeren bij de Organisatie voor het Verbod op Chemische Wapens (OPCW) in Den Haag, en hoe de MIVD dat had weten te verijdelen.

Met publicaties (waaronder Ongekend en onderscheidend, een geautoriseerde geschiedenis van de dienst en diens voorlopers) en een publiek symposium gaf de MIVD in 2022 meer inzicht in het werk van de dienst en de gevaren die er tegen Nederland en bondgenoten zijn. Zo waarschuwde de MIVD Nederlandse bedrijven dat Russische inlichtingendiensten bezig waren om door middel van dekmantelbedrijven westerse sancties te ontduiken. Ook waarschuwde de dienst dat de GRU routers had gehackt van Nederlandse particulieren en MKB-bedrijven. Zorgelijk, omdat de GRU via die routers cyberoperaties kan uitvoeren tegen Nederland of bondgenoten. De persconferentie over de verijdelde OPCW-hack illustreert een belangrijke reden waarom de diensten meer naar buiten zijn gaan treden: om de samenleving inzicht te geven in gevaren tegen Nederland (en bondgenoten). De prominente dreigingen tegen Nederland tussen 2018 en 2023 zijn bijna allemaal veelomvattende uitdagingen die om een weerbare samenleving vragen. Cyberveiligheid is niet alleen een prioriteit voor de diensten, het is een opgave

voor bijna iedereen. Economische spionage treft kennisinstellingen en bedrijven. Extremisme is een uitdaging voor iedere burger die een democratisch debat wil voeren – haatzaaien, intimidatie en geweld staan dat in de weg.
De diensten spelen bij het tegengaan van die dreigingen een unieke rol. Maar de hele samenleving moet tegen die dreigingen weerbaar worden. De unieke kennis van de diensten draagt daar aan bij. Daarom brachten de diensten de afgelopen jaren tal van openbare publicaties uit. Recent nog over cyberdreigingen, Ruslands' inval in Oekraïne, en anti-institutioneel-extremisme.

Thema 5:
Vragen vanuit de krijgsmacht ...

De krijgsmacht is niet alleen first responder, maar ook de last line of defence. De focus van de MIVD is in het belang van de nationale veiligheid daarom nu al gericht op onderzoek ten behoeve van factoren die van belang zijn voor de opbouw van de toekomstige krijgsmacht, de gereedstelling van de huidige krijgsmacht en doeltreffende inzet van de krijgsmacht. Het gaat daarbij ook om het treffen van maatregelen ter bescherming van de veiligheid of paraatheid van de krijgsmacht. Het gaat daarbij niet alleen om inlichtingen bij de feitelijke inzet van de krijgsmacht, maar ook het in kaart brengen van de intenties, capaciteiten en activiteiten van potentiële vijanden en het ondersteunen van de krijgsmacht bij de optimale voorbereiding van het conflict van de toekomst. De inlichtingen dienen eveneens het kabinet te ondersteunen voorafgaand aan de besluitvorming over missies, zowel in het kader van de handhaving van de internationale rechtsorde als in nationaal of bondgenootschappelijk verband. Zij zijn onmisbaar ten behoeve van de inzet van de krijgsmacht in het verlengde van de grondwettelijke taken en het bedienen van de krijgsmacht voor het optreden in vredestijd, tijden van oplopende spanning en oorlogstijd. Daarnaast doet de MIVD onderzoek bij en naar de defensie industrie en verstrekt hierover inlichtingen waaronder de toeleverende militair technologische en industriële basis ten behoeve van de inrichting en bescherming van de krijgsmacht en politieke besluitvorming.
De geopolitieke veranderingen maken het voorstelbaar dat Nederland betrokken raakt bij een grootschalig conflict (zie thema 2). Het kunnen voeren van dit conflict stelt hoge eisen aan de diensten om ook in oorlogsomstandigheden de inlichtingenvergaring en met name de (near) realtime distributie van inlichtingen naar de krijgsmacht en met partners resilient vorm te geven om de besluitvorming op strategisch, operationeel en tactisch niveau te ondersteunen. Vanuit de krijgsmacht is een brede vraag naar inlichtingen om voorbereid te zijn op mogelijke missies en opkomende (ook hybride) dreigingen. Deels kan voor deze inlichtingen een beroep worden gedaan op openbare informatie. Vaak is voor een goed begrip van de situatie, echter de inzet van bijzondere bevoegdheden van de MIVD noodzakelijk. Daarbij kan het gaan om , bijvoorbeeld, het formuleren van scenario's, het identificeren van mogelijke doelen en het voorspellend vermogen. Deze brede vraag vereist keuzes, zodat de MIVD zo effectief en gericht mogelijk wordt ingezet en de krijgsmacht over de meest relevante inlichtingen beschikt. In veel landen waarvoor de krijgsmacht aandacht heeft is juist weinig informatie voorhanden. Er zullen dan ook keuzes moeten worden gemaakt in goede samenspraak met de krijgsmachtonderdelen. Juist dan moet de MIVD in staat zijn om effectief zijn bevoegdheden in te zetten om de krijgsmacht van de juiste inlichtingen te voorzien.

... en inzet op intensievere samenwerking

De MIVD is onderdeel van de inlichtingen- en veiligheidsketen van Defensie. De samenwerking is de afgelopen jaren geïntensiveerd op het gebied van bijvoorbeeld opleiden, trainen, personeelsuitwisseling en het onderling delen van informatie en inlichtingen. De samenwerking ten aanzien van Afghanistan, Mali, Irak, Syrië, de Baltische staten en Soedan werpt zijn vruchten af. De verdere verschuiving van need to know naar need to share is noodzakelijk. Om de betrouwbare en veilige uitwisseling van openbare en geclassificeerde data en inlichtingenproducten mogelijk te maken wordt

een vernieuwde grensverleggende IT (GrIT)-infrastructuur aangelegd. De krijgsmacht, die (inter)nationaal in een multi-domein omgeving slagvaardig moet kunnen opereren, wordt door deze intensievere samenwerking een informatiegestuurde organisatie.

Thema 6:
Een nieuwe wet, voor een nieuwe tijd, maar de praktijk wringt …

Op 1 mei 2018 trad de Wiv 2017 volledig in werking. Het was de uitwerking van een toen vijf jaar oud advies van de commissie Dessens om de diensten techniekonafhankelijke en toekomstbestendige bevoegdheden te geven, in het bijzonder de bevoegdheid van kabelinterceptie. Mobiel bellen en internetverkeer verliepen inmiddels bijna volledig via glasvezelkabels. Dataverkeer over die kabels kon zicht geven op vijandige hackers, de (reis)bewegingen van terroristen, of communicatie van extremisten. Voor de veiligheid van Nederland moesten de diensten die kunnen onderzoeken. Daarbij hoorden volgens de commissie Dessens ook moderne waarborgen: garanties voor de privacy van burgers. Het kabinet breidde het aantal nieuwe waarborgen nog uit, in reactie op het referendum (zie thema 4). Maatschappelijke groepen en burgers hadden daarbij vooral zorgen uitgesproken over 'ongerichte interceptie': hoe diensten op de kabel naar (met name buitenland-se) dreigingen zoeken, zolang ze die nog niet precies hebben onderkend.

De diensten mogen bijzondere bevoegdheden pas inzetten na toestemming van de (betrokken) minister, en onder toezicht van de onafhankelijke Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). De Wiv 2017 regelde daarbovenop een extra controle. De nieuwe, nog op te richten, Toetsingscommissie Inzet Bevoegdheden (TIB) zou de verleende toestemming – bijvoorbeeld voor ongerichte interceptie – ook nog onafhankelijk beoordelen op rechtmatigheid. Zonder die toets vooraf, mogen de diensten bepaalde bijzondere bevoegdheden niet inzetten. De nieuwe wet had enorme impact op de diensten. Het implementeren ervan heeft lang geduurd en bleek voor de diensten weerbarstiger dan zij hadden ingeschat. Het vroeg veel van de diensten, zowel incidenteel als structureel. Het hart van het inlichtingenproces – het verwerven en verwerken van gegevens – moest ervoor opnieuw worden ingericht. De Algemene Rekenkamer (ARK) en de Evaluatiecommissie Wiv 2017 (ECW) onderzochten twee jaar later de effecten daarvan. Die waren enerzijds positief: de waarborgen waren zoals beoogd versterkt. De Wiv 2017 had bij de diensten gezorgd voor betere gegevensverwerking, verantwoording en toetsing.

Anderzijds waren er negatieve gevolgen. De diensten bleken minder te kunnen innoveren en dreigden minder wendbaar te worden in het omgaan met bij uitstek buitenlandse dreigingen. De slagkracht en de toekomstbestendigheid van de diensten stonden onder druk. Volgens de Algemene Rekenkamer had een uitvoeringstoets vooraf zulke knelpunten in kaart kunnen brengen, maar die was niet gedaan. Ook hadden de diensten geen overgangstermijn gehad, noch het budget gekregen om de wet uit te voeren.
Na de onderzoeken kregen de diensten het budget om de verloren slagkracht te herstellen. Op advies van de ECW zal de Wiv 2017 op termijn grondig worden herzien. Ondertussen moest tijdelijke wetgeving de acute knelpunten verhelpen. De betrokken ministers dienden in december 2022 de Tijdelijke wet cyberoperaties in bij de Tweede Kamer, om de diensten alsnog in staat te stellen effectiever op te treden tegen cyberaanvallen uit onder meer Rusland, China en Iran.

… de compliance versterkt, de inlichtingenpositie onder druk

Dat er (meer) toetsing en toezicht is gekomen, heeft waarde voor de diensten. Zo heeft de wet geleid tot een betere datahuishouding. Die was aan modernisering toe. Goed functionerend, onafhankelijk toezicht draagt bovendien bij aan maatschappelijk vertrouwen. De Wiv 2017, maar ook de TIB en de CTIVD (en hun oordelen en rapporten) zorgden er bovendien voor dat de AIVD en MIVD processen beter zijn gaan vastleggen. Het interne toezicht kreeg er een grote impuls door, en de toestemmingsaanvragen zijn steeds professioneler geworden. Dat is wel ten dele ten koste gegaan van

het operationele werk. De nieuwe aanvragenprocessen vroegen zoveel extra tijd en capaciteit van teams dat zij minder tijd konden besteden aan onderzoek.

De nieuwe wet gaf ook frictie. In de Wiv 2017 staan normen en begrippen die niet duidelijk worden uitgelegd. Dat komt omdat de wet techniekneutraal bedoeld is. Een onbedoeld gevolg was echter dat de diensten en de toezichthouders over begrippen soms verschilden van inzicht. De wet geeft geen mogelijkheid om de zaak dan aan een derde, zoals een bestuursrechter, voor te leggen. Dat gaf patstellingen met de toezichthouders, en legde een klein, maar belangrijk deel van de onderzoeken stil.

De Wiv 2017 heeft het functioneren van de diensten tenslotte op één gewenst punt juist niet beïnvloed. De grote modernisering die de wet had moeten brengen – kabelinterceptie – is nauwelijks van de grond gekomen. Tien jaar na het eerste advies, en ondanks jaren van voorbereidingen, blijft onderzoek in het domein waar tegenwoordig vrijwel alle communicatie plaatsvindt, in de praktijk steken. De diensten enerzijds en de TIB anderzijds verschillen van inzicht over de inzet van het middel. Het risico blijft zo bestaan dat reële dreigingen tegen Nederland onvoldoende worden gezien.

Conclusies

De AIVD en MIVD werden tussen 2018 en 2023 geconfronteerd met nieuwe dreigingen, terwijl bestaande nog om prioriteit vroegen. De noodzaak te groeien en werkprocessen ingrijpend te veranderen, terwijl nog herstel nodig was.

Dat bracht knelpunten en professionele dilemma's met zich mee. Het heeft van de diensten het uiterste gevraagd. De diensten hebben hun wettelijke taken alleen kunnen blijven vervullen, door verstrekkende stappen te zetten. Drie daarvan zijn al aan bod gekomen:

In de eerste plaats moesten de diensten werken aan de opbouw van (nieuwe) kennisposities, en het herstel van slagkracht. Daarvoor waren extra investeringen nodig van het kabinet.

In de tweede plaats zijn de diensten intensiever gaan samenwerken, met elkaar en met partners. Dat maakte het mogelijk in relatief kort tijdsbestek de onderzoekscapaciteit te vergroten, en de effectiviteit van inlichtingen te vergroten – de mate waarin andere partijen op basis van inlichtingen konden handelen.

In de derde plaats hebben de diensten grote flexibiliteit opgebracht. De MIVD en AIVD hebben ingrijpend geschoven in prioriteiten, werkprocessen, organisatie-inrichting en bedrijfsvoering, om te voldoen aan de eisen van de nieuwe wet, de praktijk van statelijke- en cyberdreigingen, en het werken met technologie en data.

Als die optelsom van opgaven in de praktijk wrong, en het functioneren van de diensten onder druk stond, hebben de AIVD en de MIVD dat ook aangegeven. Bij een goede taakvervulling horen de juiste middelen, waaronder technische middelen als kabelinterceptie. En wettelijke kaders die passen bij de dreiging. De samenleving mag erop rekenen dat de diensten ook de komende jaren in het belang van Nederland zullen doorgaan met hun intensieve samenwerking en met het vormen van een moderne datahuishouding.

Een laatste reden waarom het de diensten is gelukt hun taken te vervullen, verdient het om hier nog speciaal benoemd te worden. Dat zijn de mensen van de AIVD en MIVD. Inlichtingenwerk is mensenwerk. De druk waaronder de diensten hebben gefunctioneerd is gevoeld door hen – de bewerkers, analisten en acquisiteurs. De flexibiliteit die moest worden opge-

bracht, is opgebracht door hen – de ICT'ers, juristen, beleidsmedewerkers en HR-medewerkers. Van alle AIVD'ers en MIVD'ers is veel gevraagd. Terugkijken heeft het voordeel van overzichtelijkheid. In de veranderende werkpraktijk van de afgelopen jaren was die er niet altijd meteen. Zoals beschreven bij thema 2 kwam het aan op learning by doing als de omstandigheden geen uitstel toelieten.

De mensen van de inlichtingen- en veiligheidsdiensten doen hun werk voor de veiligheid van Nederland en de bescherming van de krijgsmacht. Dat is wat hen motiveert onder uitdagende omstandigheden hun taak te blijven vervullen met moed en integriteit. Ongeacht of dat in het inlichtingenproces is, of in het ondersteunende werk. Het gevolg van ieders inzet is een lange lijst operationele successen.

Veel daarvan zijn nooit helemaal of helemaal nooit publiekelijk te delen, maar wat al openbaar is gemaakt spreekt boekdelen over het werk van de diensten tussen 2018 en 2023. De MIVD en AIVD verstoorden op allerlei momenten de activiteiten van Russische inlichtingen- en veiligheidsdiensten – die zo'n dominante rol speelden in het dreigingsbeeld de afgelopen jaren. Zo verhinderde de MIVD in 2018 een hack op de Organisatie voor het Verbod op Chemische Wapens (2018). Twee jaar later ontmaskerde de AIVD het werk van een Russische inlichtingenofficier die hier een aanzienlijk netwerk had opgebouwd. In 2022 verklaarde Nederland zeventien Russische inlichtingenofficieren tot persona non grata, en werd een Russische inlichtingofficier met een uitgebreid coververhaal aan de grens teruggestuurd. De diensten hebben in enkele gevallen voorkomen dat Rusland uit Nederland kennis en techniek kon halen voor zijn kernwapenprogramma.

De AIVD en MIVD droegen ook bij aan een heel nieuw instrumentarium waarmee de overheid zo nodig kan optreden tegen (heimelijke) economische activiteiten van China. Zoals de investeringstoets, het nog op te stellen toetsingskader kennisveiligheid, de exportcontrole van dual-use en militaire goederen, en de algemene beveiligingseisen voor defensieopdrachten (ABDO).

De diensten hebben cyberdreigingen uit diverse landen vroeg onderkend en aanvalsstructuren van statelijke actoren in kaart gebracht. En op allerlei niveau's en manieren bijgedragen aan de cyberveiligheid van overheid, kennisinstellingen en topsectoren.

Dankzij inlichtingen van de diensten zijn tussen 2018 en 2023 ook verschillende dreigingen van jihadisten en rechts-terroristen weggenomen, en zijn uiteindelijk mensen opgepakt die bewindspersonen (ernstig) bedreigden.
Dit soort operationele successen zijn het werk van de mensen van de MIVD en de AIVD. Hun inzet heeft Nederland veiliger gemaakt en mensenlevens gered. Nergens spreekt hun functioneren meer uit.