Toezichtrapport

over het handelen van de AIVD in relatie tot de verdenking van het lekken van staatsgeheimen door NCTV-medewerkers

CTIVD nr. 81

Vastgesteld op 14 oktober 2025

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 81

TOEZICHTRAPPORT

over het handelen van de AIVD in relatie tot de verdenking van het lekken van staatsgeheimen door NCTV-medewerkers

Inhoudsopgave

CTIVD nr. 81

TOEZICHTRAPPORT

over het handelen van de AIVD in relatie tot de verdenking van het lekken van staatsgeheimen door NCTV-medewerkers

1 Hoofdboodschap

Op 26 oktober 2023 zijn twee personen aangehouden op verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie. Betrokkenen hadden beschikking (gehad) over deze staatsgeheimen in het kader van hun werkzaamheden voor de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) heeft aanleiding gezien om onderzoek te doen naar het handelen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) in het kader van deze casus. Centraal staat daarbij de vraag of de AIVD rechtmatig heeft gehandeld ten aanzien van de uitvoering van veiligheidsonderzoeken, de invulling van de zorgplicht en de uitvoering van de *National Security Authority* (NSA)-taak met betrekking tot internationale geheime informatie.

Uit ons onderzoek blijkt dat de AIVD op onderdelen onvoldoende invulling heeft gegeven aan de uitvoering van zijn taken. De rode draad in het onderzoek is dat de AIVD zijn taken beter kan vervullen wanneer in zijn processen doorlopend aandacht is voor informatie-uitwisseling tussen verschillende onderdelen. Op zichzelf is compartimentering tussen verschillende onderdelen van de AIVD een belangrijke waarborg. Compartimentering moet echter niet onnodig in de weg staan aan informatie-uitwisseling, indien en voor zover de informatie noodzakelijk is voor de goede taakuitvoering van een ander organisatieonderdeel. Zo is gebleken dat de beveiligingsautoriteit (BVA) van de AIVD niet op de hoogte was van gebreken omtrent de informatiebeveiliging bij de NCTV, terwijl de afdeling die de NSA-taak vervult er wel van op de hoogte was. Ook is gebleken dat het beleid onvoldoende was om efficiënte informatie-uitwisseling tussen de Unit Veiligheidsonderzoeken (UVO) en (onder meer) inlichtingenteams mogelijk te maken.

De CTIVD concludeert dat de AIVD op onderdelen onzorgvuldig dan wel onrechtmatig heeft gehandeld. Deze conclusies worden in de afzonderlijke hoofdstukken beschreven. Kort samengevat zijn deze conclusies als volgt:

- Het beleid en de werkwijze ten aanzien van veiligheidsonderzoeken kennen tekortkomingen in de interne informatie-uitwisseling, de beoordeling van persoonlijke gedragingen en het instellen van periodieke en incidentele herhaalonderzoeken.
- De veiligheidsonderzoeken van 2015, 2018 en 2020 zijn conform wet- en regelgeving uitgevoerd. Het veiligheidsonderzoek van 2005 is onzorgvuldig verlopen.
- De AIVD heeft op onderdelen onvoldoende voldaan aan de wettelijke zorgplicht omtrent geheimhouding.
- De AIVD heeft onrechtmatig persoonsgegevens gedeeld met de NCTV.
- De AIVD heeft onvoldoende invulling gegeven aan de NSA-taak.

Voorgaande betekent niet als zodanig dat de AIVD de gebeurtenissen in de NCTV-casus had kunnen voorkomen. De AIVD is voor de beveiliging van zijn gerubriceerde informatie immers mede afhankelijk van partners in het hele stelsel van informatiebeveiliging en de integriteit van personen die met deze informatie werken.

2 Aanleiding en scope

2.1 Aanleiding: de NCTV-casus

Op 26 oktober 2023 zijn personen aangehouden op verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie. Beide personen hadden in het kader van hun functie bij de NCTV toegang tot staatsgeheime informatie. De NCTV beschikt over staatsgeheime informatie in het kader van zijn taken. Betrokken personen worden in dit rapport aangeduid als persoon 1 en persoon 2.

De AIVD heeft onder meer tot taak om veiligheidsonderzoeken uit te voeren. Personen 1 en 2 beschikten naar aanleiding van een veiligheidsonderzoek over een verklaring van geen bezwaar (VGB). Ook heeft de AIVD een zorgplicht ten aanzien van de bescherming van zijn staatsgeheime gegevens. Deze zorgplicht blijft (gedeeltelijk) gelden wanneer de AIVD informatie verstrekt aan de NCTV. Daarnaast heeft de AIVD een taak als NSA. In deze hoedanigheid heeft de AIVD een verantwoordelijkheid met betrekking tot de bescherming van internationaal gerubriceerde informatie. De CTIVD doet onderzoek naar de rechtmatigheid van het handelen van de AIVD ten aanzien van deze taken.

Staatsgeheime informatie: op grond van het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) moet informatie waarvan de geheimhouding is geboden vanwege het belang van de Staat, zijn bondgenoten of van één of meer ministeries worden voorzien van een passend niveau van rubricering. Als informatie staatsgeheim is dan is een van de volgende rubriceringen op het document opgenomen: Staatsgeheim CONFIDENTIEEL (Stg. C.), Staatsgeheim GEHEIM (Stg. G.) en Staatsgeheim ZEER GEHEIM (Stg. ZG).

2.2 Wat is er onderzocht?

De CTIVD heeft op 25 oktober 2023 besloten een onderzoek in te stellen naar het handelen van de AIVD en de MIVD. Het onderzoek richt zich op drie aspecten:

1. de uitvoering van veiligheidsonderzoeken door de AIVD op grond van de Wet veiligheidsonderzoeken (Wvo);
2. de invulling van de zorgplicht door de AIVD en de MIVD in verband met het verstrekken van staatsgeheime informatie aan de NCTV;
3. de uitvoering van de taak als NSA door de AIVD met betrekking tot internationaal gerubriceerde informatie.

Het onderzoek richt zich niet op de eventuele inzet van (bijzondere) bevoegdheden door de AIVD ten aanzien van personen. Ook richt het onderzoek van de CTIVD zich niet op het handelen van de NCTV. Dit valt niet binnen het mandaat van de CTIVD. De Auditdienst Rijk heeft op 29 november 2024 een onderzoeksrapport uitgebracht over het beveiligingsproces van staatsgeheime of vertrouwelijke informatie bij onder meer de NCTV. De Auditdienst Rijk komt op basis van het onderzoek tot de conclusie dat de basis voor de beveiliging van staatsgeheime en/of vertrouwelijke informatie bij de NCTV niet op orde was.

Dit rapport ziet op de AIVD. Over de MIVD wordt in een afzonderlijk rapport gerapporteerd.

2.3 Scope

Op basis van vooronderzoek in de systemen van de AIVD is de scope van het onderzoek bepaald. In zijn algemeenheid geldt dat het onderzoek van de CTIVD zich richt op de periode voorafgaand aan het bekend worden van de NCTV-casus. Tenzij anders wordt vermeld is de onderzoeksperiode afgebakend tot medio 2023. Dit betekent dat maatregelen die de AIVD heeft getroffen naar aanleiding van de NCTV-casus niet door de CTIVD zijn onderzocht. Als genomen maatregelen tijdens het onderzoek aan de orde zijn gekomen, wordt hier melding van gemaakt zonder dat er nader onderzoek naar is gedaan.

De scope van het onderzoek ten aanzien van de uitvoering van concrete veiligheidsonderzoeken is beperkt tot de momenten waarop er veiligheidsonderzoeken zijn uitgevoerd in 2005, 2015, 2018 en 2020 ten aanzien van de in de NCTV-casus betrokken personen. De CTIVD heeft in het kader van dit onderwerp enerzijds onderzoek gedaan naar het beleid en de werkwijze en anderzijds onderzocht of de constateringen, processen en beslissingen die ten grondslag liggen aan de verleende verklaringen van geen bezwaar (VGB) worden gesteund door het onderliggende dossier. Voor zover de bevindingen zien op beleid of de werkwijze zijn de momenten van afgifte van de betreffende VGB als peildatum gehanteerd. De CTIVD heeft zich bij de beoordeling van de uitvoering van de veiligheidsonderzoeken steeds gebaseerd op dezelfde informatie als de informatie die destijds bekend was bij de medewerkers van de UVO.

Het onderzoek naar de zorgplicht is ten aanzien van het beveiligingsperspectief beperkt tot drie bevindingen in het kader van de NCTV-casus. Het onderzoek naar de zorgplicht ziet ook op het exploiteren van gegevens. De scope van dit onderdeel is beperkt tot de verstrekking van gegevens aan de NCTV. Ook heeft de CTIVD ten aanzien van een specifieke externe verstrekking van persoonsgegevens beoordeeld of die rechtmatig was. De verstrekking van gegevens aan andere (overheids)organisaties valt niet binnen de scope van dit onderzoek.

Het onderzoek naar de inrichting van de NSA-taak is beperkt tot overheidsorganisaties. Dit betekent dat geen onderzoek is gedaan naar de inrichting van de NSA-taak ten opzichte van private bedrijven. Wat de concrete uitvoering van de taak betreft, is uitsluitend gekeken naar de uitoefening ten aanzien van de NCTV in de periode van 2013 tot medio 2023.

2.4 Aanpak

Het onderzoek is gestart met een vooronderzoek, waarbij de CTIVD een eerste onderzoek heeft gedaan in de systemen van de AIVD. Op basis van dit vooronderzoek zijn de onderzoeksvragen geformuleerd. Deze vragen zijn onderzocht op basis van documentatie van de AIVD en gesprekken. Er is niet gesproken met de NCTV. Alle bevindingen waarin de NCTV een rol speelt, zijn gebaseerd op documentatie en toelichting van de AIVD.

De CTIVD beoordeelt de bevindingen in het kader van rechtmatigheid. Het beoordelingskader wordt bepaald door de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) en de Wvo. De specifieke bepalingen worden toegelicht in de verschillende hoofdstukken. Waar de CTIVD tot een oordeel komt, maakt zij een onderscheid tussen onrechtmatig en onzorgvuldig handelen. Als de bevindingen hier aanleiding toe geven, doet de CTIVD aanbevelingen ten aanzien van de werkwijze van de diensten.

Onrechtmatig: er wordt gehandeld in strijd met de wet, bijvoorbeeld als niet wordt voldaan aan de wettelijke vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. De AIVD handelt ook onrechtmatig als een wettelijke grondslag voor handelen ontbreekt.

Onzorgvuldig: er is een tekortkoming in beleid, werkwijze of processen die (toekomstige) onrechtmatigheden in de hand kan werken.

Een conceptversie van het rapport is toegestuurd aan de AIVD en de minister van Binnenlandse Zaken en Koninkrijkrelaties. Zij hebben een reactie gegeven op de feiten en bevindingen in het rapport. Ook heeft er een controle plaatsgevonden ter voorkoming van openbaarmaking van staatsgeheime informatie. Deze reactie is meegenomen in dit vastgestelde rapport.

2.5 Leeswijzer

Het rapport is als volgt opgebouwd:
- Hoofdstuk 3 beschrijft het beleid en de werkwijze ten aanzien van veiligheidsonderzoeken (onderzoekaspect 1).
- Hoofdstuk 4 beschrijft de veiligheidsonderzoeken in de NCTV-casus (onderzoekaspect 1).
- Hoofdstuk 5 beschrijft de invulling van de zorgplicht (onderzoekaspect 2).
- Hoofdstuk 6 beschrijft de uitvoering van de NSA-taak (onderzoekaspect 3).

Ieder hoofdstuk start met een korte conclusie. De bevindingen en begrippen die in deze conclusie staan worden nader uitgelegd in het hoofdstuk zelf. De hoofdstukken bevatten kleurenkaders. De betekenis van de kaders is als volgt:
- Grijze kaders bevatten uitleg over gebruikte terminologie.
- Blauwe kaders bevatten uitleg over wetgeving.
- Paarse kaders bevatten aanbevelingen. De aanbevelingen zijn ten behoeve van de leesbaarheid genummerd op volgorde van de paragrafen.

Vanwege het staatsgeheime karakter van onderzochte informatie is bij hoofdstuk 4 en 5 een geheime bijlage opgenomen. Het openbare rapport over deze onderwerpen is op een aantal onderdelen meer abstract beschreven. De geheime bijlage bevat een verdere concretisering van bevindingen op basis van staatsgeheime informatie. In de geheime bijlage staan geen onrechtmatigheden die niet zijn vermeld in het openbare rapport. Twee aanbevelingen zijn vanwege de nauwe verwevenheid met staatsgeheime informatie uitsluitend opgenomen in de geheime bijlage.

3 Beleid en werkwijze ten aanzien van veiligheidsonderzoeken

3.1 Conclusie: het beleid en de werkwijze kennen tekortkomingen ten aanzien van de interne informatie-uitwisseling, de beoordeling van persoonlijke gedragingen en het instellen van periodieke en incidentele herhaalonderzoeken.

De CTIVD heeft onderzoek gedaan naar de veiligheidsonderzoeken die zijn uitgevoerd naar de personen in de NCTV-casus. In dit kader is ook gekeken naar het beleid dat op de momenten van uitvoering gold. De AIVD heeft voldoende beleid voor het uitvoeren van veiligheidsonderzoeken. Sinds 2002 is dat beleid vastgelegd in beleidsdocumenten en medewerkers zijn hiermee bekend. De CTIVD heeft op een aantal punten tekortkomingen in het beleid en de werkwijze geconstateerd.

De informatie-uitwisseling tussen verschillende onderdelen van de AIVD was onvoldoende vastgelegd in het beleid. Er was geen proces ingericht hoe informatie uit andere teams met medewerkers van de UVO kon worden gedeeld. Inlichtingeninformatie kon alleen door middel van een interne mededeling met de UVO worden gedeeld. De AIVD hanteerde een te hoge lat voor het versturen van een interne mededeling aan de UVO. Daarnaast kon een medewerker van de UVO aan een ander team vragen informatie die uit naslagen kwam te duiden. Dat team bepaalde zelf welke informatie wel en niet werd gedeeld. Daar was geen beleid of werkproces voor ingericht.

De CTIVD is verder van oordeel dat het beleid weinig houvast biedt voor de toetsingswijze en de weging van het criterium persoonlijke gedragingen en omstandigheden.

Ook is in het beleid niet goed opgenomen welke verantwoordelijkheid de AIVD zelf heeft voor het instellen van periodieke en incidentele herhaalonderzoeken. De AIVD legt de verantwoordelijkheid hiervoor volledig bij de werkgever. De AIVD legt naar het oordeel van de CTIVD de Wet veiligheidsonderzoeken op dit punt verkeerd uit en moet hierin ook zelf verantwoordelijkheid nemen.

Bovenstaande bevindingen worden in dit hoofdstuk nader toegelicht. In paragraaf 3.2 wordt in generieke zin het verloop van het veiligheidsonderzoek beschreven. In deze paragraaf wordt achtereenvolgens ingegaan op: het administratieve onderzoek, de interne gegevensverstrekking, het veldonderzoek en de beoordeling. In paragraaf 3.3 wordt ingegaan op NATO- en EU-*clearances* en in paragraaf 3.4 op het beleid ten aanzien van herhaalonderzoeken.

3.2 Het veiligheidsonderzoek

Vertrouwensfunctie: een functie die de mogelijkheid biedt de nationale veiligheid te schaden, bijvoorbeeld als een persoon in zijn vertrouwensfunctie toegang heeft tot staatsgeheime informatie.

Veiligheidsonderzoek: een onderzoek naar gegevens die uit het oogpunt van de nationale veiligheid van belang zijn voor de vervulling van een vertrouwensfunctie.

Op grond van de Wet veiligheidsonderzoeken (Wvo) stelt de AIVD een veiligheidsonderzoek in naar een persoon als die persoon een vertrouwensfunctie gaat bekleden of een functie bekleedt die als vertrouwensfunctie wordt aangewezen (hierna: de betrokkene). De werkgever meldt betrokkene aan bij het hoofd van de AIVD. De UVO voert vervolgens het veiligheidsonderzoek uit. Er zijn verschillende categorieën veiligheidsonderzoeken, waaronder A-, B- en C-veiligheidsonderzoeken. A is de zwaarste categorie, met het meest uitgebreide onderzoek, daarna volgt het B-onderzoek en tot slot het C-onderzoek.

Na het veiligheidsonderzoek wordt een Verklaring van Geen Bezwaar (VGB) afgegeven of geweigerd. Een VGB kan worden geweigerd als er vanuit het belang van de nationale veiligheid een bezwaar bestaat dat de betrokkene op de vertrouwensfunctie wordt geplaatst door de werkgever. Een afgegeven VGB heeft geen einddatum. Zolang de betrokkene in dezelfde vertrouwensfunctie en bij dezelfde werkgever werkt, blijft dezelfde VGB van kracht. Na een periode van vijf jaar of een veelvoud daarvan sinds het afgeven van de VGB kan er een nieuw veiligheidsonderzoek worden gestart naar de betrokkene die een vertrouwensfunctie vervult (het periodieke herhaalonderzoek). Als er binnen deze periode nieuwe feiten en/of omstandigheden zijn die een hernieuwd veiligheidsonderzoek rechtvaardigen, kan op elk moment een hernieuwd veiligheidsonderzoek worden gestart (het incidentele herhaalonderzoek).

Artikel 8 Wvo bepaalt dat een VGB slechts kan worden geweigerd als *"onvoldoende waarborgen aanwezig zijn dat de betrokkene onder alle omstandigheden de uit de vertrouwensfunctie voortvloeiende plichten getrouwelijk zal volbrengen of als het veiligheidsonderzoek onvoldoende gegevens heeft kunnen opleveren om daarover een oordeel te geven."*

Het onderzoek van de CTIVD richt zich op vier uitgevoerde veiligheidsonderzoeken. Naar persoon 1 is in 2005 een A-onderzoek en in 2018 een B-onderzoek verricht. Naar persoon 2 zijn in 2015 en 2020 B-onderzoeken uitgevoerd. De CTIVD beoordeelt in hoofdstuk 4 hoe de vier veiligheidsonderzoeken zijn uitgevoerd. Alvorens daarop in te gaan wordt in dit hoofdstuk beschreven welk beleid gold ten tijde van die vier verschillende veiligheidsonderzoeken en welke processen er werden gevolgd. Eerst wordt in deze paragraaf ingegaan op het ten tijde van de uitgevoerde veiligheidsonderzoeken geldende beleid en proces ten aanzien van de volgende stappen in een veiligheidsonderzoek: het administratieve onderzoek (paragraaf 3.2.1), eventuele interne gegevensverstrekking aan de UVO (paragraaf 3.2.2), het veldonderzoek (paragraaf 3.2.3) en de beoordeling (paragraaf 3.2.4). Vervolgens wordt ook ingegaan op de afgifte van *clearances* (paragraaf 3.3) en het beleid ten aanzien van herhaalonderzoeken (paragraaf 3.4).

3.2.1 Het administratieve onderzoek

Opgave Persoonlijke Gegevens (OPG) (voorheen: Staat van Inlichtingen): dit is een formulier waarin de betrokkene alle relevante informatie over hemzelf invult, op basis waarvan de AIVD onderzoek doet naar (risico's op) kwetsbaarheden. Alle antwoorden samen brengen zo goed mogelijk in kaart of de betrokkene in een vertrouwensfunctie een gevaar kan vormen voor de nationale veiligheid. Als de betrokkene een grote schuld heeft, kan hij bijvoorbeeld kwetsbaarder zijn voor chantage.

Een veiligheidsonderzoek begint met het administratieve onderzoek. Het administratieve onderzoek baseert zich op de OPG. De onderzoeksassistent bekijkt en beoordeelt de antwoorden op de vragen in de OPG. Daarnaast trekt de onderzoeksassistent de betrokkene na in verschillende systemen, zoals de Basisregistratie Personen, het Bureau Kredietregistratie en de eigen systemen van de AIVD. De onderzoeksassistent beoordeelt in overleg met een andere onderzoeksassistent of met een bewerker of de betrokkene in een van die naslagen negatief bekend is.

Als de betrokkene niet negatief bekend is en er geen kwetsbaarheden voortvloeien uit de verstrekte gegevens, wordt een VGB afgegeven. Twijfelt de onderzoeksassistent over een resultaat, dan overlegt hij met een bewerker. De onderzoeksassistent en de bewerker beoordelen gezamenlijk of een dossier moet worden doorgestuurd naar een diepteteam, dat nader onderzoek doet. In A-onderzoeken wordt ook altijd een veldonderzoek gedaan.

De CTIVD stelt vast dat dit proces in de gehele onderzoeksperiode gelijk is gebleven. In de loop der jaren zijn bepaalde naslagen toegevoegd of weggelaten en zijn de meeste naslagen geautomatiseerd. De CTIVD constateert op basis van gesprekken met de AIVD dat de medewerkers van de UVO bekend waren met het beleid en het werkproces voor het uitvoeren van het administratieve onderzoek in de veiligheidsonderzoeken.

3.2.2 De interne gegevensverstrekking

Als tijdens het administratieve onderzoek of op een later moment tijdens een veldonderzoek blijkt dat betrokkene bekend is in de systemen van de AIVD, dan kan de bewerker navraag doen bij het team van wie die informatie is. Het team kan de informatie duiden en beschrijven in welke hoedanigheid en waarom de betrokkene voorkomt in de systemen van de AIVD, zodat de bewerker dit resultaat kan meewegen in het kader van het veiligheidsonderzoek.

Taken AIVD: in het kader van de nationale veiligheid heeft de AIVD onder andere als taak:
a. onderzoek doen naar organisaties en personen die een dreiging vormen (A-taak);
b. veiligheidsonderzoeken uitvoeren (B-taak);
c. veiligheidsmaatregelen bevorderen (C-taak);
d. inlichtingen over het buitenland inwinnen (D-taak);
e. dreigings- en risicoanalyses opstellen (E-taak);
f. naslag doen naar bepaalde personen of organisaties (F-taak).

Interne gegevensverstrekking: verstrekking van gegevens aan personen die bij de AIVD werken maar uitvoering geven aan een andere taak. Bijvoorbeeld de verstrekking van gegevens uit een inlichtingenteam (de A- of D-taak) of het weerbaarheidshuis (C-taak) aan medewerkers van de UVO (B-taak).

De Wiv 2017 kent een gesloten stelsel van gegevensvertrekking. Dit geldt voor zowel interne als externe gegevensverstrekking. Het gesloten stelsel betekent dat de AIVD alleen informatie mag verstrekken als voor die verstrekking een wettelijke grondslag bestaat. Op grond van artikel 61 Wiv 2017 kan interne gegevensverstrekking plaatsvinden, voor zover dat noodzakelijk is voor een goede uitvoering van de aan de desbetreffende ambtenaar opgedragen taak. Het artikel strekt ertoe de schending van de persoonlijke levenssfeer zoveel mogelijk te beperken en onnodige verspreiding van gegevens tegen te gaan.

Binnen de AIVD geldt het *need to know*-principe. AIVD-medewerkers hebben alleen toegang tot informatie als zij die informatie nodig hebben voor het uitvoeren van de aan hen opgedragen taak. Dit betekent onder meer dat medewerkers die zich bezighouden met de uitvoering van veiligheidsonderzoeken (de B-taak) niet zomaar toegang hebben tot inlichtingeninformatie (de A- en D-taak). Er wordt naar gestreefd de kring van personen die kunnen kennisnemen van bepaalde gegevens zo klein mogelijk te houden.

De informatie-uitwisseling tussen de verschillende onderdelen van de AIVD was onvoldoende vastgelegd in beleid

Informatieverstrekking tussen de UVO en (onder meer) inlichtingenteams is in het belang van het veiligheidsonderzoek. De AIVD wil hiermee bijvoorbeeld voorkomen dat personen die in het kader van een inlichtingenonderzoek target van de AIVD zijn (geweest) en waarbij is gebleken dat zij een gevaar (kunnen) vormen voor de nationale veiligheid, op een vertrouwensfunctie worden geplaatst. Medewerkers van de UVO kunnen daarom informatie vragen aan inlichtingenteams als de betrokkene in het veiligheidsonderzoek voorkomt in de systemen van de AIVD. Daarnaast kan het andersom voorkomen dat bij een inlichtingenonderzoek blijkt dat een target een VGB heeft. Ook dan moet worden afgewogen of de informatie kan worden gedeeld met de UVO.

De CTIVD stelt vast dat de AIVD onvoldoende beleid had over het uitwisselen van informatie tussen de A- en D-taak enerzijds en de B-taak anderzijds. De enige mogelijkheid om bijvoorbeeld inlichtingen-informatie met medewerkers van de UVO te delen, was door middel van een interne mededeling (zie hierna). In de praktijk kwam het voor dat de UVO bij het verrichten van een veiligheidsonderzoek erachter kwam dat er bijvoorbeeld inlichtingeninformatie over een betrokkene bekend was bij de AIVD. De medewerkers van de UVO konden op dat moment het inlichtingenteam vragen om die inlichtingeninformatie te duiden. Het inlichtingenteam bepaalde zelf welke inlichtingeninformatie het deelde met de medewerkers van de UVO. Voor het bepalen welke informatie wel of niet werd gedeeld met de medewerkers van de UVO bestond destijds geen beleid of werkinstructie.

Binnen het management van de UVO is gesignaleerd dat er weinig informatie werd uitgewisseld tussen de UVO en inlichtingenteams. Ook kwam het niet of nauwelijks voor dat er interne mededelingen werden verstuurd aan de UVO door inlichtingenteams. Voor zover bekend is in de onderzoeksperiode geen verdere opvolging gegeven aan de signalering van het management.

De gehanteerde werkwijze bij het naslaan van personen laat ruimte voor fouten

Daarnaast constateert de CTIVD dat de door de UVO gehanteerde werkwijze bij het naslaan van een betrokkene ruimte laat voor fouten. Dit kan met name een risico zijn bij herhaalonderzoeken.

De UVO doet namelijk geen algemene zoekslag in de AIVD-systemen, wanneer een betrokkene in een veiligheidsonderzoek reeds is geregistreerd in het centrale personenregistratiesysteem, waarin documenten aan personen worden gekoppeld. De AIVD gaat ervan uit dat met een zoekslag in dit centrale personenregistratiesysteem alle documenten over betrokkene worden gevonden en dat er geen documenten worden gemist. In een van de gesprekken is opgemerkt dat deze werkwijze is onderzocht en dat is gebleken dat er met deze werkwijze zeer weinig documenten worden gemist. Uit onderzoek van de CTIVD is gebleken dat het in de praktijk wel kan leiden tot een onvolledig beeld van beschikbare informatie, omdat documenten niet structureel aan het centrale personenregistratiesysteem worden gekoppeld.

Aanbeveling 1
Maak beleid en een proces voor de informatie-uitwisseling gedurende het veiligheidsonderzoek tussen de inlichtingenteams (A- en D-taak) enerzijds en de medewerkers van de UVO (B-taak) anderzijds.

De AIVD hanteerde een te hoge lat voor het uitbrengen van een interne mededeling

Ambtsbericht: een ambtsbericht is een exploitatieproduct van de AIVD. De term is niet wettelijk verankerd, maar uit de toelichting bij de Wiv 2002 blijkt dat op grond van een dergelijk bericht een bevoegd gezag naar verwachting maatregelen tegen een persoon zal treffen. Het wordt bijvoorbeeld gebruikt om informatie te delen met het Openbaar Ministerie.

Tot 2023 was de interne mededeling het enige in het beleid opgenomen proces om informatie uit het inlichtingenproces te delen met de UVO. De interne mededeling werd behandeld als een intern ambtsbericht. Bij een ambtsbericht moet de boodschap worden onderbouwd met onderliggende stukken, zodat de informatie van de AIVD kan worden gecontroleerd. Deze zelfde lat werd binnen de AIVD gehanteerd bij een interne mededeling. Er werd pas een interne mededeling verstuurd als de informatie zodanig concreet was dat op basis daarvan een VGB kon worden geweigerd of ingetrokken. Deze informatie moest de toets kunnen doorstaan van een eventuele bezwaar- of beroepsprocedure.

De CTIVD is van oordeel dat dit een te strikte interpretatie is van artikel 61 Wiv 2017. Informatie-uitwisseling tussen de inlichtingenteams en de UVO is mogelijk als die noodzakelijk is voor een goede taakuitvoering van de desbetreffende medewerker van de UVO en/of de inlichtingenteams die de gegevens ontvangt. Ook informatie die (nog) onbevestigd of onvoldoende concreet is voor een weigering of intrekking van de VGB kan relevant zijn voor de vraag of de UVO een (herhaal)onderzoek moet starten, bijvoorbeeld omdat de informatie al wel vraagtekens kan oproepen over de persoonlijke gedragingen van iemand. In het veiligheidsonderzoek kan vervolgens door de UVO worden uitgezocht en geduid wat die informatie moet betekenen voor de VGB van de betrokkene. De UVO moet in de gelegenheid zijn hierover een eigen afweging te maken. Daarbij speelt mee dat de UVO juist in het kader van het veiligheidsonderzoek, dus met een andere insteek dan inlichtingenteams, onderzoek kan doen naar persoonlijke gedragingen en omstandigheden, zoals integriteit en eerlijkheid.

In de gesprekken heeft de AIVD toegelicht dat inmiddels een ruimer beleid is geïmplementeerd ten aanzien van de interne mededeling. De AIVD maakt informatie-uitwisseling tussen de UVO en inlichtingenteams mogelijk door middel van een interne melding, waaraan minder hoge eisen worden gesteld dan aan de interne mededeling. De CTIVD heeft geen nader onderzoek gedaan naar deze nieuwe ontwikkeling, omdat die buiten de scope van het onderzoek valt.

Aanbeveling 2
Concretiseer in het beleid wanneer en op welke wijze inlichtingenteams inlichtingeninformatie kunnen delen met de UVO ten behoeve van een veiligheidsonderzoek.

3.2.3 Het veldonderzoek

Referent: iemand die iets over een persoon kan vertellen en door de betrokkene in de OPG is opgegeven.

Informant: iemand die door AIVD wordt benaderd om over een betrokkene te vertellen die niet door de betrokkene is opgegeven.

In deze paragraaf wordt uitgegaan van het beleid en proces dat gold in 2005, omdat in hoofdstuk 4 de uitvoering van de veiligheidsonderzoeken aan het beleid wordt getoetst en alleen bij het veiligheidsonderzoek van 2005 een veldonderzoek is uitgevoerd. In alle A-onderzoeken en in doorgestuurde B- en C-onderzoeken werd een diepgaander onderzoek gedaan, het veldonderzoek. In deze tweede fase van het veiligheidsonderzoek werd zowel onderzoek gedaan naar de betrokkene als naar personen in diens omgeving. In het veldonderzoek konden extra naslagen worden gedaan en gesprekken worden gevoerd met de betrokkene en referenten en/of informanten. In 2005 werd bij het veldonderzoek op A-niveau in ieder geval een gesprek gevoerd met de betrokkene. Tijdens het gesprek konden verschillende onderwerpen aan bod komen die ook in de OPG werden uitgevraagd, zoals de financiële situatie, familie, verslavingen en buitenlandse reizen. Ook een gesprek met een referent of informant was mogelijk. Bij twijfel kon de afdeling Juridische Zaken (JZ) worden ingeschakeld voor advies. De resultaten van de naslagen, het proces en de beslissingen die aan de hand daarvan werden gemaakt door de bewerker, moesten worden vastgelegd in het procesformulier.

3.2.4 De beoordeling

Bij het beoordelen van de verzamelde informatie gaat het om de vraag of aan de kandidaat-vertrouwensfunctionaris wel of niet een verklaring van geen bezwaar kan worden gegeven. Daarvoor mag alleen de in het kader hieronder genoemde informatie gewogen worden. Een VGB kan worden geweigerd als onvoldoende waarborgen aanwezig zijn dat de betrokkene onder alle omstandigheden de uit de vertrouwensfunctie voortvloeiende plichten getrouwelijk zal volbrengen.

Op grond van artikel 7 Wvo wordt bij het veiligheidsonderzoek uitsluitend gelet op de volgende gegevens:

a. justitiële en strafvorderlijke gegevens;
b. gegevens over deelneming of steunverlening aan activiteiten die de nationale veiligheid kunnen schaden;
c. gegevens over lidmaatschap van of steunverlening aan organisaties die doeleinden nastreven die aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor de democratische rechtsorde;
d. gegevens over overige persoonlijke gedragingen en omstandigheden, naar aanleiding waarvan betwijfeld mag worden of de betrokkene de uit de vertrouwensfunctie voortvloeiende plichten onder alle omstandigheden getrouwelijk zal volbrengen.

Het beleid van de AIVD concretiseert onderdelen b en c door de belangrijkste aandachtsgebieden te benoemen, waaronder de aantasting van grondrechten, ontregeling van politieke besluitvorming, terrorisme en spionage tegen Nederlandse belangen. In 2005 werd bij de beoordeling van het onderdeel d ”overige persoonlijke gedragingen en omstandigheden” gelet op drie risicofactoren, namelijk onharmonieus gedrag, afhankelijkheidsproblemen en loyaliteitsproblemen.

Onharmonieus gedrag: gedacht kan worden aan het vertonen van onverantwoord, impulsief, leugenachtig en bedrieglijk gedrag.

Afhankelijkheidsproblemen: hierbij wordt gekeken naar ongewenste factoren, zoals alcohol, drugs en gokken, maar ook financiële kwetsbaarheid. Voor financiële kwetsbaarheid wordt gekeken naar de verhouding tussen inkomsten/bezittingen en uitgaven/verplichtingen en aan de financiële belangen die aan de vertrouwensfunctie zijn verbonden. Aandacht voor de financiële situatie kan ook indicaties opleveren voor andere afhankelijkheden, zoals het bestaan van dubbele belangen en integriteitsrisico’s.

Loyaliteitsproblemen: bijvoorbeeld als de betrokkene zich niet wil of kan verbinden met de Nederlandse samenleving en haar democratische en rechtsstatelijke waarden en normen. Gedacht kan worden aan druk van de familie of van derde landen. Zo is er bijvoorbeeld aandacht voor onwenselijke (politieke) binding in het moederland. Hierbij wordt gelet op partijbinding, bezit van onroerend goed, financiële tegoeden in of toekomstplanning gericht op het moederland, familie in het moederland en nog bestaande verplichtingen ten opzichte van het moederland.

Sinds 2009 is het beleid vastgelegd in de openbaar toegankelijke Leidraad persoonlijke gedragingen. Sindsdien wordt bij de beoordeling van de “overige persoonlijke gedragingen en omstandigheden” getoetst op de volgende criteria: eerlijk, onafhankelijk, loyaal, integer en veiligheidsbewust. Bij veiligheidsonderzoeken waarin alleen een administratief onderzoek wordt uitgevoerd, zoals de veiligheidsonderzoeken in 2015, 2018 en 2020, zijn deze criteria lastiger te toetsen, omdat er geen gesprekken met de betrokkene of met referenten of informanten plaatsvinden. Bij de naslagen in het administratieve onderzoek wordt bijvoorbeeld wel gekeken naar de financiële situatie van de betrokkene. Het criterium eerlijkheid kan worden getoetst door de antwoorden van de betrokkene op de vragen in de OPG te vergelijken met de corresponderende uitkomsten van de naslagen. Als de betrokkene bijvoorbeeld in zijn OPG invult dat hij geen schulden heeft terwijl uit de financiële naslag blijkt dat hij weldegelijk (grote) schulden heeft, kan dat een indicatie zijn dat betrokkene niet eerlijk is. In het administratieve onderzoek worden de resultaten van de naslagen altijd vergeleken met de antwoorden van de betrokkene in de OPG.

Er is weinig houvast voor de beoordeling van persoonlijke gedragingen en omstandigheden
Voor de beoordeling van een aantal te toetsen criteria, zoals justitiële documentatie en schulden, heeft de AIVD richtlijnen opgesteld. Voor bepaalde misdrijven, hoogte van straffen of hoogte van schulden, stuurt de onderzoeksassistent het veiligheidsonderzoek door naar een diepteteam (in het geval van B- of C-onderzoeken) of naar een team dat beoordeelt of het dossier naar een diepteteam moet. Voor andere persoonlijke gedragingen of omstandigheden zijn die richtlijnen er niet. De beoordeling is afhankelijk van de omstandigheden van het geval, dus precieze richtlijnen zijn lastig in beleid vast te leggen. Dit maakt het naar het oordeel van de CTIVD belangrijk dat een duidelijke procedure wordt gevolgd en dat afwegingen over persoonlijke gedragingen en omstandigheden worden vastgelegd. Dit speelt met name wanneer het gaat over subjectieve signalen over negatieve persoonlijke gedragingen en omstandigheden.

Aanbeveling 3
Concretiseer het beleid om zorgvuldige besluitvormingsprocedures en vastlegging van afwegingen over persoonlijke gedragingen en omstandigheden te waarborgen voor de gevallen waarin twijfel bestaat over het al dan niet afgeven van een VGB.

3.3 NATO- en EU-clearance

Personnel Security Clearance (PSC): De *clearance* is een door of namens de NSA (zie hoofdstuk 6) af te geven verklaring waarbij wordt bevestigd dat de betrokkene tot een bepaalde datum toegang mag hebben tot vertrouwelijke EU-, NATO- en ESA-informatie tot een bepaald niveau. De uitvoering van de onderzoeken is qua systematiek te vergelijken met veiligheidsonderzoeken. De geldigheid van een *clearance* is maximaal vijf jaar.

Met een veiligheidsonderzoek op B-niveau kan de betrokkene toegang krijgen tot documenten met EU-rubricering “EU-*Secret*” en “NATO-*Secret*”. Dit is vergelijkbaar met de Nederlandse rubricering Stg. GEHEIM. Uit een gesprek met de AIVD blijkt dat voor de afgifte van een *clearance* geen extra onderzoek wordt gedaan, omdat de eisen die worden gesteld aan een veiligheidsonderzoek voor afgifte van een VGB zwaarder zijn dan de eisen die gelden voor afgifte van een NATO- of EU-*clearance*. Als de betrokkene een VGB op niveau B krijgt, ontvangt hij, als deze is aangevraagd, automatisch ook een *clearance* voor EU-/NATO-*Secret* gerubriceerde documenten. Om een *clearance* uit het systeem te genereren, moet de onderzoeksassistent wel handmatig extra brieven aanmaken.

3.4 Beleid ten aanzien van herhaalonderzoeken

Periodiek herhaalonderzoek: een veiligheidsonderzoek dat wordt gestart als er een periode van vijf jaren of een veelvoud daarvan is verstreken sinds de afgifte van de VGB. Uitgangspunt is dat veiligheidsonderzoeken voor betrokkenen met een VGB op A-niveau iedere vijf jaar worden herhaald en voor betrokkenen met een VGB op B- en C-niveau minimaal eens in de tien jaar. De procedure en inhoud van een periodiek herhaalonderzoek zijn vrijwel gelijk aan die van een initieel onderzoek.

Incidenteel herhaalonderzoek: een veiligheidsonderzoek naar aanleiding van relevante nieuwe feiten en/of omstandigheden. De betrokkene kan deze zelf opgeven, bijvoorbeeld als die een nieuwe partner heeft, maar er kan ook nieuwe informatie zijn binnengekomen bij de AIVD of de BVA van de organisatie waar de betrokkene werkt. Voor een incidenteel herhaalonderzoek geldt geen termijn. Dit kan op ieder moment worden aangevraagd en uitgevoerd.

De AIVD legt de wet verkeerd uit

Op grond van artikel 9 Wvo is de minister van Binnenlandse Zaken en Koninkrijksrelaties bevoegd een periodiek of incidenteel herhaalonderzoek te doen instellen. De tekenbevoegdheid ten aanzien van een herhaalonderzoek is gemandateerd aan het hoofd van de AIVD. Deze tekenbevoegdheid is vervolgens belegd bij het hoofd van de afdeling Veiligheidsonderzoeken.

De AIVD legt de verantwoordelijkheid voor het uitvoeren van periodieke en incidentele herhaalonderzoeken volledig bij de werkgever en ziet geen rol voor zichzelf bij het opstarten van een herhaalonderzoek. Naar het oordeel van de CTIVD legt de AIVD de wet op die manier verkeerd uit. Uit de Memorie van Toelichting bij de Wiv 2002 blijkt namelijk dat voor de werkgever een rol is weggelegd bij het signaleren van bijvoorbeeld functiewijzigingen. Hoewel de werkgever een rol heeft, houdt deze signaalrol naar het oordeel van de CTIVD niet in dat de werkgever daarmee als enige verantwoordelijk is voor het instellen van een herhaalonderzoek. Ook de tekenbevoegdheid voor het instellen van een herhaalonderzoek wijst erop dat de AIVD verantwoordelijkheid draagt voor het doen instellen van een herhaalonderzoek. De CTIVD stelt vast dat de AIVD, naast de werkgever, ook zelf een wettelijke verantwoordelijkheid heeft voor het uitvoeren van periodieke herhaalonderzoeken en incidentele herhaalonderzoeken. Ten aanzien van het incidentele herhaalonderzoek geldt dit wanneer er feiten en omstandigheden over de vertrouwensfunctionaris bij de AIVD bekend zijn die een herhaalonderzoek rechtvaardigen.

De AIVD neemt onvoldoende verantwoordelijkheid voor instellen herhaalonderzoek

De AIVD houdt de inzender (de werkgever) verantwoordelijk voor het doen instellen van een herhaalonderzoek. Dit geldt zowel voor een periodiek herhaalonderzoek, als voor een incidenteel onderzoek. De AIVD geeft als voornaamste reden dat de werkgever als enige partij overzicht heeft van de mensen die (nog) op de vertrouwensfunctie zitten. Accountmanagers van de AIVD onderhouden wel contact met inzenders om hen erop te wijzen bij te houden welke werknemers een VGB (nodig) hebben en wanneer zij in aanmerking komen voor een herhaalonderzoek. Bij nieuwe feiten en omstandigheden moeten deze accountmanagers de inzender ertoe bewegen een herhaalonderzoek aan te vragen. Als een inzender een herhaalonderzoek aanvraagt, moet dat worden uitgevoerd door de UVO.

De AIVD zag in de periode rond 2004 wel een rol voor zichzelf weggelegd bij het instellen van periodieke herhaalonderzoeken. Dit betrof specifiek herhaalonderzoeken voor personeel van twee ministeries die beschikten over een VGB op A-niveau.

Aanbevelingen 4 en 5

4. Neem in beleid op hoe de AIVD invulling geeft aan de discretionaire bevoegdheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties om periodieke herhaalonderzoeken in te stellen.
5. Neem in beleid op hoe de AIVD invulling geeft aan de discretionaire bevoegdheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties om incidentele herhaalonderzoeken in te stellen, in het geval dat bij de AIVD feiten en omstandigheden over een vertrouwensfunctionaris bekend zijn.

Terugkijken naar de inhoud van een eerder veiligheidsonderzoek is geen standaard werkwijze

De algemene werkwijze van de UVO is dat bij een herhaalonderzoek alleen wordt betrokken of de vorige VGB is afgegeven of geweigerd. Medewerkers van de UVO kijken niet naar de inhoud van het vorige veiligheidsonderzoek. Daarnaast wordt bij het herhaalonderzoek in principe teruggekeken tot het vorige veiligheidsonderzoek. Bij een regulier herhaalonderzoek op A-niveau vijf jaar na afgifte van de VGB, wordt bijvoorbeeld teruggekeken tot de initiële afgifte van de VGB, ondanks de terugkijktermijn van tien jaar. Deze werkwijze brengt risico's met zich in de gevallen waar bij eerdere afgifte twijfels over de afgifte van een VGB of bijzonderheden in het onderzoek zijn geweest. Met de gehanteerde werkwijze komen dergelijke twijfels of bijzonderheden niet aan het licht, omdat deze ook niet separaat worden vastgelegd.

Aanbeveling 6

Leg twijfels of bijzonderheden over het al dan niet afgeven van een VGB vast. Raadpleeg bij een herhaalonderzoek het procesformulier van het vorige veiligheidsonderzoek, zodat indien nodig extra aandacht kan worden gegeven aan onderwerpen waarbij twijfel bestond of bijzonderheden waren.

4 Uitvoering van de veiligheidsonderzoeken in de NCTV-casus

4.1 Conclusie: de veiligheidsonderzoeken van 2015, 2018 en 2020 zijn conform wet- en regelgeving uitgevoerd. Het veiligheidsonderzoek van 2005 is onzorgvuldig verlopen.

Het veiligheidsonderzoek naar persoon 1 in 2005 was onzorgvuldig. Zo is de vastlegging van het proces en de besluitvorming onvoldoende. Hierdoor is niet te achterhalen waarom de AIVD een VGB op A-niveau heeft afgegeven. Dit is belangrijk, omdat concrete signalen over negatieve persoonlijke gedragingen onvoldoende zijn onderzocht. Daarnaast is er een spoedprocedure voor de afgifte van de VGB gevolgd, ondanks dat er volgens de AIVD twijfels over waren.

Tussen 2005 en 2018 is geen herhaalonderzoek uitgevoerd. Het veiligheidsonderzoek naar persoon 1 in 2018 is conform wet- en regelgeving en beleid uitgevoerd. De CTIVD heeft wel een aantal tekortkomingen in de uitvoering van het veiligheidsonderzoek van 2018 geconstateerd. Het terugkijken naar de inhoud van een eerder veiligheidsonderzoek is geen standaard werkwijze. Daarnaast is gesignaleerd dat het formulier waarin persoonlijke gegevens worden opgegeven niet volledig is ingevuld door persoon 1. Dit is geen aanleiding geweest voor nader onderzoek. De afgifte van de NATO- en EU-*clearance* aan persoon 1 in 2018 was rechtmatig.

De veiligheidsonderzoeken naar persoon 2 in 2015 en 2020 zijn conform wet- en regelgeving en beleid uitgevoerd. De afgifte van de VGB's op B-niveau aan persoon 2 zijn rechtmatig. Ook de afgiftes van de NATO- en EU-*clearance* aan persoon 2 in 2015 en 2020 zijn rechtmatig.

Bovenstaande bevindingen worden in dit hoofdstuk nader toegelicht. In paragraaf 4.2 wordt ingegaan op de uitvoering van de veiligheidsonderzoeken naar persoon 1. In paragraaf 4.3 komen de veiligheidsonderzoeken naar persoon 2 aan bod.

4.2 Uitvoering van veiligheidsonderzoeken naar persoon 1

De AIVD heeft in 2005 en 2018 een veiligheidsonderzoek verricht naar persoon 1. De bevindingen over deze veiligheidsonderzoeken en de tussenliggende periode worden in deze paragraaf beschreven.

4.2.1 Veiligheidsonderzoek A 2005

In 2005 heeft de AIVD naar persoon 1 een veiligheidsonderzoek op niveau A uitgevoerd. Het onderzoek is met spoed uitgevoerd. In het administratieve onderzoek zijn verschillende naslagen gedaan, waaronder een aantal niet-standaard naslagen. Het veldonderzoek is uitgebreider geweest dan gebruikelijk. Naar aanleiding van de gesprekken die zijn gevoerd in het veldonderzoek is nader administratief onderzoek gedaan. In één naslag is door de AIVD een specifieke vraag gesteld waaruit kan worden afgeleid dat er bij de medewerkers van de UVO twijfels waren over de onafhankelijkheid van persoon 1. De CTIVD concludeert op basis van drie bevindingen dat het veiligheidsonderzoek op A-niveau naar persoon 1 in 2005 onzorgvuldig is uitgevoerd. Deze worden hieronder toegelicht.

De vastlegging van het proces en de besluitvorming was onvoldoende

Tijdens het veldonderzoek is niet steeds (volledig) vastgelegd welke stappen er zijn genomen en welke resultaten die stappen hebben opgeleverd. Uit het onderzoeksrapport kan worden afgeleid dat er meer onderzoekhandelingen zijn uitgevoerd dan is vastgelegd in het procesformulier. In gesprekken hebben ook medewerkers van de UVO gezegd dat de vastlegging erg summier was ten opzichte van de omvang van het onderzoek. Uit het procesformulier kan niet worden opgemaakt welke afwegingen er bij het besluit tot afgifte van de VGB zijn gemaakt. Hierdoor is niet te achterhalen waarom persoon 1 een VGB heeft gekregen, ondanks negatieve signalen die blijkens het onderzoeksrapport bekend waren bij de medewerkers van de UVO.

Concrete negatieve persoonlijke gedragingen van persoon 1 lijken onvoldoende te zijn onderzocht

Uit het veldonderzoek zijn signalen naar voren gekomen dat persoon 1 kwetsbaar zou kunnen zijn en mogelijk niet-integer gedrag heeft vertoond. Deze signalen zagen op de persoonlijke gedragingen en omstandigheden van persoon 1, die de AIVD toetst aan de hand van de risicofactoren onharmonieus gedrag, afhankelijkheidsproblemen en loyaliteitsproblemen. Ten aanzien van een aantal signalen is opvolging gegeven met nader onderzoek. Andere signalen lijken niet verder te zijn onderzocht. De CTIVD is van oordeel dat voor een aantal concrete signalen van negatieve persoonlijke gedragingen en omstandigheden nader onderzoek aangewezen was. Dit nader onderzoek lijkt onvoldoende te hebben plaatsgevonden. Daarover is in ieder geval niets vastgelegd in het procesformulier.

In de geheime bijlage bij dit rapport wordt deze bevinding nader toegelicht.

Ondanks twijfels is een spoedprocedure gevolgd

Op basis van het procesformulier stelt de CTIVD vast dat de VGB met spoed is behandeld, wat inhoudt dat een dossier prioriteit krijgt bij de behandeling ervan ten opzichte van andere dossiers. De VGB was in verband met spoed al aan persoon 1 verzonden voordat alle onderzoeksresultaten in het procesformulier waren vastgelegd. De afronding van het veiligheidsonderzoek heeft plaatsgevonden in een korte periode. In het gesprek over dit veiligheidsonderzoek heeft de AIVD gesignaleerd dat er in een korte periode opvallend veel gesprekken zijn gevoerd met persoon 1 en informanten. Dit duidt volgens de AIVD op twijfels over het al dan niet afgeven van een VGB. De CTIVD is van oordeel dat wanneer er twijfels zijn over de afgifte van een VGB er moet worden afgestapt van een spoedprocedure, omdat een spoedprocedure een negatieve impact kan hebben op de kwaliteit van het onderzoek of oordeelsvorming. Vanwege dit risico vindt de CTIVD het onzorgvuldig dat ondanks de twijfels in dit geval de VGB met spoed is afgegeven.

4.2.2 Periode tussen 2005 en 2018

Tussen 2005 en 2018 is er geen herhaalonderzoek uitgevoerd naar persoon 1

De CTIVD stelt vast dat er voor persoon 1 tussen 2005 en 2018 geen herhaalonderzoek heeft plaatsgevonden, terwijl hij in die periode steeds een vertrouwensfunctie heeft bekleed. Uit de gesprekken met de AIVD is gebleken dat de AIVD de verantwoordelijkheid voor het aanvragen van een periodiek herhaalonderzoek bij de werkgever legt (zie paragraaf 3.8). De werkgever heeft in 2018 voor het eerst een verzoek tot het uitvoeren van een herhaalonderzoek ingediend.

4.2.3 Veiligheidsonderzoek B 2018

Het veiligheidsonderzoek op B-niveau naar persoon 1 in 2018 is naar het oordeel van de CTIVD conform wet- en regelgeving en beleid uitgevoerd. De *clearances* voor toegang tot NATO- en EU-gerubriceerd materiaal zijn rechtmatig verleend. De CTIVD heeft wel geconstateerd dat de in 2018 gehanteerde werkwijze op een aantal onderdelen onzorgvuldig was. Deze onzorgvuldigheden worden hierna toegelicht.

Een onvolledig of onjuist ingevuld OPG kan aanleiding zijn voor nader onderzoek

Persoon 1 heeft de OPG op een aantal punten niet volledig en/of niet juist ingevuld. Desgevraagd heeft de AIVD toegelicht dat OPG's vaker onzorgvuldig worden ingevuld door betrokkenen en dat hieruit niet per definitie kan worden afgeleid dat de betrokkene niet eerlijk is. Als de onderzoeksassistent op basis van andere resultaten geen aanleiding heeft te vermoeden dat de betrokkene opzettelijk gegevens achterhoudt, kan die ervoor kiezen niets te doen met de onvolledigheid of onjuistheid. De CTIVD begrijpt dat een betrokkene een keer een fout kan maken bij het invullen van de OPG. Wanneer meerdere vragen onvolledig en/of onjuist worden beantwoord, kan dit wel een signaal zijn dat een betrokkene niet eerlijk is. Eerlijkheid is een van de factoren waaraan persoonlijke gedragingen worden getoetst. Er kan bijvoorbeeld aanleiding zijn om de zaak door te sturen naar een diepteonderzoek en de betrokkene hierop te bevragen tijdens een gesprek. In dit specifieke geval was het voorstelbaar geweest dat het niet volledig en/of niet juist invullen van de OPG door persoon 1 aanleiding was om het dossier door te sturen voor nader onderzoek.

Aanbeveling 7
Maak beleid hoe medewerkers van de UVO in het kader van het criterium "eerlijk" moeten omgaan met niet volledig of niet juist ingevulde OPG's.

De medewerkers van de UVO hadden een onvolledig beeld

In de "Beleidsregel beoordelingsperiodes en onvoldoende gegevens veiligheidsonderzoeken" is opgenomen dat bij een A-veiligheidsonderzoek de gegevens over een periode van in beginsel tien jaar direct voorafgaande aan de aanmelding worden beoordeeld, bij een B-onderzoek in beginsel over een periode van acht jaar en bij een C-veiligheidsonderzoek, tot begin 2018, in beginsel over een periode van acht jaar en sindsdien over een periode van vijf jaar. Dit wordt de terugkijktermijn genoemd.

Als gevolg van de terugkijktermijn hadden de medewerkers van de UVO bij het onderzoek in 2018 niet de beschikking over concrete relevante informatie. Dit kan mede het gevolg zijn van de beperkte raadpleging van het veiligheidsonderzoek 2005 of door de in de beleidsregel opgenomen terugkijktermijn. Naar het oordeel van de CTIVD is er een categorie van informatie die dusdanig relevant is dat er geen terugkijktermijn moet gelden.

In de geheime bijlage bij dit rapport wordt deze bevinding nader toegelicht.

4.3 Uitvoering van de veiligheidsonderzoeken naar persoon 2

De AIVD heeft in 2015 en 2020 een veiligheidsonderzoek verricht naar persoon 2. De bevindingen over deze veiligheidsonderzoeken worden in deze paragraaf beschreven.

Het veiligheidsonderzoek in 2015 is conform wetgeving en beleid uitgevoerd

In 2015 is naar persoon 2 een veiligheidsonderzoek op B-niveau gestart. Er heeft in lijn met het beleid alleen een administratief onderzoek plaatsgevonden. Omdat er geen onregelmatigheden uit de naslagen zijn gebleken, heeft de AIVD een VGB afgegeven. De CTIVD heeft bij haar onderzoek geen onregelmatigheden geconstateerd. Het veiligheidsonderzoek naar persoon 2 in 2015 is conform wet- en regelgeving en intern beleid uitgevoerd. Er was bij de AIVD geen informatie over persoon 2 bekend die tot weigering van een VGB of tot een ander proces had moeten leiden.

Het veiligheidsonderzoek in 2020 is conform wetgeving en beleid uitgevoerd

De werkgever van persoon 2 heeft haar in 2020 aangemeld voor een herhaalonderzoek, waarbij ook een *clearance* voor toegang tot gerubriceerde NATO- en EU-informatie is aangevraagd. Ook dit onderzoek heeft geen onregelmatigheden uitgewezen. Het veiligheidsonderzoek is conform wet- en regelgeving en intern beleid uitgevoerd. Er was bij de AIVD geen informatie over persoon 2 bekend die tot weigering van een VGB of tot een ander proces had moeten leiden.

5 Zorgplicht geheimhouding AIVD

5.1 Conclusie: De AIVD heeft op onderdelen onvoldoende voldaan aan de wettelijke zorgplicht omtrent geheimhouding.

De diensthoofden zijn verplicht om zorg te dragen voor de geheimhouding van vertrouwelijke en staatsgeheime gegevens. Bij het verstrekken van gegevens aan andere (overheids)instanties moet de AIVD actie ondernemen wanneer er signalen zijn over tekortschietende informatiebeveiliging bij deze (overheids)instanties. Daarnaast moet de AIVD bij het delen van inlichtingenproducten steeds de afweging maken of de beoogde ontvanger de betreffende informatie nodig heeft voor zijn functie of taak en zorgdragen voor veilige verzending. Zo wordt voorkomen dat geheime informatie breder verspreid wordt dan nodig is.

De CTIVD stelt vast dat de BVA van de AIVD niet op de hoogte was van signalen over tekortschietende informatiebeveiliging bij de NCTV, terwijl bij een ander onderdeel binnen de AIVD hierover wel informatie bekend was. De BVA heeft door de gemiste signalen geen actie kunnen ondernemen. Daarnaast stelt de CTIVD vast dat de AIVD geen verantwoordelijkheid heeft genomen voor eventuele risico's van het systeem waarmee staatsgeheime gegevens tussen overheidsinstanties worden verzonden.

Bij het delen van informatie zijn het bieden van handelingsperspectief en het *need to know*-principe de belangrijkste uitgangspunten. De CTIVD constateert echter dat, met het oog op de inhoud van bepaalde documenten die bij persoon 1 zijn aangetroffen, de AIVD in de onderzoeksperiode in een aantal gevallen informatie met de NCTV heeft gedeeld waarvan niet kan worden achterhaald waarom deze informatie van belang was voor het werk van de NCTV. Dit is onzorgvuldig. Als gevolg van de NCTV-casus wordt tegenwoordig kritischer gekeken naar de inhoud en ontvangers van gedeelde gegevens.

Vanuit het managementkader van de AIVD zijn mondeling persoonsgegevens gedeeld met de NCTV. De CTIVD is van oordeel dat deze externe gegevensverstrekking niet past binnen het gesloten stelsel van gegevensverstrekking van de Wiv 2017 en dus onrechtmatig was. Daarnaast heeft de AIVD onrechtmatig gehandeld door pas na vier jaar vast te leggen dat persoonsgegevens zijn gedeeld.

Bovenstaande bevindingen worden in dit hoofdstuk nader toegelicht. In paragraaf 5.2 wordt ingegaan op de wettelijke zorgplicht. In de daarop volgende paragrafen worden de bevindingen ten aanzien van de invulling van de zorgplicht vanuit beveiligingsperspectief en de bevindingen naar het beleid en de uitvoering van exploitaties toegelicht. In de laatste paragraaf wordt ingegaan op een concreet geval van verstrekking van persoonsgegevens aan de NCTV.

5.2 De wettelijke zorgplicht van de AIVD omtrent de geheimhouding van gegevens

In artikel 23 van de Wiv 2017 is opgenomen dat de hoofden van de diensten zorg dragen voor de geheimhouding van daarvoor in aanmerking komende gegevens, de geheimhouding van bronnen waaruit gegevens afkomstig zijn en de veiligheid van de personen met wier medewerking gegevens worden verzameld.

Op basis van artikel 24 Wiv 2017 moet er onder meer worden zorg gedragen voor voorzieningen van technische en organisatorische aard ter beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens alsmede tegen onbevoegde gegevensverwerking.

De zorgplicht van de AIVD en de MIVD voor het geheimhouden van gegevens is belegd bij de diensthoofden. Zij moeten hiervoor concrete maatregelen treffen, zodat de diensten voortdurend controle hebben op de wijze waarop gegevens worden verwerkt. Dit onderzoek richt zich op de vraag of deze zorgplicht voldoende is nageleefd in de context van het verstrekken van informatie aan de NCTV. Daarbij rijst de vraag of de zorgplicht voor de geheimhouding van gegevens blijft gelden, nádat deze verstrekt zijn aan andere overheidsorganisaties, zoals in dit onderzoek aan de NCTV.

Naast de wettelijke zorgplicht van de hoofden van de diensten is er ook een verantwoordelijkheid voor de ontvangende overheidsinstanties zelf. Op basis van het VIRBI 2013 hebben ontvangers namelijk een eigen verantwoordelijkheid voor de bescherming van geheime informatie waarmee zij werken. Het VIRBI bevat regels over de beveiliging van staatsgeheime informatie, maar regelt geen centrale autoriteit die binnen de Rijksoverheid verantwoordelijk is voor of toezicht houdt op de bescherming van staatsgeheime informatie. De verantwoordelijkheid voor de beveiliging van staatsgeheime informatie wordt belegd voor ieder departement afzonderlijk bij de secretaris-generaal (SG) van een ministerie. Wanneer de diensten informatie delen met overheidsinstanties als de NCTV, mogen zij er redelijkerwijs van uitgaan dat deze instanties daar volgens de regels en afspraken mee omgaan en toereikend informatiebeveiligingsbeleid hanteren. De CTIVD toetst daarom de invulling van de zorgplicht van de diensthoofden, met inachtneming van de verantwoordelijkheid van de ontvangende instanties.

De AIVD stelt zich op het standpunt dat wanneer de diensten hun gegevens delen met andere overheidsinstanties, de AIVD in eerste instantie wel eigenaar blijft van de gegevens. Daarmee blijft de zorgplicht voor de geheimhouding van deze gegevens in zekere mate gelden. Op basis van deze verantwoordelijkheid en het uitgangspunt dat de AIVD voortdurend controle moet hebben op de wijze waarop gegevens worden verwerkt, moet de AIVD de volgende punten waarborgen:

- De AIVD is verantwoordelijk voor de veilige verzending van gegevens aan de juiste ontvangers. Dit wordt onder meer vormgegeven doordat het systeem NL-NET waarmee gegevens worden verzonden eigendom is van de AIVD.
- De AIVD houdt bij het verzenden van gegevens rekening met de need to know van de ontvangers. Zo wordt voorkomen dat geheime informatie breder verspreid wordt dan nodig is.
- Wanneer de AIVD signalen ontvangt over de beveiliging van de ontvangende partij, dan heeft de Beveiligingsautoriteit (BVA) AIVD de verantwoordelijkheid om in actie te komen. Bijvoorbeeld door het voeren van een gesprek met de ontvangende partij of – wanneer het personele beveiligingsmaatregelen betreft – het doen van een interne mededeling.

De CTIVD heeft in het licht van het uitgangspunt van voortdurende controle over gegevensverwerking en de hiervoor genoemde verantwoordelijkheden onderzoek gedaan naar de invulling van de zorgplicht in het kader van exploitatie van de AIVD aan de NCTV. Dit betreft enerzijds een onderzoek naar de invulling van de zorgplicht vanuit beveiligingsperspectief en anderzijds een onderzoek naar het beleid en de uitvoering van exploitaties. Dit wordt hieronder nader toegelicht.

5.3 Invulling zorgplicht vanuit beveiligingsperspectief

Op basis van de wettelijke vereisten en de eigen invulling van de AIVD hiervan, verwacht de CTIVD dat de AIVD gepast handelt wanneer er signalen zijn dat de beveiliging van staatsgeheime gegevens in gevaar raken of als er signalen zijn dat de inrichting of werking van veiligheidsmaatregelen tekortschiet. De CTIVD heeft hierover twee bevindingen.

De AIVD heeft signalen over de informatiebeveiliging bij de NCTV gemist

Binnen de AIVD was informatie bekend over mogelijke gebreken omtrent de beveiliging van internationale geheime informatie bij de NCTV. De BVA was niet op de hoogte van informatie waarover de NSA-afdeling beschikte. Als de BVA deze informatie had gehad, had zij hierop moeten handelen. De informatie betreft de resultaten van EU-inspecties ten aanzien van de informatiebeveiliging van de NCTV van 2013 en 2019. Deze resultaten waren ook relevant voor de werkzaamheden van de BVA, aangezien het een aanwijzing betrof dat er sprake was van tekortschietende informatiebeveiliging bij een organisatie die met AIVD-producten werkt. Uit onderzoek van de CTIVD blijkt dat er geen afstemming plaatsvindt tussen de BVA en de NSA-afdeling, terwijl beide een taak vervullen op het gebied van informatiebeveiliging. Hierdoor heeft de BVA in de onderzoeksperiode geen actie kunnen ondernemen richting de NCTV. De AIVD heeft op dit punt niet voldaan aan de zorgplicht.

Ook was de BVA er niet van op de hoogte dat een aantal AIVD-medewerkers reeds voorafgaand aan de casus signalen hadden omtrent gebrekkige informatiebeveiliging bij de NCTV. De BVA heeft hier nooit melding van ontvangen.

Aanbevelingen 8 en 9

8. Waarborg informatiedeling tussen de afdelingen die zicht hebben op signalen over de informatiebeveiliging bij andere (overheids)organisaties waarmee wordt samengewerkt.
9. Vergroot de bekendheid en bevorder de meldingsbereidheid om vermoedens over gebrekkige informatiebeveiliging bij andere (overheids)organisaties bij de BVA van de AIVD te melden.

NL-NET is niet geaccrediteerd

NL-NET: De NCTV ontvangt gerubriceerde documenten van onder meer de AIVD via het systeem NL-NET. Dit systeem is ontwikkeld door en in beheer bij de AIVD en wordt gebruikt als digitale brievenbus om (internationaal) gerubriceerde informatie met andere overheidsinstellingen te delen.

De AIVD is eigenaar van NL-NET en daarmee verantwoordelijk voor de naleving van de beveiligingseisen. Onderdeel van de beveiligingseisen is dat een systeem wordt geaccrediteerd. In het accreditatieproces wordt het systeem getoetst aan de geldende normen. Zo worden eventuele risico's geïdentificeerd. Deze risico's worden vervolgens beheerst of geaccepteerd (restrisico's). Dit proces is voor NL-NET niet volledig doorlopen, waardoor NL-NET niet geaccrediteerd is. Gevolg hiervan is dat er geen verantwoordelijkheid wordt genomen voor openstaande (rest)risico's van het systeem, terwijl andere gebruikers wel moeten kunnen vertrouwen op de veilige werking van het systeem.

Aanbeveling 10
Draag er zorg voor dat NL-NET voldoet aan beveiligingseisen, zodat veilige verzending wordt geborgd.

5.4 Invulling zorgplicht bij exploitatie van producten

Exploitatie: de AIVD kan door middel van berichten vertrouwelijke en staatsgeheime informatie delen met onder meer overheidsorganisaties ('de afnemers'). De AIVD heeft hiervoor verschillende exploitatieproducten, bijvoorbeeld ambtsberichten, inlichtingenberichten, inlichtingenanalyses of dreigingsinschattingen.

De Wiv 2017 kent een **gesloten stelsel van informatieverstrekking**. De AIVD kan slechts informatie delen met andere personen of instanties als hiervoor een specifieke wettelijke grondslag bestaat. De wetgever heeft dit wenselijk geacht gelet op het bijzondere karakter van de gegevens die door (of ten behoeve van) de diensten worden verwerkt. De bedoeling is om onwenselijke sfeervermenging tussen het werk van de diensten en andere overheidstaken te voorkomen.

Als de AIVD informatie deelt met de NCTV, dan moet dit plaatsvinden binnen het gesloten stelsel van informatieverstrekking. De zorgplicht blijft tevens gelden, wat betekent dat informatie uitsluitend kan worden gedeeld als deze informatie *need to know* is voor de ontvanger. Daarmee wordt voorkomen dat informatie breder verspreid raakt dan nodig. De CTIVD heeft in het licht van het *need to know*-principe een aantal bevindingen.

Handelingsperspectief en het *need to know*-principe zijn belangrijke uitgangspunten voor exploitatie

De inlichtingenteams van de AIVD bepalen welke informatie zij willen delen met welke afnemers. Deze afweging wordt voor ieder product afzonderlijk gemaakt. Uitgangspunt is dat de AIVD afnemers in staat wil stellen te handelen. Dit bieden van handelingsperspectief is daarom een belangrijke geobjectiveerde toets. Daarnaast kunnen onder meer politiek-bestuurlijke afwegingen een rol spelen. Bij die afwegingen speelt het *need to know*-principe en de bescherming van brongegevens een belangrijke rol. Daarbij kan het wel gebeuren dat in het kader van politiek-bestuurlijk informeren bepaalde organisaties of onderdelen van organisaties aan de verzendlijst worden toegevoegd.

Onzorgvuldig is dat niet herleidbaar is waarom bepaalde documenten met de NCTV zijn gedeeld

De NCTV is voor de uitvoering van zijn taak afhankelijk van de informatie van de AIVD. De AIVD deelt daarom regelmatig inlichtingenberichten, inlichtingenanalyses en dreigingsinschattingen met de NCTV, wanneer dit handelingsperspectief biedt aan de NCTV. Bijvoorbeeld over onderwerpen als terrorisme en binnenlandse veiligheid. De CTIVD heeft in haar onderzoek navraag gedaan naar de afwegingen waarom bepaalde geheime inlichtingenberichten aan de NCTV zijn verzonden en waarom bepaalde EU-berichten sinds 2013 automatisch aan de NCTV werden doorgezonden. De AIVD kan niet (meer) reconstrueren in welke context de voorgelegde inlichtingenberichten zijn verzonden en wat het handelingsperspectief van de NCTV bij deze berichten was. Ook is niet bekend hoe het *need to know*-principe is afgewogen. Hetzelfde geldt voor de afweging om automatisch EU-berichten door te zenden. De CTIVD vindt het in het kader van de zorgplicht onzorgvuldig dat niet is vastgelegd waarom bepaalde inlichtingenberichten met de NCTV zijn gedeeld. Hierdoor kan achteraf niet meer worden vastgesteld waarom het noodzakelijk was om de informatie met de NCTV te delen.

Aanbeveling 11
Leg in beleid vast waarom (categorieën van) producten worden gedeeld met andere overheidsinstanties. Besteed daarbij aandacht aan het bieden van handelingsperspectief en het *need to know*-principe.

Gevolg van de NCTV-casus is dat kritischer wordt gekeken naar verzendlijst en inhoud berichten

Hoewel buiten de scope van het onderzoek, is tijdens het onderzoek aan de orde gekomen dat de NCTV-casus aanleiding heeft gegeven om nadrukkelijker te kijken naar de afnemers waaraan de AIVD berichten wil verzenden en naar de inhoud van deze berichten. De CTIVD heeft de werking van deze wijziging niet nader onderzocht. De CTIVD vindt dit wel een begrijpelijke ontwikkeling. Onderdeel van de nieuwe werkwijze is dat wordt beoordeeld of bepaalde afnemers wel of niet standaard op de verzendlijst behoren te staan. Dit is een wijziging op de werkwijze die rond 2014 is geïntroduceerd, waarbij is besloten om vanuit de AIVD meer actief aan andere overheden te exploiteren, zodat het belang van de uitvoering van de D-taak (het doen van onderzoek naar landen) breder gedragen zou worden binnen de overheid.

Ook wordt er mede naar aanleiding van de NCTV-casus kritischer gekeken naar de inhoud van de berichten. De AIVD let beter op het noemen van personen en het prijsgeven van operationele details.

5.5 Concreet geval van informatieverstrekking aan de NCTV

Op grond van artikel 62 Wiv 2017 kan de AIVD mededeling doen aan andere personen of instanties over door de AIVD verwerkte gegevens. Nadrukkelijke eis is dat deze gegevensverstrekking alleen kan plaatsvinden in het kader van een goede taakuitvoering van de diensten. Op grond van artikel 8, tweede lid, Wiv 2017 voert de AIVD in het belang van de nationale veiligheid vijf taken uit (zie kader in paragraaf 4.2). De gegevensverstrekking moet een van die taken dienen en moet altijd in het belang van de nationale veiligheid zijn.

Op grond van artikel 70 Wiv 2017 moet aantekening worden gehouden van de verstrekking van persoonsgegevens.

De AIVD heeft onrechtmatig persoonsgegevens verstrekt aan de NCTV

De diensten zijn in het kader van een goede taakuitvoering bevoegd om gegevens te verstrekken aan onder andere de NCTV op basis van artikel 62 Wiv 2017. De CTIVD heeft tijdens het onderzoek geconstateerd dat vanuit het managementkader van de AIVD mondeling persoonsgegevens zijn gedeeld met de NCTV. De CTIVD komt tot de conclusie dat deze gegevensverstrekking niet in het kader van de goede uitvoering van één van de taken van de AIVD was. Dat betekent dat de gegevensverstrekking niet heeft plaatsgevonden op grond van artikel 62 Wiv 2017.

De CTIVD is van oordeel dat er ook geen andere toepasselijke wettelijke grondslag voor de gegevensverstrekking aan de NCTV bestond. De AIVD heeft onrechtmatig gehandeld door zonder wettelijke grondslag (persoons)gegevens uit inlichtingen te delen met de NCTV.

Deze bevinding is nader onderbouwd in de geheime bijlage bij dit rapport.

De AIVD heeft onrechtmatig gehandeld door de verstrekking van persoonsgegevens niet vast te leggen

Van dit gesprek is pas vier jaar later een verslag gemaakt. Tot dit moment was er geen melding of verslag van dit gesprek in de AIVD-systemen. De AIVD heeft in de periode tussen het gesprek en de vastlegging daarvan niet voldaan aan het voorschrift van artikel 70 Wiv 2017, waarin is bepaald dat er aantekening moet worden gehouden van de verstrekking van persoonsgegevens. Daarmee heeft de AIVD onrechtmatig gehandeld.

6 Uitvoering van de National Security Authority-taak door de AIVD

6.1 Conclusie: De AIVD heeft onvoldoende invulling gegeven aan de NSA-taak

De AIVD heeft als *National Security Authority* (NSA) een verantwoordelijkheid met betrekking tot de bescherming van internationaal gerubriceerde informatie. De taak van de NSA omvat onder meer het accrediteren en inspecteren van de fysieke en digitale informatiebeveiliging van (overheid)instanties die internationaal gerubriceerde informatie kunnen verwerken. Het huidige beleid ten aanzien van de uitvoering van deze taak dateert van 2021. Dit beleid is slechts op hoofdlijnen uitgewerkt. Ook wordt in het beleid de verantwoordelijkheid voor de controle op personele beveiliging niet goed belegd. Bovendien stelt de CTIVD vast dat het Nederlandse stelsel niet goed aansluit op de internationale regelgeving en dat het beleid hier meer duidelijkheid over kan bieden.

De AIVD heeft in de periode vanaf januari 2013 tot mei 2023 onvoldoende invulling gegeven aan de NSA-taak ten aanzien van de NCTV. Het gerubriceerde netwerk van de NCTV is nooit volwaardig geaccrediteerd; er is eenmaal in 2013 een tijdelijke toestemming gegeven. Inspecties van de Europese Unie hebben gebreken aan het licht gebracht, maar hieraan heeft de AIVD onvoldoende opvolging gegeven. Vastlegging van uitgevoerde activiteiten ontbreekt.

De CTIVD constateert dat de voorgaande bevindingen moeten worden bezien in de context van een beperkte capaciteit voor de uitvoering van de NSA-taak bij overheidsinstellingen en het ontbreken van formele doorzettingsmacht richting overheidsinstellingen. Dit lijkt in de weg te hebben gestaan aan een goede uitvoering van de NSA-taak ten opzichte van de NCTV.

De voorgaande bevindingen worden hieronder nader toegelicht. Gestart wordt met een beschrijving van de NSA-taak van de AIVD. Hierna volgen bevindingen met betrekking tot het beleid, de uitvoering van de NSA-taak ten opzichte van de NCTV en de beperkte capaciteit en doorzettingsmacht.

6.2 De NSA-taak van de AIVD

Internationaal gerubriceerde informatie: gerubriceerde informatie die afkomstig is van de Europese Unie, de NAVO of de Europese ruimtevaartorganisatie ESA. Voor internationaal gerubriceerde informatie bestaan andere rubriceringsniveaus die vergelijkbaar zijn met de Nederlandse rubriceringsniveaus. Internationaal gerubriceerde informatie dient te worden beveiligd conform internationaal gestelde eisen.

In Nederland kan op verschillende plekken worden gewerkt met internationaal gerubriceerde informatie. Daarbij kan het gaan om gerubriceerde informatie van onder meer de Europese Unie, de NAVO of de Europese ruimtevaartorganisatie ESA. De AIVD heeft als *National Security Authority* (NSA) een centrale verantwoordelijkheid met betrekking tot de bescherming van deze gerubriceerde informatie. De taak van de NSA omvat onder meer het accrediteren en inspecteren van de fysieke en digitale informatiebeveiliging van (overheids)instanties die dergelijke internationaal gerubriceerde informatie verwerken, waaronder de NCTV.

Voor gerubriceerde informatie van de EU zijn de regels opgenomen in het besluit van de Raad van de Europese Unie van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie (hierna: het EU-Besluit). In artikel 16 is bepaald dat iedere lidstaat een NSA aanwijst en wat de taken van de NSA zijn.

Voor gerubriceerde informatie van de NAVO zijn de regels opgenomen in het document *Security Within the North Atlantic Treaty Organization (NATO), note by the Secretary General* van 17 juni 2002. In bijlage B is de verantwoordelijkheid van de NSA beschreven.

Voor gerubriceerde informatie van de ESA zijn de regels opgenomen in het document *Regulations of the European Space Agency, Security Regulations,* ESA/REG/004, d.d. 1 juli 2020. In artikel 2 staat dat elke lidstaat een NSA aanwijst die verantwoordelijk is voor de veiligheid van gerubriceerde informatie van de ESA.

De AIVD is als NSA verantwoordelijk voor (het toezicht op) de beveiliging van internationaal vertrouwelijke informatie en voor het periodiek inspecteren en evalueren van deze beveiliging. Op basis van de internationale regelgeving constateert de CTIVD dat van de NSA in ieder geval het volgende wordt verwacht:

- Voorafgaand aan de verwerking van internationaal gerubriceerde informatie beoordeelt de AIVD de beveiliging van de internationaal vertrouwelijke informatie bij overheidsinstellingen, zodat deze informatie conform de internationale regelgeving is beschermd.
- De AIVD inspecteert en evalueert de getroffen beveiligingsmaatregelen periodiek.
- In de beoordeling van de AIVD worden de volgende aspecten betrokken: de personele beveiliging, de fysieke beveiliging en de beveiliging van communicatie- en informatiesystemen.

Accreditatie: de NSA geeft een accreditatie af wanneer aan alle eisen is voldaan om het juiste beveiligingsniveau te waarborgen. In de accreditatie wordt het maximale rubriceringsniveau gespecificeerd en de voorwaarden, zoals geldigheidsduur, beschreven. Dit wordt ook wel een **approval to operate** genoemd. Als nog niet aan alle eisen is voldaan maar de restrisico's acceptabel zijn, wordt geen accreditatie maar wel een **interim approval to operate (IATO)** afgegeven. Deze IATO heeft een beperkte geldigheidsduur en er worden verbeteractiviteiten met tijdslijnen meegegeven.

6.3 Beleid

De CTIVD heeft verschillende bevindingen over de wijze waarop het beleid ten aanzien van de uitvoering van de NSA-taak is ingericht. Deze worden hieronder toegelicht.

De AIVD beschikt sinds 2021 over een beleid op hoofdlijnen

Het beleid van de AIVD ten aanzien van de NSA-taak is voor het eerst opgesteld in 2021. In de periode voor 2021 beschikte de AIVD niet over een beleid, terwijl de internationale regelgeving reeds dateert uit 2002 (NAVO) en 2013 (EU).

In 2023 is het beleid verder uitgewerkt. Het beleid beschrijft de uitvoering van de NSA-taak ten opzichte van overheidsinstellingen alleen op hoofdlijnen. Hoe dit in de praktijk uitwerking krijgt, is niet in het beleid beschreven. De CTIVD vindt dit onzorgvuldig, omdat het beperkt formuleren van beleid een risico is voor de rechtmatige en zorgvuldige uitvoering van de NSA-taak.

De AIVD legt de verantwoordelijkheid voor de aanvraag en verlenging van personnel security clearances certificates bij overheidsinstellingen bij de werkgever

> **Personnel security clearance certificate (PSCC)**: medewerkers van een bedrijf die in aanraking (kunnen) komen met gerubriceerde NAVO, EU of ESA informatie en/of toegang krijgen tot deze organisaties moeten beschikken over een PSCC. Voor de afgifte van een PSCC wordt een veiligheidsonderzoek uitgevoerd door de UVO van de AIVD.

Uit het beleid van en gesprekken met de AIVD blijkt dat de controle op de naleving van de verlening en verlenging van PSCC's aan medewerkers met toegang tot internationaal gerubriceerde informatie geen vast onderdeel is van accreditaties of inspecties door de NSA bij de overheid. De NSA laat hiermee na toe te zien op de toepassing van (bijvoorbeeld) artikel 7 van het EU-besluit waarin is opgenomen dat toegang tot gerubriceerde EU-informatie uitsluitend wordt verleend als personen een veiligheidsonderzoek op het juiste niveau hebben gehad. Dit is onrechtmatig. De NSA zou de naleving van dit vereiste een vast onderdeel moeten maken van haar werkwijze met betrekking tot zowel accreditaties als inspecties.

Het Nederlandse stelsel sluit niet goed aan op internationale regelgeving

Het beleid is gebaseerd op de verschillende internationale regelgeving (EU, NAVO en ESA). De CTIVD concludeert op basis van deze regelgeving dat er een centrale verantwoordelijkheid voor het toezicht op de beveiliging van internationaal gerubriceerde informatie bij nationale instellingen is neergelegd bij de NSA. Ter illustratie, de EU-regelgeving spreekt van 'de regeling van beveiliging' door de NSA. Het beleid van de AIVD zoekt echter ook aansluiting bij het Nederlandse decentrale stelsel van het VIRBI 2013, waarbij de SG's van departementen verantwoordelijk zijn voor de omgang met (internationaal) gerubriceerde informatie en het toezicht daarop. In het NSA-beleid is dit onder meer verwoord als het 'zorgdragen voor voldoende beveiliging'. De AIVD vervult daarom in de praktijk een toezichthoudende rol. De CTIVD signaleert dat er een discrepantie bestaat tussen de formulering in internationale regelgeving en de toepassing in het Nederlandse stelsel. Het EU-besluit biedt landen de ruimte om de NSA-taak te implementeren op een wijze die past bij de nationale situatie, zolang dit in lijn is met de gedachte van de internationale regelgeving. Het beleid kan handvatten bieden om hier invulling aan te geven.

Aanbevelingen 12, 13 en 14

12. Concretiseer het NSA-beleid. Houd bij de formulering van het beleid rekening met de verwachtingen vanuit internationale regelgeving.
13. Maak de controle op de naleving van de afgifte en verlenging van PSCC's onderdeel van accreditaties en inspecties.
14. Betrek de gesignaleerde discrepantie tussen internationale regelgeving en het Nederlandse stelsel bij de herziening van het VIRBI 2013.

6.4 Uitvoering van de NSA-taak bij de NCTV

De CTIVD constateert dat de AIVD in de periode van januari 2013 tot mei 2023 onvoldoende invulling heeft gegeven aan de NSA-taak met betrekking tot de NCTV. De CTIVD baseert dit oordeel op een combinatie van bevindingen, die hieronder worden toegelicht.

De AIVD heeft de NCTV alleen in 2013 een tijdelijke *approval to operate* verleend

In 2013 heeft de AIVD een *Interim Approval to Operate* verstrekt voor de duur van een jaar, waarbij voorwaarden voor opvolging zijn gegeven waaraan de NCTV binnen een jaar moest voldoen. Niet is vastgelegd of en hoe de opvolging hierop heeft plaatsgevonden. Er heeft geen verlenging van de tijdelijke toestemming plaatsgevonden en een definitieve toestemming is niet verleend. Vervolgens heeft de AIVD in 2017 geconstateerd dat het gerubriceerde netwerk van de NCTV niet was geaccrediteerd en dat die accreditatie dat jaar zou plaatsvinden. Dit is niet gebeurd. Het gerubriceerde netwerk van de NCTV is derhalve gedurende de onderzoeksperiode nooit geaccrediteerd door de NSA.

De AIVD was op de hoogte van de gebreken in de informatiebeveiliging bij de NCTV, maar heeft geen opvolging gegeven

In aanvulling op de NSA voert de Europese Unie eens per vijf jaar inspecties van beveiligingsmaatregelen uit bij Nederlandse overheidsinstellingen, vanwege de verwerking van EU-gerubriceerde informatie. Deze inspecties hebben in 2013 en 2019 plaatsgevonden bij onder meer de NCTV. Beide inspecties hebben geleid tot bevindingen, waarover ook de AIVD is geïnformeerd. De AIVD heeft vervolgens in 2017 geconcludeerd dat de aanbevelingen van de Europese Unie uit 2013 door de NCTV zijn opgevolgd. Deze conclusies zijn niet verenigbaar met de uitkomsten van de opvolgende EU-inspectie in 2019 waarin is geconcludeerd dat de NCTV geen controle heeft over de EU-gerubriceerde informatie. Niet gebleken is dat de AIVD in de onderzoeksperiode voldoende opvolging heeft gegeven aan de uitkomsten van de inspecties in 2013 en 2019 door de Europese Unie.

De NSA-afdeling heeft de informatie over de gebreken bij de NCTV niet gedeeld met de BVA

De CTIVD constateert dat er geen informatie-uitwisseling heeft plaatsgevonden tussen de NSA-afdeling en de BVA. Informatie-uitwisseling tussen deze afdelingen is geen standaard werkwijze. Als vanuit de NSA-afdeling informatie gedeeld was over kwetsbaarheden in de informatiebeveiliging bij de NCTV, dan had de AIVD op basis van de wettelijke zorgplicht activiteiten kunnen ondernemen (zie hoofdstuk 5).

De vastlegging van de uitvoering ontbreekt

Voor zover de AIVD in 2013 en 2017 NSA-activiteiten heeft verricht met betrekking tot de NCTV, is de vastlegging van de uitgevoerde stappen en afwegingen gebrekkig. De CTIVD heeft vrijwel geen documentatie aangetroffen met betrekking tot de afgifte van de *Interim Approval to Operate* in 2013 en een uitgevoerde inspectie in 2017.

Aanbeveling 15
Zorg voor betere vastlegging van de uitvoering van de NSA-taak. Leg dit vast in het beleid.

De NSA heeft geen toestemming gegeven voor het werken met NL-NET

De CTIVD concludeert voorts dat de AIVD geen invulling heeft gegeven aan de NSA-taak met betrekking tot het eigen AIVD-systeem NL-NET dat wordt gebruikt om gerubriceerde documenten met onder meer de NCTV te delen. Voor dit systeem is geen tijdelijke of permanente toestemming om internationaal gerubriceerde informatie te verwerken.

Aanbeveling 16
Betrek in de accreditatie van NL-NET de standaarden voor internationaal gerubriceerde informatie.

6.5 NSA-afdeling heeft beperkte capaciteit en doorzettingsmacht

Op basis van gevoerde gesprekken constateert de CTIVD dat de AIVD over een zeer beperkt aantal NSA-inspecteurs beschikt, die samen verantwoordelijk zijn voor de uitvoering van de NSA-taken met betrekking tot alle Nederlandse overheidsinstellingen en een groot aantal bedrijven. De medewerkers ervaren een beperkte doorzettingsmacht in hun werkzaamheden ten aanzien van overheidsinstellingen. Dit is het gevolg van een mix van factoren:

- Formele bevoegdheden in regelgeving ontbreken.
- In de praktijk is de capaciteit die besteed kan worden aan overheidsinstellingen zeer beperkt.
- De bestuurlijke prioriteit is laag. De uitvoering van de NSA-taak staat heel beperkt op de agenda van de dienstleiding en bij overheidsorganisaties is de naleving van de regelgeving niet op hoog niveau of met voldoende urgentie belegd. Dit heeft tot gevolg dat de doorzettingsmacht op bestuurlijk niveau ook laag is.

De CTIVD stelt vast dat deze mix factoren een risico is voor de zorgvuldige uitoefening van de NSA-taak en in deze casus heeft zich dit ook gemanifesteerd.

De beperkte bezetting heeft mede tot gevolg dat de AIVD pas in 2021 het beleid voor de NSA-taak heeft opgesteld en dat dit in 2023 verder is uitgewerkt. Ook de constatering dat de AIVD onvoldoende invulling heeft gegeven aan de NSA-taak moet in deze context worden bezien.

Aanbeveling 17
Adresseer de onderliggende factoren – het ontbreken van regelgeving, capaciteit en bestuurlijke prioritering – die een zorgvuldige uitvoering van de NSA-taak bemoeilijken in relatie tot overheidsorganisaties. Onder meer om te bewerkstelligen dat de NSA over voldoende doorzettingsmacht en escalatiemogelijkheden beschikt.

Postbus 85556, 2508 CG Den Haag

T 070 315 58 20
E info@ctivd.nl | www.ctivd.nl