Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

36 721 Initiatiefnota van de leden Six Dijkstra en Omtzigt over centraal toezicht op staatsgeheimen

Nr. 2

INITIATIEFNOTA

1. Inleiding

Afgelopen december werd een rapport van de Auditdienst Rijk (ADR) openbaar met daarin de resultaten uit het onderzoek naar de diefstal van staatsgeheime informatie door een oud-medewerker van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het cluster Contraterrorisme, Extremisme en Radicalisering (CTER) van de Landelijke Eenheid van de politie. De hoofdboodschap van de ADR was zowel glashelder als vernietigend: «De NCTV en de politie hebben hun eigen kwetsbaarheid gecreëerd».[1] Er was namelijk niet slechts sprake van een spionerende medewerker, maar van een werkomgeving waarin de beveiliging van staatsgeheime en vertrouwelijke informatie in de basis niet op orde bleek. Noch de NCTV, noch de politie hadden aandacht voor het risico op *insider threat*.
De belangrijkste bevindingen van de ADR waren als volgt: Basale beveiligingsmaatregelen zoals het beperken van toegangsrechten werden niet getroffen; risicoanalyses werden door het management niet serieus genomen en werden daarom na verloop van tijd maar helemaal niet meer opgesteld, er was geen actuele baseline van beveiligingsmaatregelen; er werd niet gestuurd op controles van beveiligingsmaatregelen; de administratie van gebruikte USB-sticks en de daarop opgeslagen informatie was niet op orde; de Verklaringen van Geen Bezwaar (VGB's) van medewerkers waren in voorkomende gevallen al lange tijd verlopen; en er was geen monitoring van hoe medewerkers staatsgeheime informatie behandelden. Dit alles is onacceptabel in een omgeving waarin de meest gevoelige en vertrouwelijke informatie van de Nederlandse staat verwerkt wordt.

Hoewel het feit dat een NCTV- en politiemedewerker in opdracht van een Marokkaanse inlichtingendienst Nederlandse staatsgeheimen kon stelen op zichzelf zeer ernstig is, kun je als overheid nooit met volledige zekerheid ieder spionagerisico uitsluiten. Echter, omdat de leiding van de betreffende organisaties blijkens het ADR-rapport geen belang hechtte

[1] Kamerstuk 36600-VI-123, bijlage «Rapport Onderzoek Beveiligingsproces van staatsgeheime vertrouwelijke informatie bij NCTV en politie».

kst-36721-2
ISSN 0921 - 7371
's-Gravenhage 2025

aan de beveiliging van staatsgeheimen, kon deze diefstal jarenlang onopgemerkt blijven. We hebben hier te maken met waarschijnlijk het grootste schandaal in het Nederlandse nationale veiligheidsdomein uit de recente geschiedenis.

Het kabinet heeft in haar reactie op het ADR-rapport aangegeven alle aanbevelingen op te volgen en maatregelen te treffen om het beveiligingsniveau van de NCTV en het CTER-cluster van de politie flink op te schroeven. Dat is belangrijk, maar niet voldoende. De *checks and balances* hebben gefaald. Als de ADR geen onderzoek had gedaan naar de beveiliging van deze organisaties, dan was het ondermaatse niveau daarvan tot op heden niet aan het licht gekomen. Dit onderschrijft het belang van extern en onafhankelijk toezicht op de beveiliging van staatsgeheimen, iets wat ook met opvolging van de aanbevelingen pijnlijk genoeg nog steeds niet gerealiseerd zal worden. In het licht van het hoge statelijke dreigingsniveau, is deze situatie niet acceptabel.

In deze initiatiefnota wordt voorgesteld om de wettelijke basis omtrent staatsgeheimen te verstevigen en een centrale toezichthouder aan te wijzen voor het toezicht op staatsgeheim gerubriceerde informatie binnen alle onderdelen van de overheid die deze verwerken. Eerst lichten de initiatiefnemers in een probleemanalyse toe waarom de huidige toezichtsituatie niet voldoende is om de bescherming van de nationale veiligheid (specifiek: een zorgvuldige omgang met staatsgeheimen) te waarborgen, vervolgens onderbouwen ze hoe de toezichtsituatie er idealiter wel uit zou moeten zien en ten slotte komen ze met een voorstel van hoe deze organisatorisch ingericht kan worden.

2. Probleemanalyse

Er zit een grote kwetsbaarheid in het huidige stelsel van toezicht op staatsgeheimen.
Momenteel is de verantwoordelijkheid voor het toezien op de beveiliging van een overheidsdepartement verdeeld over drie verdedigingslinies. De eerste verdedigingslinie bestaat uit de ambtenaren van het departement zelf die een eigen verantwoordelijkheid hebben om verantwoord en alert met beveiligingsrisico's om te gaan (denk aan het houden aan een veilig wachtwoordbeleid, waakzaamheid voor phishingmails en een voorzichtige omgang met USB-sticks). De tweede verdedigingslinie bestaat uit specifieke functionarissen als de beveiligingscoördinator (BVC), die als taak hebben om risicomanagement uit te voeren. De beveiligingsautoriteit (BVA) van een ministerie moet ten slotte als derde verdedigingslinie onafhankelijk toezien op de eerste twee verdedigingslinies en daarover kunnen rapporteren. De verantwoordelijkheid voor de beveiliging van staatsgeheimen is daarin niet anders dan voor de algemene beveiliging, de beveiligingseisen zijn alleen hoger. Zo is de BVA-Justitie en Veiligheid (J&V) verantwoordelijk voor onafhankelijk toezicht op de manier waarop de NCTV met de beveiliging van staatsgeheim gerubriceerde informatie omgaat, en moet daarover rapporteren aan de secretaris-generaal (SG) van het eigen departement J&V als eindverantwoordelijke.

Door deze opzet is de BVA echter niet volledig onafhankelijk, omdat deze is ondergebracht in het departement waarover zij toezicht houdt en via de lijn verantwoording aflegt aan de leiding daarvan, terwijl ze hiërarchisch en HR-matig afhankelijk zijn van diezelfde leiding. Wanneer de hoogste ambtenaren geen of onvoldoende belang hechten aan de beveiliging van een departement, verzwakt dit de positie en effectiviteit van de BVA binnen het departement, omdat die geen escalatiemogelijkheden heeft.

Dit is geen hypothetische situatie. De ADR heeft geconstateerd dat dit jarenlang het geval was binnen de NCTV. Het managementteam (MT) van de NCTV (verantwoordelijk voor de eerste verdedigingslinie) toonde dusdanig lang zo weinig interesse in het treffen en monitoren van beveiligingsmaatregelen, dat vanaf een bepaald moment helemaal geen rapportages over informatiebeveiliging meer aan het MT gestuurd werden. De BVC werd als tweede verdedigingslinie buitenspel gezet omdat toezichtrapportages geen impact hadden en daarom vanaf 2020 maar helemaal niet meer werden opgesteld, en de monitoring op beveiligingsmaatregelen per 2021 werd stilgezet. Dit alles gebeurde in een tijd waarin nota bene de NCTV regelmatig waarschuwingen over digitale (statelijke) dreigingen en cyberaanvallen publiceerde, zoals in het Dreigingsbeeld Statelijke Actoren 2 uit 2022.
De verslapping van de beveiliging bleek niet voldoende om de BVA te alarmeren en de situatie te doen escaleren. In haar nota van mei 2022 stelt de BVA-J&V dat «de voortgang op basis van de aangeleverde informatie voldoende is», waarbij niet wordt ingegaan op het feit dat de basis van beveiligingsmaatregelen van de NCTV gedateerd is en accreditatie van staatsgeheime netwerk ontbreekt, zo meldt de ADR. Het kabinet wijdt dit in haar reactie aan het feit dat de informatiepositie van de BVA niet op orde was. Ze zegt toe dat het toezicht versterkt zal worden, maar de bestaande structuren blijven in de nieuwe situatie intact.[2] Het feit dat de BVA afhankelijk is van de klaarblijkelijk zeer summiere informatie die het departement zelf aanlevert en fundamentele beveiligingsonderdelen niet standaard verifieert, toont aan dat ook de derde verdedigingsline gefaald heeft. Niet doordat de functionarissen onvoldoende functioneerden, maar doordat de organisatorische inrichting van de BVA dusdanig is dat die onmogelijk haar taken adequaat kan uitvoeren.[3]

De conclusie is helder: zolang het leiderschap van een departement onvoldoende waarde hecht aan beveiliging, bieden de huidige toezicht-structuren onvoldoende weerstand om staatsgeheimen te beschermen tegen statelijke spionage. Zeker in het licht van het meest recente Dreigingsbeeld Statelijke Actoren, waarin gesteld wordt dat statelijke actoren onder meer door belangrijke geopolitieke ontwikkelingen «in toenemende mate en op verschillende manieren de nationale veiligheids-belangen [bedreigen]»[4], is dat onaanvaardbaar.

3. Gevolgen en impact van huidige gebreken

Het directe gevolg is dat staatsgeheimen en gevoelige informatie over Nederlandse burgers via een medewerker van de NCTV en het CTER-cluster van de politie jarenlang naar de Marokkaanse inlichtingen-dienst doorgesluisd konden worden. Onderwijl had het management structureel geen actueel beeld van de werking van beveiligingsmaatre-gelen zoals logging en compartimentering. Hierdoor konden verdachte handelingen niet tijdig onderkend worden, zoals dat staatsgeheime informatie via gegevensdragers of geprinte documenten het gebouw verlieten.

Dit soort misstanden schaadt Nederland en onze veiligheid op meerdere manieren. De internationale reputatie van Nederland kan een behoorlijke deuk oplopen door hoe de nationale veiligheid jarenlang veronachtzaamd is. Dit kan erin resulteren dat partnerlanden minder gewillig zijn om

---

[2] Kamerstuk 36600-VI-123, bijlage «Reactie op aanbevelingen».
[3] Kamerstuk 2025D03999, «Antwoord op vragen van de leden Six Dijkstra en Mutluer over het onderzoeksrapport Beveiligingsproces van staatsgeheime vertrouwelijke informatie bij NCTV en politie van de Audit Dienst Rijk, alsmede de kabinetsreactie daarop».
[4] AIVD, MIVD en NCTV (2022), «Dreigingsbeeld Statelijke Actoren 2».

informatie met Nederlandse (inlichtingen)diensten te delen, wat direct gevolgen kan hebben voor onze slagkracht tegen terrorisme, ondermijnende criminaliteit en spionage en hybride oorlogsvoering door statelijke actoren. Dezelfde risico's worden gelopen wanneer potentiële bronnen minder genegen zijn met onze diensten samen te werken, omdat ze er onvoldoende overtuigd van zijn dat de Nederlandse overheid veilig en onherleidbaar met hun inzichten en kennis omgaat.

Daarnaast is vooralsnog niet bekend hoeveel Nederlanders gedupeerd zijn door dit lek. De NCTV heeft in het verleden zonder geldige wettige grondslag privacygevoelige gegevens van Nederlandse personen verzameld en verspreid.[5] Binnen het CTER-cluster van de politie werden jarenlang registraties bijgehouden van burgers die onterecht als terrorist of extremist te boek stonden, zonder dat die burgers dit konden aanvechten, meldde de Nationale ombudsman in zijn rapport «Blind vertrouwen?».[6] Het is voorstelbaar dat als gevolg hiervan vertrouwelijke gegevens van onschuldige burgers bij de autoriteiten van Marokko terecht zijn gekomen, en deze mensen als gevolg hiervan gechanteerd of onder druk gezet worden.
Overigens is het onderliggende probleem groter dan de geconstateerde misstanden bij de NCTV. In zijn rapportage maakt de ADR namelijk eveneens melding van structurele gebreken in de beveiliging van staatsgeheimen binnen het CTER-cluster van de politie. Dit zijn de enige twee organisaties die grondig onderzocht zijn en het is daarmee onbekend wat in de praktijk de beveiligingssituatie bij de rest van de overheid is. Met andere woorden: we weten niet hoe groot het probleem daadwerkelijk is. In het verleden is gebleken dat ook andere departementen hun staatsgeheimen onvoldoende beveiligd hebben. Zo heeft de Algemene Rekenkamer in het verleden gerapporteerd over onvolkomenheden bij het Ministerie van Buitenlandse Zaken in hoe wordt omgegaan met staatsgeheim gerubriceerde informatie van de EU en de NAVO.[7]

4. De wankele wettelijke basis

Een onderliggend probleem is dat de manier waarop de Nederlandse staat omgaat met staatsgeheime rubriceringen wettelijk gezien erg wankel is. De Commissie van onderzoek naar het Non Lethal Assistance (NLA)-programma in Syrië meldde in 2022 daarover het volgende:

«De bevoegdheid tot het rubriceren van informatie tot staatsgeheim is niet wettelijk geregeld, ook de criteria voor rubricering zijn niet wettelijk vastgelegd. In beginsel kan elke ambtenaar – ervaren of onervaren – de opsteller van een gevoelig stuk zijn en een voorstel tot rubricering doen.»[8]

De Commissie merkte op dat er geen duidelijke procedure bestond voor de omgang met staatsgeheim gerubriceerde informatie binnen de ambtelijke organisatie van het Ministerie van Buitenlandse Zaken, wat tot gevolg had dat deze «regelmatig» gedeeld en gearchiveerd werd «op een wijze die niet is toegestaan op basis van het rubriceringsniveau». Daarnaast kan een departement zich ook onttrekken aan parlementaire controle, geschiedschrijving en waarheidsvinding door informatie te hoog te rubriceren en daarmee niet openbaar te maken. De Kamer heeft momenteel geen instrumenten om de rubricering van staatsgeheim gerubriceerde informatie aan te vechten. Dit creëert een scheve

---

[5] NRC (2021), «NCTV volgt heimelijk burgers op sociale media».
[6] Nationale ombudsman (2024), «Blind vertrouwen?».
[7] Algemene Rekenkamer (2019), «Resultaten verantwoordingsonderzoek 2018 Ministerie van Buitenlandse Zaken».
[8] Commissie van onderzoek NLA-programma in Syrië (2022), «Rapport».

verhouding tussen de regering en het parlement, des te meer omdat in de praktijk de situatie kan ontstaan dat informatie niet actief aan de Kamer verstrekt wordt vanwege het hoge rubriceringsniveau daarvan en deze zelfs niet ter vertrouwelijke inzage aan de betreffende Kamercommissies beschikbaar gesteld wordt. Dit schaadt het parlementaire inlichtingenrecht conform artikel 68 Grondwet.

Reeds in 2010 heeft de Commissie-Davids een aanbeveling gedaan om staatsgeheime rubricering periodiek aan een toetsing te onderwerpen om te bepalen of derubricering verantwoord is. Zij stelt dat hier een taak voor de Algemeen Rijksarchivaris en het Ministerie van Onderwijs, Cultuur en Wetenschap ligt.[9]

De aanbeveling van de Commissie-Davids wordt herhaald door de Commissie van onderzoek NLA-programma in Syrië. Uit haar rapportage over de Nederlandse interventie in de Syrische burgeroorlog blijkt hoe het mis kan gaan als cruciale informatie te lang te hoog gerubriceerd blijft. De Nederlandse inzet was in strijd met het non-interventiebeginsel geldend in het internationale recht, zo concludeert de Commissie. Zij benoemt dat door het kabinet richting de Tweede Kamer «een weinig expliciet en realistisch beeld» van het NLA-programma geschetst werd, waarbij risico's niet expliciet benoemd maar juist bewust toegedekt werden. Dit leidde er volgens de Commissie toe dat de aan de Kamer verstrekte informatie het beeld van een «illusie van controle» opriep. Zo werd niet vermeld dat de door Nederland geleverde goederen ingezet konden worden in de gewapende strijd in Syrië, noch dat de regering niet zelfstandig kon vaststellen of de door Nederland gesteunde Syrische groeperingen al dan niet terroristisch of extremistisch van aard waren. Omdat cruciale informatie lange tijd staatsgeheim gerubriceerd bleef, kon de Kamer pas na herhaalde informatieverzoeken (en Wob-verzoeken vanuit de journalistiek) de voor haar controlerende taak noodzakelijke informatie boven tafel krijgen.

Ook de Commissie-Sorgdrager haalt in haar recente rapport de «hartenkreet» van de Commissie-Davids aan om rubricering periodiek te toetsen, na misstanden omtrent het achterhouden van informatie door het kabinet.[10] Lange tijd maakte deze niet bekend dat Nederland de actor was in een luchtaanval gericht op een ISIS-faciliteit in de Noord-Irakese stad Hawija in 2015. Bij deze wapeninzet waren door de ontploffing van in de faciliteit aanwezige explosieven minimaal 70 burgerslachtoffers gevallen en was een groot aantal gebouwen en huizen in de omgeving verwoest of beschadigd. Nederland hanteerde het uitgangspunt van nul burgerslachtoffers bij luchtaanvallen, maar kon het targetingproces niet zelfstandig beoordelen vanwege haar gebrek aan een eigen inlichtingenpositie en haar beperkte toegang tot inlichtingen van *Five Eyes*-partners. Dit terwijl de toenmalige Minister van Defensie aan de Tweede Kamer had gemeld dat Nederland wel toegang had tot de relevante informatie. Toen de Kamer jaren later in een technische briefing vertrouwelijk geïnformeerd werd over de wapeninzet, bleven de locatie, de datum en het aantal burgerslachtoffers onvermeld.

Ondanks dat er sprake is van een terugkerend probleem omtrent de wettelijke basis van rubriceringen, is tot op heden door de regering niets met de aanbeveling van de Commissie-Davids gedaan. De initiatiefnemers roepen de regering op om deze aanbeveling alsnog op te volgen.

---

[9] Commissie-Davids (2010), «Eindrapport van de Commissie van Onderzoek Besluitvorming Irak».

[10] Commissie-Sorgdrager (2024), «Rapport van de Commissie van onderzoek wapeninzet Hawija».

5. Een behoefte aan staatsgeheime voorzieningen

Naast de gebreken rondom toezicht en wetgeving, is er ook sprake van technische belemmeringen. Uit deels vrijgegeven ambtelijke stukken blijkt dat er een behoefte bestaat aan meer en betere voorzieningen voor het verwerken van staatsgeheimen binnen de overheid en de uitwisselen daarvan met partners.[11] Men constateert dat het landschap van geschikte ICT-voorzieningen versnipperd is en dat het onvoldoende lukt om marktpartijen aan de rijksoverheid te binden voor het ontwikkelen van dergelijke voorzieningen. Vanzelfsprekend brengt dit ernstige risico's met zich mee voor de verantwoorde omgang met staatsgeheimen binnen overheidsdepartementen. Als de veilige kanalen niet op orde zijn, worden ambtenaren gedwongen om daarvoor ongeschikte kanalen te gebruiken, die een zwakker beveiligingsniveau hebben.

Voor het beschermen van onze staatsgeheimen is het randvoorwaardelijk om de ICT-systemen op orde te hebben. Hiervoor is het nodig om als Nederland een sterke *high assurance*-industrie te hebben en de status van Nederland als autonoom cryptografieproducerend land te borgen, conform de door de regering overgenomen Kamermotie-Six Dijkstra.[12] In het kader van de nationale en internationale weerbaarheid is het van belang dat Defensie en de defensie-industrie een prominentere rol gaan spelen om de innovatie en ontwikkeling van *high assurance*-producten als sensitieve technologie te bevorderen,[13] zodat voldoende benodigde voorzieningen voor gerubriceerde informatie binnen de overheid en onder andere bij defensiepartners uitgerold kunnen worden.

6. Toewerken naar één centrale toezichthouder

Samenvattend is de wettelijke basis van staatsgeheimen onvoldoende op orde, bestaat er een behoefte aan meer en betere systemen voor het verwerken en delen van staatsgeheimen, en is het stelsel van accreditatie en toezicht, net als andere delen van de overheid, volledig departementaal verkokerd. Omdat de basis niet op orde is en niet onafhankelijk op naleving wordt toegezien, kan systematische nalatigheid jarenlang ongemerkt en ongestraft voortbestaan zolang de leiding van een departement geen prioriteit aan beveiliging stelt.
Overigens is het niet zo dat er geen enkele vorm van extern toezicht op de beveiliging van staatsgeheimen is. Voor bepaalde typen gerubriceerd informatie heeft de Nederlandse overheid wel een centrale toezichthouder aangesteld. Via internationale beveiligingsverdragen is bepaald dat ieder land binnen het betreffende samenwerkingsverband een centrale toezichthouder aanstelt in de vorm van de National Security Authority (NSA). De NSA is belast met toezicht op staatsgeheime informatie met een rubricering van de EU, de NAVO, de European Space Agency (ESA), of bilaterale samenwerkingspartners. In Nederland is dit mandaat voor niet-militaire gerubriceerde informatie belegd bij de Directeur-Generaal

---

[11] Kamerstuk 26 643-1232, bijlage «Digitaliseringsfiches incl. overzichtstabel», fiche 11 (BZK) – «digitale autonomie rijksoverheid», bijlage 2 – «Verbeteren Hoog gerubriceerde informatievoorziening (HGI)».

[12] Kamerstuk 26 643-1255.

[13] Zie Besluit toepassingsbereik sensitieve technologie: «High Assurance-producten zijn software- en/of hardwarematige informatiebeveiligingsproducten, vaak met cryptografische component, die gebruikt worden voor de bescherming van de confidentialiteit, integriteit en/of beschikbaarheid van sensitieve informatie(systemen) die door onderdelen van de Nederlandse overheid worden gebruikt. Dit omvat bijvoorbeeld gerubriceerde diplomatieke, militaire en overige gevoelige gegevens (waaronder staatsgeheimen), vitale processen en steeds meer ook gegevens die sensitief zijn vanuit het perspectief van economische veiligheid.» High Assurance is gericht op informatiebescherming volgens de hoogste beveiligingsnormen bedoeld om weerstand te bieden tegen aanvallen van statelijke actoren en andere *advanced persistent threats* (APT's).»

van de AIVD,[14] die ondermandaat[15] verleend heeft aan functionarissen van het Nationaal Bureau Verbindingsbeveiliging[16] (NBV).[17] Het NBV is vanuit deze rol ook verantwoordelijk voor de accreditatie (d.w.z.: toestemming vooraf) van de systemen die overheidsdepartementen gebruiken voor verwerking van de verschillende typen internationale staatsgeheimen.
In de praktijk is dus de situatie dat in Nederland (om verdragsrechtelijke redenen) voor toezicht op EU-, NAVO- en ESA-staatsgeheimen in de vorm van de NSA er een toezichthouder bestaat die over departementen heen een taak heeft, terwijl voor onze nationale staatsgeheimen alle toezicht binnen hetzelfde departement belegd is. Hoewel historisch verklaarbaar, is het grote verschil tussen de regimes voor toezicht op nationaal en internationaal gerubriceerde informatie onlogisch. Met het oog op de actuele en reële spionagedreiging vanuit antagonistische landen is deze bovendien niet houdbaar.
Overigens is deze probleemanalyse niet nieuw. Dit probleem werd onder andere in 2023 aan de kaak gesteld in een rapport van het adviesbureau Twynstra-Gudde in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.[18] Het rapport constateert kwetsbaarheden in hoe in Nederland staatsgeheimen beveiligd worden en doet meerdere heldere aanbevelingen, waaronder die om het toezicht op nationaal gerubriceerd materiaal gelijk te trekken met het toezicht op internationaal gerubriceerd materiaal.

Tot op heden heeft het kabinet zover bekend niets met deze aanbevelingen gedaan en ook na het lek bij de NCTV lijkt het kabinet blijkens de kabinetsreactie op het ADR-rapport niet van plan het toezicht op de beveiliging van staatsgeheimen structureel te versterken. Het kabinet lijkt onvoldoende de ernst van de zaak, door grootte van het probleem, en het belang van adequate beveiliging van staatsgeheimen voor onze binnenlandse en buitenlandse veiligheid in te zien. Bovendien laat het kabinet hiermee een kans liggen om naar aanleiding van het NCTV-lek een duidelijk signaal te geven dat ze de materie serieus neemt en de benodigde maatregelen neemt om lekken en spionage in de toekomst te voorkomen.

7. Eisen aan de toezichthouder

Gegeven de probleemstelling, bepleiten de initiatiefnemers dat er toegewerkt wordt naar één centrale onafhankelijke toezichthouder voor de beveiliging van staatsgeheim gerubriceerde informatie in Nederland, waar deze zich ook bevindt of vandaan komt.

Een toezichthouder als zodanig moet, om optimaal te kunnen functioneren, aan de volgende vijf eisen voldoen:
1. Het toezicht moet centraal en integraal zijn;
2. de toezichthouder moet doorzettingsmacht hebben;
3. het toezicht moet functioneel en rechtspositioneel onafhankelijk zijn;
4. het toezicht moet bindend zijn; en
5. het toezicht moet uniform zijn voor alle typen nationaal en internationaal gerubriceerde informatie.

---

[14] Mandaatbesluit National Security Authority, artikel 1.
[15] Mandaatbesluit National Security Authority, artikel 2 lid 1.
[16] Ook bekend als (onderdeel van) de Unit Weerbaarheid. Zie: https://www.aivd.nl/onderwerpen/informatiebeveiliging/bescherming-van-digitale-overheidsdiensten. Geraadpleegd op 27 maart 2025.
[17] Zie: https://www.aivd.nl/onderwerpen/informatiebeveiliging/verdragsrechtelijke-taken/national-security-authority-nsa. Geraadpleegd op 27 maart 2025.
[18] Twynstra-Gudde (2023), «Digitale Kroonjuwelen – Gegevens, documenten en registraties van Nationaal Belang».

Hierbij zien de initiatiefnemers een breed «real-time»- en «end-to-end»-toezicht voor zich. Hierbij is te denken aan de implementatie en uitvoering van wet- en regelgeving omtrent staatsgeheimen; de rubricering en derubricering van informatie; het beheer en de administratie van ICT-systemen, dossiers, communicatiekanalen en gegevensdragers; de wijze en frequentie van bestuurlijke verantwoording; het handelen van medewerkers; het veiligheidsbewustzijn binnen de organisatie; de actualiteit van VGB's; en de implementatie van technische risicobeheersingsmaatregelen zoals netwerksegmentatie, gebruikersmonitoring en het toekennen van afnemen van rechten. De toezichthouder moet als zodanig adequaat in staat gesteld worden om een volledig en actueel beeld te verkrijgen van de feitelijke omgang met staatsgeheimen op elk departement. Daarbij moet zij een departement kunnen verplichten om alle voor het toezicht benodigde informatie te verstrekken.

Hiernaast is het een groot voordeel (maar geen vereiste) als de toezichthouder toegang heeft tot actuele staatsgeheime dreigingsinformatie om de juiste en adequate beveiligingsmaatregelen te kunnen bepalen.

Het NBV van de AIVD, zoals eerder genoemd, is op dit moment middels het ondermandaat NSA al toezichthouder op internationaal (EU-, NAVO- en ESA-)gerubriceerde informatie. Het NBV is daarnaast reeds verantwoordelijk voor de accreditatie van de bijbehorende staatsgeheime systemen. Bovendien heeft het NBV veel kennis en expertise in huis op het gebied van beveiliging van staatsgeheimen en, als onderdeel van de AIVD, toegang tot actuele (digitale) dreigingsinformatie van o.a. statelijke actoren. Het zou daarom voor de hand liggen de NSA-rol van het NBV uit te breiden naar nationale staatsgeheimen, ware het niet dat de directeur-generaal (DG) AIVD als mandaathouder direct verantwoording aflegt aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties. Daarmee is het NBV functioneel en rechtspositioneel niet onafhankelijk van de regering, in tegenstelling tot een autoriteit of (tot op zekere hoogte) een rijksinspectie.

Voorts houdt het NBV enkel toezicht op internationale staatsgeheimen in het civiele domein, want voor het militaire domein is de NSA-taak belegd bij het Hoofd van de afdeling Beveiligingsautoriteit bij de Directie Bedrijfsvoering en Evaluatie van het Ministerie van Defensie. Een deel van deze verantwoordelijkheid is gedelegeerd aan de militaire Designated Security Authority (DSA) binnen het Bureau Industrieveiligheid (BIV) van de MIVD. Voor deze organisatieonderdelen geldt eveneens dat deze niet onafhankelijk van de regering zijn.
Dit maakt dat het niet mogelijk is het NBV aan te stellen als centrale, integrale en onafhankelijke toezichthouder. Toch is de zeer specialistische kennis van het NSA-onderdeel binnen het NBV, diens verwevenheid met de AIVD-taak tot bevordering van maatregelen «ter beveiliging van gegevens waarvan de geheimhouding door de nationale veiligheid wordt geboden»[19] en diens toegang tot staatsgeheime dreigingsinformatie te waardevol om aan dit organisatiedeel voorbij te gaan. Hetzelfde geldt mutatis mutandis voor het NSA-onderdeel binnen Defensie. Deze partijen zouden een operationele rol kunnen blijven spelen op het vlak van accreditatie, beleid en advies.

Er zal dus een nieuwe onafhankelijke toezichthouder aangesteld moeten worden. Dit zou een nieuwe, aparte instantie kunnen zijn. Een andere optie is om de toezichtstaak onder te brengen bij een reeds bestaande autoriteit. De in de ogen van de initiatiefnemers enige voor de hand liggende optie zou dan de huidige toezichthouder op de nationale

[19] Wiv 2017, artikel 8 lid 2 onder c.

veiligheid zijn, te weten de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). De CTIVD houdt toezicht op de inzet van bijzondere bevoegdheden door de AIVD en MIVD. Echter, de CTIVD heeft op het moment geen enkele toezichthoudende bevoegdheid ten opzichte van enig ander overheidsdepartement dan de inlichtingen- en veiligheidsdiensten. De inhoudelijke expertise van de CTIVD ligt bovendien op het terrein van rechtmatige inzet van bevoegdheden, en betreft daarmee niet de specialistische kennis van de beveiliging van staatsgeheim gerubriceerd materiaal. Het heeft dus wat voeten in de aarde om een centrale toezichthouder op staatsgeheimen aan te stellen. Bij de inbedding hiervan dienen zorgvuldig de voor- en nadelen van de verschillende scenario's onderzocht te worden.

8. Beslispunten

De initiatiefnemers komen tot de volgende beslispunten:

Beslispunt 1:

De initiatiefnemers bevelen aan dat de wettelijke basis voor staatsgeheimen op orde gebracht wordt. De Kamer wordt derhalve verzocht in te stemmen de regering te verzoeken:

a) per wet te regelen wie op welke gronden informatie staatsgeheim kan rubriceren en derubriceren, hoe de controle hierop plaatsvindt en welke mogelijkheden het parlement en burgers hebben om een rubricering ter discussie te stellen of ongedaan te maken, conform de aanbeveling van de Commissie van onderzoek naar het NLA-programma in Syrië;
b) een proces in te richten om rubricering aan een periodieke inhoudelijke toets te onderwerpen, conform de aanbeveling van de Commissie-Davids, eveneens benadrukt door de Commissie-Sorgdrager en de Commissie van onderzoek naar het NLA-programma in Syrië;
c) in overleg met de Kamer de tijdelijke commissie Grondrechten en constitutionele toetsing van de Tweede Kamer een expliciete taak te geven in het kunnen aanvechten van onterechte rubriceringen; en
d) de Kamer op korte termijn middels een hoofdlijnennotitie te informeren over het wetsvoorstel waarin deze procedures precies ingevuld zullen worden en over het beoogde tijdspad.

Beslispunt 2:

De initiatiefnemers bevelen aan dat een centrale, onafhankelijke toezichthouder aangesteld wordt op de omgang met alle vormen van nationaal en internationaal staatsgeheim gerubriceerde informatie binnen de overheid, inclusief politie en opsporingsdiensten, en bij toeleveranciers. Deze toezichthouder dient doorzettingsmacht en bindende bevoegdheden te krijgen. Het volledige mandaat van de NSA-rol (zowel civiel als militair) dient bij het hoofd van deze instantie belegd te worden, in plaats van bij de DG AIVD respectievelijk het Hoofd BA Defensie. De Kamer wordt derhalve verzocht in te stemmen de regering te verzoeken:

a) te onderzoeken en te bepalen wat de beste organisatorische inbedding van een toezichthouder als zodanig zou zijn, waarbij deze ofwel een nieuwe instantie zou kunnen zijn, ofwel ondergebracht zou kunnen worden bij een bestaande toezichthouder zoals de CTIVD;
b) te inventariseren bij EU- en NAVO-partnerlanden met centraal toezicht op nationaal en internationaal gerubriceerde informatie wat de *best practices* zijn en deze te verwerken in het aanstellingskader;
c) specifiek in kaart te brengen wat de benodigdheden voor het realiseren van huisvesting en Stg-werkplekken voor deze toezichthouder zijn en

indien nodig met een aanpak te komen voor het realiseren van aanvullende huisvesting;
d) de Kamer te informeren over het plan, de juridische, personele en financiële gevolgen, en het tijdspad omtrent het aanstellen van de toezichthouder;
e) te komen met de benodigde wetgeving om de toezichthoudende instantie mandaat te verschaffen, doorzettingsmacht te geven, de onafhankelijkheid van de instantie te borgen en het toezicht bindend te maken, waarin vastgelegd wordt dat «real-time» en «end-to-end»-toezicht op de omgang met, en beveiliging van, staatsgeheimen binnen het mandaat van de toezichthouder valt;
f) te komen met aanpassingen van de betreffende regelgeving, waaronder het mandaatbesluit National Security Authority, het besluit VIRBI 2013, de Rubriceringsregeling Politie 2015 en het besluit BVA-stelsel 2021; en
g) te zorgen voor voldoende mogelijkheden voor parlementaire controle, waarbij vastgelegd wordt dat de Commissie op de Inlichtingen- en Veiligheidsdiensten (CIVD) van de Tweede Kamer de geheime (bijlages van) rapportages van de Minister en verslagen van de toezichthouder ontvangt en dat de toezichthouder rechtstreeks en zonder toestemming van het kabinet mag communiceren met het parlement.

Beslispunt 3:

De initiatiefnemers bevelen aan dat de verantwoordelijkheid voor accreditatie, beleid en advies omtrent alle vormen van nationaal en internationaal staatsgeheim gerubriceerde informatie op een centraal niveau belegd wordt in plaats van op een departementaal (SG-)niveau. Bepaald dient te worden of deze coördinerende taak geheel of functioneel ondergebracht kan worden bij de huidige NSA Civiel en NSA/DSA Militair binnen het NBV van de AIVD respectievelijk de Directie Bedrijfsvoering en Evaluatie van het Ministerie van Defensie en het BIV van de MIVD. De Kamer wordt derhalve verzocht in te stemmen de regering te verzoeken:
a) te onderzoeken en bepalen welke organisatorische constructie het meest passend is voor het beleggen van de verantwoordelijkheid voor accreditatie, beleid en advies en in dit traject naast de NSA's ook BVA Rijk te betrekken;
b) een kader vast te leggen voor de (verplichte) uitwisseling van informatie tussen de coördinerende instantie(s) en de toezichthouder;
c) te onderzoeken welke instantie het meest passend is voor de accreditatie, het beleid en het advies omtrent staatsgeheim gerubriceerde informatie binnen de keten van toeleveranciers en hierbij te overwegen of het Nationaal Bureau Industrieveiligheid (NBIV), een samenwerkingsverband in oprichting tussen de AIVD en MIVD, hiervoor verantwoordelijk gemaakt kan worden; en
d) op een vastgesteld moment de gekozen constructie te evalueren, eventuele knelpunten in kaart te brengen en te bepalen of aanpassingen nodig zijn.

Beslispunt 4:

De initiatiefnemers bevelen aan dat de regering zorgdraagt voor voldoende extra beveiligde ICT-systemen om binnen de overheid staatsgeheim gerubriceerde informatie te kunnen verwerken en onderling of met bijvoorbeeld defensiepartners te delen. In het kader van de nationale (en internationale) weerbaarheid dient de ontwikkeling van *high assurance*-producten tot hoge prioriteit gesteld te worden binnen de innovatieagenda van het defensiedomein. De Kamer wordt derhalve verzocht in te stemmen de regering te verzoeken:

a) te komen met een plan van aanpak en een tijdslijn voor de realisatie van een algemene voorziening voor het verwerken en delen van staatsgeheim gerubriceerde informatie;
b) gepast nationaal industriebeleid te voeren op het onderwerp *high assurance* en zo nodig wetenschappelijk onderzoek te stimuleren; en
c) de hoofdverantwoordelijkheid voor de ontwikkeling van toekomstbestendige staatsgeheime informatiesystemen naar het defensiedomein te brengen, waarbij het Ministerie van Defensie een grotere taak krijgt ten aanzien van niet alleen het beschermen, maar ook het bevorderen van Nederlandse *high assurance*-producten en hiervoor middelen in de Defensiebegroting gealloceerd worden.

9. Conclusie

Het desastreuze lek bij de NCTV en de politie heeft laten zien dat de beveiliging van staatsgeheimen binnen onderdelen van de overheid onvoldoende serieus wordt genomen en dat de *checks and balances* hieromtrent tekortschieten. Het is een serieuze systeemkwetsbaarheid dat Nederland geen centraal toezicht kent op de omgang met staatsgeheimen door overheidsdepartementen en hun partners. In de ogen van de initiatiefnemers is het daarom noodzakelijk dat er een stevig, volledig, onafhankelijk en bindend toezicht wordt gecreëerd. Middels de door de initiatiefnemers in de aanbevelingen geschetste constructie kan hieraan worden voldaan. In aanvulling hierop is het nodig dat de wettelijke basis omtrent de rubricering en derubricering van staatsgeheimen (en de parlementaire controle daarop) verstevigd wordt, evenals dat er voldoende technische voorzieningen beschikbaar zijn en ontwikkeld worden om staatsgeheimen daar waar nodig met de hoogst mogelijke beveiligingsstandaarden te kunnen blijven verwerken en uitwisselen. Hoewel de in deze initiatiefnota voorgestelde reorganisatie ingrijpend is, is het met het oog op de toenemende statelijke spionagedreiging noodzakelijk dat er structurele verbeteringen komen in hoe we de veiligheid van onze staatsgeheimen waarborgen. We mogen niet langer accepteren dat de beveiliging van onze staatsgeheimen geen adequaat en onafhankelijk toezicht kent en dat de nationale veiligheid hierdoor mogelijk opnieuw in het gedrang komt – met onoverzienbare gevolgen.

10. Financieel kader

De voorstellen die worden gedaan in deze initiatiefnota hebben financiële gevolgen. Dit heeft ermee te maken dat wordt voorgesteld toe te werken naar één centrale toezichthouder voor de beveiliging van staatsgeheim gerubriceerde informatie.

De initiatiefnemers stellen voor structureel € 500.000 ter beschikking te stellen voor de nieuwe toezichtstaken die voortvloeien uit deze initiatiefnota en dit bedrag te dekken uit de begroting van de AIVD en MIVD, waar de huidige NSA Civiel- en DSA Militair-onderdelen onder vallen. In aanvulling daarop is het afhankelijk van het scenario en de concrete invulling hoeveel geld benodigd is voor structureel onafhankelijk toezicht.

Daarnaast worden in de initiatiefnota voorstellen gedaan over de verantwoordelijkheid voor accreditatie, beleid en advies. De initiatiefnemers stellen voor dit te dekken uit de huidige gelden die reeds op de begrotingen zijn toegewezen aan de verscheidene instanties die een taak hebben op het gebied van accreditatie, beleid en advies omtrent staatsgeheim gerubriceerde informatie, zoals de AIVD, de MIVD, het Ministerie van Defensie en de BVA Rijk.

Ten slotte opperen de initiatiefnemers dat de regie en coördinatie omtrent de ontwikkeling van *high assurance*-producten binnen de overheid en bij defensiepartners, waaronder voorzieningen voor het verwerken en delen van staatsgeheim gerubriceerde informatie, belegd wordt bij het Ministerie van Defensie en de betreffende investeringen uit de defensiebegroting gedekt worden. De geraamde kosten voor de realisatie van de benodigde ICT-voorzieningen zijn vertrouwelijk.[20]

11. Verantwoording

Deze initiatiefnota is in concept ter consultatie voorgelegd aan prof. mr. Paul Bovend'Eert, prof. dr. Bart Jacobs en mr. drs. Rowin Jansen. Het commentaar van deze experts is verwerkt in de uiteindelijke tekst.

Six Dijkstra
Omtzigt

[20] Kamerstuk 26 643-1232, bijlage «Digitaliseringsfiches incl. overzichtstabel», fiche 11 (BZK) – «digitale autonomie rijksoverheid», bijlage 2 – «Verbeteren Hoog gerubriceerde informatievoorziening (HGI)».