Rapport Beveiligingsketen militaire objecten

30 juni 2005

INHOUD

1. INLEIDING

1.1. De aanleiding

De Algemene Rekenkamer constateert eind 2003 dat de beveiliging van militaire objecten in het algemeen goed is opgezet maar dat de uitvoering daarbij 'risicovol' achterblijft[1]. Defensie start daarop in december met een verbeterprogramma en ziet nauwgezet toe op de voortgang van de verbetermaatregelen. Gelijktijdig loopt het invoeren van het nieuwe besturingsmodel. Ook dit heeft gevolgen voor de manier waarop de defensiebrede beveiligingsketen is georganiseerd. Begin 2005 wordt het nauwgezette toezicht op de verbeterinspanningen teruggedraaid en zijn de concept reorganisatieplannen van de beveiligingsautoriteit gereed.

Als op 11 april 2005 de wapenroof op de vliegbasis Gilze-Rijen wordt ontdekt laaien de oude vragen weer op. Hoe kan het dat het toch weer mis ging? Is het een incident of is er meer aan de hand? Is de informatievoorziening over beveiliging wel betrouwbaar? De Minister maakt in een kamerbrief bekend dat er een projectgroep is opgericht die zich richt op de hele beveiligingsketen van defensie.

1.2. De opdracht[2]

De projectgroep krijgt de volgende twee opdrachten.

- Formuleer concrete toekomstbestendige voorstellen voor een verbetering van de effectiviteit van de defensiebrede beveiligingsketen, waarbij de uitgangspunten van het besturingsmodel een gegeven zijn.

- Formuleer zo mogelijk concrete maatregelen (bestendigheid van zeker drie tot vijf jaar) voor de verbetering van de beveiliging op korte termijn.

1.3. De structuur van het rapport

Hoofdstuk twee beschrijft kort de werkwijze en de taakafbakening. Hoofdstuk drie belicht de defensiebrede beveiligingsketen. De knelpunten in de keten volgen in hoofdstuk vier en in hoofdstuk vijf volgen voorstellen voor een verbetering van de beveiligingsketen en enkele maatregelen voor de verbetering van de beveiliging op korte termijn.

---

[1] Concept rapport van bevindingen, officiële rapport is van 4 februari 2004

[2] Zie instellingsbeschikking, F/2005007292, 1 juni 2005, toegevoegd als bijlage B

2. WERKWIJZE

2.1. Inleiding

Dit hoofdstuk beschrijft hoe de opdracht is vertaald en afgebakend, hoe gegevens zijn verzameld en tot een afweging is gekomen.

2.2. De 'defensiebrede beveiligingsketen'

De *keten* bestaat uit de instanties die binnen defensie betrokken zijn bij *beveiliging*. Beveiliging is in het thans geldende defensie beveiligingsbeleid van 1997 onderverdeeld in fysieke beveiliging, personele beveiliging en informatiebeveiliging. Vooral de eerste twee zijn van belang zijn voor dit onderzoek[3]. Aangenomen is dat het VIR 1994 de informatiebeveiliging zeker stelt. Maar omdat informatiebeveiliging nauw is verweven met fysieke en personele beveiliging zijn ook hiervan aspecten meegenomen. Het gaat vooral om de relatie tussen beleid, uitvoering en toezicht. Dit heeft drie redenen:

- het onderzoek van de Algemene Rekenkamer in 2003 concludeert dat de uitvoering achter blijft bij het beleid;
- het nieuwe besturingsmodel leidt tot een verschuiving in de verantwoordelijkheid voor beleid, uitvoering en toezicht;
- Zowel tijdens het onderzoek van de Algemene Rekenkamer in 2003, als bij de inventarisatie van de beveiligingsmaatregelen van de wapenkamers naar aanleiding van de wapenroof in 2005 komt naar voren dat er verschillen bestaan tussen de werkelijke situatie op een object en de rapportages daarover.

De wapenroof in Gilze-Rijen zelf is geen onderwerp van onderzoek. De opslag van wapens *in het algemeen* is wel meegenomen als belangrijk onderdeel van de fysieke beveiligingsketen.

2.3. Onderzoeksvragen

- Hoe zijn de fysieke, personele en informatiebeveiligingsketens georganiseerd? (hoofdstuk drie)
- Welke knelpunten doen zich voor in beleid, (uitvoering) en toezicht en de relatie tussen deze functies? (hoofdstuk vier)
- Wat wordt aan die knelpunten gedaan en welke aanvullende maatregelen zijn nodig? (hoofdstuk vier en vijf)

---

[3] Fysieke beveiliging is het totaal van organisatorische, bouwkundige en elektronische maatregelen (OBE-mix). Personele beveiliging omvat de screening van in- en extern personeel

2.4. Een eerste stap.

Het onderzoek richt zich niet direct op de uitvoering[4], maar op de keten als randvoorwaarde voor een goede uitvoering. Als de keten goed is ingericht kan de keten zelf de uitvoering verder verbeteren. Dit onderzoek moet daarom worden gezien als een eerste stap, waarmee een tweede stap mogelijk wordt.

2.5. Interviews en klankbordgroep

De zeven defensieonderdelen, de PCDS en de deskundigen die bij het uitvoeren en toezicht zijn betrokken (ADD, MIVD, DIO, DICTU en de beveiligingsautoriteit) zijn geïnterviewd In de bijlage A is de leidraad voor de interviews opgenomen. Gesproken is met zowel de verantwoordelijken (beveiligingscoördinatoren) als met de uitvoerders op defensieonderdeels-stafniveau. Daarnaast zijn eerdere onderzoeken, reorganisatievoorstellen, de verbetermonitor van de DFEZ, toprapportages etc. gebruikt. Twee maal kwam de klankbordgroep bijeen om de bevindingen en aanbevelingen door te spreken.

2.6. Relatie met andere initiatieven

De Algemene Rekenkamer is in mei begonnen met het 'vervolgonderzoek beveiliging militaire objecten'. De Algemene Rekenkamer onderzoekt de positie van de beveiligingsautoriteit, de screening van in- en extern personeel en de informatievoorziening aan de minister. De Algemene Rekenkamer stelt de vraag of de Minister van Defensie ervoor gezorgd heeft dat de beveiliging van militaire objecten in opzet en werking voldoen aan het ambitieniveau. Hiervoor worden de zes objecten die in 2003 niet bleken te voldoen bezocht en nog eens tien andere objecten.

Na de wapenroof op Gilze-Rijen heeft de Minister onmiddellijk laten inventariseren of de beveiliging van alle wapenkamers en munitiecomplexen van Defensie daadwerkelijk voldoet aan de beveiligingsnormen. Dit heeft tot enkele aanvullende korte termijn maatregelen geleid.

Het Coördinatieberaad Nationale Taken en Terrorismebestrijding werkt aan een herziening van het terrorismebestrijdingbeleid Beveiliging maakt een belangrijk onderdeel uit van dit beleid.

[4] Het onderzoek is beperkt in tijd en capaciteit. Onderzoek naar de daadwerkelijke stand van zaken op objectniveau kan, gezien de breedte van het onderzoek, daardoor niet worden meegenomen. De ADD en de Algemene Rekenkamer doen wel steekproeven op het objectniveau.

3. DE DEFENSIEBREDE BEVEILIGINGSKETEN

3.1. Inleiding

In dit hoofdstuk wordt de defensiebrede beveiligingsketen beschreven: de organisatiestructuur de organisatiedelen, de processen fysieke beveiliging, personele beveiliging en informatiebeveiliging, de verbeteraanpak van de afgelopen 1½ jaar en enkele ontwikkelingen rond de keten. Het is gebaseerd op het defensie beveiligingsbeleid van 1997.

3.2. De kern van de beveiligingsketen, een dubbele structuur.

- De secretaris-generaal is verantwoordelijk voor het vaststellen van het beveiligingsbeleid. De beveiligingsautoriteit ontwikkelt en evalueert namens de secretaris-generaal het beveiligingsbeleid, draagt dit over aan de defensieonderdelen en ziet toe op de deugdelijkheid van de beveiliging bij de defensieonderdelen.

- De commandanten van de defensieonderdelen zijn verantwoordelijk voor de uitvoering van de beveiliging en hebben hiervoor een beveiligingscoördinator aangewezen. De coördinatoren stellen namens de commandanten het krijgsmachtdeelbeleid / defensieonderdeelbeleid vast en controleren de uitvoering hiervan en bepalen tevens namens de bevelhebber het te accepteren risico[5].

- De lagere commandant is verantwoordelijk voor de uitvoering, controle en evaluatie van de beveiliging binnen zijn eenheid en kan hiervoor een veiligheidsfunctionaris aanwijzen. Hier is de structuur van de keten gebaseerd op het krijgsmachtdeelbeleid / defensieonderdeelbeleid, waardoor op dit niveau verschillen optreden.

3.3. Toezichthouders in de keten

Naast het externe toezicht door de Algemene Rekenkamer worden controles uitgevoerd door:

- de leidinggevenden, die toezicht houden door eigen inspecties, met name in het operationele domein;

- de ADD, waar één medewerker belast is met de “onafhankelijke toezichtsrol” voor fysieke beveiliging en zes medewerkers belast zijn met toezicht op de informatiebeveiliging;

- de beveiligingsautoriteit als beleidsmaker, die de uitvoering van het beleid toetst;

[5] Doordat er keuzevrijheid is voor de defensieonderdelen om objecten in één van de standaard risicocategorieën in te delen. Ook accepteren zij in voorkomende gevallen restrisico.

- de afdeling onderzoeken interne beheersing, die binnen de defensieonderdelen onderzoek doet naar de beveiligingsketen;

- de veiligheidsfunctionaris, die tot op objectniveau de beveiligingsmaatregelen controleert.

3.4. Uitvoerende en toeleverende schakels in de beveiligingsketen

- De uitvoering van de bewakingstaak is in handen van de KL-bewakingsorganisatie, het marine bewakingskorps, ingehuurde bedrijven en bewakingseenheden van de KLu.

- De MIVD doet de veiligheidsonderzoeken voor defensiepersoneel op veiligheidsfuncties en bij ABDO-bedrijven, administreert de resultaten (verklaring van geen bezwaar), handelt bezwaarschriften af bij het niet verlenen of intrekken van de verklaring van geen bezwaar en levert dreiginginformatie. De MIVD maakt nadrukkelijk geen risicoanalyse.

- De CDS heeft (in de toekomst nog meer) een rol bij behoeftestellingen (uitgezonderd informatiebeveiliging: DIO) en is verantwoordelijk voor wapenbeheer en beveiliging in uitzendgebieden. De CDS maakt ook de risicoafweging en bepaalt de alerteringsstatus in Nederland.

- DIO en DICTU hebben een grote rol bij de technische invulling van informatiebeveiliging (standaardisatie etc). Informatiebeveiliging is niet los te zien van fysieke en personele beveiliging.

- De HDP beheert Peoplesoft en maakt het administreren van veiligheidsonderzoeken in dat systeem in de toekomst mogelijk.

- De DAB coördineert de ontwikkeling van beleid rond nationale taken en de bestrijding van het terrorisme. Dit heeft raakvlakken met de fysieke beveiliging en het beveiligingsbeleid, zoals de ontwikkeling van het “alerteringssysteem terrorisme”.

- De DMO heeft veel fysieke objecten onder beheer, waaronder veel munitie- en wapenopslagplaatsen.

- De DGW&T heeft een belangrijke rol in het realiseren van bouwtechnische en elektronische beveiligingsmaatregelen.

De manier waarop deze schakels samenwerken is in de volgende paragrafen uitgewerkt in de processen fysieke-, personele- en informatiebeveiliging.

3.5. Het proces fysieke beveiliging

- **Belang vaststellen**. Het belang van een object wordt uitgedrukt in categorieën van CAT-1 (hoogste belang) tot CAT-4. Dit is een verantwoordelijkheid van de lijn. De krijgsmachtsleutelpuntenlijst is een tweede instrument om de belangen vast te stellen. Hierbij ligt de nadruk op het operationele belang, dat wordt vastgesteld door operationele commandanten.

- **Dreiging**. Er was een jaarlijkse generieke dreigingsanalyse van de MIVD. Dit jaar is dat veranderd: vanaf nu brengt de MIVD twee maal per jaar de Cintrep-dreigingsbeeld terrorisme Nederland uit. De MIVD levert verder vooral dreigingsanalyses tegen specifieke objecten. In aanvulling daarop is in 1999 door de krijgsmachtdelen een daderprofiel opgesteld. Een goed beeld van de dreiging is een belangrijk gegeven voor de risicoanalyse: 'waartegen moet ik beveiligen?' Dit daderprofiel is niet formeel vastgesteld.

- **Risicoanalyse**. Het defensiebeveiligingsbeleid schrijft een risicobenadering voor bij het vaststellen van de benodigde beveiligingsmaatregelen per object. Voor informatiebeveiliging is er een voorgeschreven instrument voor de risicoanalyses: CRAMM, waaruit (als nevenproduct) ook maatregelen voor de fysieke beveiliging komen. Voor fysieke beveiliging zelf is er geen defensiebrede standaard. De defensieonderdelen gebruiken wel een eigen standaard, bijvoorbeeld de integrale veiligheidszorg systematiek bij de KL.

- **Beveiligingsplan opstellen.** In de beveiligingsplannen staan de te nemen maatregelen die uit de risicoanalyse naar voren zijn gekomen. Omdat er geen defensiebrede risicoanalyse methode voor fysieke beveiliging is komen de beveiligingsplannen per defensieonderdeel op een eigen manier tot stand.

- **Fysieke beveiliging uitvoeren.** Het uitvoeren van organisatorische, bouwkundige en elektronische (OBE) maatregelen die in de plannen zijn opgenomen. Bij het uitvoeren van bouwkundige en elektronische maatregelen zijn onder andere DGW&T, DTO en particuliere firma's betrokken. OBE maatregelen vullen elkaar aan. Een commandant kan besluiten OBE maatregelen niet uit te voeren en accepteert daarmee een groter beveiligingsrisico.

- **Toezicht houden.** Toezicht is trapsgewijs georganiseerd: er is toezicht door Algemene Rekenkamer, de ADD, DFEZ[6], de OIB van de defensieonderdelen, de beveiligingsautoriteit, de beveiligingscoördinator

[6] Voor wat betreft het verbeterprogramma van 2004

de veiligheidsfunctionaris en de lijn functionaris. Daarbij kijken de verschillende instanties naar verschillende punten in het proces.

3.6. Het proces personele beveiliging

- **Veiligheidsmachtigingsniveau toekennen**. Dit is een verantwoordelijkheid van de lijn. De vereiste machtiging voor functies wordt vastgesteld met een format van de MIVD. Dit is niet dwingend voorgeschreven maar een hulpmiddel. De MIVD toetst incidenteel bij het uitvoeren van veiligheidsonderzoeken of functies juist zijn gewaardeerd.

- **Veiligheidsonderzoeken uitvoeren**. Het gaat om initiële en herhalingsonderzoeken. De onderzoeken worden door de MIVD uitgevoerd en er bestaan afspraken over de doorlooptijd[7]. Een onderzoek resulteert in het al dan niet verstrekken van een verklaring van geen bezwaar.

- **De externe screening.** Ook personeel dat tijdelijk bij defensie werkt moet worden gescreend als zij in aanraking kunnen komen met gevoelige informatie. Bedrijven die defensieopdrachten uitvoeren moeten in sommige gevallen voldoen aan de ABDO-regeling en komen voor een deel ook voor screening door de MIVD in aanmerking.

- **Personele informatie beheren**. Dit gebeurt nu nog overal op basis van eigen database of toepassingen (zoals IVAN-3). De bedoeling is dat het beheren van aan veiligheidsmachtigingen gerelateerde informatie onderdeel wordt van Peoplesoft.

- **Toezicht op het onderzoek en beroepsmogelijkheid.** Na het niet verstrekken of intrekken van een verklaring van geen bezwaar bestaat er een beroepsmogelijkheid. De behandeling ervan is ondergebracht bij de MIVD.

3.7. Het proces informatiebeveiliging

- Een nieuw informatiesysteem wordt beoordeeld op onder andere beveiligingsaspecten door de DIO. Deze beoordeling is opgenomen in de kaders van de Defensie informatie voorzienings architectuur.

- Als er beveiligingsaspecten zijn is het aan de beveiligingsautoriteit om daarvoor criteria vast te stellen. Als die criteria er nog niet zijn, vraagt de DIO aan de beveiligingsautoriteit die te ontwikkelen. Dat is bijvoorbeeld bij de PDA's en USB-poorten gebeurd.

[7] De wettelijke termijn in acht weken. Afgesproken is dat de minder diepgaande onderzoeken in twee tot drie weken worden afgerond.

- De rollen bij de ontwikkeling van informatiesystemen zijn alsvolgt: de DIO is opdrachtgever en de DICTU neemt de opdrachten in projectvorm aan. Momenteel lopen er bij DICTU zes projecten die aan beveiliging gerelateerd worden. In deze gevallen is de beveiligingsautoriteit de behoeftesteller. DTO of de industrie voeren de projecten uit. Nadat de projecten zijn afgerond worden de informatiesystemen in beheer genomen, soms door DICTU.

- Voor bestaande systemen geldt dat elke lijnmanager / systeembeheerder (Defensie gebruikt 3300 applicaties) informatiebeveiligingsplannen moet maken. Dit is opgelegd door het VIR 1994 en een lijnverantwoordelijk. Defensie heeft ervoor gekozen dat met het CRAMM instrument te doen. Door enige bundeling zijn 800 beveiligingsplannen opgesteld met daarin duizenden maatregelen. Hier heeft de beveiligingsautoriteit de rol van normsteller.

- De informatiebeveiligingsplannen worden op toereikendheid getoetst door de ADD.

- Bij systemen met externe koppelingen of die hoog geclassificeerde gegevens bevatten moet voor de daadwerkelijke ingebruikname accreditatie plaatsvinden door zorg van de beveiligingsautoriteit.

- De beveiligingsautoriteit schakelt hiervoor wederom de ADD in, die nagaat of de maatregelen in de informatiebeveiligingsplannen daadwerkelijk zijn genomen. Omdat het gaat over duizenden maatregelen gebruikt men hiervoor steekproeven.

- Omdat informatiesystemen kunnen veranderen moeten elke twee jaar de informatiebeveiligingsplannen worden herzien.

3.8. Verbeteren van de beveiliging met de FIMAB-methode

De beveiligingsautoriteit heeft in 2003 de onderwerpen die door de Algemene Rekenkamer zijn genoemd uitgewerkt voor de defensieonderdelen[8]. De defensieonderdelen (toen nog zonder de CDC en DMO, maar wel met DICO) vertaalden die in eigen verbeterplannen, waarvan medio december 2003 de eerste versies worden opgeleverd.

De aanpak volgt de FIMAB-methode[9] waarbij de bedoeling is dat de verbeterplannen van de defensieonderdelen procesmatig (DFEZ) en inhoudelijk (beveiligingsautoriteit) gemonitord worden. Hiervoor wordt maandelijks een voortgangsrapportage verstuurd door de defensieonderdelen aan de DFEZ en de beveiligingsautoriteit. Dit komt bovenop de reguliere rapportages.

---

[8] Nota BA / 2003008015, dd 20 november 2003, aanpak beveiligingsrisico's.

[9] De methode die eerder gebruikt is om het financiële en materiele beheer in orde te brengen. Essentie: decentrale verantwoordelijkheid en nauwgezet en systematisch volgen van de verbeteringen.

Tijdens het verbeterproces zijn er in maart, juni en december gesprekken gevoerd tussen de beveiligingsautoriteit, DFEZ en de beveiligingscoördinatoren over de voortgang. In oktober 2004 deed de ADD een onderzoek, waarbij een steekproef wordt genomen op dezelfde wijze als de Algemene Rekenkamer deed in 2003.

Dit onderzoek levert voldoende zekerheid op om in december de maandelijkse rapportagecyclus te verlaten en de nog openstaande actiepunten in de verbeterplannen bedrijfsvoering op te nemen.

In december 2004 stelt de beveiligingsautoriteit het kwaliteitsplan beveiliging 2005 e.v. op. Het beoogt de kwaliteit van de beveiliging niet alleen te handhaven maar ook 'structureel en duurzaam' op een hoger niveau te brengen. Het is mogelijk dat elementen uit het kwaliteitsplan als verbeterpunten worden opgedragen aan de defensieonderdelen, maar dat is nog niet gebeurd.

3.9. Overige ontwikkelingen

- Na de aanslagen in Amerika op 11 september 2001 zijn veel initiatieven genomen op het gebied van beveiliging. Voor defensie zijn die uitgewerkt in het actieplan Defensie en Terrorisme. Hierin werden tientallen maatregelen afgekondigd. Medio 2004 stelde de directie beleidsevaluatie vast dat het merendeel van die maatregelen nog 'in uitvoering' was. De DAB werkt momenteel aan een actualisatie van het actieplan.

- De hernieuwde belangstelling voor beveiliging, in combinatie met de wens beveiliging minder belastend voor de bedrijfsvoering te maken en de mogelijkheden van de technologie is een andere belangrijke drijfveer, die binnen Defensie ook zichtbaar is. Bijvoorbeeld biometrie-toepassingen, waarmee op Schiphol ervaringen worden opgedaan, het IVZ-concept van de KL, waarmee de KL zwaarder dan voorheen leunt op elektronische beveiligingsmaatregelen. Het gebruik van Peoplesoft voor personeelsbeveiliging en het ontwikkelen van instrumenten door TNO voor het standaardiseren van de criteria voor fysieke beveiligingsplannen.

- Het project SAMSON A16D, herinrichting integrale beveiliging, dat geleid heeft tot een geplande uitbreiding van de beveiligingsautoriteit met twee VTE'n. Het oprichten van een dienstencentrum is vertraagd, de discussie hierover loopt nu onder leiding van de beveiligingsautoriteit.

3.10. Samenvatting

De beveiligingsketen bestaat uit veel spelers en er zijn veel ontwikkelingen. Kenmerkend, maar niet ongebruikelijk binnen defensie, is de dubbele structuur: de 'lijn' die verantwoordelijk is naast de functionele lijn, waarin de vakkennis is georganiseerd. Een opvallend punt is de vrijheid voor defensieonderdelen voor het invullen van het defensie beveiligingsbeleid door lokale regelgeving.

4. BEVINDINGEN

4.1. Inleiding

In hoofdstuk drie zijn de defensiebrede beveiligingsketen, de drie processen en het verbetertraject geschetst. In dit hoofdstuk worden knelpunten gesignaleerd. Het gaat hier uitdrukkelijk om de mening van de onderzoekers.

4.2. Beveiliging, een kwestie van attitude

- Als beveiliging goed is geregeld oogst de verantwoordelijke functionaris geen waardering. Problemen trekken echter wel brede aandacht. Beveiliging is daarom geen 'populair' onderwerp. Dit legt druk op de coördinatie door de beveiligingsexperts: het is vaak een kwestie van 'trekken en duwen' en vragen om managementaandacht uit de 'verantwoordelijkheidslijn'.

- Er moet veel aandacht aan calamiteiten besteed worden. Calamiteiten werken als een aanmoediging maar als de storm voorbij is zakt de aandacht weer weg.

- Door de beperkte omvang van de functionele lijn worden beleidsmatige, uitvoerende en toezichthoudende taken overgelaten aan andere spelers in de keten waarvoor beveiliging in meer of mindere mate een neventaak is.

- Beveiliging is een zaak van iedereen, maar bewustzijn op de dagelijkse werkplek laat te wensen over[10]. De uitvoerende beveiligingsfunctionarissen zijn hier wel van afhankelijk.

- Het aspect beveiligingsbewustzijn krijgt weinig aandacht bij de initiële militaire opleidingen (enkele uren). Dit is een verantwoordelijkheid van de operationele commandant, immers hij heeft het beheer over het militair personeel. Wel speelt beveiligingsbewustzijn een rol als 'opvoedend' element tijdens de opleiding. Beveiligingsspecialisten geven ook gastlessen.

- Niet is aangetroffen dat instromende burgermedewerkers op een vergelijkbare manier kennis over beveiliging meekrijgen. Dit is een verantwoordelijkheid van de lijnmanagers van de defensieonderdelen.

- De DICTU voert het project 'beveiligingsbewustwording' uit. Hierbij wordt een instrument ontwikkeld voor de beveiligingscoördinatoren. Die kunnen daarmee zelf beveiligingsbewustzijnscampagnes opzetten. Dit project heeft minder voortgang gemaakt dan verwacht, omdat het moeite kostte om

[10] Een respondent merkte op dat het veiligheidsbewustzijn tijdens een missie goed is, en dat een militair thuis ook om veiligheid denkt. Maar eenmaal achter zijn bureau wordt het een taak voor de veiligheidsfunctionaris.

samen met de defensieonderdelen tot een programma van eisen te komen. Uiteindelijk heeft de projectorganisatie de knoop doorgehakt. Begin 2006 is dit project klaar. Het project richt zich op informatiebeveiliging, waarbij ook de uit informatiebeveiliging voortkomende fysieke en personele beveiligingsmaatregelen zijn meegenomen.

- Defensieonderdelen hebben het defensiebrede project beveiligingsbewustwording niet afgewacht. Er wel degelijk initiatieven genomen[11].

Subconclusie: de afhankelijkheid van functionele lijn van de andere schakels in de beveiligingsketen is een permanent risico gezien de attitude ten aanzien van beveiliging.

4.3. De beveiligingsautoriteit, een autoriteit?

- De ketenverantwoordelijken voor beveiliging komen niet bij elkaar. Het 'hoogste' overleg is het beveiligingsautoriteit / beveiligingscoordinator overleg, waarin de beveiligingsautoriteit niet met de beveiligingscoördinatoren, zoals de bedoeling is, maar met de uitvoerders, beveiligingsexperts op defensieonderdeelniveau praat. Dat komt omdat de beveiligingscoördinatoren vinden dat het overleg te veel over het detail van de uitvoering gaat. De beveiligingsautoriteit vindt het niet deelnemen van de beveiligingscoördinatoren zelf geen probleem, zolang de deelnemers maar beslissingsbevoegd zijn.

- De beveiligingsautoriteit stond altijd aan de zijlijn, ondanks de rol die het defensie beveiligingsbeleid aan de beveiligingsautoriteit toedichtte. De beveiligingsautoriteit had tot voor kort ook niet de ambitie om daar iets aan te doen. Dat is pas veranderd na het invoeren van het nieuwe besturingsmodel. De ambitie is er nu wel, maar de reorganisatieplannen en het nieuwe beleid weerspiegelen deze opzet nog onvoldoende.

- De beveiligingsautoriteit is vooral zichtbaar voor de defensieonderdelen na een calamiteit.

- De beveiligingsfunctionarissen zelf zijn bijna unaniem van mening dat de kennis en de capaciteit van de beveiligingsautoriteit onvoldoende is om als voortrekker te fungeren. Vragen aan de beveiligingsautoriteit blijven soms te lang liggen of worden gesteld aan anderen in de beveiligingsketen. Defensieonderdelen hebben eigen expertisecentra. Beveiligingsexpertise zit ook nog bij ADD, DGW&T, MIVD, DTO en DIO.

- In lijn met het nieuwe besturingsmodel zou het defensie beveiligingsbeleid uitvoerbaar beleid moeten worden. De beveiligingsvoorschriften van de

[11] Bijvoorbeeld het uitbrengen van een veiligheidsagenda 2005 bij de KL.

krijgsmachtsdelen kunnen dan vervallen. Nieuw beleid (defensie beveiligingsbeleid 2005) is in ontwikkeling[12].

Subconclusie: de beveiligingsautoriteit is in de opzet (zeker met het nieuwe besturingsmodel) wel de centrale spil, maar de verbindende elementen (kennis, beleid en toezicht) in de keten zijn te zwak[13]. De beveiligingautoriteit moet centraal uitvoerbaar beleid maken, daadwerkelijk zicht hebben op de uitvoering en de kennis in het vakgebied bundelen.

4.4. Terrorisme en beveiliging

- De DAB heeft de regie over 'nationale taken en terrorismebestrijding' op zich genomen nadat een onderzoek medio 2004 over het actieplan defensie en terrorisme aantoonde dat er geen regie was. De DAB zet beleidsmatig de lijnen uit via het coördinatieberaad nationale taken en terrorismebestrijding. In een werkgroep worden beveiligingszaken aangepakt.

- De beveiligingsautoriteit heeft aangegeven niet de capaciteit te hebben om in die discussie zijn rol *als beveiligingsautoriteit* op zich te nemen[14]. De beveiligingsautoriteit is wel in de werkgroep vertegenwoordigd.

- De nationale coördinator terrorismebestrijding (NCTB) ontwikkelt de dreiging terrorisme Nederland (DTN). Het is bedoeld als naslagwerk dat het bestaande algemene dreigingsprofiel aanvult. De MIVD heeft hieraan een bijdrage geleverd.

- Er zijn verschillende interdepartementale overleggen, die in onderling verband optreden. De directeur juridische zaken neemt deel aan de interdepartementale 'evaluatie driehoek'. Hierin worden besluiten genomen over te nemen beveiligingsmaatregelen, die door het 'uitvoeringsoverleg' zijn geadviseerd. Hierin zitten namens defensie vertegenwoordigers van de defensiestaf, de KMar en de BSB. In het 'afstemmingsoverleg bewaken en beveiligen' neemt namens defensie de MIVD deel. In dit overleg wordt over dreiging en risico gesproken en informatie uitgewisseld. Er is geen directe lijn naar de beveiligingsautoriteit wanneer die nodig is, bijvoorbeeld bij een dreiging tegen een defensieobject, of wanneer de alertering moet worden gewijzigd.

- De aansluiting van het defensie alerteringssysteem op het nationale alerteringssysteem terrorisme is nog niet rond. Defensie moet zich hierin actief opstellen, met als inzet om het defensiesysteem sterk te laten gelden bij de afstemming.

---

[12] De defensieonderdelen kregen het concept DBB 2005 tijdens ons onderzoek voor het eerst te zien, waardoor een aantal respondenten zich hierover nog geen mening hadden gevormd.

[13] Zie ook vorige paragraaf

[14] Het gaat hier niet om de coördinerende rol van de DAB

Subconclusie: De beveiligingsautoriteit heeft een te beperkte rol in de doorontwikkeling van het beleid rond Defensie en terrorisme en neemt niet deel aan de interdepartementale overlegstructuren op dit terrein.

4.5. De rol van de CDS

- De CDS kan zijn trechterrol uitoefenen door bij het opstellen van beleid de uitvoerbaarheid te toetsen. Dat betekent niet dat de CDS de huidige rol van de defensieonderdelen overneemt: het 'vertalen' van het beleid[15].

- Bij alarmering en het afkondigen van verscherpte beveiligingsmaatregelen is een integrale afweging nodig omdat de middelen voor beveiliging ook gebruikt kunnen worden voor operationele inzet. Daarom kan alleen de CDS dit goed beoordelen.

- De CDS maakt de risicoafweging. De beveiligingsautoriteit adviseert de CDS bij het nemen van maatregelen. De MIVD levert daarvoor de dreigingsappreciatie aan op het gebied van spionage, subversie, sabotage en terrorisme.

Subconclusie: De CDS kan zijn trechterrol invullen zonder dat daarmee de beleidsbepalende rol van de beveiligingsautoriteit in het geding komt. De CDS heeft een primaire rol bij de afweging van belangen bij inzet.

4.6. De defensieonderdelen, behoefte aan eenduidigheid

- Het (nieuwe) beleid en het kwaliteitsplan geven nog niet die eenduidigheid en voor de uitvoering bruikbare normen waar behoefte aan is.

- Standaardisatie is maar deels mogelijk. Hoe verder gestandaardiseerd wordt, en hoe concreter het beleid wordt, des te minder recht kan worden gedaan aan de lokale omstandigheden. Uitvoerbaar beleid maken kan alleen als de eenduidige normen de mogelijkheid voor uitzonderingen in de uitvoering openlaat.

- Elk defensieonderdeel heeft zijn eigen beveiligingsvoorschrift, dat bovendien van elkaar verschilt[16]. Dat merken vooral CDC en DMO, die de

---

[15] Voor de duidelijkheid en vooruitlopend op hoofdstuk vijf: die vertaalslag behoort ook te verdwijnen bij de defensieonderdelen.

[16] bijvoorbeeld KL. De KL heeft het beveiligingsbeleid moeten herzien omdat het niet meer kon terugvallen op dienstplichtigen voor de beveiliging. Dit kreeg gestalte in het Integrale veiligheidszorg concept (IVZ), met de bedoeling om met een mix van maatregelen een hoge graad van veiligheid te halen tegen de laagst mogelijke kosten. Daarbij komen ook brandweer, ARBO en milieuaspecten aan de orde. IVZ is gebaseerd op de Haagse Methodiek (DHM ™).

door de krijgsmachtdelen overgedragen organisatiedelen op één standaard willen brengen. Dat is vooral lastig bij fysieke beveiliging.

- De meeste defensieonderdelen verwachten dat er uiteindelijk een defensiebreed bewakingscorps komt.

- De verantwoordelijkheid voor de uitvoering van de beveiliging ligt nu bij de commandanten en moet daar ook blijven liggen, ook na de eventuele komst van een defensiebreed bewakingscorps.

- In het concept defensie beveiligingsbeleid 2005 worden industrieveiligheid en documentveiligheid geïntroduceerd als hoofdaandachtsgebieden, naast de bekende fysieke, personele en informatiebeveiliging. Deze verbijzondering is onnodig: industrieveiligheid omvat alle aspecten van fysieke, personele en informatiebeveiliging maar wordt toegepast op civiele bedrijven. Documentveiligheid is een aspect van informatiebeveiliging.

- Beveiligingsexpertise is schaars. Binnen Defensie zijn maar enkele 'echte' beveiligingsexperts werkzaam. Inlichtingen en veiligheid is alleen bij de KLu een separaat vakgebied, de MIVD streeft ernaar het vakgebied bij de andere krijgsmachtdelen ook zo in te vullen.

- De defensiestaf heeft een studie verricht naar een overkoepelend 'intelligence corps' zoals vele landen dit kennen. Hierin zijn zowel inlichtingen als veiligheidsfunctionarissen vertegenwoordigd.

Subconclusie: De defensieonderdelen hebben behoefte aan centrale aansturing door de beveiligingsautoriteit en ondersteuning met expertise Er lijken geen zwaarwegende bezwaren te zijn om toe te werken naar een defensiebreed bewakingscorps.

4.7. Uitvoering fysieke beveiliging

- De attractieve wapens worden nu niet als CAT-1 aangemerkt[17]. De mogelijke imago schade is echter groot en dit zou zwaarder in de risicoafweging moeten worden meegewogen.

- De krijgsmachtsleutelpuntenlijst is eind 2002 aangeboden bij het ontwikkelen van een defensiebreed calamiteitenplan (maatregel van de taakgroep defensie en terrorisme). De sleutelpuntenlijst is niet actueel. Het beheer is nog niet goed geregeld[18]. De relevantie van de

[17] Attractief is niet gedefinieerd, maar zou kunnen omvatten: wapens waarmee eenvoudig aanslagen of overvallen mee kunnen worden gepleegd, zoals explosieven, ontstekers, handgranaten, klein kaliber wapens en draagbare lanceersystemen e.d.

[18] Dit werd 1 jaar geleden ook al geconstateerd bij het onderzoek naar de realisatie van het terrorismebestrijdingbeleid

krijgsmachtsleutelpuntenlijst is met het in leven roepen van de Nationale coordinator bewaken en beveiligen niet meer wat hij vroeger was.

- De perspectief voor het bepalen van het belang van een object op de krijgsmachtsleutelpuntenlijst is anders dan bij de CAT-1 tot CAT-4 indeling. Toch zouden de verschillen tussen beide methoden bij juist gebruik klein moeten zijn.

- Het daderprofiel is een belangrijk uitgangspunt voor de te nemen beveiligingsmaatregelen. Het profiel dat is opgesteld in 1999 werd herzien door een werkverband van de defensieonderdelen. Dit heeft sinds eind 2003 stilgelegen. De behoefte werd weer actueel nadat TNO voor de ontwikkeling van criteria voor fysieke beveiligingsplannen een formeel daderprofiel nodig had. Het profiel is nog niet rond.

- Technisch is steeds meer mogelijk. Het accent in de OBE-mix verschuift langzaam en onder (externe) druk naar meer elektronische oplossingen en minder organisatorische (personeelsafhankelijke) oplossingen[19]. Dat heeft als voordeel dat met minder personeel meer beveiligd kan worden[20]. Elektronische maatregelen maken organisatorische maatregelen echter niet overbodig. Een voorbeeld hiervan is de Smartcard, die door slecht beheer als beveiligingsmaatregel minder effectief is geworden.

Subconclusie: Bij de uitvoering zijn enkele concrete maatregelen nodig, die geen direct effect hebben op de structuur van de keten.

4.8. Uitvoering personele beveiliging

- De defensieonderdelen constateren op basis van eigen gegevens dat de achterstand in de veiligheidsonderzoeken vrijwel is ingelopen.

- Het wachten is op beheersfunctionaliteiten bij Peoplesoft[21]. De meeste defensieonderdelen overbruggen de periode met eigen beheersinstrumenten. Het is een risico om juist tijdens grootschalige reorganisaties het beheer van personele gegevens niet centraal te regelen.

- De afhandeling van bezwaarschriften bij intrekking van de verklaring geen bezwaar is sinds het opheffen van de ABG in handen van een oud-medewerker van de MIVD. Om te voorkomen dat hierdoor de MIVD het

[19] Bijvoorbeeld bij de KMAR (biometrie) en de KL (MIPSS)

[20] Iemand merkte op: 'om te voorkomen dat over enkele jaren de aandacht voor beveiliging weer verslapt, zou je zoveel mogelijk routinetaken in systemen moeten borgen.

[21] Er lopen twee initiatieven voor het standaardiseren van de personele beveiliging. De KLu propageert het defensiebreed als standaard opnemen van IVAN-4, wat op Peoplesoft kan worden aangesloten. De KM neemt IVAN-4 over. De BA wil Peoplesoft. De KL neemt deel aan een onderzoek naar de invoering van een module in Peoplesoft.

eigen werk moet beoordelen wil de MIVD dit laten uitbesteden aan het Centrum Arbeidsverhoudingen (CAOP). Dit kost geld, terwijl binnen defensie onafhankelijke capaciteit beschikbaar is voor dit werk bij JuZa-P.

- De DMO heeft onlangs geïnventariseerd welke projecten er lopen waarvoor de ABDO regeling van toepassing is.

Subconclusie: Voor een correcte afhandeling van bezwaarschriften moet de keten worden aangepast. Het centraliseren van de gegevens met Peoplesoft vertraagd.

4.9. Uitvoeren informatiebeveiliging

- Beveiligingsfuncties worden ingevuld door niet beveiligingsdeskundigen. De kennis moet aangevuld worden door inhuur, met name bij het opstellen van informatiebeveiligingsplannen[22]. Door gebruik te maken van inhuur is voor de informatiebeveiliging noodzakelijke kennis weer deels verloren gegaan.

- De beveiligingsautoriteit heeft met het project IBI een aanpak ontwikkeld die het opstellen van nieuwe en het updaten van bestaande beveiligingsplannen aanmerkelijk vereenvoudigt. Er zijn 400 plannen ‘over elkaar heen gelegd’ waarna bleek dat die voor 95% binnen vijftien standaard beveiligingsniveaus onder te brengen zijn met een relatief eenvoudige beslissingsboom. Hierdoor wordt de ontwikkeltijd van informatiebeveiligingsplannen teruggebracht van 100 à 200 uur tot ongeveer twee uur. De aanpak maakt het in de toekomst ook mogelijk de beveiligingsmaatregelen in pakketten toe te wijzen aan de juiste elementen in de beveiligingsketen en de uitvoering te monitoren.

Subconclusie: De nieuwe aanpak rond de ontwikkeling van informatiebeveiligingsplannen belooft de beleids- en de toezichthoudende functie van de beveiligingsautoriteit op het gebied van informatiebeveiliging fors te versterken.

4.10. Toezicht, papieren werkelijkheid

- Omdat er zoveel objecten te bekijken zijn, kan er alleen maar steekproefsgewijs gecontroleerd worden, zelfs op het niveau van veiligheidsfunctionaris. Objecten zijn, mede hierdoor, soms jarenlang niet daadwerkelijk bekeken, waarbij soms ten onrechte werd aangenomen dat beveiligingsmaatregelen genomen zijn.

- De beveiligingsautoriteit krijgt informatie over de situatie op objectniveau doorgaans alleen op indirecte manier, via de beveiligingscoördinator.

[22] Het gaat hier om een inhaalslag. De kosten van de inhuur worden door de beveiligingsautoriteit ingeschat op 40 a 50 miljoen Euro.

- Als de beveiligingsplannen in orde zijn, is de neiging om de situatie in de praktijk te controleren klein.

- Naast de zes personen voor informatiebeveiliging heeft de ADD één onafhankelijke deskundige (auditor) aangetrokken voor fysieke beveiliging. Het is een beveiligingsexpert die meer als adviseur dan als controleur fungeert.

- De onderzoeken van de ADD zijn voor de beveiligingsautoriteit een middel om wel informatie uit de eerste hand te krijgen. Voor fysieke beveiliging staat dit nog in de kinderschoenen: het gaat hier om vier onderzoeken in de afgelopen twee jaar. De ADD heeft nog geen fysieke beveiligingsplannen gecontroleerd omdat een norm voor de totstandkoming van de plannen ontbreekt. Hiervoor loopt een ontwikkelingstraject bij TNO. Voor informatiebeveiliging is er meer informatie voor handen, met name door de rol van de ADD bij de accreditatie.

- In 2004 hebben OIB's onderzoek gedaan naar de personele beveiliging.

- De MIVD vermoedt dat zij lang niet alle beveiligingsincidenten doorgemeld krijgen van de defensieonderdelen.

- Strikt volgens het besturingsmodel geredeneerd kan de BA niet beleidsverantwoordelijke èn toezichthouder zijn. Drie mogelijkheden doen zich voor: 1) de toezichtsrol wel binnen de BA beleggen, maar in een aparte afdeling, 2) de rol geheel bij de ADD neerleggen, 3) een nieuwe, geheel onafhankelijke entiteit oprichten.

Subconclusie: Het stelsel van toezichthouders uit het defensiebeveiligingsbeleid is niet in staat om de keten van voor tot achter van juiste managementinformatie te voorzien. Het opstellen van een controleplan is een belangrijke stap in de goede richting. Maar er zit spanning in de huidige belegging van rollen en het besturingsmodel.

4.11. Het verbeterprogramma in de hand?

- De invulling van de verbetermaatregelen in 2004 was soms niet in lijn met de intentie van het daadwerkelijk en in de praktijk controleren van de genomen beveiligingsmaatregelen[23]. Teruggevallen werd op randvoorwaardelijke zaken en een 'papieren' werkelijkheid zoals het opstellen van regels en het nog eens analyseren van de database.

[23] De Algemene Rekenkamer zegt in haar rapport: de te treffen verbetermaatregelen kunnen slechts worden vastgesteld door inspecties op de objecten zelf en de situatie te vergelijken met de al dan niet aanwezige verbeterplannen."

- Ondanks het door de BA geschreven format voor de verbeterplannen en de gesprekken in de loop van 2004 tussen de beveiligingsautoriteit, de DFEZ en de beveiligingscoördinatoren over het verloop van de verbetermaatregelen hebben de defensieonderdelen niet het gevoel *inhoudelijk* te zijn gestuurd.

- Net als bij de reguliere bedrijfsvoering was ook het toezicht op het verbeterprogramma in 2004 *indirect*: ook daar beperkten de beveiligingsautoriteit en DFEZ zich tot het praten met de beveiligingscoördinatoren. Het was het nodig om los van de intensieve monitoring van de verbetermaatregelen vragen over de voortgang direct aan de defensieonderdelen te stellen[24].

- De ADD heeft van 6 juli tot 21 september 2004 een "quick scan" gedaan bij 19 objecten om daarmee een uitspraak te kunnen doen over de tussenstand van de gerealiseerde beveiliging rond 1 oktober 2004[25]. Het onderzoek richtte zich daardoor indirect op de uitvoering van het *verbeterprogramma*: de ADD heeft bijvoorbeeld niet vastgesteld of verbetermaatregelen, zoals de grootschalige inventarisatie, daadwerkelijk zijn uitgevoerd.

- Het kwaliteitsprogramma 2005 e.v. heeft geen eigen financiële middelen. De synopsis van het plan is in een brief aan de kamer meegedeeld. In het Departementaal Beraad werd besloten dat het plan eerst nog verder moest worden uitgewerkt voordat het kan worden aangenomen. De uitwerking ligt nu stil in afwachting van de ontwikkelingen, waaronder dit onderzoek. Het plan heeft nog niet tot concrete opdrachten aan defensieonderdelen geleid, wat uiteindelijk wel de bedoeling is. Wel zijn enkele nog openstaande verbeterpunten uit 2004 meegenomen in de nieuwe verbeterplannen van de defensieonderdelen.

- De beveiligingsautoriteit werkt aan de opzet van een dienstencentrum (SAMSON 16D) samen met de defensieonderdelen. In 'expertmeetings' is afgesproken dat het dienstencentrum niet ten koste gaat van de beveiligingscapaciteit bij de defensieonderdelen. Het krijgt de functionaliteiten kenniscentrum, vooral aangaande het maken van beveiligingsplannen, en toezichthouden (samen met de veiligheidsfunctionarissen). Hoe het dienstencentrum binnen de formatieplafonds gecompenseerd wordt is nog niet besproken.

Subconclusie: De manier waarop de regie en het toezicht op de verbeterplannen is uitgevoerd was typisch voor de normale gang van zaken in de beveiligingsketen de laatste jaren: er bleef inhoudelijk veel ruimte voor de

---

[24] Illustratief is een nota van 14 mei 2004, BA / 2004003162 , waar de secretaris-generaal de defensieonderdelen verzoekt te bevestigen of de deadlines voor de verbetermaatregelen personele beveiliging gehaald zijn.

[25] Alle aspecten van fysieke en personele beveiliging kwamen daarbij aan de orde.

defensieonderdelen en het toezicht was indirect. Het kwaliteitsplan 2005 e.v. moet nog zijn beslag krijgen in de verbeterplannen van de defensieonderdelen.

5. MAATREGELEN

5.1. inleiding

De knelpunten leidden in het vorige hoofdstuk tot subconclusies over de defensiebrede beveiligingsketen en de processen fysieke en personele beveiliging. In dit afsluitende hoofdstuk wordt bezien wat er gedaan moet worden om de knelpunten op te lossen.

5.2. Maatregelen voor de keten (lange termijn).

Beveiligingsbewustzijn (zie 4.2.). De afhankelijkheid van functionele lijn van de andere schakels in de beveiligingsketen is een permanent risico gezien de attitude over beveiliging. Het belang van beveiligingsbewustzijn wordt wel onderkend, maar met name gericht op de werknemers in het algemeen.

- Het instrument dat DICTU ontwikkelt moet ook geschikt worden gemaakt voor beveiligingsbewustzijn in de fysieke en personele processen. Actie BA.

- Gebruik militaire opleidingen bewuster om de basis te leggen voor beveiligingsbewustzijn. Zorg ervoor dat de burgermedewerkers ook het nodige meekrijgen. Ontwikkel hiervoor standaard opleidingsmodules. Actie BA / DO'n.

Beleid, centraal omdat het moet (zie 4.3.). De beveiligingsautoriteit is in de opzet (zeker met het nieuwe besturingsmodel) wel de centrale spil, maar de verbindende elementen (kennis, beleid en toezicht) in de keten zijn te zwak. De beveiligingautoriteit moet centraal uitvoerbaar beleid maken.
Er zijn wel pogingen gedaan om de verbindende elementen te versterken, zoals het nieuwe beleid, het kwaliteitsplan, de uitbreiding van de beveiligingsautoriteit en de discussie rond het dienstencentrum. Deze kwaliteitsimpulsen zijn nog niet allemaal even geloofwaardig. Kies overtuigend voor een centrale aansturing en trek de logische conclusies:

- Het defensieonderdeelsbeleid verdwijnt zodra de beveiligingsautoriteit is uitgebreid. Aanvankelijk worden het huidige defensieonderdeelsbeleid een aanhangsel bij het defensie beveiligingsbeleid 2005. Later worden de regelingen geleidelijk verwerkt in het defensie beveiligingsbeleid zelf. De defensieonderdelen worden bij dit proces betrokken. Actie BA.

- Maak het nieuwe beveiligingsbeleid concreter door het ontwikkelen van standaard fysieke beveiligingsplannen in de lijn met de standaard voor informatiebeveiligingsplannen. Bijvoorbeeld een standaard beveiligingsplan voor een wapenkamer. In de standaardplannen moet voldoende ruimte zijn voor lokale afwijkingen. Actie BA.

- De beveiligingsautoriteit is minder afhankelijk van de beveiligingscoördinatoren, door de SG aan de beveiligingscoördinatoren te koppelen en de beveiligingsautoriteit aan de uitvoerders. Actie SG/BC.

- De kennis bij de beveiligingsautoriteit wordt versterkt door deels kennis bij de beveiligingsautoriteit te concentreren en deels kennis bij andere instanties te ontsluiten met kennismanagementmethodieken[26]. De beveiligingsautoriteit is het kenniscentrum. Relevante kenniskringen moeten worden geformaliseerd[27]. Actie BA.

Terrorismebestrijding (zie 4.4.). De beveiligingsautoriteit heeft een te beperkte rol in de doorontwikkeling van het beleid rond Defensie en terrorisme en neemt niet deel aan de interdepartementale overlegstructuren op dit terrein.

- De beveiligingsautoriteit moet capaciteit vrij (kunnen) maken om zijn rol in de beleidsontwikkeling in te vullen. De rol van de DAB en de DS blijft daarmee onaangetast. Zie ook het 1e punt van de vorige alinea.

- De procedures voor de aansluiting tussen de interdepartementale overleggen over terrorisme en beveiliging en de defensiebrede beveiligingsketen (de beveiligingsautoriteit) moeten procedureel worden geregeld. Actie CBNT.

De CDS (zie 4.5.). De CDS kan zijn trechterrol invullen zonder dat daarmee de beleidsbepalende rol van de beveiligingsautoriteit in het geding komt. De CDS heeft een primaire rol bij de afweging van belangen bij inzet. Dit levert twee korte termijn maatregelen op:

- Leg de rol van de CDS, de beveiligingsautoriteit en de MIVD bij het afkondigen van beveiligingsmaatregelen vast. Actie BA.

- De defensieonderdelen houden hun eigen beveiligingscoördinatoren en blijven deelnemen aan de beleidsontwikkeling.

Eenduidigheid (zie 4.6.). De defensieonderdelen hebben behoefte aan centrale aansturing door de beveiligingsautoriteit en ondersteuning met expertise. Er lijken geen zwaarwegende bezwaren te zijn om toe te werken naar een defensiebreed bewakingscorps.

- Werk toe naar een defensiebreed bewakingscorps onder de CDC, waar de defensieonderdelen een klant-leverancier relatie mee

[26] Hiervoor kan gebruik gemaakt worden van de pilot “kennismanagement bestuursstaf”

[27] Vaststellen welke kennis nodig is, wie die kennis heeft en vervolgens die kennis managen.

hebben[28]. De verantwoordelijkheid voor de uitvoering blijft bij de defensieonderdelen, met name de lijnorganisatie, liggen. Het bewakingscorps garandeert standaarden in opleiding en werkwijze. Actie SG.

- Onderzoek de mogelijkheid van een carrièrepatroon in de beveiliging. De beveiligingsautoriteit laat de defensieonderdelen inventariseren over hoeveel functies het gaat. De HDP kijkt of daar patronen in aan te brengen zijn en legt de relatie met het nieuwe personeelsbeleid. Het gaat hier niet om het personeel bij de bewakingscorpsen. Actie HDP.

Uitvoering (zie 4.7. tot en met 4.9.). Dit processen leveren vooral korte termijn maatregelen op, zie volgende paragraaf.

Toezicht, beter organiseren (zie 4.10.). Het stelsel van toezichthouders uit het defensiebeveiligingsbeleid is niet in staat om de keten van voor tot achter van juiste managementinformatie te voorzien. Het opstellen van een controleplan is een belangrijke stap in de goede richting. Maar er zit spanning in de huidige belegging van rollen en het besturingsmodel.

- Los de spanning in de huidige belegging van rollen en het besturingsmodel op door te kiezen uit de drie voorgestelde beleggingen van het toezicht. In die keuze spelen argumenten mee die buiten dit onderzoek vallen, zoals de richting waarin de ADD zich verder wil ontwikkelen en hoe Defensie in zijn algemeenheid wil omgaan met toezichthouders[29]. Actie: SG

- Ieder controleplan bevat een algemeen deel (waarmee de beveiligingsautoriteit zijn toezichthoudende rol invult) en een defensieonderdeel specifiek deel (waarmee de defensieonderdelen hun eigen verantwoordelijkheid kunnen waarmaken). Actie BA, DO'n.

- Het controleplan moet zeker stellen dat elk object periodiek daadwerkelijk wordt bezocht, de norm daarvoor wordt door de beveiligingsautoriteit vastgesteld. Actie: BA.

- De ADD controleert of de toezichthouders de controleplannen daadwerkelijk uitvoeren en doet steekproeven. Actie: ADD.

[28] Voorwaarde is dat een oplossing wordt gevonden om in de behoefte aan bewakingspersoneel voor uitgezonden eenheden bij de KLu te voorzien.

[29] Zie bijvoorbeeld de discussie over de militaire luchtvaartautoriteit

- De ADD neemt geen beleidsontwikkelende initiatieven meer over van de beveiligingsautoriteit en beperkt zicht tot haar rol als controleur. Actie: ADD

Verbeteren (zie 4.11). De manier waarop de regie en het toezicht op de verbeterplannen is uitgevoerd was typisch voor de normale gang van zaken in de beveiligingsketen de laatste jaren: er bleef inhoudelijk veel ruimte voor de defensieonderdelen en het toezicht was indirect. Het kwaliteitsplan 2005 e.v. moet nog zijn beslag krijgen in de verbeterplannen van de defensieonderdelen, maar is nu nog te ruim van opzet.

- De bespreking van de voortgang van de verbeterpunten vindt plaats in het reguliere overleg tussen de beveiligingsautoriteit en de defensieonderdelen. Dit heeft als positief neveneffect dat defensieonderdelen dit overleg ook kunnen gebruiken om van elkaar te leren.

- De uitvoerbaarheid van het beleid komt ook via dit overleg standaard aan de orde.

5.3. Concrete maatregelen (korte termijn)

- Gezien het belang van beveiliging en het werk dat moet worden verzet om de beveiliging structureel op een hoog niveau te brengen en te houden (waaronder de aanbevelingen in dit rapport) noodzaakt een uitbreiding van de beveiligingsautoriteit. De beveiligingsautoriteit wordt daarom in capaciteit versterkt met vier VTE'n[30]. Dit zijn militaire medewerkers van het niveau luitenant-kolonel / kapitein-luitenant–ter-zee, afkomstig van de vier krijgsmachtdelen. In de uitbreiding zit ook iemand met een juridische achtergrond. Actie SG.

- De verantwoordelijken voor beveiliging (de SG en de beveiligingscoördinator) komen 2x per jaar bijeen om de grote lijnen af te stemmen. Tijdens deze bijeenkomsten wordt ook aandacht besteed aan beveiligingscultuur in de 'verantwoordelijkheidslijn'. Actie SG.

- De uitvoerders (de beveiligingsautoriteit en de beveiligingsexperts bij de beveiligingscoördinator) hebben maandelijks overleg om de beleidslijnen in te vullen. Belangrijke aandachtspunten zijn het kwaliteitsplan 2005 e.v. en het nieuwe defensie beveiligingsbeleid 2005. Actie BA.

- Attitudeverandering is ketenbreed noodzakelijk, niet alleen bij de gewone werknemer, maar ook bij de verantwoordelijken. Dit wordt ingevuld door centraal een beveiligingsbewustwordingsproject te starten, gericht op de beide doelgroepen. Actie BA.

[30] Deze komen bovenop de twee reeds toebedachte VTE'n uit SAMSON maatregel 16D.

- Het onderwerp beveiligingscultuur wordt meegenomen in bedrijfsvoeringsmetingen (zoals INK). De beveiligingsautoriteit coördineert dit. Actie: DO'n, BA.

- De beveiligingsautoriteit is het kenniscentrum, en geeft dat gestalte door 1) essentiële kennisgebieden vast te stellen, die aansluiten bij de drieslag fysieke, personele en informatiebeveiliging, 2) relevante kennis van binnen en buiten defensie te verzamelen. Daarbij moet ook gebruik worden gemaakt van benchmarking met civiele beveiligingsorganisaties. 3) Die kennis beschikbaar te maken voor iedereen in de beveiligingsketen[31]. Actie: BA.

- De MIVD stelt in opdracht van de beveiligingsautoriteit een herzien (en paars) daderprofiel op, waarin terrorisme aandacht krijgt. Er wordt daarvoor aangesloten op de dreiging terrorisme Nederland. De beveiligingsautoriteit trekt de consequenties uit dit nieuwe daderprofiel. Actie MIVD / BA.

- De MIVD verschaft ook dit jaar de *generieke* dreigingsanalyse op. Dit komt naast de bijdragen die de MIVD al leverde aan het dreigingsbeeld terrorisme Nederland. Actie: MIVD.

- In de defensiebrede risicoanalyse voor 2006 en de risicoanalyse van de defensieonderdelen voor 2006 wordt specifiek aandacht besteedt aan het onderwerp beveiliging. Indien nodig worden aanvullende beheersingsmaatregelen genomen. Actie DBE / DO'n.

- Huur een beveiligingsexpert in om de verdere ontwikkeling van het nieuwe beveiligingsbeleid als 'expert' en als 'buitenstaander' te kunnen bespoedigen. Actie BA.

- De krijgsmachtsleutelpuntenlijst verdwijnt. In plaats van een actualisatie van de krijgsmachtsleutelpuntenlijst wordt eenmalig een slag gemaakt om te beoordelen of de objecten van de lijst die nog niet als CAT-1 of CAT-2 object zijn opgenomen alsnog die classificatie moeten krijgen. Actie DO'n.

- Bepaal wat attractieve wapens zijn en sla de wapens die niet direct nodig zijn op in één centraal CAT-1 object. CDS stelt vast wat 'niet direct' in dit geval inhoudt. Actie CDS, DO'n.

[31] De mensen die over relevante kennis beschikken kunnen overal in de organisatie zitten. Door deze mensen te identificeren en van hun kennis gebruik te maken hoeft niet alle relevante kennis binnen de beveiligingsautoriteit zelf te worden belegd. Wel moet de beveiligingsautoriteit weten waar die kennis te halen is.

- De Smartcard en de opvolger ervan wordt verbonden met het MIPSS[32]. Dit opent de deur om MIPSS voor alle defensieobjecten uit te rollen. Actie BA.

- Als voorbereiding op het toewerken naar een defensiebreed bewakingscorps wordt het bewakingscorps voor de vier resterende objecten in Den Haag uitgevoerd door één bewakingscorps. Gebruik deze pilot ook om de gestandaardiseerde beveiligingsplannen te testen. Actie BA / BC-BS.

- Het kwaliteitsplan 2005 e.v. wordt door de beveiligingsautoriteit in samenspraak met de beveiligingsketen doorontwikkeld in het verbeterplan 2005 e.v. met daaraan actienemers die in de hele keten kunnen zitten (wie moet wat bereikt hebben op welk moment). Daarbij worden ook de maatregelen uit dit rapport meegenomen. Actie BA.

- De beveiligingsautoriteit stelt voor de uitvoeren van het verbeterplan een communicatieplan op. Het communicatieplan richt zich (net als het verbeterplan zelf) op de hele keten. Actie BA.

- De bezwaarprocedure bij intrekking van de verklaring van geen bezwaar wordt ondergebracht bij JuZa-P en niet uitbesteed aan de CAOP. Actie SG / JuZa-P.

- Begin 2006 wordt de voortgang van dit rapport, als onderdeel van het verbeterplan 2005 e.v. door een externe instantie bekeken. Actie SG

- Ontwerp een introductieprogramma op beveiligingsgebeid voor intredende burgermedewerkers. Actie DO'n, BA.

- Doe onderzoek naar de mogelijkheden die de moderne techniek bied op het gebied van beveiliging.

BIJLAGEN:
A - Leidraad interviews
B – instellingsbeschikking
C – verschillen in de keten

[32] Het Military Peacetime Security System waar belangrijke objecten met elektronische detectie en toegangsbeheersingsapparatuur op zijn of worden aangesloten.

Bijlage A, Leidraad bij de interviews

- Het rapport van de Algemene Rekenkamer
  - Rol van de beveiligingsautoriteit bij de verbeterinspanningen
  - Niveau van stafbehandeling
  - Stand van zaken
  - Monitoring (door de beveiligingsautoriteit)
  - Het kwaliteitsplan van de beveiligingsautoriteit voor 2005 e.v.

- Opslag van wapens
  - Afwijkingen van het defensiebeleid
  - Manier waarop risicoanalyse is toegepast

- Het defensiebeveiligingsbeleid 1997
  - Hoe doorvertaald?
  - Het nieuwe beleid van 2005?
  - Krijgsmachtsleutelpuntenlijst

- De beveiligingsautoriteit?
  - Als deskundige
  - Als sturende instantie
  - Als toezichthouder

- De organisatie rond beveiliging
  - beveiligingscoördinator Staf?
  - Uitvoering?
  - Effecten reorganisaties?
  - Project opvolging SMARTCARD

- De informatie over beveiliging
  - Informatie in toprapportages, wie stelt vast
  - Waar ligt de grens tussen papier en werkelijkheid?
  - Informatie over de dreiging, hoe werkt dat?
  - Daderprofiel, doorvertaling terrorisme

- Personeelsbeveiliging
  - Achterstand?
  - Relatie functie / personeel, hoe is de informatie georganiseerd

- Ideaalbeeld toekomstige keten
  - Beleid als trade-off: standaardiseren vs maatwerk
  - Dienstencentrum?
  - Opleidingen
  - Systemen
  - Toezicht

Bijlage B, instellingsbeschikking

Bijlage C, verschillen in de keten

De defensieonderdelen hebben tot nu toe ieder een eigen beveiligingsbeleid. Het niet standaardiseren leidt tot verschillen in de uitvoering door de beveiligingsketen. Deze verschillen komen in het rapport hier en daar naar voren. In deze bijlage wordt een aantal in het oog springende verschillen nog eens opgesomd. Deze opsomming is niet limitatief, er kwamen nog meer kleinere zaken verschillen naar voren tijdens het onderzoek.

- Het voor de DMO en het CDC lastig om de nieuw toetredende eenheden op een standaard te krijgen, met name op het punt van fysieke beveiliging

- Het voor de ADD onmogelijk om de totstandkoming van de fysieke beveiligingsplannen te beoordelen.

- Inlichtingen en veiligheid is alleen bij de KLu een separaat vakgebied.

- Systemen zouden, juist bij beveiliging, defensiebreed moeten worden toegepast. Denk daarbij aan het MIPPS, dat alleen de KL gebruikt en IVAN-4, dat bij de KLu gebruikt wordt.

- De KL sluit als enige aan bij civiele beveiligingsconcepten, zoals de ‘Haagse methode’.

- De KLu gebruikt als enige eigen bewakingspersoneel.

- Ieder defensieonderdeel vult op eigen wijze in hoe in opleidingen aandacht aan beveiliging wordt besteed.