

Vergaderjaar 2003–2004

29 415

Beveiliging militaire objecten

Nr. 2

RAPPORT

Inhoud

	Samenvatting	5	4.5	Overige aspecten	19
			4.6	Veiligheidsinbreuken	19
1	Inleiding	8	4.7	Evaluatie werking	20
1.1	Algemeen	8	4.8	Test Algemene Rekenkamer	20
1.2	Aanleiding onderzoek	8	4.9	Getroffen maatregelen	21
1.3	Doel- en probleemstelling	9			
1.4	Aanpak onderzoek	10	5	Personele beveiliging	22
1.5	Leeswijzer	10	5.1	Algemene Beveiligingseisen voor Defensie	
				Oprachten	22
2	Beleid, normen en organisatie	11	5.2	Werking in de praktijk	23
2.1	Beleid	11	5.3	Getroffen maatregelen	23
2.2	Begrippen en normen	11	5.4	Screening intern personeel	23
2.2.1	Begrippen	11	5.5	Getroffen maatregelen	24
2.2.2	Normen	11			
2.3	Organisatie	12	6	Conclusies en aanbevelingen	25
2.3.1	Verantwoordelijke functionarissen	12	6.1	Conclusies	25
2.3.2	Overleg	13	6.2	Aanbevelingen	25
2.3.3	Toezicht	13			
2.3.4	Rapportage	14	7	Reactie en nawoord	26
			7.1	Reactie minister	26
3	Uitwerking beveiligingsbeleid	15	7.2	Nawoord Algemene Rekenkamer	27
3.1	Rol Beveiligingsautoriteit	15			
3.1.1	Algemeen	15	Bijlage 1	Tabel conclusies en aanbevelingen	28
3.2	Rol onderdelen	15			
3.2.1	Toezicht Beveiligingsautoriteit	16			
4	Fysieke beveiliging objecten	18			
4.1	Inleiding	18			
4.2	Veiligheidsfunctionaris	18			
4.3	Beveiligingsplan	18			
4.4	Personele, financiële en materiële middelen	19			

SAMENVATTING

Inleiding

De Algemene Rekenkamer heeft van april tot september 2003 een onderzoek uitgevoerd naar de beveiliging van militaire objecten. Beveiliging van militaire objecten bij defensie is van groot belang. Aanslagen op bijvoorbeeld commando- of computercentra en wapensystemen kunnen de defensieorganisatie verlammen. Voorts beschikt defensie over grote voorraden wapens, munitie en springstoffen, waarvan het essentieel is dat zij niet in verkeerde handen komen.

Het Ministerie van Defensie hanteert, als het gaat om de beveiliging van militaire objecten, het begrip Integrale Beveiliging. Hieronder verstaat het ministerie:

- fysieke beveiliging (organisatorische, bouwkundige en elektronische maatregelen);
- personele beveiliging (screening intern en extern personeel);
- informatiebeveiliging (geautomatiseerde systemen).

In dit onderzoek komen de fysieke en personele beveiliging aan bod. De informatiebeveiliging maakt onderdeel uit van het jaarlijkse, reguliere onderzoek van de Algemene Rekenkamer van de jaarverslagen van de departementen, in dit geval het Ministerie van Defensie¹.

Onderzocht is wat het defensie Beveiligingsbeleid is, hoe dit is doorvertaald naar de verschillende defensieonderdelen en hoe dit beleid in de praktijk wordt toegepast.

Conclusies en aanbevelingen

De belangrijkste conclusie van het onderzoek is dat de opzet van de gekozen systematiek van beveiliging in het algemeen goed is, maar dat de uitvoering in de praktijk daarbij risicovol achterblijft. Zes van de 19 onderzochte militaire objecten voldoen niet aan de eisen die aan de fysieke beveiliging gesteld moeten worden. De defensieorganisatie loopt hier grote risico's, omdat gewichtige belangen van de Staat in het geding zijn.

In een aantal gevallen onderkent defensie de bestaande onvolkomen beveiligingssituatie, maar het verantwoordelijke management accepteert het – uitgaande van een tijdelijke situatie.

De Algemene Rekenkamer beveelt de minister aan er zorg voor te dragen dat de fysieke beveiliging van militaire objecten in de praktijk wordt uitgevoerd.

Een tweede belangrijke conclusie is dat de invulling van de functie van de Beveiligingsautoriteit onvoldoende gestalte heeft gekregen. De defensieonderdelen geven zelf invulling aan het beveiligingsbeleid. Dit leidt tot verschillende invalshoeken bij de invulling daarvan.

De Beveiligingsautoriteit is namens de secretaris-generaal belast met het ontwikkelen en evalueren van het beveiligingsbeleid, de overdracht hiervan aan de onderdelen, en oefent toezicht uit op de deugdelijkheid van de beveiliging. Hij dient daarover te rapporteren aan de secretaris-generaal.

De Algemene Rekenkamer constateert dat de Audit Dienst Defensie (ADD) het feitelijke toezicht op de opzet en werking van de beveiliging uitvoert. De ADD doet dit door middel van audits naar de stand van de beveiliging.

¹ Het rapport bij het Jaarverslag Defensie (RJV Defensie) maakt deel uit van de rapportage van de Algemene Rekenkamer op Verantwoordingsdag, elke derde woensdag van mei.

Deze actie is in het voorjaar van 2003 gestart na een verzoek van de secretaris-generaal.

De Algemene Rekenkamer beveelt de minister van Defensie aan om daadwerkelijk invulling te geven aan de functie van de Beveiligingsautoriteit, waardoor deze zijn beleidsbepalende, beleidsuitdragende en toezichthoudende functie kan vervullen.

Een derde belangrijke conclusie van de Algemene Rekenkamer is dat de toepassing van de regeling Algemene Beveiligingseisen Defensie Opdrachten veel te wensen overlaat. Deze regeling stelt eisen aan het kennismaken door derden van gerubriceerde informatie dan wel andere gewichtige belangen van de Staat.

Bij defensie kunnen niet gescreende derden kennis nemen van gerubriceerde informatie of andere gewichtige belangen van de Staat. Daarnaast komt het bij het interne personeel regelmatig voor dat personen zonder (geldig) veiligheidsonderzoek vertrouwensfuncties vervullen. Bij twee onderdelen gold dit, ten tijde van het onderzoek, voor circa 50% of meer van de vertrouwensfuncties. Bij één onderdeel waren inmiddels wel maatregelen genomen om aan deze ongewenste situatie een einde te maken.

Met het oog op de ernst van de bevindingen heeft de defensieorganisatie vooruitlopend op de formele afronding van het onderzoek intussen maatregelen genomen, die – in afwijking van de gebruikelijke werkwijze van de Algemene Rekenkamer – reeds in het rapport zijn opgenomen.

Reactie minister van Defensie

De minister van Defensie heeft op 19 december 2003 gereageerd op het conceptrapport van de Algemene Rekenkamer. In zijn reactie stelt de minister dat hij ervoor zal zorgen dat de fysieke beveiliging van militaire objecten in de praktijk wordt uitgevoerd. Hij zegt toe dat de tekortkomingen in de beveiliging bij vijf van de zes militaire objecten in januari 2004, zonodig met alternatieve- of interimmaatregelen, verholpen zijn. Bij het zesde object zal dit in februari 2004 het geval zijn. Verder gaat het Ministerie van Defensie een grootschalige inventarisatie houden om te bezien of de bevindingen van de Algemene Rekenkamer ook voor de niet bezochte objecten gelden. Op basis van deze inventarisatie zal defensie maatregelen ter verbetering formuleren, die in verbeterplannen worden opgenomen.

De directie financieel-economische zaken en de Beveiligingsautoriteit zullen de verbeterplannen bewaken volgens dezelfde controlesystematiek als de verbeterplannen voor de onderwerpen financieel en materieel beheer. De minister geeft aan dat het ministerie de functie van de Beveiligingsautoriteit en de daadwerkelijk invulling daarvan mee zal nemen in de studie naar de nieuw te vormen bestuursstaf en bij de herstructurering van de defensieorganisatie. Daarbij zal de minister de bevindingen van de Algemene Rekenkamer ten aanzien van de invulling van de functie van de Beveiligingsautoriteit, mee laten wegen.

De minister stelt voorts dat hij, als het gaat om toezicht op de uitvoering van het beleid, hecht aan de verantwoording van de bevelhebbers aan hem. Volgens de minister moet de bevelhebber voor de invulling van zijn rapportage aan de minister steunen op zowel zijn ondercommandanten als de betrokken veiligheidsfunctionarissen en de beveiligingscoördinator. Een, met personeel, ingevulde beveiligingsorganisatie is daarvoor een

randvoorwaarde aldus de minister. In de verbeterplannen zijn inspecties opgenomen van de beveiligingsorganisatie door de Audit Dienst Defensie.

De minister stelt dat hij de conclusies en aanbevelingen van de Algemene Rekenkamer ter harte neemt op het punt van de regeling Algemene Beveiligingseisen voor Defensie Opdrachten. Het ministerie gaat dit punt in de verbeterplannen oppakken door een combinatie van een inventarisatie van lopende werkzaamheden op militaire objecten en een intensievere voorlichting over de toepassing van de regeling. Daarnaast zal de Audit Dienst Defensie in de integrale beveiligingsaudits beoordelen of de regeling ook wordt gehandhaafd.

Over de personele beveiliging van intern personeel deelt de minister mee, dat het overgrote deel van het bestand vertrouwensfuncties binnen defensie is geactualiseerd. Daarnaast vindt er een grootschalige inventarisatie plaats van de bijbehorende verklaringen van geen bezwaar. Uit de voorlopige resultaten blijkt, aldus de bewindsman, dat vrijwel iedere werknemer in het bezit is van een verklaring van geen bezwaar op het juiste niveau maar dat deze vaak ouder is dan vijf jaar. De minister spreekt de verwachting uit dat de personele beveiliging ultimo 2004 door een grote inspanning op orde zal zijn.

Nawoord Algemene Rekenkamer

De Algemene Rekenkamer heeft met instemming kennis genomen van de maatregelen die de minister reeds genomen heeft en de maatregelen die hij aankondigt. Door deze maatregelen zullen de beveiliging bij objecten en de personele beveiliging, zowel voor intern als extern personeel, sterk kunnen verbeteren. Echter, om te voorkomen dat de aandacht voor beveiliging in de toekomst weer verslapt, zal het ministerie de aandacht voor beveiliging systematisch in de organisatie moeten inbedden. De Algemene Rekenkamer zal de ontwikkelingen met aandacht blijven volgen en stelt zich voor over enige tijd een vervolgonderzoek uit te voeren.

1 INLEIDING

1.1 Algemeen

Beveiliging van militaire objecten bij defensie is altijd van groot belang geweest. Allereerst gaat het hier om het voorkomen van uitholling van de slagkracht van de defensieorganisatie. Aanslagen op bijvoorbeeld commando- of computercentra en wapensystemen kunnen de defensieorganisatie verlammen. Voorts beschikt defensie over grote voorraden wapens, munitie en springstoffen, waarvan het essentieel is dat zij niet in verkeerde handen komen.

Na de val van de Berlijnse muur, als duidelijkste teken van de ingrijpende wijzigingen van de internationale veiligheidssituatie, bracht de minister van Defensie in 1993 de Prioriteitennota uit. In deze nota werd bepaald dat de opkomstplicht voor dienstplichtig personeel zou worden opgeschort. De krijgsmachtdelen hebben zich hierdoor op nagenoeg alle taakvelden moeten herbezinnen; zo ook op het terrein van bewaken en beveiligen. Het grootst waren de veranderingen bij de Koninklijke Landmacht (KL), traditioneel het krijgsmachtdeel met de meeste dienstplichtigen. De statische, objectgebonden bewaking werd hier van oudsher voornamelijk uitgevoerd door dienstplichtig personeel (o.a. acht Infanterie beveiligingscompagnieën). Vanaf 1997 (afzwaaien laatste lichtingsploeg) waren er echter geen dienstplichtigen meer beschikbaar voor beveiliging.

Om toch een aanvaardbaar veiligheidsniveau te waarborgen, heeft defensie in 1997 het begrip Integrale Beveiliging ingevoerd. Daarbij ligt, meer dan in het oude concept van statische bewaking en beveiliging, de nadruk op risicomanagement. Dat wil zeggen het in evenwicht brengen van te beveiligen belangen, de onderkende kwetsbaarheden daarvan en de mogelijke optredende dreigingen. Door middel van het uitgebreid toepassen van organisatorische, bouwkundige en elektronische beveiligingsvoorzieningen (de zogeheten «OBE-mix») heeft de krijgsmacht een grote personeelsreductie bereikt. Sindsdien ziet de krijgsmacht af van het oude concept van statische, objectgebonden bewaking, en zet de krijgsmacht (deels ingehuurd) burger beveiligingspersoneel in. Dit alles heeft ertoe geleid dat lang niet alle van de circa 630 Nederlandse defensie terreinen en -objecten ook daadwerkelijk actief worden beveiligd. De hiermee gemoeide personele en financiële middelen zijn niettemin aanzienlijk: 2100 fte'en en € 108 miljoen voor 2002.

1.2 Aanleiding onderzoek

De gebeurtenissen van 11 september 2001 vormden aanleiding te bezien op welke wijze de Algemene Rekenkamer, door middel van onderzoek, een bijdrage kan leveren aan de effectieve bestrijding van bedreigingen van terroristische aard. Eén van de onderwerpen die, uit een daartoe door de Algemene Rekenkamer gehouden inventarisatie, naar voren kwam was de beveiliging van militaire objecten.

De gebeurtenissen op 11 september 2001 in de Verenigde Staten plaatsten het onderwerp beveiliging manifest op de politieke agenda. Voor de bestrijding van terrorisme heeft het Ministerie van Defensie actief meegewerkt aan het actieplan Terrorismebestrijding en Veiligheid, dat de regering op 5 oktober 2001 aan de Tweede Kamer aanbood (Tweede Kamer, vergaderjaar 2001–2002, 27 925, nr 10).

Als uitvloeisel van het actieplan werd een ambtelijke taakgroep defensie en terrorisme ingesteld die een rapport heeft opgesteld, dat op 18 januari 2002 aan de Tweede Kamer is aangeboden (Tweede Kamer, vergaderjaar 2001–2002, 27 925, nr 40). De taakgroep deed aanbevelingen, gericht op de bewaking en beveiliging van defensieobjecten, terreinen, personeel en informatie- en communicatie-systemen.

De belangrijkste aanbevelingen van de taakgroep op het gebied van de beveiliging van militaire objecten waren:

- het aanpassen van de standaarduitrusting van bewakings- en beveiligingspersoneel;
- snelle implementatie van beveiligingsplannen, uitbreiding van bewakingseenheden, alsmede het verbeteren van de borging van beveiligingsniveaus door uitvoering van verscherpte controles en inspecties;
- het versnellen van de ontwikkeling van een defensiebreed calamiteitenplan voor alle vitale objecten en systemen, alsmede het aanvullen van lokale informatiebeveiligingsplannen met calamiteitenparagrafen;
- het versnellen van de uitvoering van informatiebeveiligingsmaatregelen.

1.3 Doel- en probleemstelling

Met het onderzoek beoogt de Algemene Rekenkamer te bereiken dat de beveiliging van militaire objecten op het vereiste niveau wordt gebracht. Zij wil de minister, waar mogelijk, aanbevelingen aanreiken die de kwaliteit van de beveiliging van militaire objecten op het gewenste niveau brengt.

Het Ministerie van Defensie hanteert, als het gaat om de beveiliging van militaire objecten, het begrip Integrale Beveiliging. Hieronder wordt verstaan de:

- fysieke beveiliging;
- personele beveiliging;
- informatiebeveiliging (geautomatiseerde systemen).

In dit onderzoek komen de fysieke en personele beveiliging aan bod. De personele beveiliging omvat de screening van intern en extern personeel. De informatiebeveiliging is buiten beschouwing gelaten, omdat dit al ruime aandacht krijgt in het kader van het reguliere onderzoek voor het Rapport bij het Jaarverslag (RJV Defensie)¹. Waar in dit onderzoek wordt gesproken over beveiliging van militaire objecten heeft dit uitsluitend betrekking op de fysieke en personele beveiliging daarvan.

De probleemstelling van het onderzoek luidt als volgt: heeft de minister van Defensie ervoor zorg gedragen dat de beveiliging van militaire objecten in opzet en werking voldoet aan het geformuleerde ambitieniveau?

Afgeleid van deze probleemstelling heeft de Algemene Rekenkamer de volgende onderzoeksvragen gehanteerd:

- wat is het Defensie Beveiligings Beleid (DBB)?
- is het DBB goed doorvertaald naar de verschillende defensieonderdelen?
- hebben de defensieonderdelen hun objecten op basis van het DBB geclassificeerd?
- zijn voor deze objecten conform dit beleid beveiligingsplannen opgesteld?

¹ De RVJ's van de departementen worden door de Algemene Rekenkamer gepubliceerd op Verantwoordingsdag, de derde woensdag van mei.

- zijn de geplande maatregelen ook daadwerkelijk genomen en werken deze maatregelen in de praktijk zoals voorzien?
- wordt de minister van Defensie van voldoende informatie voorzien om zich een goed oordeel te kunnen vormen over de opzet en werking van het vastgestelde beveiligingsbeleid?

1.4 Aanpak onderzoek

Door middel van het raadplegen van Kamerstukken, dossieronderzoek en gesprekken met medewerkers van het bureau van de Beveiligingsautoriteit (BA) is het DBB in kaart gebracht.

Voor het onderzoek zijn de navolgende acht defensie organisatie onderdelen onderscheiden:

- De Centrale Organisatie (CO);
- Koninklijke Marine (KM);
- Koninklijke Landmacht (KL);
- Koninklijke Luchtmacht (KLu);
- Koninklijke Marechaussee (KMar);
- Defensie Interservice Commando (DICO); met daaronder ressorterend: agentschap Dienst Gebouwen, Werken en Terreinen (DGW&T) en agentschap Defensie Telematica Organisatie (DTO).

Bij deze onderdelen is de Algemene Rekenkamer door middel van dossieronderzoek en gesprekken met (medewerkers van) de Beveiligings Coördinator (BC) nagegaan hoe de doorvertaling van het DBB gestalte heeft gekregen. Hierbij is zij tevens nagegaan welke classificatiemethode voor de beveiliging van objecten de onderdelen hanteren.

Vervolgens heeft de Algemene Rekenkamer per onderdeel een aantal objecten geselecteerd, in totaal 19 stuks. Bij deze objecten heeft zij onderzoek ter plaatse gedaan, om nader te bezien welke factoren een rol spelen bij de uitvoering van het beveiligingsbeleid. Bij het aantal van 19 objecten kan worden opgemerkt dat de Algemene Rekenkamer vaak meer eenheden binnen een object als één object heeft gerekend. Zo heeft zij een brigade van de Koninklijke Marechaussee als één object gerekend terwijl de brigade uit het brigadegebouw en twee afzonderlijke doorlaatposten bestaat. Ook een vliegbasis is als één object gerekend terwijl er meer dan 30 eenheden uit de hoogste categorie (zie par. 2.2.2) op de vliegbasis aanwezig zijn. Het aantal waarnemingen, op basis van te beveiligen eenheden, is daardoor (veel) groter dan 19. Bij dit deel van het onderzoek zijn gesprekken gevoerd met de veiligheidsfunctionaris per object en is nagegaan of er een beveiligingsplan aanwezig was, wat de kwaliteit daarvan was en of de voorziene maatregelen ook daadwerkelijk waren getroffen en in de praktijk naar behoren functioneerden.

1.5 Leeswijzer

Hoofdstuk 2 beschrijft het DBB, de normen en de organisatie. Hoofdstuk 3 gaat over de uitwerking van het beleid. Aan de orde komt ook de rol van de BA. Hoofdstuk 4 beschrijft de bevindingen op objectniveau. Hoofdstuk 5 gaat in op de beveiligingseisen bij de inschakeling van extern en intern personeel.

2 BELEID, NORMEN EN ORGANISATIE

2.1 Beleid

Richtinggevend op het gebied van beveiliging binnen defensie is het centrale Defensie Beveiligings Beleid (DBB), vastgesteld bij besluit van de SG van 20 juni 1997 en uitgegeven op 13 augustus 1997. Dit is de eigenlijke raamregeling, waarin het beveiligingsbeleidskader voor het Ministerie van Defensie wordt aangegeven. Binnen dit kader dienen de onderdelen systematisch en vergelijkbaar met alle aspecten van beveiliging om te gaan.

De doelstelling van het DBB is de waarborging van de betrouwbaarheid van de bedrijfsprocessen van het Ministerie van Defensie. Een belangrijk uitgangspunt is dat er van adequate beveiliging alleen sprake kan zijn, als er evenwicht bestaat tussen de te beveiligen belangen, de bedreigingen en de getroffen beveiligingsmaatregelen.

2.2 Begrippen en normen

2.2.1 Begrippen

Militaire beveiliging op nationaal grondgebied richt zich op de beveiliging van:

- militaire objecten en gebieden;
- militaire personele- en materiële middelen en activiteiten.

Een militair object is gedefinieerd als een gebouw, een terrein, een (werk)ruimte, een compartiment, een schip, een vliegtuig en een onderzeeboot, alsmede een gedeelte daarvan. (bron: Richtlijnen inzake de toepassing van het integraal voorschrift Defensie. Ministeriële publikatie (MP) 10-10).

Onder beveiligen wordt verstaan het nemen van maatregelen ter bescherming van een eenheid, gebied, object, personeel, materieel of (informatie)systeem met als doel schade of verlies te voorkomen. Onder bewaken verstaat defensie het systematisch en onafgebroken toezicht houden op en waarnemen van een gebied, object, personeel, materieel of (informatie)systeem teneinde te waarschuwen of te alarmeren bij inbreuken op de veiligheid daarvan.

2.2.2 Normen

Voor de beveiligingsnormering zijn objecten- naar gelang van zwaarte- ingedeeld in 4 categorieën (bron: DBB, bijlage C). Per categorie geldt een aparte beveiligingsnorm, waarbij Stg staat voor Staatsgeheim:

- categorie 1, Stg zeer geheim gerubriceerde informatie/zeer vitale belangen: object waarvan het goed functioneren of het veilig stellen van het daarin opgeslagene van het hoogste belang is voor de veiligheid van de Staat of van zijn bondgenoten, dan wel voor de instandhouding van de slagkracht van de Nederlandse krijgsmacht of die van de bondgenoten. Deze objecten dienen zodanig te worden beveiligd dat bij elke zich voordoende dreiging te allen tijde een directe interventie kan plaatsvinden;
- categorie 2, Stg geheim gerubriceerde informatie/vitale belangen: objecten waarvan het goed functioneren of het veilig stellen van het daarin opgeslagene van groot belang is voor de veiligheid van de

Staat of van zijn bondgenoten, dan wel voor de instandhouding van de slagkracht van de Nederlandse krijgsmacht of die van bondgenoten. Deze objecten dienen zodanig te worden beveiligd dat bij een te voorziene dreiging een tijdige interventie plaats kan vinden;

- categorie 3, Stg confidentieel gerubriceerde informatie/overige gewichtige belangen: objecten waarvan het niet functioneren een beperkte nadelige invloed heeft of het niet veilig stellen van het daarin opgeslagene schade aan de veiligheid of andere gewichtige belangen van de Staat of zijn bondgenoten tot gevolg kan hebben. Deze objecten dienen zodanig beveiligd te worden dat schade zoveel mogelijk wordt voorkomen;
- categorie 4, overige informatie/belangen: tot deze categorie behoren alle niet onder de categorie 1 tot en met 3 vallende informatie en/of belangen. Standaard voorzorgsmaatregelen zijn voldoende.

De navolgende wet- en regelgeving genereert normen op basis waarvan de beveiliging van militaire objecten voornamelijk is gebaseerd:

- Wet Bescherming staatsgeheimen;
- Wet Openbaarheid Bestuur;
- MP 10-10 deel 2 (Beveiliging NATO/WEU-gegevens), deel 3 (Beveiliging van staatsgeheimen en vitale onderdelen/objecten), deel 4 (Beveiliging van gemerkte gegevens);
- Wet Bescherming Persoonsgegevens;
- Besluit Voorschrift Informatiebeveiliging Rijksdienst 1994;
- Aanwijzing van de SG V/5 Internetgebruik;
- Defensie Beveiligings Beleid;
- Aanwijzing van de SG A/872 Integriteit.

2.3 Organisatie

2.3.1 *Verantwoordelijke functionarissen*

Het DBB, dat is vastgesteld bij besluit van de Secretaris-Generaal (SG) van het Ministerie van Defensie, omvat een hoofdstuk over de integrale veiligheid. Hierbij is omschreven welke functionarissen verantwoordelijk zijn voor de integrale beveiliging.

De SG is belast met de algemene zorg voor de beveiliging en als zodanig verantwoordelijk voor het vaststellen van het beveiligingsbeleid en de daarop gebaseerde voorschriften. Met de daaraan verbonden dagelijkse werkzaamheden is de Beveiligingsautoriteit (BA) belast.

De BA is namens de SG belast met het ontwikkelen en evalueren van het beveiligingsbeleid en de overdracht hiervan aan de bevelhebbers, commandant DICO en plaatsvervangend secretaris-generaal. Daarnaast verricht de BA accreditatie-werkzaamheden in het kader van het beveiligingsbeleid, ziet hij toe op de goede uitwerking van het beveiligingsbeleid bij het Ministerie van Defensie en stelt definities vast met betrekking tot de gewenste defensie-beveiligingsinfrastructuur. De BA coördineert daarnaast de technologische aspecten van de beveiliging.

De bevelhebber, commandant DICO en plaatsvervangend secretaris-generaal zijn verantwoordelijk voor de uitvoering van het beveiligingsbeleid binnen hun ressort. Voor de uitvoering van de daaraan verbonden dagelijkse werkzaamheden hebben de bevelhebber, commandant DICO en plaatsvervangend secretaris-generaal een Beveiligingscoördinator (BC) aangewezen.

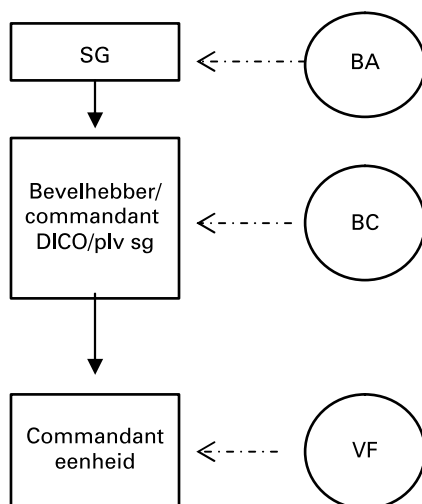
De lagere commandant is verantwoordelijk voor de uitvoering van het beveiligingsbeleid binnen zijn bevoegdheidsgebied.

Bij de uitvoering van deze taken wordt de commandant meestal bijgestaan door een daartoe aangestelde veiligheidsfunctionaris (VF).

Het hoofd van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) is belast met:

- het verrichten van veiligheidsonderzoeken als bedoeld in de Wet Veiligheidsonderzoeken;
- het verzamelen van gegevens welke nodig zijn voor het treffen van maatregelen: a) ter voorkoming van activiteiten die ten doel hebben de veiligheid of paraatheid van de krijgsmacht te schaden. b) ter beveiliging van gegevens betreffende de krijgsmacht waarvan de geheimhouding is geboden. c) ter bevordering van een juist verloop van mobilisatie en concentratie der strijdkrachten.

Schematisch ziet de organisatorische structuur er als volgt uit:



2.3.2 Overleg

De BA wordt in zijn werkzaamheden geadviseerd door het zogenaamde BA/BC beraad, waarbij de BC de bevelhebber vertegenwoordigt. Naast dit regulier overleg vindt bilateraal overleg plaats tussen de BA en één of meer BC's over knelpunten op het gebied van veiligheid. Daarnaast is er ook overleg door de BA met specialisten in zogenaamde «expertgroepen». De MIVD levert de reguliere dreigingsanalyses aan, maar zonnodig vindt in dit kader ook overleg plaats tussen de BA en het Defensie Crisis Beheersings Centrum (DCBC), de inlichtingendiensten AIVD, MIVD, NRI en het NCC (Nationaal Coördinatie Centrum).

2.3.3 Toezicht

Het toezicht op de beveiliging is nader uitgewerkt in het DBB: de BA oefent toezicht uit op de deugdelijkheid van de beveiliging en rapporteert zijn bevindingen schriftelijk aan de SG. Bij de onderdelen coördineert de BC het beleid. Bij de objecten rapporteert de veiligheidsfunctionaris zijn bevindingen, zo mogelijk schriftelijk, aan de commandant dan wel het hoofd van dienst.

Om een goede uitvoering van het beveiligingsbeleid te waarborgen is een regelmatige beoordeling van de uitvoering, prestaties en effecten van het gevoerde beveiligingsbeleid en het stelsel van de geïmplementeerde beveiligingsmaatregelen noodzakelijk. De controles zullen conform het vastgestelde defensiebeveiligingsbeleid periodiek moeten plaatsvinden door:

- de veiligheidsfunctionaris namens de commandant (beveiligingsmaatregelen);
- de beveiligingscoördinator namens de bevelhebber (krijgsmachtdebeleid);
- de beveiligingsautoriteit namens de SG (beleid);
- de MIVD (militaire veiligheid).

2.3.4 Rapportage

Om de doeltreffendheid van de beveiliging en het beveiligingsbeleid te kunnen beoordelen en zo nodig preventieve, detectieve, repressieve en/of correctieve maatregelen te kunnen treffen, is het noodzakelijk dat de voor de beveiliging verantwoordelijke functionarissen op de hoogte worden gehouden van de toestand van de beveiliging in hun bevoegdheidsgebied. Een regelmatige rapportage over de toestand van de beveiliging draagt daartoe bij. Volgens het vastgestelde defensiebeveiligingsbeleid dient de rapportage plaats te vinden door middel van incidenten- en statusrapportages (zoals toprapportages, zie par. 3.2.1).

3 UITWERKING BEVEILIGINGSBELEID

3.1 Rol Beveiligingsautoriteit

3.1.1 Algemeen

De BA is namens de SG belast met het ontwikkelen van het beleid, de overdracht hiervan aan de bevelhebbers, het toezicht op de goede uitwerking en het evalueren van het beveiligingsbeleid.

De functie van BA is, na het officiële vertrek van de laatste BA in maart 2003, niet ingevuld. Reeds geruime tijd daarvoor vervulde de toenmalige BA de functie als neventaak.

De BA wordt bijgestaan door een bureau BA met een formatie van 7 fte'en; bezetting 8 (7 burgerfunctionarissen, 1 militair), van wie 2 deeltijders.

De BA heeft een nadere uitwerking van het gestelde in het DBB gegeven in Ministeriële Publikaties (MP) en wel in de delen: MP10-10/2 (Beveiliging NAVO/WEU gegevens), MP10-10/3 (Beveiliging van staatsgeheimen en vitale onderdelen/objecten); MP10-10/4 (Beveiliging van gemerkte gegevens).

De delen zijn vastgesteld op verschillende data:

- deel 10/10/2 is van november 1998;
- deel 10/10/3 is van 1 oktober 1992;
- deel 10/10/4 is van 1 juni 1993.

Oorspronkelijk was ook voorzien in uitgifte van de delen 5 Handboek beveiliging materieel en personeel en 6 Beveiliging van geautomatiseerde gegevensverwerkende systemen.

De uitgifte van deel 5 is in de ontwikkelingsfase stopgezet omdat het vanwege de decentrale verantwoordelijkheid voor de uitvoering van de beveiliging niet doelmatig bleek om een defensiebreed geldend handboek in te voeren. De geplande ontwikkeling van deel 6 werd in de praktijk ingehaald door de uitgifte van het Voorschrift Informatiebeveiliging Rijksoverheid. Om praktische redenen is daarom de uitwerking van het (deel)beleid informatiebeveiliging niet vastgelegd in een nieuw deel 6, maar in separate defensiebreed geldende beleidsdocumenten.

De uitvoering van het defensiebeleid is gedecentraliseerd. Om deze reden is er door de BA geen overkoepelend plan van aanpak voor de uitvoering van integrale beveiliging gemaakt. De wijze waarop hier invulling aan wordt gegeven is een verantwoordelijkheid van de defensieonderdelen. Door verschillen in taakstelling kan dit in de praktijk leiden tot een verschillende aanpak van de uitvoering van het beleid.

3.2 Rol onderdelen

De Algemene Rekenkamer is nagegaan op welke wijze de doorvertaling en uitvoering van het beveiligingsbeleid bij de acht organisatieonderdelen concreet gestalte heeft gekregen.

Sommige onderdelen hebben de informatiebeveiliging als invalshoek voor het beveiligingsbeleid van het onderdeel gekozen. Ze kijken vanuit de informatiebeveiliging welke aanvullende maatregelen voor de fysieke beveiliging noodzakelijk zijn.

Andere onderdelen werken met beveiliging gebaseerd op het principe van integrale veiligheidszorg. Hierbij worden naast de beveiligingsaspecten ook andere aspecten meegenomen, zoals brandweezorg, milieuzorg en Arbozorg. Tussen de onderdelen die werken met het principe van de integrale veiligheidszorg zijn wel verschillen in diepgang en uitwerking van het beleid vast te stellen.

Weer andere onderdelen leggen de nadruk bij de beveiliging op de Krijgsmachtsleutelpuntenlijst. Dit is een lijst van vitale objecten die essentieel worden geacht voor de operationele inzet van de krijgsmacht. De bevelhebbers, commandant DICO en plaatsvervangend secretaris-generaal bepalen welke objecten op deze lijst worden geplaatst. Er hoeft per definitie geen overeenstemming te zijn tussen de objecten, die volgens het DBB als te beveiligen objecten zouden moeten worden aangemerkt en de objecten op de Krijgsmachtsleutelpuntenlijst. Een commandant kan bijvoorbeeld bepaalde materiële voorzieningen, die hij van vitaal belang acht voor de operationele inzet, op de Krijgsmachtsleutelpuntenlijst plaatsen terwijl deze volgens het DBB tot categorie 4 behoren. Andersom kan het DBB voorschrijven dat bijvoorbeeld bepaalde informatie tot categorie 1 behoort terwijl de commandant deze van geen belang acht voor de operationele inzet.

3.2.1 Toezicht Beveiligingsautoriteit

In het kader van het DBB oefent de BA toezicht uit op de deugdelijkheid van de beveiliging. Hij rapporteert zijn bevindingen schriftelijk aan de SG.

Om een goede uitvoering van het beveiligingsbeleid te waarborgen, is een regelmatige beoordeling van de uitvoering, prestaties en effecten van het gevoerde beveiligingsbeleid en het stelsel van de geïmplementeerde beveiligingsmaatregelen noodzakelijk. De controles zullen conform het vastgestelde defensiebeveiligingsbeleid periodiek moeten plaatsvinden door:

- de veiligheidsfunctionaris namens de commandant (beveiligingsmaatregelen);
- de beveiligingscoördinator namens de bevelhebber (krijgsmachtdebeleid);
- de Beveiligings Autoriteit namens de SG (beraad);
- de MIVD (militaire veiligheid).

De Algemene Rekenkamer is nagegaan op welke wijze de BA hierover wordt geïnformeerd.

De voornaamste rapportagelijijn loopt via de zogenoemde toprapportages, een driemaal per jaar uit te brengen rapportage. Hierin wordt onder meer gevraagd naar de stand van zaken betreffende de fysieke en personele beveiliging, maar het accent ligt vanwege de druk die de invoering van het VIR met zich meebrengt toch vooral op de deeltaak Informatiebeveiliging. Wel is het aandeel van de fysieke en personele beveiliging in de toprapportages merkbaar groeiende. De bijdrage van de BA in dit geheel is een appreciatie van de beveiligingsbijdragen in de toprapportages ten behoeve van de SG voor het politiek beraad.

De informatievraag geschiedt op basis van de door de BA aangegeven matrix.

Verder wordt de BA onder meer via de incidentenrapportage (tweemaal per jaar) en door middel van overleg op de hoogte gehouden van de ontwikkelingen.

Het feitelijke toezicht op de opzet en werking van de beveiliging wordt – namens de BA – uitgevoerd door de Audit Dienst Defensie (ADD), door middel van audits naar de stand van de beveiliging. Deze actie is in het voorjaar van 2003 gestart na een verzoek van de SG. Inmiddels is in juli 2003 een rapport Quick scan fysieke en personele beveiliging aan de BA aangeboden. Hierin wordt speciale aandacht gevraagd voor de volgende punten:

- het in overeenstemming brengen van de personele beveiliging met de bestaande wet- en regelgeving;
- het opstellen van richtlijnen door de BA ten aanzien van de beveiligings-eisen die worden gesteld aan onderdelen, die van groot belang zijn voor de instandhouding van de slagkracht.

4 FYSIEKE BEVEILIGING OBJECTEN

4.1 Inleiding

De Algemene Rekenkamer is bij 19 militaire objecten nagegaan of het beveiligingsbeleid optimaal werd uitgevoerd. Daarbij heeft zij gelet op de volgende voorwaarden: zij heeft gekeken of er bij de objecten veiligheidsfunctionarissen en -plannen aanwezig zijn. Voorts heeft zij onderzocht welke organisatorische, bouwkundige en elektronische maatregelen de onderdelen hebben getroffen of zullen treffen om een met de beveiligingscategorieën overeenkomend niveau van beveiliging te realiseren. Tevens is onderzocht welke middelen de minister van Defensie hiervoor ter beschikking heeft gesteld en of deze toereikend zijn. Vervolgens keek de Algemene Rekenkamer naar enkele overige aspecten, zoals evalueren en testen van de beveiliging.

Zij deed dit door bezoeken aan 19 geselecteerde defensieobjecten bij de acht organisatieonderdelen, verdeeld over hoofdkwartieren, magazijnen en overige objecten (waaronder onder andere een zend- en ontvangststation, een kazerne, een vliegbasis en een kantoorpand). Driekwart van de objecten komt uit de hoogste categorieën.

4.2 Veiligheidsfunctionaris

Niet alle militaire objecten hebben een veiligheidsfunctionaris (VF). Bij sommige objecten is de functie van veiligheidsfunctionaris een hoofdtaak en in andere gevallen een neventaak. Bij 6 van de 19 objecten is de VF-functie onvervuld, danwel is onduidelijk wie formeel verantwoordelijk is voor de uitoefening van deze functie. Dit is het geval bij 4 onbemande objecten. In één geval is een medewerker ter plekke aangewezen als VF bij het bezoek van de Algemene Rekenkamer.

De VF bij de onderzochte objecten volgde in de regel geen specifieke opleiding voor zijn functie.

Opvallend is voorts het grote aantal vacatures bij bureaus van de VF-en. Personen die bij bureaus van de VF werken worden vaak langdurig aan hun functie onttrokken door bijvoorbeeld uitzendingen.

4.3 Beveiligingsplan

De Algemene Rekenkamer is nagegaan of er op het niveau van de objecten een beveiligingsplan is en zo ja, op welke wijze de maatregelen (op het gebied van beveiliging) daarin zijn opgenomen.

Het merendeel van de objecten heeft een beveiligingsplan, zij het dat het in 6 van de 19 gevallen om concepten gaat, die nog door de verantwoordelijke commandant moeten worden goedgekeurd. Voor 2 objecten is slechts een verouderd c.q. onvolledig beveiligingsplan beschikbaar, terwijl voor 2 andere objecten in het geheel geen plan voorhanden is. De beveiligingsplannen zijn in het algemeen opgesteld volgens de zogenaamde Haagse Methodiek, danwel een variant hiervan. De uitwerking hiervan leidde, door de toegepaste methoden, tot per organisatieonderdeel verschillende uitkomsten.

In het beveiligingsplan van een aantal objecten staat dat de bestaande beveiligingsmaatregelen rond het object niet voldoende zijn.

4.4 Personele, financiële en materiële middelen

De beschikbaarheid van voldoende personele, financiële en materiële middelen vormt een belangrijke voorwaarde bij de uitvoering van het beveiligingsbeleid. De Algemene Rekenkamer is nagegaan welke middelen de onderdelen hiervoor hebben ingezet en of deze toereikend zijn.

De P-, F- en M-middelen nodig voor de beveiliging van militaire objecten worden in het algemeen niet in de – puur operationele – beveiligingsplannen aangegeven.

Uit de gehouden interviews maakt de Algemene Rekenkamer op dat defensie voor beveiligingsmaatregelen die beslist nodig zijn, uiteindelijk geld vrijmaakt, maar dat er voor verdergaande beveiligingsmaatregelen nauwelijks geld wordt verstrekt. Deze formulering duidt er al op dat de objecten zelf veelal niet de beschikking hebben over een beveiligingsbudget. Afhankelijk van de hoogte van de investering moeten de onderdelen op een hoger niveau in de organisatie (de resultaat verantwoordelijke eenheid danwel de staf van het organisatieonderdeel) een beroep doen.

De beschikbaarheid van voldoende beveiligingspersoneel op de objecten vormt ook een punt van zorg. In zijn algemeenheid geldt dat de formatie krap voldoende is om de beveiligingstaken uit te voeren; dit leidt ertoe dat in het weekend en bij ziekte regelmatig surveillanceronden uitvallen.

4.5 Overige aspecten

Het beveiligingsplan vermeldt de concreet te nemen maatregelen. De Algemene Rekenkamer constateert dat deze vereiste maatregelen bij vele objecten traag tot nagenoeg niet worden geïmplementeerd. In een aantal gevallen gaat het zelfs om maatregelen, die betrekkelijk eenvoudig zijn te realiseren, zoals bijvoorbeeld het plaatsen van detectiemiddelen. Hierdoor bestaat bij een aantal objecten een restrisico, dat de verantwoordelijke commandant kennelijk accepteert.

Interne voorlichting en opleiding beschouwt de Algemene Rekenkamer als essentieel voor het welslagen van (de uitvoering van) het beveiligingsbeleid.

Geen van de objecten beschikt over een voorlichtingsplan, waarin aandacht wordt besteed aan het aspect beveiliging.

In de praktijk heeft de Algemene Rekenkamer overigens nog de meeste voorlichtingsaffiches aangetroffen in de kamers van de VF-en zelf.

Opleidingen op het gebied van beveiliging (met name betreft dit interne bedrijfsopleidingen) worden veelal centraal geregeld. Bij één organisatieonderdeel bestaan problemen bij het behoud van de verkregen vaardigheden, zoals het toepassen van gewelddsmiddelen en het schieten (geven van voldoende instructie-uren aan het beveiligingspersoneel).

4.6 Veiligheidsinbreuken

De Algemene Rekenkamer heeft onderzocht of de lagere niveaus van de defensieorganisatie beschikken over juiste en voldoende sturingsinformatie en die ook weer doorgaven aan het hogere niveau.

In de praktijk blijkt dit met name neer te komen op de veiligheidsinbreuken. Veiligheidsinbreuken zijn vrijwel altijd onderwerp van interne rapportage aan de commandant en ook aan de BC van het betrokken

organisatieonderdeel. In het algemeen wordt volgens een standaard format volstaan met een beschrijving van de geconstateerde incidenten, zonder nadere analyse en eventuele follow-up. Een constant en frequent terugkerend incident betreft het niet afsluiten van deuren en ramen in gebouwen na kantoortijd.

4.7 Evaluatie werking

Om een goede uitvoering van het beveiligingsbeleid te waarborgen is een regelmatige beoordeling van onder meer (het gehele stelsel van) de geïmplementeerde beveiligingsmaatregelen noodzakelijk. Deze controles dienen – namens de commandant – periodiek plaats te vinden door de informatiebeveiligings-/veiligheidsfunctionaris (DBB, punt 2.8).

De Algemene Rekenkamer heeft in de beveiligingsplannen evenwel geen plan of beschrijving voor het testen van de getroffen beveiligingsvoorzieningen aangetroffen. Niettemin hebben toch nog 6 VF-en aangegeven zelf speciale testen uit te voeren.

De Algemene Rekenkamer is vervolgens nagegaan of er periodiek een in- en/of externe audit van het beveiligingssysteem wordt gehouden en of daarvoor een procedure was.

In de beveiligingsplannen van slechts enkele organisatieonderdelen is aangegeven dat er audits moeten worden uitgevoerd hoewel dit naar de mening van de Algemene Rekenkamer noodzakelijk is. Slechts bij 7 van de 19 objecten blijkt een dergelijke interne security-audit inmiddels ook te zijn uitgevoerd.

De ADD verricht thans een defensiebrede audit op beveiligingsbeleid. Twee van de door de Algemene Rekenkamer onderzochte objecten zijn inmiddels ook door de ADD geëvalueerd. De bevindingen stemmen overeen.

4.8 Test Algemene Rekenkamer

De Algemene Rekenkamer heeft bij de onderzochte objecten als regel ook zelf een praktijktest uitgevoerd, door bijvoorbeeld een beveiligingsronde mee te maken. Bij deze testen heeft zij een ruim aantal tekortkomingen in de beveiliging geconstateerd.

Voorbeelden van gebreken die de Algemene Rekenkamer bij de objecten heeft geconstateerd:

- niet gegarandeerde aanrijtijd en/of patrouillefrequentie;
- elektronische detectie of signalering ontbreekt;
- burgers op defensieterrein zonder begeleiding en zichtbare identificatie;
- cameratoezicht onvoldoende dekkend;
- interne regels voor het aanbieden van te vernietigen documenten overtreden;
- op eenvoudige wijze toegang tot object mogelijk;
- verwijderen classificatie van bouwtekeningen;
- op vrij betreedbaar grasveld geplaatste koeling van server;
- open deuren die beslist gesloten moeten zijn.

Bezien per objectcategorie (hoofdkwartieren, magazijnen en overige objecten) acht de Algemene Rekenkamer de beveiligingssituatie bij:

- de hoofdkwartieren toereikend, zij het met uitzondering van één object;
- de magazijnen toereikend, met uitzondering van twee objecten;
- de overige objecten toereikend, met uitzondering van drie objecten.

Zes van de 19 onderzochte objecten voldoen dus niet aan de eisen die aan de fysieke beveiliging gesteld moeten worden.

In een aantal van die zes gevallen onderkent defensie de bestaande onvolkomen beveiligingssituatie overigens wel, maar heeft het verantwoordelijke management deze – uitgaande van een tijdelijke situatie – geaccepteerd.

In enkele gevallen acht de Algemene Rekenkamer de situatie dusdanig alarmerend, dat zij aanbeveelt alsnog per direct aanvullende beveiligingsmaatregelen te treffen, zodat gewichtige belangen van de Staat niet in gevaar komen.

4.9 Getroffen maatregelen

Door het bureau BA wordt, aan de hand van de objectverslagen van de Algemene Rekenkamer, intussen al gewerkt aan een verbeterplan. Door het bureau BA wordt daarbij niet uit het oog verloren, dat de waarnemingen van de Algemene Rekenkamer bij de 19 onderzochte objecten zich ook elders kunnen voordoen.

5 PERSONELE BEVEILIGING

5.1 Algemene Beveiligingseisen voor defensie opdrachten

MP 10-10/3, artikel 45, behandelt het buiten de rijksdienst brengen van staatsgeheimen. Voor de defensieorganisatie is de zogenaamde regeling Algemene Beveiligingseisen voor Defensie opdrachten (ABDO-regeling) van toepassing. De ABDO-regeling stelt eisen aan het kennismaken door derden van gerubriceerde informatie dan wel andere gewichtige belangen van de Staat. Derden kunnen op twee manieren te maken krijgen met gerubriceerde informatie:

- defensie brengt gerubriceerde informatie, voor een goede voortgang van de werkzaamheden, buiten de defensieorganisatie,
- defensie schakelt natuurlijke of rechtspersonen in voor werkzaamheden aan een object van defensie.

Alvorens gerubriceerde informatie buiten defensie gebracht wordt, dient de SG of een door hem aangewezen ambtenaar vast te stellen dat het buiten de defensieorganisatie brengen van de gerubriceerde informatie noodzakelijk is voor een goede voortgang van de werkzaamheden en dat er voldoende waarborgen aanwezig zijn, dat de gerubriceerde informatie zal worden beveiligd.

Voordat natuurlijke of rechtspersonen worden ingeschakeld bij opdrachten waarbij gerubriceerde informatie dan wel andere gewichtige belangen van de Staat in het geding zijn of waarbij deze op grond van de te verrichten werkzaamheden ontstaan, dient de verwervende instantie zich vooraf bij de MIVD ervan te overtuigen dat die natuurlijke of rechtspersonen hiervoor geautoriseerd zijn.

Van belang in dit verband is het onderscheid in behoeftesteller en verwervende instantie:

- onder behoeftesteller wordt verstaan (de commandant van) het militaire object dat om de uit te voeren werkzaamheden vraagt;
- onder verwervende instantie wordt verstaan de instantie die de opdracht gunt.

Bij defensie zijn behoeftesteller en verwervende instantie over het algemeen gescheiden. Binnen defensie is de Dienst Gebouwen, Werken en Terreinen (DGW&T) de verwervende instantie op het gebied van infrastructurele aanbestedingen. DGW&T beheert het onroerend goed van defensie in technische en juridische zin en zorgt voor de bouw en het onderhoud. Daarbij gaat het om het voorbereiden van nieuwbouw- en onderhoudswerkzaamheden, het aanbesteden van werken en het voeren van directie tijdens de uitvoering. Ook de bediening en controle van installaties behoort tot de taken van de directie. Een vergelijkbare situatie doet zich voor ten aanzien van de Defensie Telematica Organisatie (DTO). DTO draagt zorg voor een doeltreffende en doelmatige dienstverlening op het gebied van informatie- en communicatie-technologie. Beide organisaties zijn agentschappen.

De ABDO-regeling voorziet er in dat de verwervende instantie zorg draagt voor, onder andere, de rubriceringsaanduidingen binnen de opdracht, melding van plaatsing van de opdracht aan de MIVD, periodieke melding van aan de opdrachtnemer verstrekte gerubriceerde informatie en melding van de afloop van de opdracht.

5.2 Werking in de praktijk

De Algemene Rekenkamer constateert dat er in de praktijk veel onduidelijkheid bestaat over wie in het kader van deze regeling welke verantwoordelijkheden heeft: de behoeftesteller of de verwervende instantie. Dit blijkt uit het volgende:

- bij de onderzochte objecten, waarvan een groot aantal behorend tot de hoogste categorie, gaat men er vanuit dat de verwervende instantie verantwoordelijk is voor de uitvoering van de ABDO-regeling;
- van de veiligheidscoördinator van DGW&T heeft de Algemene Rekenkamer vernomen dat de commandanten van de objecten binnen de verschillende beleidsterreinen van defensie verantwoordelijk zijn voor de uitvoering van de ABDO-regeling. De plaatsvervangend directeur van één van de uitvoerende directies van DGW&T deelt deze mening;
- bij het onderzoek heeft de Algemene Rekenkamer veelal niet gerubriceerde tekeningen etc. van categorie 1 en 2 objecten aangetroffen. Navraag bij de bezochte uitvoerende directie van de DGW&T levert op, dat deze directie zich op het standpunt stelt dat er niet met gerubriceerde tekeningen, bestekken etc van categorie 1 en 2 objecten gewerkt kan worden in verband met de openbare aanbesteding van werken. Reden om deze stukken niet te rubriceren.

Vorenstaande situatie leidt er toe dat:

- volgens de veiligheidscoördinator van de DGW&T er heel weinig gebruik wordt gemaakt van de ABDO-regeling. Als dit voorkomt, dan is dit op verzoek van de commandanten van objecten;
- slechts bij enkele van de onderzochte gerubriceerde objecten, voorzover van toepassing, is de veiligheidsfunctionaris of commandant op de hoogte van de toepassing van de ABDO-regeling bij de uitvoering van werkzaamheden door derden aan het object;
- het hoofd van de sectie Industrieveiligheid van de MIVD desgevraagd te kennen gaf, dat de ABDO-regeling, met betrekking tot het uitvoeren van gerubriceerde werkzaamheden door derden op defensie-objecten, slecht wordt nageleefd;
- bij categorie 1 en 2 objecten uiterst voorzichtig wordt omgegaan met gerubriceerde gegevens, terwijl aan dit aspect bij de externe aanbesteding en uitvoering van werkzaamheden op deze objecten onvoldoende aandacht wordt besteed.

5.3 Getroffen maatregelen

De commandant DICO heeft naar aanleiding van de bevindingen van de Algemene Rekenkamer intussen al een commissie van onderzoek ingesteld die tot taak heeft vast te stellen wat de oorzaak is van de constatering van de Algemene Rekenkamer, in te schatten welke schade is geleden en aanbevelingen te doen ter voorkoming van het geconstateerde. De commissie heeft in november 2003 haar rapport aan de commandant DICO uitgebracht.

5.4 Screening intern personeel

De Wet veiligheidsonderzoeken regelt de wijze waarop functionarissen, op daarvoor in aanmerking komende functies, onderwerp dienen te zijn van veiligheidsonderzoeken. Deze veiligheidsonderzoeken hebben, al naar gelang van de aard van de functie, een verschillende diepgang. In de regel dient eens in de vijf jaar een herhaling van het onderzoek plaats te vinden.

De Algemene Rekenkamer is nagegaan op welke wijze de personele beveiliging bij de objecten in de normale bedrijfsvoering is geregeld. Hierbij heeft de Algemene Rekenkamer een aantal tekortkomingen geconstateerd:

- een tweetal VF-en heeft bij functieaanvaarding een niet bijgehouden administratie inzake de afgegeven verklaringen van geen bezwaar aangetroffen en zijn dus noodgedwongen gestart vanuit een achterstandssituatie. De hieruit voortvloeiende inhaalslag, resulterend in een stuwmeer aan aanvragen (herhalings-) veiligheidsonderzoek bij de MIVD, is in volle gang maar nog niet afgerond;
- bij één object is de personele beveiligingstaak slecht geregeld en wordt zij onvoldoende uitgevoerd.

De personele beveiliging voldoet in deze gevallen derhalve niet aan de gestelde wet- en regelgeving.

Als defensiebreed naar de praktijk wordt gekeken, dan levert dat het volgende beeld op.

Bij drie van de acht onderzochte onderdelen bestaat geen systeem waarin de vertrouwensfuncties systematisch zijn vastgelegd. Daarnaast hebben eveneens drie onderdelen geen zicht op de geldigheid van de verklaringen van geen bezwaar die zijn afgegeven na een veiligheidsonderzoek. In de praktijk komt het dan ook regelmatig voor dat personen van wie de geldigheidsduur van de verklaring van geen bezwaar is overschreden vertrouwensfuncties vervullen. Bij twee onderdelen geldt dit ten tijde van het onderzoek voor circa 50% van de vertrouwensfuncties. Bij een van deze onderdelen waren inmiddels wel maatregelen getroffen om aan deze ongewenste situatie een einde te maken.

5.5 Getroffen maatregelen

Naar aanleiding van de bevindingen van de Algemene Rekenkamer heeft de secretaris-generaal intussen al verbetermaatregelen genomen. In zijn brief van 13 november 2003, BA/2003007820, aan de organisatieonderdelen stelt de secretaris-generaal dat binnen zes maanden geheel voldaan dient te zijn aan het gestelde in de Wet op de veiligheidsonderzoeken. Binnen die periode dienen de organisatieonderdelen aan te kunnen tonen, dat voor al het personeel op vertrouwensfuncties een verklaring van geen bezwaar is afgegeven op het bij de functie behorende niveau die niet ouder is dan vijf jaar.

6 CONCLUSIES EN AANBEVELINGEN

6.1 Conclusies

De Algemene Rekenkamer concludeert dat:

- de invulling van de functie van de Beveiligingsautoriteit onvoldoende gestalte heeft gekregen waardoor organisatieonderdelen zelf invulling zijn gaan geven aan het beveiligingsbeleid. Dit leidt tot verschillende invalshoeken bij de invulling daarvan. Tot maart 2003, het tijdstip van inschakeling van de Audit Dienst Defensie, heeft het ontbroken aan daadkrachtig toezicht door de Beveiligingsautoriteit op de organisatieonderdelen;
- bij zes van de 19 onderzochte defensieobjecten voldoet de beveiliging niet aan de daaraan te stellen eisen. De problemen zitten daarbij niet zozeer in de gekozen beveiligingssystematiek, die over het algemeen goed is. Het achterblijven van de uitvoering brengt echter wel risico's met zich mee;
- de regeling Algemene Beveiligingseisen Defensie Opdrachten wordt slecht toegepast waardoor niet gescreend extern personeel kennis kan nemen van gerubriceerde informatie of andere gewichtige belangen van de Staat;
- de Wet veiligheidsonderzoeken, die de screening van defensiepersoneel op vertrouwensfuncties regelt, wordt in de praktijk slecht toegepast waardoor ten tijde van het onderzoek bij twee onderdelen 50% of meer van de vertrouwensfuncties werd vervuld door personeel zonder geldige screening.

6.2 Aanbevelingen

De Algemene Rekenkamer beveelt de minister van Defensie aan om daadwerkelijk invulling te geven aan de functie van de Beveiligingsautoriteit, waardoor deze zijn beleidsbepalende, beleidsuitdragende en toezichthoudende functie kan vervullen. Daarnaast beveelt de Algemene Rekenkamer aan er zorg voor te dragen dat de fysieke beveiliging van militaire objecten in de praktijk wordt uitgevoerd.

Ten slotte zou defensie de regeling Algemene Beveiligingseisen Defensie Opdrachten onverkort moeten toepassen en de Wet veiligheidsonderzoeken moeten naleven.

7 REACTIE EN NAWOORD

7.1 Reactie minister

De minister van Defensie heeft op 19 december 2003 gereageerd op het conceptrapport van de Algemene Rekenkamer. In zijn reactie stelt de minister dat hij ervoor zal zorgen dat de fysieke beveiliging van militaire objecten in de praktijk wordt uitgevoerd. Hij zegt toe dat de tekortkomingen in de beveiliging bij vijf van de zes militaire objecten in januari 2004, zonedig met alternatieve of interimmaatregelen, verholpen zijn. Bij het zesde object zal dit in februari 2004 het geval zijn. Verder gaat het Ministerie van Defensie een grootschalige inventarisatie houden om te bezien of de bevindingen van de Algemene Rekenkamer ook voor de niet bezochte objecten gelden. Op basis van deze inventarisatie zal defensie maatregelen ter verbetering formuleren, die in verbeterplannen worden opgenomen.

De directie financieel-economische zaken en de Beveiligingsautoriteit zullen de verbeterplannen bewaken volgens dezelfde controlesystematiek als de verbeterplannen voor de onderwerpen financieel en materieel beheer. De minister geeft aan dat het ministerie de functie van de Beveiligingsautoriteit en de daadwerkelijk invulling daarvan mee zal nemen in de studie naar de nieuw te vormen bestuursstaf en bij de herstructurering van de beveiligingsorganisatie. Daarbij zal de minister de bevindingen van de Algemene Rekenkamer ten aanzien van de invulling van de functie van de Beveiligingsautoriteit, mee laten wegen.

De minister stelt voorts dat hij, als het gaat om toezicht op de uitvoering van het beleid, hecht aan de verantwoording van de bevelhebbers aan hem. Volgens de minister moet de bevelhebber voor de invulling van zijn rapportage aan de minister steunen op zowel zijn ondercommandanten als de betrokken veiligheidsfunctionarissen en de beveiligingscoördinator. Een, met personeel, ingevulde beveiligingsorganisatie is daarvoor een randvoorwaarde aldus de minister. In de verbeterplannen zijn inspecties opgenomen van de beveiligingsorganisatie door de Audit Dienst Defensie.

De minister stelt dat hij de conclusies en aanbevelingen van de Algemene Rekenkamer ter harte neemt op het punt van de regeling Algemene Beveiligingseisen voor Defensie Opdrachten. Het ministerie gaat dit punt in de verbeterplannen oppakken door een combinatie van een inventarisatie van lopende werkzaamheden op militaire objecten en een intensievere voorlichting over de toepassing van de regeling. Daarnaast zal de Audit Dienst Defensie in de integrale beveiligingsaudits beoordelen of de regeling ook wordt gehandhaafd.

Over de personele beveiliging van intern personeel deelt de minister mee, dat het overgrote deel van het bestand vertrouwensfuncties binnen defensie is geactualiseerd. Daarnaast vindt er een grootschalige inventarisatie plaats van de bijbehorende verklaringen van geen bezwaar. Uit de voorlopige resultaten blijkt, aldus de bewindsman, dat vrijwel iedere werknemer in het bezit is van een verklaring van geen bezwaar op het juiste niveau maar dat deze vaak ouder is dan vijf jaar. De minister spreekt de verwachting uit dat de personele beveiliging ultimo 2004 door een grote inspanning op orde zal zijn.

7.2 Nawoord Algemene Rekenkamer

De Algemene Rekenkamer heeft met instemming kennis genomen van de door de minister reeds genomen en aangekondigde maatregelen. Door deze maatregelen zullen de beveiliging bij objecten en de personele beveiliging, zowel voor intern als extern personeel, in 2004 sterk kunnen verbeteren. Echter, om te voorkomen dat op grond van de genomen maatregelen de zaak éénmalig op orde wordt gebracht maar dat in de toekomst de aandacht hiervoor weer verslapt, is het noodzakelijk deze aspecten systematisch in de organisatie van defensie in te bedden.

De Algemene Rekenkamer zal de ontwikkelingen met aandacht blijven volgen en en stelt zich voor over enige tijd een vervolgonderzoek uit te voeren.

Conclusies	Aanbevelingen	Toezeggingen
De invulling van de functie van de Beveiligingsautoriteit heeft onvoldoende gestalte gekregen waardoor organisatie-onderdelen zelf invulling geven aan het beveiligingsbeleid. Dit leidt tot verschillende invalshoeken bij de invulling daarvan.	De Algemene Rekenkamer beveelt de minister van Defensie aan om daadwerkelijk invulling te geven aan de functie van de Beveiligingsautoriteit waardoor deze zijn beleidsbepalende, beleidsuitdragende en toezichthoudende functie kan vervullen.	De invulling van de functie van de Beveiligingsautoriteit wordt meegenomen in de studie naar de nieuw te vormen bestuursstaf en bij de herstructurering van de defensie organisatie.
Tot maart 2003, inschakeling Audit Dienst Defensie, heeft het ontbroken aan daadkrachtig toezicht door de beveiligingsautoriteit op de organisatieonderdelen.		De ADD zal audits uitvoeren naar de beveiliging van militaire objecten
Bij zes van de 19 onderzochte defensie-objecten voldoet de beveiliging niet aan de daaraan te stellen eisen. De problemen zitten daarbij niet zozeer in de gekozen systematiek van beveiliging, die over het algemeen goed is, maar in het risicovol achterblijven van de uitvoering.	De Algemene Rekenkamer beveelt aan er zorg voor te dragen dat de fysieke beveiliging van militaire objecten in de praktijk wordt uitgevoerd.	Bij vijf van de zes objecten zal de beveiliging in januari 2004 op orde zijn. Bij het zesde object in februari 2004. Bij de overige objecten zal een inventarisatie worden gehouden teneinde te bezien of de door de Algemene Rekenkamer geconstateerde tekortkomingen zich ook daar voor doen. Op basis van deze inventarisatie zullen de benodigde maatregelen worden genomen.
De regeling Algemene Beveiligingseisen Defensie Opdrachten wordt slecht toegepast waardoor niet gescreend extern personeel kennis kan nemen van gerubriceerde informatie of andere gewichtige belangen van de Staat.	Defensie zou de regeling Algemene Beveiligingseisen Defensie Opdrachten onverkort moeten toepassen.	De conclusies en aanbevelingen worden ter harte genomen. Door een combinatie van een inventarisatie van lopende werkzaamheden en een intensievere voorlichting wordt aan een verbetering van de situatie gewerkt.
De Wet veiligheidsonderzoeken, die de screening van defensiepersoneel op vertrouwensfuncties regelt, wordt in de praktijk slecht toegepast waardoor ten tijde van het onderzoek bij twee onderdelen 50% of meer van de vertrouwensfuncties werd vervuld door personeel zonder geldige screening.	De Wet veiligheidsonderzoeken moet worden nageleefd.	De personele beveiliging zal ultimo 2004 op orde zijn.

Nawoord

De Algemene Rekenkamer heeft met instemming kennisgenomen van het antwoord van de Minister. De Algemene Rekenkamer overweegt op termijn een vervolgonderzoek in te stellen.