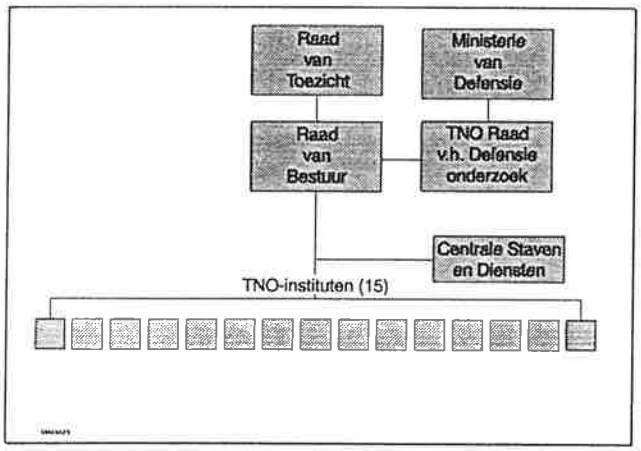
TERREIN- EN OBJECTBEWAKING

Ir. Huub van Hoof
TNO-FEL

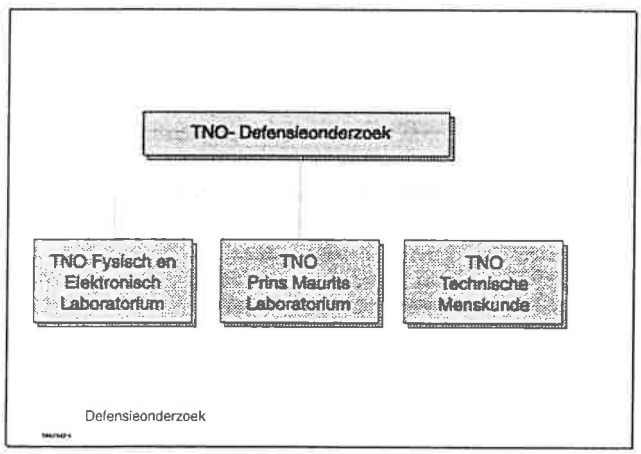
Security Beurs Utrecht
Oktober 1995

OVERZICHT

1. Inleiding TNO
2. Inleiding TNO-FEL
3. Beveiligingsconcept
4. Elektronische middelen
5. Financiële afwegingen bij beveiliging
6. Afsluiting



Er bestaan in Nederland 15 TNO instituten. Het hoogste bestuurscollege van TNO is de Raad van Toezicht. Deze Raad van Toezicht heeft een status die vergelijkbaar is met die van een Raad van Commissarissen in het bedrijfsleven. De leiding van de organisatie berust bij de Raad van Bestuur. Een speciale relatie met de overheid bestaat er ten aanzien van het defensie-onderzoek, dat binnen TNO wordt uitgevoerd. Daarvoor is de Raad van Defensieonderzoek in het leven geroepen.



Er zijn drie laboratoria binnen TNO voor defensie-onderzoek. De primaire opdrachtgever voor deze laboratoria is hier het Ministerie van defensie; een deel van de onderzoekscapaciteit is ook voor de civiele markt beschikbaar (zowel nationaal als internationaal).

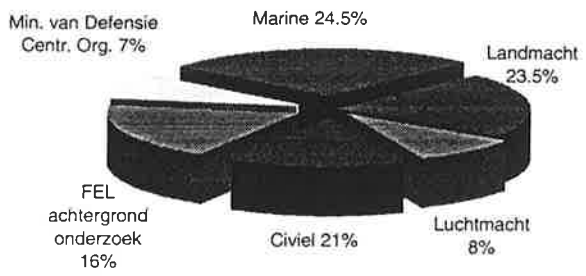
Missie TNO-DO

1 Ondersteuning van Defensie en krijgsmacht door inbreng van toegepast onderzoek en technologische ontwikkelingen
2 Bijdragen aan het Defensie-technologiebeleid, nationaal en internationaal
3 Onderzoek en ontwikkeling voor civiel gebruik op speciale gebieden ("spin-off")

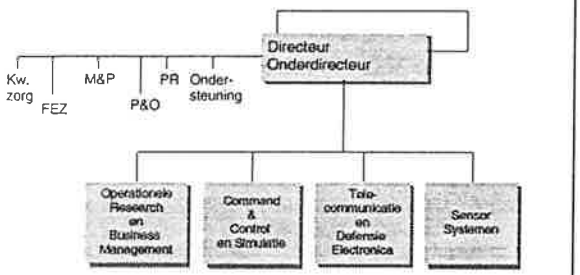
Defensieonderzoek

Enkele belangrijke thema's uit het TNO-Defensie-onderzoek zijn:
- command, control, communications and intelligence
- sensoren en sensorintegratie
- simulatie en training
- wapenbeheersing en verificatie
- nieuwe materialen
- inzet en werking van wapensystemen
- mens-machine-interface
- radar, communicatie, fysica en akoestiek
- informatietechnologie en systeemontwikkeling
- operationele research
- toxische stoffen en explosieveiligheid
- explosieven, munitie, ballistiek, wapeneffectiviteit
- zintuigelijke waarnemening, ergonomie en taakbelasting

TNO-FEL Opdrachtgevers 1994



Deze figuur geeft een indruk van de opdrachtgevers van het TNO Fysisch en Elektronisch Laboratorium (FEL). De verwachting is dat het percentage "civiel" nog een lichte groei te zien zal geven.

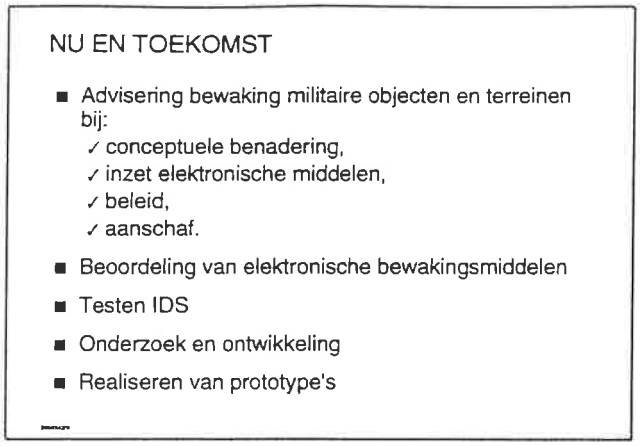


In deze figuur is het organisatiediagram van het TNO-FEL geschetst. De naamgeving van de divisies geeft globaal het werkterrein aan.

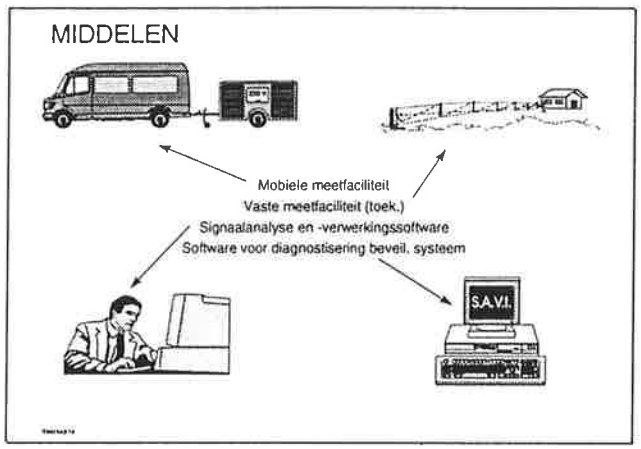
ERVARING OBJECT- EN TERREINBEWAKING

- Advisering bewaking militaire objecten en terreinen bij:
  - ✓ conceptuele benadering,
  - ✓ inzet elektronische middelen,
  - ✓ beleid,
  - ✓ aanschaf.
- Beoordeling van elektronische bewakingsmiddelen
- Testen IDS

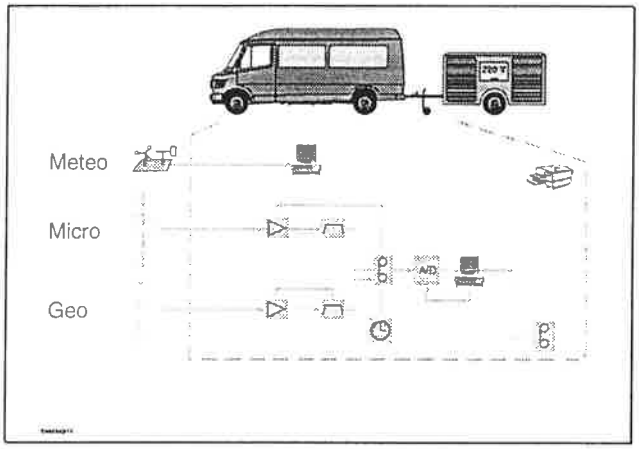
Het is duidelijk dat bij Defensie allerlei zaken spelen op het gebied van Beveiliging. Als gevolg van de rol, die de TNO Defensielaboratoria hebben t.o.v. Defensie, is bij TNO-DO kennis aanwezig van vrijwel alle aspecten op het gebied van Beveiliging. De expertise bij TNO-FEL ligt voornamelijk op het gebied van informatie-beveiliging en beveiliging van objecten en terreinen met behulp van elektronische middelen. Op het onderwerp "object- en terreinbewaking" wordt in deze presentatie wat nader ingaan. De expertise op dit gebied is voor het grootste deel opgebouwd via opdrachten van en voor Defensie. Onder meer was TNO-FEL betrokken bij advisering, beoordeling en het testen van IDS. Mede in het kader van activiteiten in NATO-verband zijn vele internationale contacten op dit gebied ontstaan.



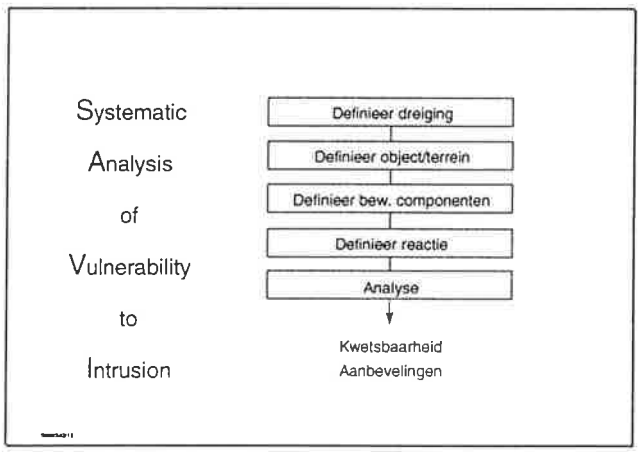
De huidige en voorgenomen activiteiten zijn weergegeven in deze figuur, en omvatten voornamelijk consultancy, het testen van IDS, onderzoek, ontwikkeling en de realisatie van prototypes en demonstrators.



Om de genoemde activiteiten te kunnen uitvoeren beschikt het FEL over een aantal faciliteiten waarvan er in deze figuur enige zijn opgesomd.



Voor onderzoek en/of metingen op locatie staat een mobiel laboratorium ter beschikking, dat is ondergebracht in een royale (verlengde) Mercedesbus. In de figuur is de bus voorzien van diverse data acquisitie apparatuur voor het onderzoek van het gedrag van seismische en akoestische sensoren onder diverse omgevingscondities.



Een ander voorbeeld van de "tools" waarover we beschikken is het software-pakket "Systematic Analysis of Vulnerability to Intrusion" (SAVI). Dit pakket is een sterk stuk gereedschap bij het evalueren van de kwaliteit van objectbeveiligingconcepten.

BEVEILIGINGSCONCEPT

"BEVEILIGEN IS INVESTEREN IN VEILIGHEID"

Coherente analyse van:

- Dreiging
- Ontmoedigingsmaatregelen
- Bewaking (IDS'n & Verificatie)
- Reactie
- Vertragingsmaatregelen

"Goed beveiligen is niet goedkoop, maar het is investeren in veiligheid (bovendien, niet of niet goed beveiligen kan soms een stuk duurder uitpakken)".
Dit citaat, dat ik ten volle onderschrijf, legt aan de ontwerper van een beveiligingssysteem de verplichting op om eerst goed na te denken alvorens daadwerkelijk te investeren. De vraag is nu hoe men bij het ontwerpen van een beveiligingsplan te werk moet gaan. Helaas bestaat er geen éénduidig recept. Dat komt omdat een aantal aspecten van invloed zijn op het ontwerp. Bovendien hangen die aspecten meestal ook weer onderling van elkaar af. De belangrijkste aspecten zijn in deze figuur weergegeven.

DREIGINGSANALYSE

- Wat beschermen tegen wie ?
- Type (gelegenheids, beroeps...)
- Hoeveel ?
- Gewapend ?
- Gewiekst ?
- Gereedschap ?
- Overdag/'s-nachts ?
- Indringen op meer plaatsen tegelijk ?
- Indringpoging te voet of per "shovel"
- Beschermen tegen "worst case" dreiging ?
- ....
- ....

De eerste vraag die men zich dient te stellen, is tegen wie of wat men zich wil beschermen (dreigingsanalyse). Om hiervan een beeld te krijgen kan men zich het soort vragen stellen zoals er een paar in deze figuur zijn gegeven.

ONTMOEDIGINGSMAATREGELEN

- Hekwerk
- Bouwkundige voorzieningen
- Sloot
- Betonnen bloembakken
- ....
- ....

Mede afhankelijk van het resultaat van de dreigingsanalyse, is het heel goed denkbaar dat met een aantal relatief simpele maatregelen de dreiging (of bepaalde soorten van de dreiging) effectief verminderd kan worden. Ik noem dit preventieve maatregelen ter ontmoediging van bepaalde groepen potentiële indringers; een paar voorbeelden zijn in de figuur genoemd.

BEWAKING (I.D.S. & VERIFICATIE)

- Kans op detectie
- Kans op valse alarmeringen
- Kans op "nuisance" alarmeringen
- Omgevingsinvloed
- Alarmverificatie

In deze figuur zijn (afgezien van de kosten) de belangrijkste zaken opgesomd die een rol spelen bij de keuze van elektronische bewakingsmiddelen.

REACTIE

- Mankracht
- Omvang
- Snelheid
- Uitrusting
- ....
- ....

Het is duidelijk dat een IDS dat een alarm kan genereren geen doel op zichzelf is. Nadat een alarm is gegenereerd (en eventueel na verificatie is gebleken dat het een terecht alarm is), dient er een reactie te komen. Het hele beveiligingsconcept staat of valt met de juiste responsie na een alarm. Degene(n) die verantwoordelijk is (zijn) voor die reactie dient daarom adequaat te zijn uitgerust om die taak te kunnen uitvoeren. Wat het betekent om "adequaat te zijn uitgerust" is afhankelijk van wat men wil bewerkstelligen bijv. voorkómen van schade, voorkómen van diefstal, arrestatie van indringer, identificatie van indringer, etc.

VERTRAGINGSMAATREGELEN

- Stel kritische tijdlijn op

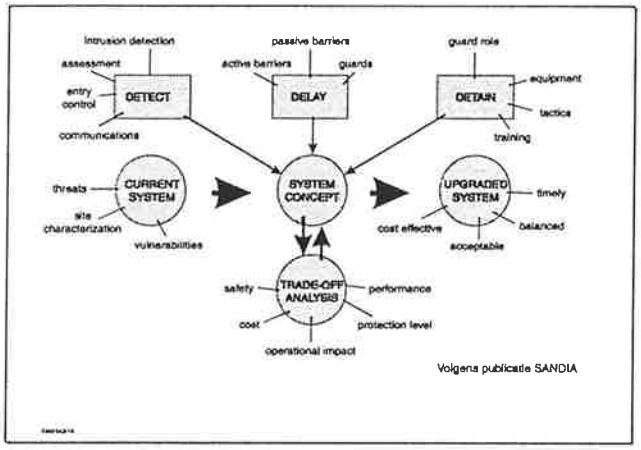
  "detectie" ➡ "indringpoging geslaagd"

- Stel kritische tijdlijn op

  "detectie" ➡ "neutralisatie indringpoging"

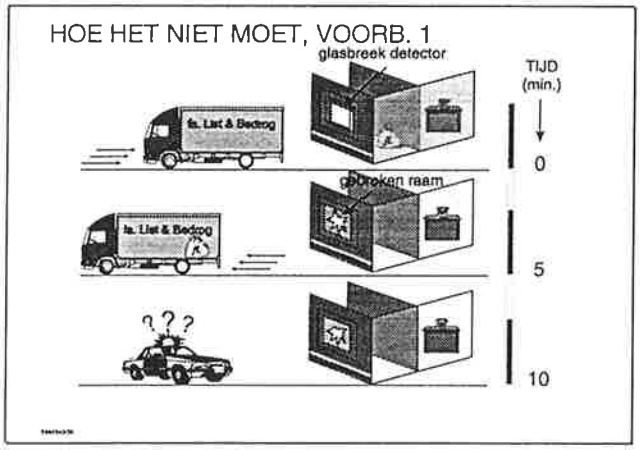
- Vergelijk deze lijnen en ontwerp obstakels (vertraging) om adequate reactie mogelijk te maken

In de vorige figuur is al het woord "snelheid" gevallen. Ook is gesteld dat een goede IDS (goede bewaking) geen enkele garantie is voor een goede beveiliging. Na een alarmering dient er een reactie te komen, en wel op tijd. Het is daarom van groot belang na te gaan hoe het vermoedelijke tijdsverloop is van de indringpoging (vanaf detectie) in vergelijking met dat van de eigen responsie hierop. Uit het vergelijken van deze "tijdlijnen" kunnen conclusies worden afgeleid voor wat betreft de noodzakelijk aan te brengen obstakels in het ene pad (vertraging), of voor het versnellen van de responsietijd. Voor grote objecten met vele sensoren en aangebrachte obstakels is SAVI bij uitstek geschikt voor het beoordelen van dit soort aspecten.
Conclusie: Voor een goed beveiligingsconcept dient tussen al de genoemde taken en functies een juiste balans gevonden te worden. Een goede analyse en het onderkennen van de onderlinge samenhang van alle aspecten is een minimum voorwaarde om te komen tot een goede oplossing van een beveiligingsprobleem.



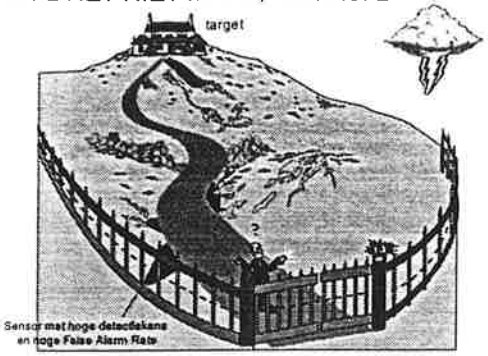
In deze figuur is in compacte vorm het voorgaande nog eens samengevat (naar een publicatie van SANDIA).

HOE HET NIET MOET, VOORB. 1



Ondanks de logica van het voorgaande ziet men toch vaak dat tegen een aantal elementaire regels gezondigd wordt. Ik heb hiervan 2 voorbeelden geillustreerd.
Het eerste voorbeeld is triviaal en spreekt voor zich: ondanks het plaatsen van een glasbreukdetector en een aansluiting op een alarmcentrale is de beveiliging van bijvoorbeeld een antieke vaas op de vensterbank slecht doordacht. Door het schatten van de tijdlijnen had de eigenaar dit zelf kunnen bedenken.

HOE HET NIET MOET, VOORB. 2



In dit voorbeeld heeft de eigenaar een IDS aangeschaft met een hoge detectiewaarschijnlijkheid. De omgevingscondities waarin het systeem moet functioneren blijken echter van dien aard dat ook de FAR relatief hoog is. Na een aantal malen valse alarmering zullen degenen die de reactie moeten verzorgen, sterk gedemotiveerd raken.

INDELING NAAR:

- Invloedssfeer van de sensor (punt, lijn, sector)
- Actieve of passieve sensoren
- Sensoren voor toepassing binnen of buiten
- Statische of gemakkelijk verplaatsbare sensoren
- ....

Aan het einde van het traject van zo'n systematische analyse zoals beschreven, volgt een aanpak, bestaande uit bijvoorbeeld het treffen van bouwkundige voorzieningen, organisatorische maatregelen, inschakelen van diensten, aanschaffing van IDS, etc. Ik ga hier niet in de volle breedte op in, maar ik zal mij beperken tot een aantal opmerkingen die speciaal betrekking hebben op elektronische sensoren bij de bewakingsfunctie. Voor een systematische opsomming van deze sensoren kunnen verschillende categorie-indelingen worden gebruikt.

VOORGESCHIEDENIS IDS

- Ontwikkeling eenvoudige/goedkope sensoren in USA t.b.v. gevechtsveld bewaking en doel-opsporing in Vietnam
- "Unattended Ground Sensors" of "Remote Sensors"
- Mystic Mission
- Toepassingen in Europa, ook IDS

De herkomst van deze middelen stamt eigenlijk uit de periode van het Vietnam-conflict. In die tijd zijn door de Amerikanen op grote schaal allerlei - niet beeldverwerkende - sensoren ontwikkeld die bedoeld waren om de waarneming voor de Amerikaanse soldaten in de Vietnamese jungle te verbeteren. Dat waren meestal expendables, klein en goedkoop, die later "remote sensors" of "unattended groundsensors" werden genoemd. Begin jaren '70 kwam die kennis naar Europa (onder meer via een door Amerikanen georganiseerde demonstratie in Duitsland: Mystic Mission) met het doel te onderzoeken of dit soort systemen ook in de Europese "environment" toegepast kon worden. Deze demonstratie heeft zeker de ontwikkeling bevorderd om deze sensoren toe te passen bij de elektronische bewaking.

BUITEN LIJNSENSOREN

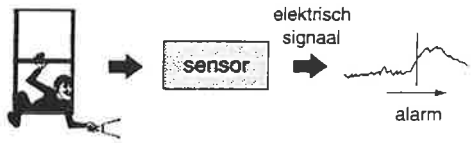
- Microgolf (bi/mono), EM veld, Seismisch, Seismisch-magnetisch, Leaky wave coax, Heksensoren, Infrarood (passief/actief)

FACTOREN VAN INVLOED

- Topografie, vegetatie, aanwezigheid wild, bodemeigenschappen, meteo, grondtrillingen, hoogspanningslijnen, EM, bliksem, etc

Deze figuur geeft een overzicht van een aantal veel voorkomende buitensensoren met daarbij een aantal omgevingscondities die bij IDS voor gebruik buiten zeker van invloed zijn.

SENSORFUNCTIE



Een indringpoging heeft een fysisch verschijnsel tot gevolg die door de sensor wordt omgezet in een elektrisch signaal. Een IDS bevat verder meer of minder intelligente elektronica die het signaal analyseert en uiteindelijk tot een oordeel komt: wel of geen indringer.

INDRINGACTIE VERSUS IDS TYPE

	Micro	EM	Seism	Seism/Mag	Leaky	Hek	IR
Norm. lopen	b	a	b	c	c	•	a
Langz. lopen	c	d	c	b	d	•	c
Hard lopen	a	e	a	d	e	•	d
Sluipen	d	a	d	e	b	•	a
Hek klimmen	•	d	•	•	•	b	•
Hek knippen	•	a	•	•	•	d	•
.....							

a, b, c, etc. : relatieve detectiekans
• : niet van toepassing

Bij de beoordeling van een IDS zijn nog de volgende opmerkingen te maken. Een indringer gaat niet volgens een standaard procedure te werk, d.w.z. dat dus ook het opgewekte sensorsignaal niet uniek is; de vorm van het signaal zal sterk afhangen van de wijze waarop de "fysische gebeurtenis" plaats heeft. De intelligentie van de elektronica of van het algoritme dient zo goed mogelijk hierin te voorzien teneinde een zo hoog mogelijke detectiebetrouwbaarheid te hebben. Als echter, door welke oorzaak dan ook, een signaal in de sensor wordt opgewekt dat enigszins lijkt op de categorie signalen die door een indringpoging wordt veroorzaakt, dan zal een IDS eveneens een alarm genereren: ditmaal dus een ongewenst alarm. Bij het maken van een keuze van IDS zijn dit zaken om rekening mee te houden. In plaats van uitvoerig per sensortype hierop in te gaan, zijn een paar voorbeelden gegeven van hulpmiddelen die bij zo'n beoordeling behulpzaam kunnen zijn. In deze figuur zijn een aantal dreigingen in matrixvorm uitgezet tegen het type IDS; de getallen in de matrix zijn willekeurig.

OMGEVINGSINVLOED VERSUS IDS TYPE

	Micro	EM	Seism	Seism/Mag	Leaky	Hek	IR
Wind	e	b	a	c	d	a	e
Harde wind	a	a	b	d	a	e	e
Regen	b	e	c	e			
Sneeuw	e	a	d	a			
Mist	d	c	a				
Lawaai	c	b					
Klein wild	c						
Groot wild	a						
Vogels	d						
Bliksem	a						
Hoogsp. leid.	a						
.....							

a, b, c, etc. : relatieve FAR

In deze figuur is een tweede hulpmiddel geïllustreerd dat gebruikt kan worden bij het beoordelen van IDS. In deze matrix kan worden aangegeven wat het verband is tussen een aantal omgevingscondities en de werking van verschillende typen IDS. Met name bij het gebruik van buitensensoren zijn dit aspecten die zeker in beschouwing moeten worden genomen.

GLOBALE KOSTEN ELEKTRONISCHE MIDDELEN

- Kosten aanschaf/installatie/integratie/opleiding: f X.=
- Ontwerpkosten: a % van f X.=
- Bedrijfskosten/afschrijving: b % van f X.= per jaar
- Kosten in stand houden: c % van f X.=

In het voorgaande is gesteld dat "beveiligen investeren is in veiligheid". Hierbij hoort natuurlijk een prijs. Die prijs wordt niet alleen bepaald door de aanschafkosten, er komen ook andere kosten bij. Maar als men besluit dat een perimeter om een object of een terrein bewaakt moet worden, dan kan men een (financiële) vergelijking te maken tussen het bewaken met moderne elektronische middelen enerzijds, en de kosten die men zou moeten maken bij een conventionele manier van bewaken (door patrouillering met mankracht).

Bij het realiseren van een beveiligingssysteem met elektronische middelen krijgt men globaal te maken met kosten van de aanschaf/installatie (IDS'n, bekabeling, centrale, evt. integratie met bestaande systemen, etc). Voordat het zover is moet er natuurlijk nagedacht worden, er moet een ontwerp en een planning gemaakt worden, en ook dat kost tijd en dus geld. Verder zijn er personele kosten, kosten voor afschrijving, voor onderhoud en reparaties etc. De kosten hiervan zijn allemaal redelijk te schatten.

VERGELIJKING KOSTEN

Moeilijk, omdat

- vermoeidheidsverschijnselen patrouille
- invloed weersomstandigheden
- afschrikking bewapende patrouille
- misleiding patrouille versus misleiding sensor
- .....

Om de kosten te schatten die men zou hebben bij patrouillering met mankracht, is een eenvoudig model gebruikt. Voor een eerlijke vergelijking moet de patrouillegang zodanig gedimensioneerd zijn dat in beide gevallen sprake is van ongeveer gelijke detectiekans. Natuurlijk is het lastig te vergelijken; het model is simpel en houdt geen rekening met het feit dat een patrouille last heeft van vermoeidheidsverschijnselen, dat de alertheid niet constant is, dat een patrouille een indringer misschien meer afschrikt, etc. Desondanks toch een vergelijking ter indicatie.

KOSTEN BEWAKING MET PATROUILLES (1)

- waarneem afstand is maximaal R meter
- hekwerk levert maximale vertraging van T_1 sec.
- indringer heeft T_2 sec. nodig om zich binnen de perimeter weer te kunnen verschuilen
- patrouille heeft een loopsnelheid van v (m/s)

Hieruit volgt:

w = door patrouille bewaakte perimeterlengte = $2[s + (T_1 + T_2)v]$ meter

Voor een perimeterbewaking met patrouillegang zitten de kosten vooral in de benodigde mankracht. Om hiervan een schatting te geven is het volgende aangenomen:

- waarneem afstand is maximaal R meter (d.w.z. voor een afstand groter dan R is een indringer niet zichtbaar of hoorbaar voor de patrouille)
- hekwerk levert een maximale vertraging van T1 sec.
- indringer heeft T2 sec. nodig om zich binnen de perimeter weer te kunnen verschuilen
- patrouille heeft een loopsnelheid van V m/s

Hieruit volgt een maximale detectieafstand patrouille-indringer van ca.

[R + (T1 + T2)V] meter.

Als verder wordt aangenomen dat de patrouille constant zicht heeft op een totale perimeterlengte van 2R ("voor en achter"), dan is de (momentaan) door een patrouille bewaakte perimeterlengte w:

w = 2[R + (T1 + T2)V] meter.

KOSTEN BEWAKING MET PATROUILLES (2)

- Uit de vorige sheet volgt: N = W/w patrouilles tegelijk nodig (W=totale perimeter lengte)
- Voor een 8 urige werkdag dus 3N patrouilles per etmaal, of 365 x 3N patrouilles per jaar
- Voor een patrouille van M personen dus (365 x 3 x N x M) mandagen per jaar
- Een werknemer werkt gemiddeld zo'n 200 dagen per jaar, dus de benodigde hoeveelheid personeel (365 x 3 x N x M)/200, d.i. ongeveer 5NM

Wat betekent dit nu voor een perimeter van totaal W meter, waarbij als eis gesteld wordt dat de hele perimeter 24 uur per etmaal onder bewaking is (zoals bij een elektronisch bewaakte perimeter) ? Uit de figuur volgt dat hiervoor dus N = W/w patrouilles tegelijk nodig zijn. Voor een 8 urige werkdag betekent dit dus 3N patrouilles per etmaal, of, 365 * 3N patrouilles per jaar. Als een patrouille uit M personen bestaat, komt men op een totaal van (365 * 3 * N * M) mandagen per jaar. Een werknemer werkt gemiddeld zo'n 200 dagen per jaar, zodat de benodigde hoeveelheid personeel ongeveer

[(365 * 3 * N * M)/200] is.

AFSLUITING

- Achtergrond op het gebied van beveiliging
- Overzicht systematische benadering bij object- en terreinbeveiliging
- "Tools" voor analyse
- Overzicht elektronische middelen, factoren van invloed
- Aangetoond dat "kosten" een relatief begrip is

Inlichtingen:
TNO-FEL
Oude Waalsdorperweg 63
2597 AK Den Haag
tel. 070 - 3264221
fax. 070 - 3280961
Email: vanHoof@fel.tno.nl

Referenties:

- Militaire Spectator 7, 1988 (pp320-325): "Onbemande grondsensors"
- Militaire Spectator 5 1989 (pp226-230): "Helikopterdetectie met akoestische middelen"
- DRG Proceedings on.future battle field ,London, Oct. 1992 (pp9.2 I-9.2 XIV): "Ground sensors"
- Militaire Spectator,.Mei 1993 (pp212-217): "Object- en terreinbeveiling"
- Beveiliging, nr.1 jaargang 7, 1994: "Indringerdetectie met behulp van seismiek"
- TNO Magazine TW, April 1994

TECHNO DAGEN

TECHNO VISION & SOLUTION

INFORMATIEBEVEILIGING, PRAKTISCH BEKEKEN

HOUDT UW INFORMATIE BESCHIKBAAR, INTEGER, VERTROUWELIJK
DINSDAG 3 OKTOBER

En

MANAGEN VAN BEVEILIGING

BEDRIJFSRISICO'S, VEILIGHEIDSBELEID EN INTEGRALE VEILIGHEIDSZORG
WOENSDAG 4 OKTOBER

DE NOODZAAK VAN INFORMATIE-BEVEILIGING, PRAKTISCH BEKEKEN

Voorzitter:
De heer R.H. van Nie RA
KPMG EDP Auditors, Den Haag

CODES, PROCEDURES,
GELDVERKEER, TELECOMMUNICATIE

Voordrachten door:

R.H. van Nie RA	KPMG EDP Auditors
E.P. Austin	General Electric Information Services
Dr.Ir. P.L. Overbeek	KPMG EDP Auditors
Ir. G.J. Schuringa	RABO Bank Nederland

HET MANAGEN VAN BEVEILIGING

Voorzitter
De heer F. van Zegveld

NIEUWE EN ONMISBARE
TECHNOLOGISCHE KENNIS

Voordrachten door:

J.C. van der Wolk	KPN Risicom Recherche BV
C.A. van Zwam	Nederlandse Veiligheidsdienst Nederland BV
Ir. H.A.J.M. van Hoof	TNO-FEL Defence Research
P.W.M. Payens	Nedap NV

MET VRIJ BEZOEK AAN DE BEURS SECURITY '95

DINSDAG 3 OKTOBER **WOENSDAG 4 OKTOBER**

JAARBEURS CONGRESCENTRUM UTRECHT, PARALLEL AAN BEURS SECURITY '95