Clingendael Centre for Strategic Studies

Oude Waalsdorperweg 63
Postbus 96864
2509 JG Den Haag

www.CCSS.nl

T 070 374 00 0047
F 070 328 09 61
info@www.ccss.nl

CCSS-rapport

CCSS-06-006

Denk- en datamodel Suspicious Signs

Deze rapportage vormde een deelaspect van een groter onderzoek

Datum	juli 2006
Auteur(s)	J.G.M. Rademaker MTL Prof. dr. R. de Wijk dr. E. Bakker J. Jansen Mr. J. Stad ir. C.J. den Hollander drs. A.A. de Jong

Rubricering rapport	Ongerubriceerd
Titel	Ongerubriceerd
Managementsamenvatting	Ongerubriceerd
Rapporttekst	Ongerubriceerd
Bijlagen	Ongerubriceerd
Exemplaarnummer	
Oplage	6
Aantal pagina's	50 (excl. distributielijst)
Aantal bijlagen	3

Het 'Clingendael Centrum voor Strategische Studies' is een joint venture van het Nederlands Instituut voor Internationale Betrekkingen 'Clingendael' en de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO.

Managementsamenvatting

Titel	:	Denk- en datamodel Suspicious Signs
Auteur(s)	:	Deze rapportage vormde een deelaspect van een groter onderzoek J.G.M. Rademaker MTL Prof. dr. R. de Wijk dr. E. Bakker J. Jansen Mr. J. Stad ir. C.J. den Hollander drs. A.A. de Jong
Datum	:	3 juli 2006
Opdrachtnr.	:	
Rapportnr.	:	CCSS-06-006

Probleemstelling

Het Clingendael Centrum voor Strategische Studies (CCSS) heeft op verzoek van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een onderzoek uitgevoerd naar een nieuw denk- en datamodel om op proactieve wijze een goede informatiepositie op te bouwen over potentiële dreigingen en risico's.
Dit rapport betreft een gedeeltelijke rapportage van het uitgevoerde onderzoek.

Beschrijving van de werkzaamheden

Tijdens het onderzoek is zowel een kwantitatieve als kwalitatieve analyse uitgevoerd om de onderzoeksvraag te beantwoorden. Hierbij is gebruik gemaakt van veel verschillende expertise en innovatieve tooling.

Resultaten en conclusies

Tijdens dit onderzoek is een denk- en datamodel ontwikkeld voor het spotten van verdachte signalen die mogelijkerwijs aanwijzingen zijn voor potentieële dregingen en risisco's.

Toepasbaarheid

Het ontwikkelde model kan helpen bij de mogelijke verdere operationalisering van de informatieanalyse capaciteit in het kader van de nationale veiligheid.

Project
Projectbegeleider
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Projectleider
J.G.M. Rademaker, TNO Defensie en Veiligheid
Projecttitel
Quick Scan Suspicious Signs
Projectnummer
Projectplanning
Start November 2003 Gereed Maart 2004
Projectteam
E. Bakker, A. de Jong, J. Jansen, R. Korteweg, J. Stad, C. van Steijn, R. de Wijk, J. de Wit

Inhoudsopgave

Managementsamenvatting **2**

Afkortingen **5**

1 Inleiding **6**
1.1 Achtergrond 6
1.2 Doelstelling 6
1.3 Definitie Suspicious Signs 6
1.4 Werkwijze 6
1.5 Engelse taal 7
1.6 Afbakening werkgebied 7
1.7 Leeswijzer 7

2 Modelvorming en analyse **8**
2.1 Inleiding 8
2.2 Denkmodel 8
2.3 Datamodel 9

3 De uitwerking van het denkmodel **14**
3.1 Uitwerking fases 14
3.2 Het onderkennen van suspicious signs per fase 17
3.3 Ernst en waarschijnlijkheid 17
3.4 De toepassing van het datamodel 19
3.5 Categorieën van gewelddadige organisaties 25
3.6 De aanpak van de analyse 28

4 Algemene analyse resultaten **32**
4.1 Inleiding 32
4.2 Werkwijze in de verschillende suspicious signs fases 32
4.3 Analyse van het inlichtingenproces 38

5 Conclusies en aanbevelingen **40**
5.1 Inleiding 40
5.2 Conclusies 40
5.3 Aanbevelingen 41

6 Referenties **43**

7 Ondertekening **44**

Bijlage(n)
A Datamodel sub-templates
B Relaties en suspicious signs fases
C Typeringen voor intelligence

Afkortingen

BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CEECE	Coalition to End Experiments on Chimpanzees in Europe
INTREPS	Intelligence reports
IVP	Inlichtingenverzamelplan
OC&W	Onderwijs, Cultuur & Wetenschap
PARANOID	Program for Analysis, Retrieval and Navigation On intelligence Data

1 Inleiding

> *'Our noise-to-signal ratio is twenty to one, that one being something useful. Not necessarily tactically useful, just remotely useful. But even this is misleading, because it's twenty to one after we've done all sorts of things to make it humanly intelligible. You have to collect, process, translate, move it down the funnel, transform it from noise into a signal, before you know if it's useful'.*
>
> Generaal Michael Hayden, directeur van de NSA geciteerd door J. Goldberg in The New Yorker (10 februari 2003)

1.1 Achtergrond

Dit onderzoek geeft een methodologische aanzet tot brede analyse van potentiële dreigingen en daarbij behorende verdachte signalen of *suspicious signs*.

1.2 Doelstelling

De opdracht aan het Clingendael Centrum voor Strategische Studies (CCSS) voor dit onderzoek bestaat uit een nieuw denk- en datamodel om op proactieve wijze een goede informatiepositie op te bouwen over potentieële dreigingen en risico's in het kader van de nationale veiligheid.

1.3 Definitie Suspicious Signs

Om potentiële dreigingen tegen personen of objecten te onderkennen, moet in een vroegtijdig stadium een aantal indicatoren zichtbaar worden gemaakt. Het vermoeden van een potentiële dreiging is aan de orde, als een aantal verdachte signalen of suspicious signs zich op enig moment in hun onderling verband voordoet. De voor dit onderzoek gehanteerde definitie van een suspicious sign is:

Een combinatie van indicaties dat een persoon of een groep van personen de potentie en/of intentie heeft een bedreiging te vormen voor personen of objecten.

Door in een vroegtijdig stadium deze indicaties waar te nemen, kunnen de juiste instanties tijdig en gepast een risicoanalyse uitvoeren en eventueel daaruit voortvloeiende bewakings- en beveiligingsmaatregelen treffen.

1.4 Werkwijze

Allereerst is een denkmodel ontwikkeld. Dit geeft aan op welke wijze inlichtingendata ten behoeve van een brede analyse van potentiële bedreigingen kunnen worden verzameld. Om vervolgens een analyse van inlichtingendata te kunnen uitvoeren, is het noodzakelijk de verzamelde informatie op een gestructureerde manier te kunnen weergeven. Het datamodel brengt deze structuur aan.

1.5 Engelse taal

In het rapport wordt veelvuldig gebruik gemaakt van engelse woorden. Hiervoor is gekozen omdat het onderscheidend vermogen van het Engels groter is en veel van het ‘jargon’ uit het Engels afkomstig is.

1.6 Afbakening werkgebied

Het stelsel Bewaken en Beveiligen reikt verder dan terrorisme; daarom is het werkgebied uitgebreid naar gewelddadige actie in algemene zin. Hieronder vallen dus ook gewelddadige criminaliteit en andere vormen van gewelddadige actie.

Voor dit rapport zijn de volgende definities gehanteerd:

Terrorisme:	**het plegen van of dreigen met op mensenlevens gericht geweld, met als doel maatschappelijke veranderingen te bewerkstelligen of politieke besluitvorming te beïnvloeden (Site www.AIVD.nl).**
Criminaliteit:	**het geheel van handelingen of het begaan van handelingen die verboden zijn of het nalaten van plichten die zijn opgelegd door de wet en waarbij de dader strafbaar is volgens deze wet (Merriam Webster online dictionary).**
Gewelddadige actie:	**actie waarbij geweld (uitoefening van macht) gebruikt wordt (Van Dale).**

1.7 Leeswijzer

Hoofdstuk 2 bevat een beschrijving van het gehanteerde denk- en datamodel. Daarnaast is beschreven hoe de informatieverwerking van de verschillende risico’s, suspicious signs en categorieën terrorisme en ‘gewelddadige’ acties is gestructureerd.
Vervolgens is in hoofdstuk drie het denkmodel verder uitgewerkt.
Tenslotte wordt het rapport afgesloten met conclusies, observaties en aanbevelingen.

2 Modelvorming en analyse

2.1 Inleiding

In dit hoofdstuk worden de uitgangspunten en het raamwerk voor de nadere analyse van de onderzoeksopdracht beschreven. Om te kunnen bepalen welke data (mogelijk) relevant zijn om suspicious signs te kunnen onderkennen, is het van belang een *denkmodel* ter beschikking te hebben. Het denkmodel gaat uit van een pro-actieve benaderingswijze, om een risico's voor personen en objecten te kunnen inschatten. Er wordt dus niet uitgegaan van het reageren op dreigingen, maar van een brede analyse van potentiële dreigingen zodat preventief of pre-emptief kan worden gehandeld.

Voor het onderzoek is ook een *datamodel* ontwikkeld dat TNO al grotendeels in eerder onderzoek had ontwikkeld. Het gaat hier om het dataverwerkingsprogramma PARANOID. Het denkmodel en het datamodel worden in dit hoofdstuk nader uitgewerkt en toegelicht.

2.2 Denkmodel

Het denkmodel geeft richting aan het vergaren van data over aanslagen en incidenten, de prioriteitsstelling daarbij en de analyse van de beschikbare gegevens. Het denkmodel geeft aan hoe en wanneer suspicious signs in welke vorm kunnen worden onderkend.

Suspicious signs zijn gedefinieerd als:

Een combinatie van indicaties dat een persoon of een groep van personen de potentie en/of intentie heeft een bedreiging te vormen voor personen of objecten.

In het denkmodel wordt ervan uitgegaan dat de aanloop naar gewelddadige actie verschillende *fases* kent, namelijk:

1 Occasion
2 Trigger
3 Rumbling
4 Work-up Process
5 Violent Action

De wijze waarop suspicious signs kunnen worden onderkend, verschilt per fase. Tijdens de eerste fase vereist dit bijvoorbeeld brede, multidisciplinaire analyses om inzicht te krijgen in trends die op termijn repercussies kunnen hebben voor de dreiging voor personen en objecten. De *trendanalyse* is hiervoor een belangrijk instrument. Tijdens de vervolgfases wordt het onderkennen van suspicious signs concreter en meer operationeel.

De benodigde capaciteit voor het vergaren van inlichtingen neemt dus in de vervolgfases toe. Daarom is *prioriteitstelling* ten aanzien van meer specifieke inlichtingen gewenst. Dit is afhankelijk van de *ernst* en *waarschijnlijkheid* van aanslagen tegen personen en objecten die bijvoorbeeld aan de trends kunnen worden ontleend. Ernst en waarschijnlijkheid spelen ook een sleutelrol bij het stellen van prioriteiten tijdens lopende activiteiten ter vergaring van inlichtingen.

Verder is voor het onderkennen van suspicious signs een *categorie-indeling* van dreigingen van groot belang. Deze bepaalt tevens de *methode* die wordt gehanteerd bij het vergaren van inlichtingen. Voor het inschatten van de risico's voor een persoon of object zal bij groepen vooral vanuit de daders worden geredeneerd; bij 'stand alone' daders of 'gekken' vanuit het slachtoffer zelf. Met andere woorden, bij het opstellen van risico-profielen moet worden bezien welke groeperingen een bedreiging voor personen of objecten kunnen vormen, terwijl ook moet worden bezien welke gevaaraantrekkende aspecten gerelateerd kunnen worden aan personen of objecten. Bij 'stand alone' daders zijn uitsluitend de gevaaraantrekkende aspecten van personen en objecten relevant.

De volgende categorieën kunnen worden onderscheiden:
1 Binnenlands religieuze organisaties
2 Buitenlandse/transnationale religieuze organisaties
3 Binnenlands etnische/separatistische organisaties
4 Buitenlandse/transnationale etnische/separatistische organisaties
5 Binnenlands politieke organisaties
6 Transnationaal politieke organisaties
7 Buitenlands politieke organisaties
8 Binnenlands criminele organisaties
9 Buitenlandse/transnationale criminele organisaties
10 'Stand alone' dader
11 'State agents' c.q. 'State agencies'

Deze indeling wordt in dit onderzoek gebruikt voor het verzamelen, verwerken en analyseren van gegevens. Om de validiteit van het denkmodel te bepalen, is daarom een aantal cases onderzocht, deze vormen geen onderdeel van deze rapportage.

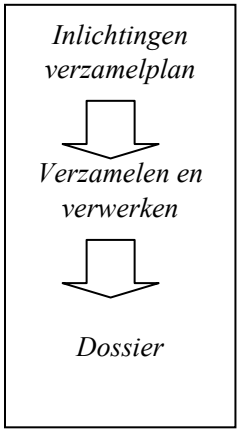
In Paragraaf 3.4 wordt de relatie tussen ernst, waarschijnlijkheid en de categorieën inzichtelijk gemaakt.

2.3 Datamodel

Het datamodel is de praktische doorvertaling van het denkmodel en bevat alle elementen die nodig zijn om de verzamelde data gestructureerd te verwerken en op te kunnen slaan als inlichtingenkennis. Het datamodel vereist allereerst een inlichtingenverzamelplan als basis voor het efficiënt verzamelen en verwerken van data.

2.3.1 Inlichtingenverzamelplan

Aan de hand van onder andere een mogelijk verdacht signaal wordt een inlichtingenverzamelplan (IVP) opgesteld om aanvullende, verifiërende en ondersteunende informatie te zoeken. Hierbij wordt een aantal vragen opgesteld met eventueel een afbakening in tijd en ruimte. Het IVP is daarmee richtinggevend bij de volgende stap in het proces, namelijk het verzamelen en verwerken van data.



Verzamelen en verwerken

Verzamelen betreft het zoeken, extraheren en registreren van gegevens over personen, organisaties, gebeurtenissen, etc. De gegevens kunnen aan diverse bronnen onttrokken worden; denk aan databases en documenten, maar ook aan de kennis van een analist of expert. Verwerken betreft het evalueren, analyseren, integreren en interpreteren van de verzamelde gegevens.

Tools, modellen en/of templates bieden ondersteuning bij het verzamelen van gegevens. Eén en ander mondt uit in de aanmaak van een gestructureerd dossier, dat de gegevensverwerking kan ondersteunen. Het dossier speelt vaak een cruciale rol bij het verzamelen en verwerken van gegevens, daarom beschrijven we het nader.

Dossier
Het dossier vormt de geïntegreerde weergave van de beschikbare gegevens. In het dossier zijn alle bekende gegevens over een onderwerp opgeslagen. Hierbij is het begrip 'onderwerp' breed te interpreteren; er kan bijvoorbeeld gedacht worden aan*: 'Vermeende toename terreur van activistengroep Lekker Fruit', 'Evaluatie '11 september'; hoe heeft het zover kunnen komen?', 'Afpersing Begrafenisonderneming Zand erover',* en *'Activiteiten MWS'*.

De gebundelde kennis over een onderwerp kan geanalyseerd worden en de resultaten daarvan kunnen worden toegevoegd aan het dossier. Ook het begrip 'analyse' is breed te interpreteren. Het gaat hier bijvoorbeeld om overzichten van gebeurtenissen die met elkaar in verband staan, om overzichten van groepssamenstellingen, maar ook om trendanalyses en intelligence reports (INTREPS).

Kortom, het dossier biedt ondersteuning bij het structureren van beschikbare en nieuw binnenkomende kennis over een bepaald onderwerp, met als doel het verkrijgen van:
- Situational awareness (wat gebeurt er nu)
- Situational assessment (wat is er nu aan de hand)
- Threat assessment (wat kan er gebeuren)

Met name de situational assessment en de threat assessment bevatten bruikbare aanknopingspunten voor eventueel uit te voeren (risico-)analyses.

Een dossier bestaat in de regel uit drie groepen:

Groep 1
Deze groep bevat zaken die gebeurtenissen in gang zetten of plaats laten vinden. Dit betreft vaak persoonlijke of groepsgebonden redenen, die op te splitsen zijn in:
- aanleidingen/motieven (motives)
- doelstellingen (objectives)

Onderstreept dient te worden dat deze redenen (samengenomen in de term mojectives, omdat ze voor het datamodel dezelfde orde of soort vertegenwoordigen) een vrij indirect karakter kunnen hebben, het kan hierbij bijvoorbeeld gaan om feiten die een subjectieve lading gekregen hebben. Denk aan belangrijke data als: *'Sterfdag van een persoon die door een groepering bestempeld is als martelaar', 'De datum 11 september', 'Volle maan'*, etc.

Groep 2
Deze groep bevat informatie over organisaties en/of personen. Deze informatie kan bestaan uit overzichten van de samenstelling van groeperingen of organisaties (organogrammen), beschikbare middelen, familiestambomen, etc.

Groep 3
Deze groep bevat verschillende activiteiten of gebeurtenissen die gelijktijdig en/of achtereenvolgens plaatsvinden om de in groep 1 opgenomen doelstellingen te verwezenlijken. De gebeurtenissen kunnen gegroepeerd zijn in categorieën als:

- incidenten: een bomaanslag, een moord, een kaping, een ontvoering, etc;
- training & opleiding: activiteiten die personen of organisaties de vaardigheden en/of deskundigheid bijbrengen waarmee een incident uitgevoerd kan worden;
- logistiek: de aanschaf en aanvoer van equipement, het onderdak van personen, het bergen van materieel, de aanschaf van equipement, ronselen personeel;
- financiën: transacties die plaatsvinden in het kader van het financieren van een incident, een training/opleiding, of een logistieke activiteit. Ook het genereren van geld behoort tot deze categorie (bankoverval, vals geld drukken, giropassen stelen en bankrekeningen plunderen, geld witwassen, etc.).

Hierna is beschreven hoe het IVP voor het datamodel tot stand komt. Verder is beschreven hoe op basis van dit plan informatie verzameld en verwerkt is.

2.3.2 Verzamelen en verwerken van informatie

Het model is zo opgezet dat de informatie uit de bronnen via een zogenaamd 'incident event template' in het dossier is opgenomen. Dit template ondersteunt de beschrijving van gebeurtenissen uit de in het denkmodel genoemde categorie 'incidenten'[1] in groep 3. Het template is een *invulformulier* waarin wordt aangegeven welke informatie met betrekking tot een incident wordt gezocht. Alle relevante elementen uit de groepen 1 (mojectives) en 2 (personen/organisaties) die in het dossier opgenomen moeten worden, zijn aan het incident event template gekoppeld en worden dus via dit template automatisch in het dossier terecht.

Het *incident event template* verwerkt de informatie via zogenaamde topics, kenmerken en relaties. Dat zijn de meest basale elementen, de bouwstenen, van het datamodel. Alle verzamelde inlichtingenkennis wordt dus via het incident event template gestructureerd aan de hand van topics, die onder te brengen zijn in de volgende *topic types*:

- person
- organisation
- event
- facility
- means
- location
- mojective

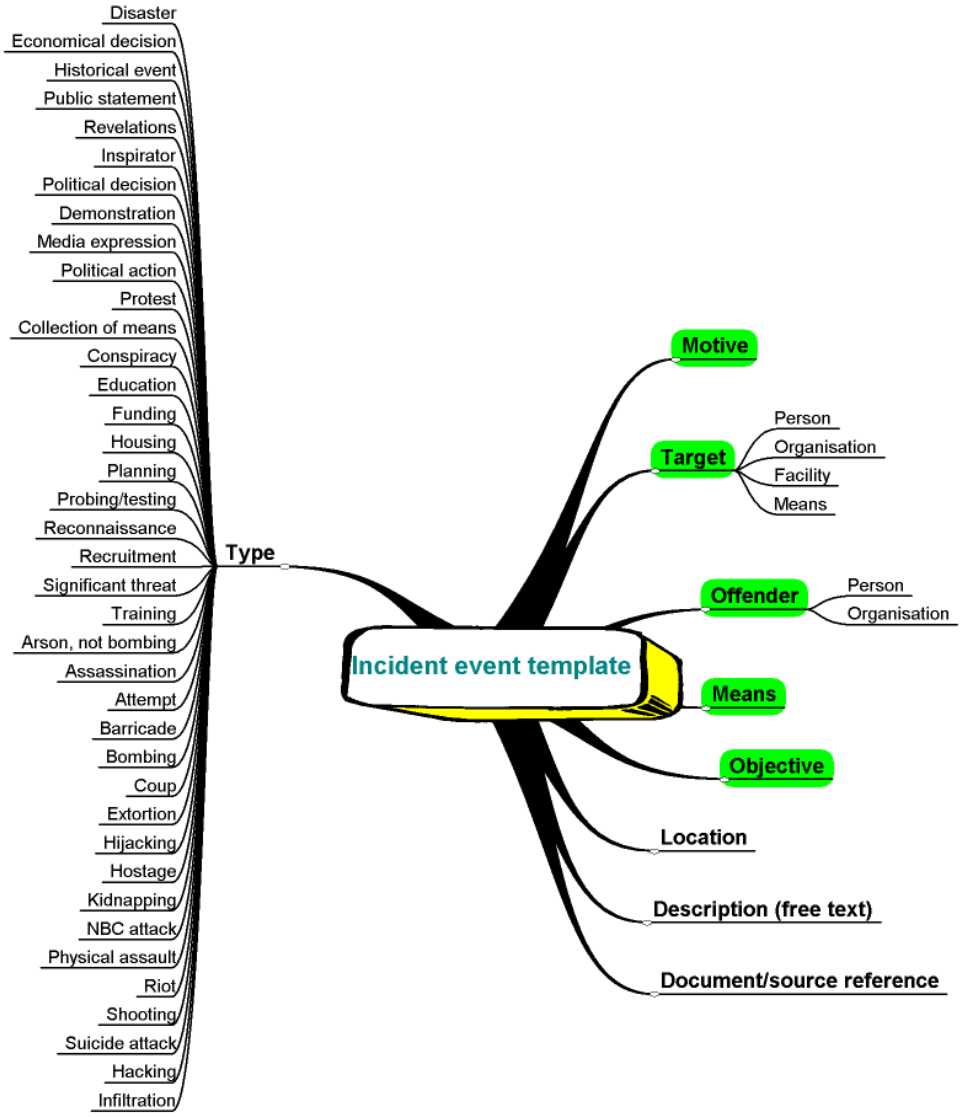
Ieder *topic* kent een set van kenmerken, bijvoorbeeld: *'person attributes: age, date of birth, profession, etc'*.

Tevens bestaan er relaties tussen topics, bijvoorbeeld: *'person X commands organisation Y'*, of, als het gaat om relaties tussen topics van hetzelfde type: *'person X is friend of person Y'*.

---

[1] Dit is het soort activiteiten waarnaar binnen dit project met name gekeken wordt.

Op het hoogste niveau ziet het incident event template er als volgt uit:



Figuur 2.1 'Incident event template'.

Verklaring van het template:
Het template laat onder meer zien met welk type topics het *incident event* beschreven wordt. Men voert een *Motive* (topic van het type mojective) in, een *Target* (topic van het type person, organisation, facility en/of means), een *Offender* (topic van het type person en/of organisation), een Means, een Objective (topic van het type mojective) en een *Location*. Merk overigens op dat bij één incident meerdere targets, offenders, etc. betrokken kunnen zijn. Het template geeft ook ruimte voor een *Description* (free text) en een *Document/source reference*
De groene 'loten' uit deze figuur worden uitgewerkt in sub-templates; op dat niveau komt men ook de kenmerken van de topic types tegen. De mogelijke relaties tussen topics van een bepaald type staan daarna beschreven. Zie voor deze nadere uitwerking bijlage A Datamodel templates.

Het met behulp van het *incident event* template opgebouwde dossier ondersteunt het verzamelen (i.e. het zoeken, extraheren en registreren) van informatie, maar stuurt dit

ook aan (dit is de in het denkmodel genoemde wisselwerking met het IVP). De verzamelde gegevens worden via de door TNO ontwikkelde tool PARANOID elektronisch opgeslagen.
Verder is de opzet van het dossier behulpzaam bij het verwerken (i.e. het evalueren, analyseren, integreren en interpreteren) van de informatie. Hierbij biedt PARANOID extra ondersteuning. PARANOID kan verbanden blootleggen tussen verschillende incidenten (en de daarbij betrokken topics en hun kenmerken en relaties); zo kan alle kennis uit het dossier geïntegreerd worden, waardoor de kracht en reikwijdte van bijvoorbeeld analyses toeneemt.

3 De uitwerking van het denkmodel

Suspicious signs hangen af van de fase in de aanloop naar een gewelddadige actie. In het onderzoek is gebruik gemaakt van de volgende vijf fases die van belang zijn voor het onderkennen van suspicious signs. Deze fases zijn:

- Occasion
- Trigger
- Rumbling
- Work-up Process
- Violent Action

De verschillende fases worden hier omschreven en waar mogelijk ook toegelicht met voorbeelden uit de database in PARANOID.

3.1 Uitwerking fases

Fase 1 *Occasion*
De eerste fase bestaat uit een aanleiding of 'occasion' die voortkomt uit de omgeving; dit is de voedingsbodem en achtergrond waardoor de resterende vier fases kunnen postvatten. Als voorbeeld kan dienen een krantenbericht van dinsdag 6 januari jl. waarin wordt beschreven dat door de opwarming van de aarde binnen 50 jaar éénderde van de op aarde levende dieren met uitsterven wordt bedreigd. Een occasion kan als een eerste suspicious sign worden opgevat. Voorbeelden van *occasions* zijn:

- *Rampen*
- *Economische beslissingen*
- *Historische gebeurtenissen*
- *Openbare beweringen*
- *Bekendmakingen*

Fase 2 *Trigger*
Een *occasion* kan tot gevolg hebben dat iemand, een groepering of een bevolkingsgroep vindt dat er iets moet gebeuren of juist bijvoorbeeld een besluit wil tegenwerken. Een trigger kan op dit niveau dus worden opgevat als een suspicious sign.
De intrede van een actor of factor die aanleiding geeft tot onrust is dan een *trigger*.
Voorbeelden van *triggers* zijn:

- *Inspirator* (Een persoon of groep die zich manifesteert en verklaart dat het zo niet kan en dat hier iets aan moet gebeuren, bijvoorbeeld Abu Jaja in een Belgisch interview over het Palestijns-Israëlisch conflict: 'Ik wil er meteen op wijzen dat het doen verdwijnen van de staat Israël niet betekent dat de joden er als groep moeten worden buiten gewerkt.' april 2003);
- *Politiek besluit dat tot commotie leidt* (bijvoorbeeld 15 miljoen Euro voor verbetering leefomstandigheden van de apen in het BPRC, besluit genomen op 18 oktober 2000 door minister Hermans van OCW);
- *Gewelddadige acties en/ of openbare uitingen tijdens het Work-up process die voor personen of groepen aanleiding zijn zich ook te willen manifesteren.*

Fase 3 *Rumbling*
In deze fase komen er uitingen van onrust die veelal te koppelen zijn aan de *Trigger*. Voorbeelden van suspicious signs tijdens de fase van *Rumbling* zijn:

- *Demonstraties (bijvoorbeeld een demonstratie tegen de PKK, 23 april 1995 in Den Haag in reactie op de oprichting van het Parlement van Kurdistan in ballingschap)*
- *Protesten (bijvoorbeeld het vrijlaten van nertsen*; *op donderdag 23 augustus 2001 werden 16 800 nertsen bevrijd uit een nederlandse pelsdierhouderij, het veroorzaken van kleine vernielingen).*
- *Media uitingen (bijvoorbeeld radio, tv, internet, mail etc.)*
- *Politieke acties*

Fase 4 *Work-up Process*
Om tot gewelddadige actie te komen zal veelal een proces van voorbereiding moeten worden doorlopen. Het betreft hier het opwerkingsproces naar gewelddadige actie. Voorbeelden van suspicious signs tijdens de fase *Work-up process* zijn:

- *Concentreren van middelen (bijvoorbeeld materiële, financiële en logistieke diensten).*
- *Samenzwering* (bijvoorbeeld Koerden aangepakt door politie, 29 maart 2001 in de binnenstad van Den Haag).
- Opleiding (bijvoorbeeld een informatiebijeenkomst door Engelse dierenactivisten);
- *Financiering* (bijvoorbeeld prostitutie, drugshandel, witwassen, vervoer illegalen, smokkel van wapens, sigaretten, drugs en alcohol).
- *Huisvesting* (bijvoorbeeld terroristen van onderdak en ID papieren voorzien).
- *Planning van de gewelddadige actie* (bijvoorbeeld gifgasaanval op Europese parlement die tussen 11 en 14 februari 2001 uitgevoerd had moeten worden door zestal Algerijnse terroristen die door de Britse geheime dienst opgepakt zijn; poging aanslag uit te voeren op NATO hoofdkwartier).
- *Testen en pogingen tot aanslagen.*
- *Verkenning* (bijvoorbeeld rapport met beschrijvingen Al Qaeda in Balkan en criminele connecties).
- *Rekrutering* (bijvoorbeeld rekruten direct sturen naar Afghanistan of Pakistan, isolatie en indoctrinatie van toekomstige rekruten).
- *Aanmerkelijke bedreiging* (bijvoorbeeld poederbrieven, bombrieven uit Bologna aan Europese instellingen in 2003, bommeldingen, dreigbrieven).
- *Training* (bijvoorbeeld Afghaanse trainingskampen, training in het werken met chemische en biologische wapens).

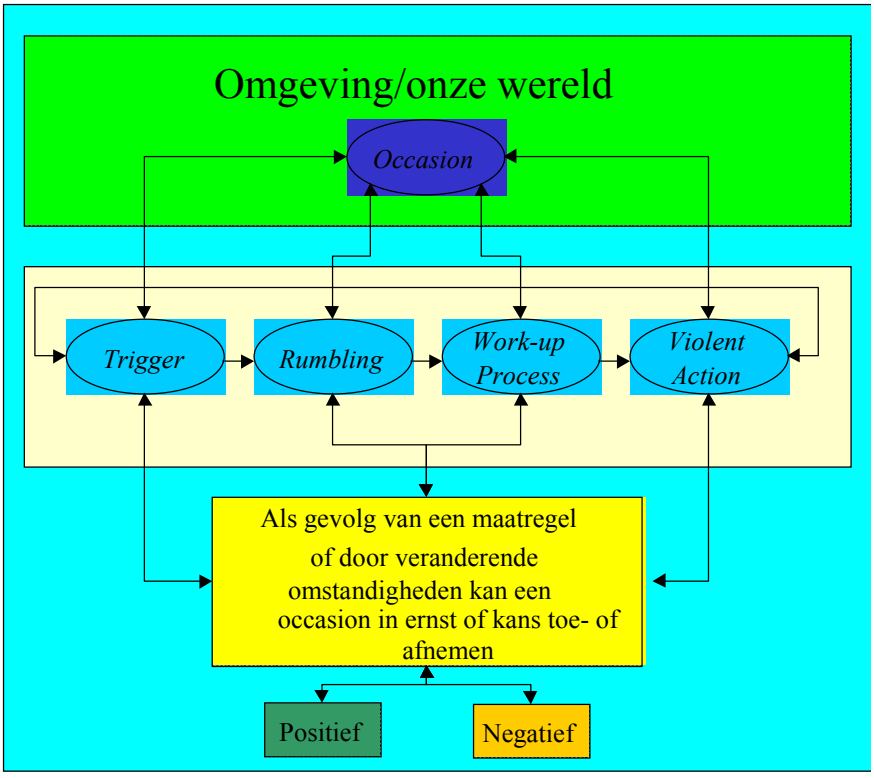
Fase 5 *Violent action*
Als laatste fase die voor de analyse van potentiële dreigingen tegen personen en objecten kan dienen zijn de daadwerkelijke gewelddadige acties in hun verschillende verschijningsvormen. Voorbeelden suspicious signs tijdens de fase van de V*iolent action* zijn:

- *Brandstichting* (bijvoorbeeld branden van auto's en (onderdelen van) bedrijven).
- *Moordaanslag* (bijvoorbeeld Pim Fortuyn 6 mei 2002 in Hilversum Mediapark, Anna Lindh 11 september 2003 in Olso, Massoud 9 september 2001).
- *Poging tot* (bijvoorbeeld aanslag op Amerikaanse ambassade beraamd door in Rotterdam gearresteerde verdachten op 13 september 2001).
- *Barricadering.*
- *Bomaanslag* (bijvoorbeeld aanslag Franse Marine en scheepvaart zoals op de Franse supertanker Limburg voor de kust van Jemen op 6 oktober 2002, McDonalds Engeland.
- *Staatsgreep.*
- *Afpersing.*

- *Hacking.*
- *Kaping.*
- *Gijzeling.*
- *Ontvoering.*
- *NBCR aanval.*
- *Fysieke bedreiging.*
- *Rel.*
- *Infiltratie.*
- *Schietpartij.*
- *Zelfmoordaanslag* (bijvoorbeeld 9-11-2002 op het World Trade Centre in New York).

Deze vijf fases vinden na elkaar plaats en oefenen ook weer invloed op elkaar uit. Dit betekent dat bij het interpreteren van de suspicious signs per fase er ook gelet moet worden op signs uit voorgaande fases om de context in het geheel te zien. Dit laatste is tweeledig: aan de ene kant zijn signs niet op zichzelf staand maar alleen in combinatie van belang. Aan de andere kant is er een verloop in de tijd waarbij de fases in elkaar overgaan en de voorgaande fases per definitie signs zijn voor opvolgende fases. Daarnaast is er ook een wisselwerking met de omgeving, waardoor de verschillende fases niet per definitie geheel doorlopen worden. Door invloeden van buitenaf is het mogelijk dat een cyclus afgebroken wordt.

Een gewelddadige actie op zijn beurt kan zelf een ‘inspirator’ zijn of leiden tot (tegen-) acties die mogelijk een nieuwe ‘inspirator’ doen ontstaan. Er is derhalve sprake van een proces dat zich kan versterken. Dit proces is visueel weergegeven in Figuur 3.1.



Figuur 3.1 Schematische weergave van het proces van gewelddadige acties.

Door het signaleren van gebeurtenissen binnen de verschillende fases kan men terug gaan naar een analyse waarbij de waardering van ernst en/of de waarschijnlijkheid van een bepaalde organisatie of vorm van gewelddadige actie opnieuw kan worden bezien. Het onderscheid tussen hoge waarschijnlijkheid (relatief veel voorkomend) en lage waarschijnlijkheid-bedreigingen en tussen zeer ernstige (grote sociale, politieke en economische consequenties) en matig tot niet ernstige aanslagen en combinaties hiervan, is voor beleidsmakers van belang. Het bepaalt mede hoeveel en welke middelen ingezet moeten worden.

3.2 Het onderkennen van suspicious signs per fase

Met name het onderkennen van suspicious signs gedurende de eerste fase vereist brede, multidisciplinaire analyses op strategisch niveau. De (internationale) omgeving moet daarbij continue worden bestudeerd.

Het onderkennen van suspicious signs kan derhalve beginnen met een geopolitieke analyse. De unipolaire wereld die na 1990 is ontstaan, met de Verenigde Staten als hegemoon, heeft onmiskenbaar tegenreacties opgeroepen. Zo is er een directe relatie tussen de opkomst van het grootschalig geweld terrorisme en deze geopolitieke ontwikkeling. Verder is de frequentie van gewelddadige actie in belangrijke mate afhankelijk van het proces van actie en reactie tussen de verschillende actoren. Het verklaren van de oorlog tegen het internationale terrorisme heeft bijvoorbeeld wereldwijd aantoonbaar voor een toename van het aantal gewelddadige activiteiten geleid.

3.2.1 Trendanalyses

Wordt naar gewelddadige actie en terrorisme op zich gekeken, dan zijn trendanalyses behulpzaam. Op basis van onderzoek en aanvullende literatuurstudie en analyses is een overzicht opgesteld van algemene trends in gewelddadige acties. Het merendeel van de trends zijn buiten terrorisme ook van toepassing op andere vormen van gewelddadige actie. Hierbij is een onderscheid mogelijk tussen mondiale en nationale trends en ontwikkelingen. Dit is van belang omdat het hiermee mogelijk is per fase te kunnen onderkennen welke informatie relevant is en doelgericht te kunnen redeneren welke gewelddadige aanslagen en acties kunnen worden verwacht. In hoofdstuk 10 is een overzicht van deze trends verwerkt door ze toe te delen aan de suspicious signs fases.

3.3 Ernst en waarschijnlijkheid

In de vervolgfases worden de te onderkennen suspicious signs concreter en meer operationeel. De benodigde capaciteit om inlichtingen te vergaren neemt navenant toe. Dit vereist prioriteitstelling op basis van twee criteria: waarschijnlijkheid en ernst.
De ernst en waarschijnlijkheid zullen steeds bij iedere fase moeten worden vastgesteld en vormen de input voor de volgende fase.
Voor het bepalen van ernst en waarschijnlijkheid is gebruik gemaakt van de nota *Nieuw stelsel bewaken en beveiligen.*

Waarschijnlijkheid

In onderstaande tabel zijn de normeringen voor waarschijnlijkheid overgenomen uit de nota *Nieuw stelsel bewaken en beveiligen.* Deze is aangevuld met een inschatting van de frequentie en voorbeelden gebaseerd op literatuurstudie en data-analyse uit de open bronnen. Het bepalen van de waarschijnlijkheid van een bepaald incident is gebaseerd

op twee criteria: de frequentie van bepaalde incidenten uit het verleden en concrete aanwijzingen en vermoedens dat een gebeurtenis geëffectueerd zal worden. De bepaling van de frequentie van incidenten is een aanvulling op de nota. In het vervolg van het rapport wordt daarom gebruik gemaakt van de combinatie tussen de historische frequentie en de waarschijnlijkheid uit de onderstaande tabel.

Tabel 3.1 'Waarschijnlijkheid definities en voorbeelden'.

Categorie	Waarschijnlijkheid (Bewaken & Beveiligen)	Historische frequentie	Voorbeelden
Zeer hoog	Concrete aanwijzingen (feiten en omstandigheden) dat een gebeurtenis geëffectueerd zal worden: bekendheid van plaats en tijd	In de afgelopen 20 jaar relatief zeer vaak voorgekomen	Brandstichting en vernieling door dierenactivisten
Hoog	Concrete aanwijzingen dat een gebeurtenis zich zal voordoen, alleen plaats en tijd zijn niet bekend. En/of een gebeurtenis wordt zeer voorstelbaar geacht	In de afgelopen 20 jaar relatief vaak voorgekomen	Fysieke en niet fysieke bedreigingen door alleenstaande daders (kogelbrieven, stalking, etc.)
Gemiddeld	Geen concrete aanwijzingen, maar de gebeurtenis is voorstelbaar	In de afgelopen 20 jaar relatief noch vaak, noch zelden voorgekomen	Moordaanslagen door criminele organisaties, aanslagen op ambassades of consulaten in Nederland
Laag	Geen concrete aanwijzingen, maar de gebeurtenis wordt nog enigszins voorstelbaar geacht	In de afgelopen 20 jaar relatief zelden voorgekomen	Moord op VIP door alleenstaande dader
Zeer laag	Geen concrete aanwijzingen en de gebeurtenis wordt evenmin voorstelbaar geacht	In de afgelopen 20 jaar relatief zeer zelden of nooit voorgekomen	Aanslag door Al Qaeda netwerk met NBCR wapens

Ernst

Bij de classificatie van de mate van ernst is gebruik gemaakt van de indicatoren waarop de classificatie in de nota *Nieuw stelsel bewaken en beveiligen* is gebaseerd. Aangezien de indicatoren in de nota niet volledig consistent waren, zijn ze aangepast of aangescherpt. Er is een aantal algemene indicatoren onderscheiden dat helpt de classificatie scherper en helderder op te zetten.

Deze indicatoren zijn:

- *Aantal dodelijke slachtoffers.*
- *Mate van maatschappelijke ontwrichting/ verstoring openbare orde.*
- *Mate van materiële schade.*
- *De mate waarin VIP's het slachtoffer zijn van de incidenten*.

Anders dan in de nota zijn deze indicatoren nader in een glijdende schaal geoperationaliseerd. In het vervolg van het rapport wordt gebruikt gemaakt van de consequenties uit de onderstaande tabel.

Tabel 3.2 'Ernst definities en voorbeelden'.

Categorie	Effect (Bewaken & Beveiligen)	Consequenties	Voorbeelden
Zeer ernstig	Massaal aantal dodelijke slachtoffers, uitval van (delen van) vitale infrastructuren (eventueel zonder dat direct mensenlevens in gevaar worden gebracht), maatschappij ontwrichting etc.	Massaal aantal dodelijke slachtoffers; ernstige maatschappelijke ontwrichting; uitval van (delen van) vitale infrastructuur;	"11 september"
Ernstig	Vrees voor het leven van één of enkele personen, samenleving ernstig geschokt	Tientallen dodelijke slachtoffers; maatschappelijke ontwrichting/ ernstig geschokte samenleving; zeer ernstige materiële schade; fysieke bedreiging van VIP categorie I en II	Moord Pim Fortuyn; RaRa aanslag op huis Aad Costo
Gemiddeld	Grootschalige openbare ordeverstoringen, grote zaakschade aan niet vitale objecten, fysieke integriteit VIP geschonden	Enkele dodelijke slachtoffers; samenleving geschokt/ grootschalige openbare ordeverstoring; ernstige materiële schade; fysieke bedreiging van VIP niet cat I en II	Aanslagen ETA in Spanje
Matig	Kleinschalige openbare ordeverstoringen, intimidatie VIP	Geen dodelijke slachtoffers; kleinschalige openbare ordeverstoring; geringe materiële schade; niet fysieke bedreiging VIP	Aanslagen dierenactivisten (Bijvoorbeeld op het BPRC)
Niet ernstig	Geen effecten voor de nationale veiligheid (inclusief de openbare orde)	Geen dodelijke slachtoffers; geen openbare ordeverstoring; geen materiële schade; geen bedreiging VIP	Vreedzame demonstratie milieuactivisten

3.4 De toepassing van het datamodel

Op basis van de structurering in het denk- en datamodel dat in de softwaretool PARANOID is verwerkt, kan beschikbare broninformatie met betrekking tot de verschillende vormen van terrorisme en gewelddadige actie worden verwerkt.

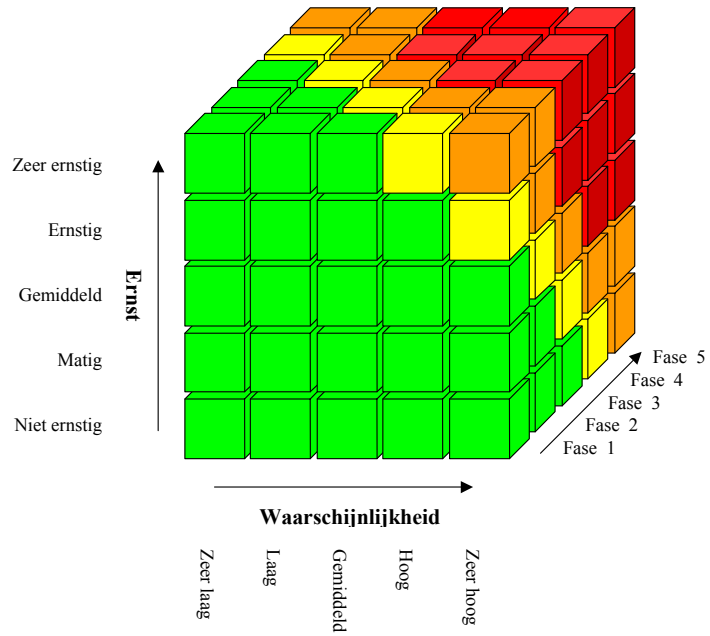
Het kan in het kader van dit onderzoek gaan om verschillende soorten informatie zoals tijdstippen van activiteiten, namen van mensen of organisaties, locaties etc. Verder kan met behulp van PARANOID worden geanalyseerd wat de historische ontwikkelingen in trends zijn en die deels kunnen worden gebruikt voor de bepaling van de waarschijnlijkheid en ernst in de toekomst. Deze indeling is van belang bij de bepaling van de risico-managementactiviteiten. Een 'hoge waarschijnlijkheid gecombineerd met zeer ernstige dreigingen' vragen meer aandacht dan dreigingen die een lage waarschijnlijkheid hebben met een beperkte ernst.

Met behulp van het datamodel en dankzij het gestructureerde karakter van de informatie kan specifiek worden gezocht naar personen, organisaties en kenmerken en kunnen deze zoekresultaten verder worden geanalyseerd.

Tevens zijn bepaalde kenmerken en activiteiten te vergelijken met andere kenmerken en activiteiten of met soortgelijke suspicious signs elders of in een andere tijdsspanne. Op basis van deze vergelijkingen is een schatting te maken in welke mate geconstateerde suspicious signs dat ook daadwerkelijk zijn en aanleiding geven tot op te stellen dreigingsanalyses en risico-analyses.

Om dit meer operationeel te maken is de kubus uit figuur 3.2 opgesteld. In deze kubus worden de elementen waarschijnlijkheid, ernst en suspicious signs fase tegen elkaar afgezet. Hierbij is het mogelijk om organisaties events of categorieën te rangschikken en te bepalen of relevante diensten iets zouden moeten ondernemen. Om een inschatting te kunnen maken van de plaats in de kubus is het in eerste instantie van belang in welke fase de events zich bevinden (Als er al aanslagen zijn gepleegd is dit in fase 5 en anders in één van de eerdere fases). Daarnaast moet een inschatting gemaakt worden van de waarschijnlijkheid van het optreden van gebeurtenissen uit deze fase, dit kan zich eventueel uitspreiden over meerdere fases aangezien er bijvoorbeeld voor sommige events wel aanwijzingen zijn en voor andere niet. Een laatste inschaling vindt plaats op basis van ernst, ook hier kunnen meerdere categorieën van toepassing zijn. De inschaling naar ernst is in de laatste drie fases al meer geoperationaliseerd door een indeling te maken naar ernst van verschillende typen events. Deze indeling is een eerste opzet en verdient zeker nader onderzoek dat buiten dit project valt.

Met deze kubus wordt maatwerk mogelijk. In deze figuur wordt een voorbeeld gegeven van een mogelijke invulling. De afzonderlijke fases worden weergegeven in figuur 3.3 t/m figuur 3.6.



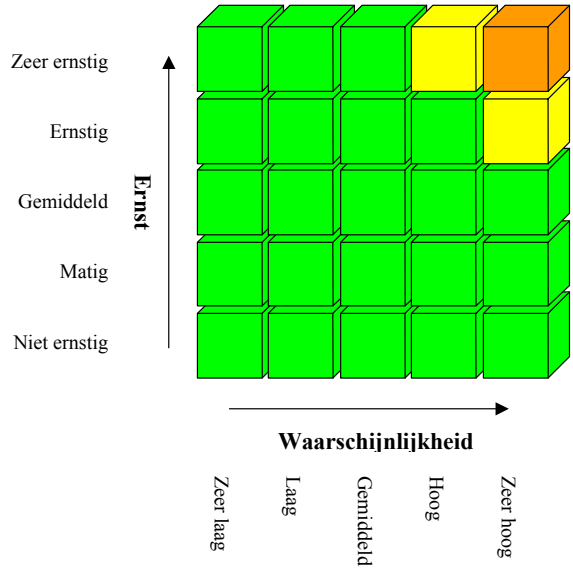
Figuur 3.2 'Ernst * kans gecombineerd met suspicious signs fases'.

Het is nu mogelijk om de diverse verschijningsvormen van de suspicious signs in dit model nader toe te delen. Hiermee wordt het mogelijk om ieder incident te classificeren in het gehanteerde model. Hierna is voor de fase 3 *Rumbling*, fase 4 *Work-up process* en fase 5 *Violent action* deze indeling gemaakt.
Deze indeling is slechts een indeling die voor het onderzoeksproject is gehanteerd. Indien deze methodiek voor de daadwerkelijke inlichtingenverwerking gehanteerd gaat worden, zal met name hierover een gedegen afspraak moeten worden gemaakt in de gehele keten, omdat dit sterk de appreciatie van de resultaten kan beïnvloeden en daarmee direct van invloed is op de te kiezen risico-analyse en te nemen besluiten ten aanzien van opsporing, bewaking en beveiliging.
Het gebruik van kleuren is slechts illustratief. Het gebruik van kleuren kan echter helpen om sneller een beeld te krijgen van het stadium, de ernst en de waarschijnlijkheid waarin zich een bepaalde dreiging bevindt.

Met het gebruik van de kubus worden 3 dimensies met elkaar in verband gebracht. Het maakt het mogelijk per 'blokje' te definiëren en normeren wat de risico-analyse moet zijn. Tevens is het mogelijk (indien deze benadering wordt gehanteerd in de gehele keten van inlichtingen – risico-besluitvorming en bewaking & beveiliging) ook de bewakings- en beveiligingsactiviteiten eraan te koppelen evenals de diensten die hieraan inhoud geven. Hierdoor ontstaat een transparant, traceerbaar en verifieerbaar stelsel. Naarmate dit stelsel zich verder ontwikkelt, kan deze procesgang steeds verder worden geoptimaliseerd (denk hierbij aan bijvoorbeeld consequence management, effectbepaling en lessons learned, maar ook kwaliteitsborging). Hiermee ontstaat duidelijkheid voor alle partijen en eenduidigheid in de wijze waarop hiermee om moet worden gegaan. In dit onderzoek is dit echter niet verder ontwikkeld.

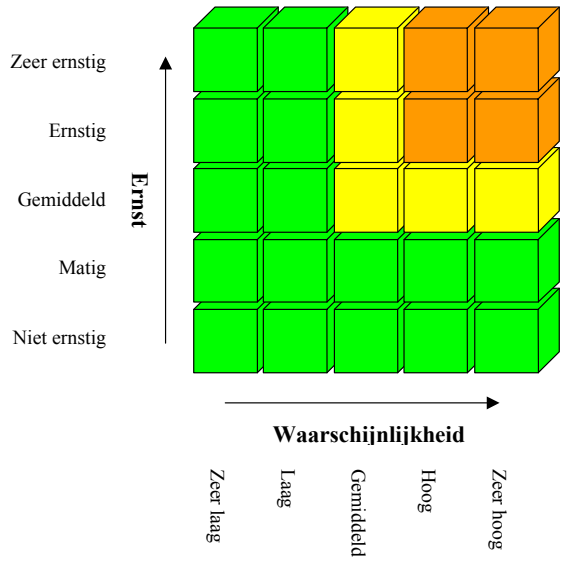
Fase 1 *Occasion*
In onderstaande figuur is te zien dat er in weinig situaties sprake is van enige noodzaak tot handelen, alleen bij Zeer Ernstige situatie gecombineerd met de Zeer Hoge waarschijnlijkheid is attentie vereist. Ook is het zo dat in deze fase geen duidelijk

onderscheid is te maken tussen incidenten met verschillende waarschijnlijkheid en ernst; in het algemeen kan deze fase gevisualiseerd worden als één groot vierkant.



Figuur 3.3 fase 1 Occasion.

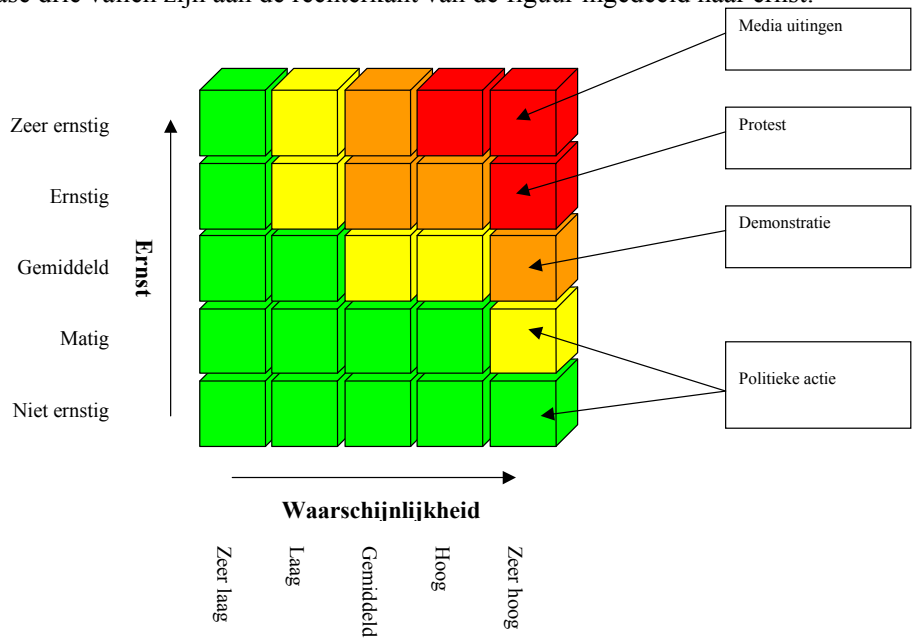
Fase 2 *Trigger*
In de tweede fase is ook het onderscheid tussen de verschillende normeringen van ernst en waarschijnlijkheid nog niet duidelijk aan te geven en ook in dit stadium is het nog niet noodzakelijk en mogelijk om op te treden.



Figuur 3.4 fase 2 Trigger.

Fase 3 *Rumbling*
In onderstaande figuur zijn de verschillende activiteiten veel beter in te delen naar ernst, maar een indeling naar waarschijnlijkheid is aan de hand van de soort activiteit niet aan te geven omdat een dergelijke activiteit op zich niets aangeeft over de kans van optreden van een violent actie is fase 5. Hiervoor zijn middelen nodig zoals historische

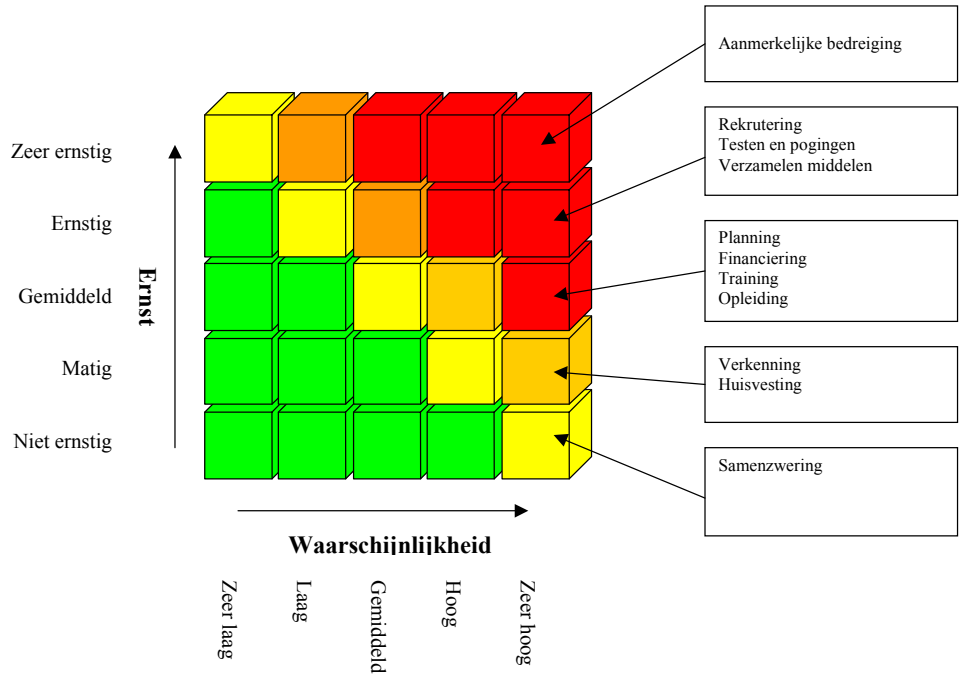
frequentie, concrete aanwijzingen en vermoedens. De verschillende activiteiten die in fase drie vallen zijn aan de rechterkant van de figuur ingedeeld naar ernst.



Figuur 3.5 fase 3 Rumbling.

De plaatsing van suspicious signs in de diverse ernst-categorieën maakt het mogelijk met deze methode de suspicious signs te classificeren. De normering die daarbij moet worden gehanteerd moet daarvoor worden ontwikkeld.

Fase 4 *Work-up process*
In de vierde fase kunnen de activiteiten ook weer ingedeeld worden naar mate van ernst en wordt in de rechterbovenhoek, de situaties met grotere ernst en grotere waarschijnlijkheid de noodzaak tot ingrijpen aangegeven door middel van de rode kleur.

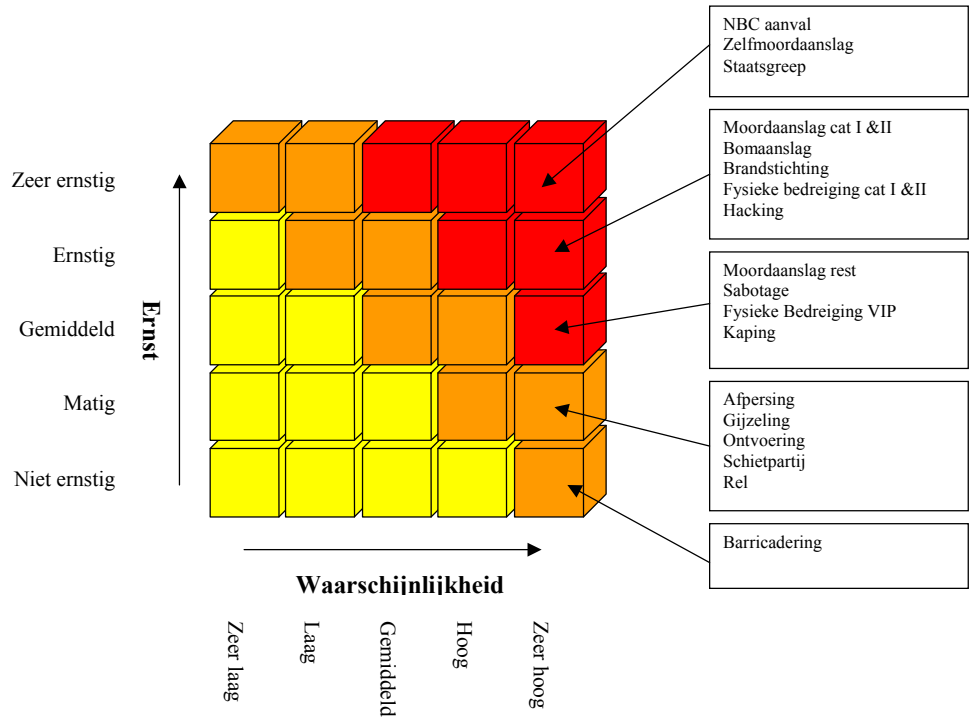


Figuur 3.6 fase 4 Work-up process.

De plaatsing van suspicious signs in de diverse ernst-categorieën maakt het mogelijk met deze methode de suspicious signs te classificeren. De normering welke daarbij moet worden gehanteerd moet daarvoor worden ontwikkeld.

Fase 5 Violent action

In de vijfde fase kunnen de activiteiten ook weer ingedeeld worden naar mate van ernst en wordt de kubus meer geel, oranje en rood van kleur om de noodzaak tot ingrijpen aan te geven.



Figuur 3.7 fase 5 Violent action.

De plaatsing van suspicious signs in de diverse ernst-categorieën maakt het mogelijk met deze methode de suspicious signs te classificeren. De normering welke daarbij moet worden gehanteerd moet daarvoor worden ontwikkeld.

3.5 Categorieën van gewelddadige organisaties

Ten behoeve van de selectie van de cases (die niet zijn opgenomen in deze rapportage) is getracht zo veel mogelijk het gehele veld van potentiële dreigingen af te dekken. Steeds zullen bij een analyse de volgende elementen moeten worden meegenomen; trends gevaaraantrekkende aspecten van personen en objecten, dadercategorieën en ernst en waarschijnlijkheid. De volgende gewelddadige organisatie categorieën zijn gehanteerd bij de selectie van de cases.

Ten eerste zijn er de motivatiecategorieën voor gewelddadige organisaties. Deze zijn religieus, etnisch/separatistisch en politiek. Deze gelden met name voor terroristische organisaties. Daarnaast kunnen criminele en staatsaangelegenheden als motivatie voor gewelddadige acties gelden. Hieraan kunnen verschijningsvormen worden gekoppeld: binnenlands, buitenlands of transnationaal. Ten tweede zijn er dadercategorieën: criminele en terroristische groeperingen en ‘stand alone’ daders.

Een categorisering voor daders van gewelddadige acties is onderscheiden naar motivatie omdat hierin vaak trends te onderkennen zijn. Zo deed politiek-links geweld met name van zich spreken in de jaren zeventig. Diverse Palestijnse groeperingen profileerden zich bijvoorbeeld op deze wijze.
Nationalistische en separatistische motieven lijken vanaf het eind van de Koude Oorlog in diverse landen een grotere rol te zijn gaan spelen. Ook ‘frame of mind’ en methode van opereren krijgen andere invulling door veranderde motivatie van personen en groepen. Zo kan de motivatie voor een dader vanuit extremistische religieuze

overtuigingen leiden tot een verharding van de strijdmethoden. Het is bijvoorbeeld zeer onwaarschijnlijk dat crimineel winstbejag zal leiden tot het plegen van een zelfmoordaanslag. In alle aanloop fasen naar een gewelddadige actie zit er onderscheid naar motivatie. Zo kan een 'trigger' bij de ene organisatie een Fatwa zijn en voor een andere categorie het coffeeshopbeleid, is voor de één een opruiende preek misschien een rumbling en is een handtekeningenactie dit voor een ander.

Een verdere categorisering is gemaakt naar buitenlands/transnationaal en Nederlands. Dit is gedaan omdat er naast motivatie nog een aantal verschillen zijn. Zo verschillen bijvoorbeeld tot op heden de doelwitten van een buitenlandse separatistische organisatie van de doelwitten die je van een binnenlandse separatistische organisatie zou verwachten. Zo zijn voor de ene groepering symbolen van vertegenwoordiging van de regering van belang (ambassades, banken etc.) en voor de andere groepering het staatshoofd of ministerie van binnenlandse zaken een belangrijk doelwit. Ook verschillen de trends. Zo is er bijvoorbeeld binnen Nederland geen separatistische beweging van de grond gekomen en treden organisaties van buitenlandse origine over het algemeen harder op. Tevens is er een verschil in de aanpak van binnenlandse en buitenlandse/ transnationale organisaties nodig. Om signs te ontdekken zul je o.a. een uitstapje naar andere media moeten maken en bijvoorbeeld moeten samenwerken met zusterdiensten om aan informatie te komen. Het work-up process van een organisatie die internationaal kan opereren is ook anders dan een organisatie die alleen binnenlands opereert omdat er bijvoorbeeld meestal meer planning en funding komt kijken voor een zelfde type actie in een ander land.

Deze indeling wordt in dit onderzoek gebruikt ter bepaling van de focus voor het verzamelen, verwerken en analyseren van informatie. Maar de indeling blijkt om nog een andere reden relevant. De methode die voor het vergaren van inlichtingen wordt gebruikt is afhankelijk van de dadercategorie. Gewelddadige acties uitgevoerd door groepen hebben als voordeel dat infiltraties en dergelijke mogelijk zijn. Dat is niet het geval bij de 'stand alone' dader. Deze wordt daarom als aparte categorie beschouwd, ook al wordt deze gemotiveerd door religieuze, etnische of andere overwegingen. Ook kan het hier om 'gekken' gaan. Omdat het vrijwel onmogelijk is potentiële 'stand alone' daders te onderkennen, zal met name naar de persoon of het object moeten worden gekeken in hoeverre deze gevaar aantrekken.
Hieronder volgt een overzicht van de 11 te onderscheiden categorieën.

Tabel 3.3 Motivatie, verschijningsvormen en categorieën.

Motivatie	**Verschijnings-vormen**	**Categorieën**
Religieus	Binnenlands Transnationaal Buitenlands	1. Binnenlands religieuze organisaties 2. Buitenlands/Transnationaal religieuze organisaties
Etnisch/ Separatistisch (E/S)	Binnenlands Transnationaal Buitenlands	3. Binnenlands E/S organisaties 4. Buitenlands/Transnationaal E/S organisaties
Politiek	Binnenlands Transnationaal Buitenlands	5. Binnenlands politieke organisaties 6. Transnationaal politieke organisaties 7. Buitenlands politieke organisaties
Crimineel	Binnenlands Transnationaal Buitenlands	8. Binnenlands criminele organisaties 9. Buitenlands/Transnationaal criminele organisaties
Religieus, etnisch, politiek, onvrede, afgunst etc.		10. 'Stand alone' dader
Staats aangelegenheden		11. 'State agents' c.q. 'State agencies'

De navolgende type cases zijn tijdens het onderzoek nader onderzocht.

- Grootschalig geweld terrorisme met verbanden met Nederland.
- Crimineel 'gewelddadige actie' met verbanden met terrorisme en Nederland.
- Geweld en terrorisme vanuit buitenland gericht op of met verbanden met Nederland.
- Dierenactivisme.
- Alleenstaande dader/'stand alone' gewelddadige actie met verbanden met Nederlandse personen of objecten.

Een nadere toelichting en verder analyse van de categorieën is buiten deze rapportage gelaten.

Tabel 3.4 ‘Categorieën in gewelddadige acties en terrorisme gekoppeld aan de focus van het onderzoek’.

Categorieën	Cases
1. Binnenlands religieuze organisaties	Grootschalig geweld terrorisme van het type Al Qaeda met verbanden met NL.
2. Buitenlandse/transnationale religieuze organisaties	
3. Binnenlands Etnisch/Separatistisch organisaties	Crimineel ‘gewelddadige actie’ met verbanden met terrorisme en NL
4. Buitenlandse/transnationale E/S organisaties	
5. Binnenlands politieke organisaties	Geweld en terrorisme vanuit buitenland gericht op diplomatieke diensten in NL
6. Transnationaal politieke organisaties	
7. Buitenlands politieke organisaties	
8. Binnenlands criminele organisaties	Dierenactivisme
9. Buitenlandse/transnationale criminele organisaties	
10. ‘Stand alone’ dader	Alleenstaande dader/‘stand alone’ gewelddadige actie
11. ‘State agents’ c.q. ‘State agencies’	

In onderling overleg met de opdrachtgever is vastgesteld dat het verzamelen van informatie zich gegeven de doorlooptijd en omvang van het onderzoek richt op een vijftal categorieën. Dit zijn:

- Grootschalig geweld terrorisme van het type Al Qaeda met verbanden met Nederland (de categorieën 2, 4, 6, 9 afdekkend).
- Crimineel ‘gewelddadige actie’ met verbanden met terrorisme en Nederland (de categorieën 3, 4, 7, 8, 9, 11 afdekkend).
- Geweld en terrorisme vanuit buitenland gericht op diplomatieke diensten etc. met verbanden met Nederland (de categorieën 2, 4, 5, 6, 8 afdekkend).
- Dierenactivisme (de categorieën 6, 7, 8 afdekkend).
- Alleenstaande dader/‘stand alone’ gewelddadige actie met verbanden met Nederlandse personen en objecten uit de nota *Nieuw stelsel bewaken en beveiligen* (de categorie 10 afdekkend).

Met deze cases is alleen categorie 1 niet afgedekt. De inschatting hiervan is dat dit overigens voor Nederland een minder relevante vorm van gewelddadige actie of terrorisme is.

3.6 De aanpak van de analyse

De structuur nodig voor de analyse is hiervoor beschreven. Hierna is de aanpak van de analyse zelf beschreven. Deze analyse is opgezet vanuit een bottom-up benadering. Dit is gedaan door cases te gebruiken.
Bij de analyse van de cases is een operationeel uitgangspunt genomen. Hierbij is uitgegaan van de categorieën personen en objecten zoals die zijn opgenomen in de nota *Nieuw stelsel bewaken en beveiligen*.

Bron: Nota nieuw stelsel Bewaken en Beveiligen [1], juni 2003.

Limitatieve lijst van personen, objecten of diensten waarvoor de Rijksoverheid als eerste verantwoordelijke besluit over extra veiligheidsmaatregelen

Categorie 1
Personen, objecten of diensten waarvoor de Rijksoverheid als eerstverantwoordelijke standaard extra veiligheidsmaatregelen (veelal persoonbeveiliging) treft.

- de leden van het Koninklijk Huis
- de Minister-President
- Koninklijk bezoek
- Buitenlandse staatshoofden/regeringsleiders
- Buitenlandse ministers van buitenlandse zaken tijdens officiële bezoeken

Categorie 2
Personen, objecten of diensten waarvoor de Rijksoverheid als eerste verantwoordelijke extra veiligheidsmaatregelen treft op basis van risico/dreiging (niet standaard)

- De overige leden van de Koninklijke familie (art. 6 en 38 Politiewet 1993)

Bepaalde nationale politici, te weten
- de bewindslieden
- fractievoorzitters in en de lijsttrekkers voor de Tweede Kamer
- de Voorzitters van de Eerste en Tweede Kamer

Bepaalde gezichtsbepalende en daardoor risico-aantrekkende personen die werkzaam zijn in de (straf)rechtspleging, te weten:
- de president en de procureur-generaal van de Hoge Raad
- de leden van het College van procureurs-generaal;
- de voorzitter van de Raad voor de Rechtspraak

Bepaalde gezichtsbepalende en daardoor risicoaantrekkende functionarissen (veelal voorzitters) van een aantal Hoge Colleges van Staat, te weten:
- de vice president van de Raad van State
- de president van de Algemene Rekenkamer
- de Nationale Ombudsman

Bepaalde hoge buitenlandse gasten of diplomatieke posten in Nederland, te weten:
- buitenlandse bewindslieden in Nederland
- alle ambassadeurs en ambassades alsmede consuls-generaal en consulaten, en de militaire attachés
- SG's of voorzitters van enkele internationale verdragsorganisaties, te weten NAVO, EU, WEU, VN
- President van de Wereldbank

Bepaalde hoge militaire bezoekers, of militaire objecten, bijvoorbeeld:
- US Chairman Joint Chiefs of Staff, Chairman Military Committee
- Nato, Supreme Allied Commander Europe/Atlantic, Afnorth

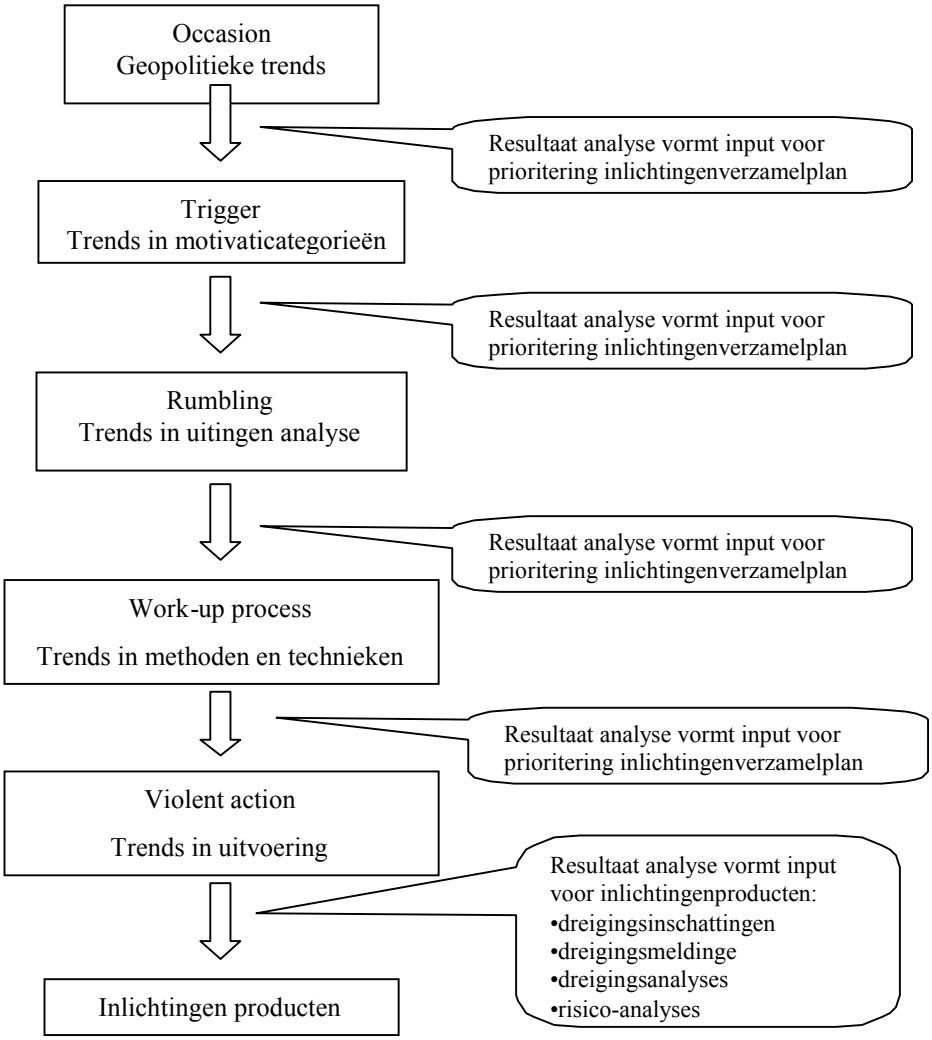
Bepaalde buitenlandse gezichtsbepalende en daardoor risicoaantrekkende functionarissen van internationale organisaties die in Nederland zijn gevestigd alsmede hun gebouwen, te weten:

- International Criminal Tribunal for the Former Yugoslavia (ICTY), te weten hoofdaanklagers en fungerend rechter en bedreigde getuigen en verdachten
- International Criminal Court (ICC) (idem.) en
- Internationaal Gerechtshof/Vredespaleis alsmede
- Organisation for Prohibition of Chemical Weapons (OPCW)

Bepaalde personen, objecten of diensten, die mogelijk risicoaantrekkend zijn en bij uitval of verstoring nationale impact hebben:

- De directeur en het gebouw van de Nederlandse Bank NV (zie artikel 6 lid 1 sub 9 Politiewet 1993) alsmede bepaalde geldtransporten
- Burgerluchtvaart (zie ook artikel 6 lid 3 Politiewet 1993)

Door steeds vanuit de persoon of het object te analyseren kan worden bezien of en welk type suspicious signs er bij deze persoon of groep personen behoort en binnen welke trends deze onderkende potentiële dreiging behoort. Het daadwerkelijk vinden van suspicious signs is afhankelijk van de beschikbare bronnen. In het achterhoofd moet worden gehouden dat bij dit onderzoek slechts gebruik is gemaakt van *open bronnen*. In het onderstaande stappenplan staan de belangrijkste stappen kort schematisch weergegeven.



Figuur 3.8 Stappenplan inlichtingenverzamel- en analyseproces.

Ernst en waarschijnlijkheid inschatting is voor iedere volgende fase van belang. De resultaten uit een voorgaande fase zijn daarmee input voor de volgende fase.

In dit rapport zijn *niet* de beschrijvingen opgenomen van de analyse van de cases volgens deze methode.

3.6.1 Analyse van de cases

Tijdens de analyse van de cases is gekeken naar verschillende elementen. Daarbij is een vast format gehanteerd. Deze elementen zijn:

- De tijdlijn waarin de diverse suspicious signs fases activiteiten zijn opgenomen.
- De doelwitten (personen en objecten).
- De motieven en doelstellingen van de spelers of organisaties die er bij betrokken waren.
- De opsomming van de belangrijkste betrokken spelers en organisaties.
- De beschrijving van eventueel gevonden verbanden met Nederland en in Nederland (met name met de ‘bovenwereld’ en het criminele circuit, zusterorganisaties, losstaande organisaties met vergelijkbare mojectives) en screendumps van relatiediagrammen van een aantal van deze significante verbanden.
- De *modus operandi*, en de eventuele veranderingen hiervan in de loop van de tijd;
- De onderkende parallellen met buitenlandse ontwikkelingen.

4 Algemene analyse resultaten

4.1 Inleiding

In dit hoofdstuk is de werkwijze in de verschillende suspicious signs fases nader toegelicht en uitgewerkt en van voorbeelden voorzien. Tenslotte is op basis van open bronnen over de organisatie en werkwijze van de inlichtingen- en veiligheidsdiensten een korte beschouwing gegeven van een aantal valkuilen en oplossingsrichtingen om deze valkuilen te omzeilen.

4.2 Werkwijze in de verschillende suspicious signs fases

Steeds is per fase een beschrijving gemaakt van de soorten analyses die in iedere fase uitgevoerd kunnen worden. Er zijn telkens voorbeelden bij gegeven en methoden geschetst om de analyses uit te voeren. Ook zijn de trends zoals in hoofdstuk 2 waren onderkend geplaatst in ieder van de fases.

4.2.1 In de Occasion fase zijn de volgende typen analyses nodig

Analyses van geopolitieke trends zoals klimaatverandering, globalisering, verhouding burger/staat, state-failure, economie, demografie en techniek, etc. Hiermee zal in een zeer vroeg stadium moeten worden onderkend dat er ontwikkelingen gaande zijn die aanleiding vormen tot toekomstige radicalisering en gewelddadige actie. Hierbij lijkt de occasion met name te ontstaan uit de koppeling die deze thema's hebben met de 'zwakke partij', die groepen in de mondiale samenleving die zich niet kunnen verweren.

Voorbeelden van occasion thematieken zijn:
Midden-Oosten problematiek, Globalisering, Dieren (-welzijn), Milieu (Klimaatopwarming), Criminaliteit, Minderheden, Verhouding burger-staat, Ingrijpen in het 'leven', Verwevenheid terrorisme en criminaliteit.

Voorbeelden van occasions zijn:
Milieu-klimaat: 'geheim' Pentagon-rapport over klimaatverandering (februari 2004), VN-conventie over opwarming van de aarde (Januari 2004) waarbij gesteld is dat over 50 jaar een derde van de landdieren met uitstreven wordt bedreigd.

Verhouding burger-staat: de dure verbouwing van het UWV-gebouw en de commotie daarover (Zomer 2003). Aantasting burgervrijheden in het kader van terrorismebestrijding, wet- en regelgeving, Big-brother ontwikkelingen door koppeling tussen ICT-systemen, slimme camera's, databestanden van politie, justitie, uitkeringsinstanties etc.

Minderheden: asielzoekers die uitgezet gaan worden (Februari 2004), Oud minister Pronk die roept dat er sprake is van 'deportatie' (Januari 2004). Problematiek van allochtonen gekoppeld aan segregatie.
Dieren: BSE-, Vogelpest-, Varkenspest- en MKZ-crises.

Globalisering: Inperking vrije verkeer werknemers uit nieuwe EU-landen en met name Polen (Januari 2004).

Trends met relevantie voor de fase occasion

- *Gebrekkige integratie van nieuwe minderheden (Nederlandse trends en ontwikkelingen)* In het bijzonder personen die behoren tot niet-westerse bevolkingsgroepen vormen een potentiële uitvalsbasis en rekruteringsterrein voor bepaalde vormen van terrorisme; een uitvalsbasis die mede gelet op de nog steeds bijzonder sterke groei van deze bevolkingsgroepen eerder groter dan kleiner wordt.

- *Een onduidelijk en 'open' toelatingsbeleid (Nederlandse trends en ontwikkelingen)* Er is nog steeds sprake van een beperkte screening van personen op banden met radicale organisaties van personen die in Nederland asiel zoeken of een visum aanvragen. Een zwakke schakel in het toelatingsbeleid vormt de afgifte van visa door ambassades en consulaten in het buitenland.

- *Toegenomen bedreiging van Nederland als onderdeel van de internationale gemeenschap (trends mogelijkheden tot terrorisme binnen Nederland).* Door de rol van Nederland als 'hoofdstad van het internationaal recht' met de huisvesting van organisaties als Eurojust, Europol, het ICC en het Joegoslavië tribunaal is er een vergrote kans op aanslagen op Nederlandse bodem. Ook draagt de steun die Nederland uitspreekt of verleent aan bondgenoten bij aan de vergroting van deze kans. In dit kader past ook de Nederlandse participatie in interventieoperaties.

- *Toegenomen toepassingen en mogelijkheden tot het plegen van cyberterrorisme (trends mogelijkheden tot terrorisme binnen Nederland).* Nederland is een van de meest 'gedigitaliseerde' landen in de wereld. Dat maakt Nederland kwetsbaar voor 'hacken' in beveiligde overheidsbestanden, platgooien van websites en bombarderen van bedrijven, instellingen en personen met e-mails waardoor verder netwerkverkeer tijdelijk onmogelijk wordt gemaakt.

- *Gunstig 'vestigingsklimaat' (Nederlandse trends en ontwikkelingen)* Er zijn enkele gunstige voorwaarden voor terroristische en criminele organisaties om hun activiteiten in Nederland te ontplooien, dit zijn: de gunstige logistieke condities, het zonder veel belemmeringen stichten van BV's en stichtingen, het 'soepele rechtssysteem' en de sterke mate van tolerantie en multiculturaliteit waardoor buitenlanders in relatieve anonimiteit in Nederland kunnen leven.

- Nauw verbonden met bovenstaande drie punten: *de illegale migratie (Mondiale trends en ontwikkelingen)* vanuit Noord-Afrika en het Midden-Oosten.

Methoden

In deze fase zijn brede strategische analyses nodig die multi-disciplinaire benadering vragen, out-of-the-box- en laterale denkers met een politieke antenne. De vele verschillende invalshoeken die daarbij nodig zijn kunnen aanleiding geven in deze fase gebruik te maken van veel verschillende expertises.

Verder kan het gebruik van hypotheses (of dreigingsscenario's) helpen om uit deze occassions de dreigingselementen te benoemen om daarmee in de volgende fases van het proces verder te gaan.

4.2.2 In de Trigger fase zijn de volgende typen analyses nodig:

Gedragswetenschappelijke analyses en *profiling* van groepen maar ook individuen en daarmee het in kaart brengen welke typen groepen of individuen triggeren op de occasions. Maar ook het matchen van deze resultaten met bekende risico-groepen en individuen.

Voorbeelden van triggers
Terrorisme en criminaliteit: Officier van Justitie Plooy die zich terugtrekt uit de zware criminaliteitsbestrijding (Februari 2004), Hells' Angels die zeggen daders te pakken van hun drie vermoorde 'maatjes' (Februari 2004).

Milieu: Kyoto-besluit en de weigering van Amerika (2001) en een aantal andere landen dit verdrag te ondertekenen, Spotjes van Green Peace over illegale houtkap etc.

Verhouding burger-staat: Verharding immigratiecontroles (Biometriescan Schiphol, Januari 2004), verhoging topsalarissen gedurende een recessie (Philips, Februari 2004).

Minderheden: Toename antisemitisme, Verharding taalgebruik (zwarte scholen, allochtonen van Marokkaanse afkomst, hoewel geboren in Nederland etc.), Allochtonen (zonder beschermende pakken) die kippen ruimen (terwijl 'blanke' Nederlanders er in volledige beschermingsmiddelen bijstaan, Zomer 2003). Hoofddoekjes afschaffing in Frankrijk (Januari 2004), constante discussie over de Islamisering.

Dieren: Ruimen van dieren met een grijper (Een aantal varkens close-up in beeld, Zomer 2003).

Ingrijpen in het 'leven' (bio-engineering): DNA van het menselijk genoom (Zomer 2003), xeno-transplantatie, statements over het terughalen van uitgestorven diersoorten, bio-kippen, genetisch gemanipuleerde voeding.

Midden-Oosten: radicalisering van de beeldvorming door bijvoorbeeld discussies over de Israëlische muur publiek te plaatsen in de categorie antisemitisch (Februari 2004).

Trends met relevantie voor de fase trigger
- *Stijging van religieus gemotiveerd terrorisme (Mondiale trend terrorisme)* De totale stijging gedurende de laatste 15 jaar van het religieus gemotiveerde terrorisme brengt met zich mee de toeloop van nieuwe tegenstanders, motieven en tactieken die de patronen van de terroristen van vandaag de dag beïnvloeden.

- *Toename van 'na-aperij' (Mondiale trend gewelddadige actie)* Steeds vaker komt het voor dat na het plaatsvinden van een gewelddadige actie een zelfde soort acties in een kort tijdsbestek steeds vaker voorkomen, te vergelijken met het volgen van een trend. Hierbij fungeert een (serieuze) aanslag, als trigger voor toekomstige acties.

- *Stijging van religieus gemotiveerde acties (Mondiale trend gewelddadige actie)* Er is een stijging waargenomen in het plegen van acties met een religieus motief. Een gevolg hiervan is dat er nieuwe doelwitten, tegenstanders, maar ook nieuwe methoden van acties plegen gehanteerd worden. Voorbeelden hiervan zijn kerkhof, abortuskliniek of gebedshuis.

- *Stijging van politiek gemotiveerde acties (Mondiale trend gewelddadige actie)* Een stijging in acties met als motief een politieke beslissing dan wel het uitblijven van politieke actie. Hieronder valt ook de toename van dierenactivisme, voor zover deze niet als terrorisme gedefinieerd is. Voorbeelden van doelwitten met een politiek motief: fokkers, moskeeën (rechts racistisch) en banken.

Methoden
Volgen en onderkennen van publieke uitingen en manifestaties die tot gewelddadige acties kunnen leiden. Zie verder methoden *occasion* fase.

4.2.3 In de Rumbling fase zijn de volgende typen analyses nodig:
Trendanalyses van allerlei vormen van uitingen in media. Vaardigheid en scancapaciteit voor het efficiënt volgen en analyseren van open bronnen, maar ook kwantitatieve analyses van dataverkeer en data-mining om daarmee patronen te onderkennen.

Voorbeelden van *Rumbling*
Dieren: bekende Nederlanders die zich opwerpen voor dieren, petities, oprichting van actiegroepen (SHAC – Stop Huntington life science bedrijf Animal Cruelty, Verenigd Koninkrijk).

Trends met relevantie voor de fase rumbling
- *Cyber 'geweld' (Mondiale trend gewelddadige actie)* Steeds vaker wordt door hackers, nerds of grappenmakers onder andere het internet gebruikt voor het aanbrengen van schade, het bedreigen van personen of het trekken van aandacht.

- *Internationalisering van extremistische politieke groeperingen (trends mogelijkheden tot terrorisme binnen Nederland)* Samenwerking en 'netwerken' bijvoorbeeld rond demonstraties rond, bijvoorbeeld, bijeenkomsten van internationale organisaties en het uitwisselen van ervaringen via het internet. Dit geldt zowel voor linkse (groene) als rechtse organisaties en zowel om organisaties met leden van Nederlandse komaf als organisaties met leden van buitenlandse komaf.

- T*oename van demonstraties en 'ludieke' acties (trends binnen Nederland)* rond conferenties of andere bijeenkomsten van internationale organisaties die mede direct in verband met globalisering kan worden gebracht.

Methoden
Onderkennen van publieke uitingen en manifestaties die tot gewelddadige acties kunnen leiden. Zie verder **Methoden** in de *occasion* fase. Daarnaast zal zeker human intelligence en signal intelligence en andere vormen van intelligence hieraan moeten bijdragen.

4.2.4 In de Work-up process fase zijn de volgende typen analyses nodig:
Analyse van uitingsvormen en hun mogelijkheden in termen van 'covert work-up'.
Goede interactie tussen inlichtingendiensten, douane, FIOD, justitie, politie en IND, etc.
Volgen van technologische ontwikkelingen voor de diverse stadia van het work-up process. Het volgen van verdachte personen, reispatronen, contacten en samenkomsten, het gebruik van verdachte infrastructuur etc.
Verder kan in deze fase, ook een black hole analyse worden uitgevoerd. Black holes blijken in de praktijk vaak een uitvalsbasis voor voorbereidende gewelddadige en terroristische activiteiten te zijn.

Voorbeelden van *work-up process* zijn:
Aan de meerdere bekende tactieken zijn de afgelopen decennia nieuwe toegevoegd, vooral dankzij nieuwe technologie of technologie die voorheen alleen beschikbaar was voor inlichtingen- en veiligheidsdiensten. Te denken valt aan het gebruik van geavanceerde camera's en afluisterapparatuur voor het observeren van potentiële doelen

en slachtoffes. Terroristen beschikken, meer dan ooit tevoren, over diverse communicatiemogelijkheden en kunnen hun publieke statements, onder andere via internet rechtstreeks aan het grote publiek presenteren.

Trends met relevantie voor de fase work-up process

- *Verdere professionalisering (Mondiale trend terrorisme).* De terroristen hebben geleerd van ervaringen uit het verleden en zijn nu beter toegerust voor het organiseren van gewelddadige actie. Zij zijn beter geschikt voor het opereren tijdens langere perioden terwijl detectie, verhindering of gevangenneming wordt voorkomen.

- *Cyber terrorisme (Mondiale trend terrorisme).* Terwijl terroristische organisaties nog geen instrumenten ontwikkeld hebben als wapen tegen vitale infrastructuur zijn het vertrouwen met de beschikbaarheid en de expertise van deze groepen over informatietechnologie een duidelijke waarschuwing.

- *Het gebruik van 'amateurs' (Mondiale trend terrorisme).* Terrorisme inspireert 'amateurs' die geen verleden hebben in terrorisme of gerelateerde activiteiten. De kennis en operationele vaardigheden van 'amateurs' nemen toe.

- *Georganiseerde misdaad en terrorisme (Mondiale trend terrorisme).* In toenemende mate is terrorisme gefinancierd door middel van criminele activiteiten. Een van de resultaten hiervan is de toegenomen interactie tussen georganiseerde misdaad/ criminele organisaties en terroristen groepen.

- *De toegankelijkheid van kennis en materiaal gerelateerd aan Weapons of Mass Destruction (WMD) (Mondiale trend terrorisme).* De trend naar hoogwaardige en hoge ernst aanslagen komt in een tijd waarin de interesse onder zowel internationale als nationale terroristen groeperingen toeneemt voor het verkrijgen van WMD. Op dit moment is er geen betrouwbare informatie dat een terroristen groepering chemisch, biologische of stralingsbronnen heeft vergaard of ontwikkeld. Maar aan de andere kant zijn kennis en componenten van WMD beschikbaar op de zwarte markt. Zelfs zijn sommige basiscomponenten en gegevens via het internet beschikbaar. Belangrijk is dat er veel diefstallen zijn van medische isotopen en andere bronnen van straling.

- *Het gebruik van diaspora groeperingen (Mondiale trend terrorisme).* In toenemende mate zijn terroristen organisaties verbonden aan zogenaamde diaspora groeperingen. Deze groeperingen zijn betrokken bij het zorgen voor onderdak, genereren van financiering, verwerving en verscheping van wapens voor terroristische organisaties. Voorbeelden uit het verleden zijn onder andere: Sikhs, Kashmiris, Sri Lankan Tamils, Ieren, Armeniërs, Libanese en Palestijnse groepen.

- *Terroristisch gebruik van voortschrijdende techniek (Mondiale trend terrorisme).* Terroristische groepen maken in toenemende mate gebruik van nieuwe informatie technologie en het internet voor het formuleren van plannen, werving van leden, communicatie tussen cellen en leden, verwerving van gelden en verspreiding van propaganda. Terroristische groepen gebruiken geautomatiseerde files, e-mail en codering voor de ondersteuning van hun operaties.

- *Het gebruik van Diaspora groeperingen (Mondiale trend gewelddadige actie).* Ook binnen de gewelddadige actie worden steeds vaker Diaspora groeperingen gebruikt, zeker binnen de georganiseerde misdaad. Denk hierbij aan Albanezen en personen uit voormalig Joegoslavië.

Methoden
In deze fase zijn zullen met name analyses in methoden en technieken van potentiële daders en groeperingen worden uitgevoerd. Verder zullen human intelligence en andere vormen van intelligence moeten worden ingezet naast de methoden uit de voorgaande fases.

In de *Violent action* fase zijn de volgende typen analyses nodig:
Wereldwijde analyse van methoden en technieken, volgen van technologische ontwikkelingen ten aanzien van wapens, explosieven, hacking, 'agents', biochemie, radiologische en electromagnetische technieken en hun proliferatie.

Trends met relevantie voor de fase violent action

- *Maximalisering van het aantal slachtoffers (Mondiale trend terrorisme)*
  Door maatschappelijke onverschilligheid zijn meer spectaculaire incidenten met een hoger aantal doden en gewonden noodzakelijk voor het trekken van aandacht. Daarnaast is er een relatie tussen doelstelling en middel. Maximale doelstellingen, zoals het verdrijven van Westerse invloeden uit de Islamitische wereld en de stichting van een pan-islamistisch staat, rechtvaardigen in de ogen van personen als Osama bin Laden catastrofale methoden.

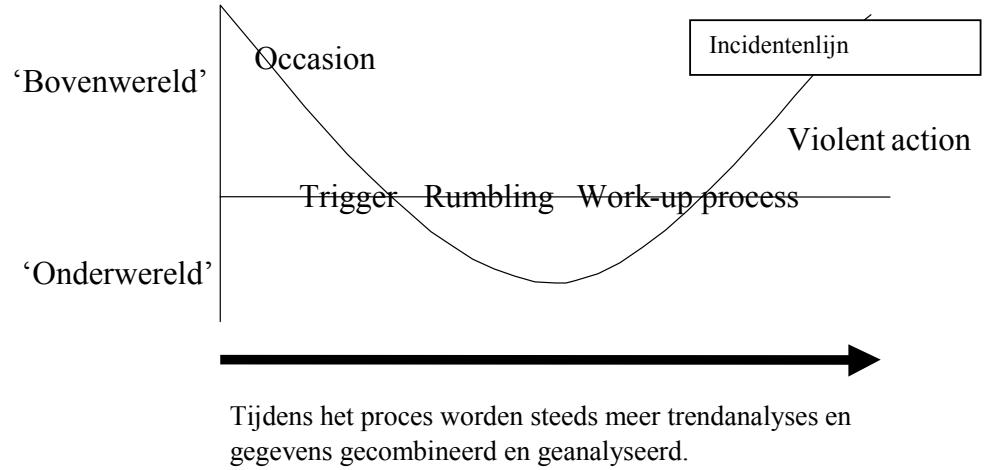
- *Verdere professionalisering (Mondiale trend terrorisme)*
  Zij zijn meer aangepast aan hun vakgebied; meer ontzagwekkend in hun capaciteit voor tactische aanpassingen en innovatief in aanvalsmethoden. Daarnaast zorgen samenwerkingsverbanden tussen terroristenorganisaties en verschillende landen - meer in het verleden dan vandaag de dag - voor een toename in dodelijke aanslagen.

- *Minder frequent opeisen van de aanslagen (Mondiale trend terrorisme)*
  De huidige terroristen lijken minder frequent verantwoordelijkheid op te eisen voor hun aanslagen.

- *Soft targets*
  Naarmate inlichtingen en veiligheidsdiensten er beter in slagen om zogeheten hard targets (VIPs, strategische infrastructuur, etc.) te beschermen worden zogeheten soft targets zoals ziekenhuizen, scholen, winkelcentra en kantoorgebouwen kwetsbaarder. Ook lijkt 'grootschalig geweld' terrorisme geen taboe te kennen met betrekking tot het plegen van aanslagen op niet-politieke doelen. Hierbij dient niet alleen gedacht te worden aan moslimterreur maar tevens aan de aanslag op de metro in Tokio. Met het doel voor ogen zoveel mogelijk angst en paniek te zaaien, zijn soft targets bovendien bijzonder aantrekkelijke doelen. Een aanslag op een dergelijk doel versterkt het idee onder de bevolking dat iedereen altijd slachtoffer kan worden.

Methoden
In de fase zullen onder andere analyses naar de trends in uitvoering moeten worden uitgevoerd. Verder zal samenwerking tussen diensten, politie en justitie benodigd zijn maar ook technologieverkenningen om te achterhalen wat de technologische mogelijkheden zijn van potentiële dadergroepen.

Alle bovengenoemde activiteiten in iedere fase die nodig zijn om de suspicious signs op te bouwen, blijven tijdens het proces relevant en nemen in intensiteit toe ingeval ernst en waarschijnlijkheid lijken toe te nemen. Wel wordt een steeds nadrukkelijker focus mogelijk.

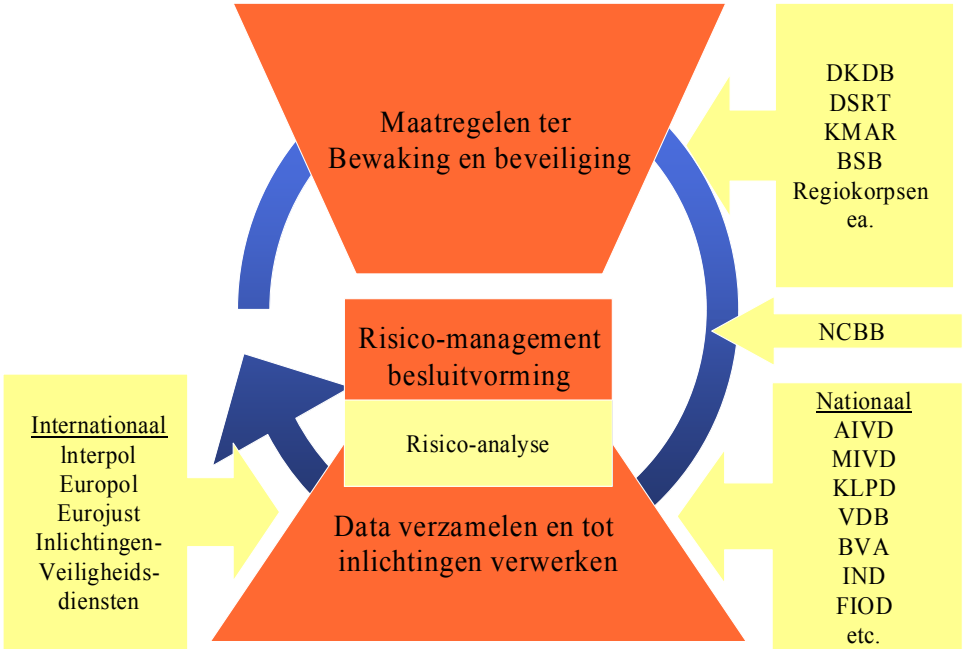


Figuur 4.1 Fase 5 Violent action externe organisaties tegen personen of objecten in Nederland.

In de fase *occasion*, *trigger* en *rumbling* zal veelal open source intelligence moeten worden gebruikt. In de fase *work-up process* en *violent action* zal ook gebruik moeten worden gemaakt van human intelligence, signal intelligence en Imagery intelligence (zie bijlage D ‘Typeringen voor intelligence’). Merk op dat een belangrijk deel van de informatie uit fase work-up en violent action met name uit andere dan open bronnen moet worden verzameld.

4.3 Analyse van het inlichtingenproces

De huidige inlichtingen- en veiligheidsorganisatie van Nederland met zijn vele verschillende diensten heeft een aantal inherente valkuilen. Bottum-up gaat het deze diensten om het optimaliseren van kennisvergaring en -gebruik. Top-down is een duidelijke scheiding van taken, verantwoordelijkheden en bevoegdheden opgelegd om daarmee de binnen een democratisch bestel benodigde transparantie te garanderen.



Figuur 4.2 Een (onvolledig) overzicht van partijen in de inlichtingen en veiligheidsketen.

De door dit laatste sterk opgedeelde inlichtingen- en veiligheidsproces kan het volgende onstaan:

Een gebrek aan 'bewustzijn': op veel verschillende plaatsen bezitten mensen (voor een deel) informatie waarvan ze zich de waarde (voor anderen) niet altijd realiseren. Van belang is daarom dat informatie 'stroomt' door de organisatie om het 'grotere beeld' te kunnen zien. Dit doet zich ook voor tussen de verschillende diensten en de vele partners in de keten.

Een gebrek aan 'aandacht': hierbij ligt de focus op ontvangen informatie. Informatie overload veroorzaakt daarbij dat de 'echte signs' niet gezien worden. Organisaties hebben de beschikking over zeer veel verschillende informatie.

Inadequate 'templates': de in templates gevatte ervaringen uit het verleden (zo ontstaan templates) volstaan niet altijd om nieuwe situaties te onderkennen. Door ontvangen informatie in standaard templates te vatten, bestaat het gevaar dat andere interpretaties niet meer kunnen of worden gemaakt.

Compartimentering: subgroepen (deelorganisaties) houden om allerlei redenen informatie voor zichzelf. Hierdoor stroomt informatie niet voldoende en ontstaat geen 'groter beeld'. Dit geldt ook voor de diensten in Nederland. Dit wordt met name versterkt door de verantwoordelijkheden en bevoegdheden van de diverse organisaties.

Oplossingen voor deze vier valkuilen zijn:
- Slimme vormen van netwerken van mensen. ICT-infrastructuur kan hieraan bijdragen.
- Helder definiëren van rollen en verantwoordelijkheden tussen met name beslissers, waarnemers (analisten) en *connectors* (mensen die een brugfunctie vervullen tussen verschillende bronnen en diensten).
- Het categoriseren van informatiesoorten op een consistente wijze waardoor zowel mensen als ICT-infrastructuur kunnen worden ingezet voor het verkrijgen van 'het grotere beeld'. Dit moet door de gehele keten op eenduidige wijze worden opgezet.
- Een hybride benadering van mensen gecombineerd met ICT waardoor de sterke punten van de mens en de techniek worden gecombineerd.

Hiermee onstaat een verder geïntegreerde informatie- en inlichtingen bouwwerk waarbinnen het mogelijk is ook de lessons learned op te sporen en deze verder in de keten ook toe te passen.

5 Conclusies en aanbevelingen

5.1 Inleiding

In dit onderzoek is nieuw denk- en datamodel ontwikkeld om op proactieve wijze een goede informatiepositie op te bouwen over potentiële dreigingen en risico's.

5.2 Conclusies

Mede gebaseerd op eerder onderzoek is een denk- en datamodel ontwikkeld dat richtinggevend kan zijn voor de ontwikkeling van het inlichtingenproces gericht op potentiële dreigingen tegen personen en objecten. Om het begrip potentiële dreigingen te definiëren en normeren is het stelsel aan definities opnieuw geformuleerd en aangevuld.

- De 'ernst' categorieën uit het stelsel bleken zich met name te richten op vitale infrastructuur en onvoldoende precies en consequent te definiëren hoe ernst ten aanzien van personen en objecten moest worden geclassificeerd.
- Omdat zowel waarschijnlijkheid als ernst samen onvoldoende aangrijpingspunten boden om potentiële dreigingen voldoende scherp te identificeren en ontwikkelingen daarbinnen te volgen, is een aantal niveaus/fases van suspicious signs ontwikkeld. Door een combinatie van waarschijnlijkheid, ernst en suspicious signs fases is het mogelijk gradaties in potentiële dreigingen te onderkennen.

Suspicious signs zijn gedefinieerd als '*een combinatie van indicaties dat een persoon of een groep personen de potentie en/of intentie heeft een bedreiging te vormen voor personen of objecten.*
Ten aanzien van suspicious signs zijn de volgende observaties te maken:

- Suspicious signs zijn op zich staande signalen die binnen een kader van meerdere suspicious signs kunnen leiden tot een daadwerkelijke aanleiding tot risico-management besluiten (opsporen, bewaken, beveiligen).
- Suspicious signs hebben betrekking op een incident in een specifieke fase. Hierbij is van belang te realiseren dat, naast de suspicious signs eigen aan de fase, de gebeurtenissen in voorgaande fases gezien kunnen worden als suspicious signs voor datgene zich in deze fase af kan spelen. Per fase moet niet alleen naar de signs van deze fase worden gekeken, maar ook naar signs uit voorafgaande fases.

Gebaseerd op literatuuronderzoek zijn trends in gewelddadige acties en terrorisme geïdentificeerd waarbij is aangegeven welke trends relevant lijken voor Nederland. Met name bestuurders en beleidsmakers ondervinden een verhoogd risico slachtoffer te worden van gewelddadige acties. Daarnaast zijn moslim jongeren een kwetsbare groep om slachtoffer te worden door ingeschakeld te worden bij gewelddadige acties.

Gebaseerd op literatuuronderzoek en dataverwerking zijn algemene mondiale en nationale trends geïdentificeerd ten aanzien van het karakter en de verschijningsvormen van gewelddadige acties en terrorisme.

5.3 Aanbevelingen

- Aangezien de verdere ontwikkeling van een risico-management methodiek buiten de scoop van dit onderzoek viel, is de beschreven methode niet volledig in al haar elementen uitgewerkt en geoperationaliseerd. Het hier gepresenteerde denk- en datamodel biedt hier echter wel de mogelijkheden voor. Het is zinvol dit nader te bezien.

- De classificatie van suspicious signs die binnen de ernst-schaal zijn gehanteerd zijn illustratief. Een apart gericht onderzoek naar deze classificatie van suspicious signs lijkt zinvol. Temeer omdat het projectteam het mogelijk lijkt risico-management maatregelen aan de suspicious signs te koppelen en deze tevens te relateren aan de verantwoordelijkheden en bevoegdheden van de diverse spelers in de bewaken-en-beveiligen-keten. Voor ieder ernst-waarschijnlijkheid-suspicious signs fase ontstaat dan een palet een mogelijkheden tot ingrijpen, inclusief de organisaties die daarvoor kunnen worden ingezet.

- De verwachting is dat de gecombineerde gegevens uit open bronnen en bijvoorbeeld politiële, juridische en financiële bronnen een veel beter inzicht geven in suspicious signs. Het lijkt zinvol dit gecombineerde onderzoek onderdeel te laten uitmaken van de werkmethoden van de dienst. En dan met name ook voor de fases trigger, rumbling en work-up process.

- Geconstateerd is dat ten aanzien van de suspicious signs fases *Trigger*, *Rumbling* en gedeeltelijk ook *Work-up proces* het veelal lastig is om uit historische bestanden informatie te verzamelen gebaseerd op open bronnen aangezien deze zaken meestal voor media geen aanleiding vormen om erover te berichten. Dit betekent dat een significant deel van de dataverzamel- en verwerkingscapaciteit benodigd zal zijn om veel schijnbaar onbelangrijke of onverdachte gegevens te identificeren.
- Trendanalyse is een belangrijke activiteit en vergt een gedegen politieke en maatschappelijke antenne op onderwerpen die niet per definitie bij inlichtingendiensten (alleen) aanwezig is.

- Multidisciplinair onderzoek is van belang om de benodigde analyses uit te voeren.

- Omdat meerdere inlichtingeninstanties ieder slechts delen van de gehele inlichtingenbehoefte afdekken, lijkt het zinvol deze trendanalyse apart te organiseren en wellicht zelfs buiten de inlichtingendiensten te positioneren bij onderzoeksinstellingen, universiteiten etc.

- Door het sterk opgedeelde inlichtingen- en veiligheidsproces kan het volgende onstaan:
  - *Een gebrek aan 'bewustzijn'*;
  - *Een gebrek aan 'aandacht'*;
  - *Inadequate 'templates'*;
  - *Compartimentering*.

  Zorg daarom voor:
  - Slimme vormen van netwerken van mensen. ICT-infrastructuur kan hieraan bijdragen.
  - Helder gedefinieerde rollen en verantwoordelijkheden tussen met name beslissers, waarnemers (analisten) en *connectors* (mensen die een brugfunctie vervullen tussen verschillende bronnen en diensten).

  - Het categoriseren van informatiesoorten op een consistente wijze waardoor zowel mensen als ICT-infrastructuur kunnen worden ingezet voor het verkrijgen van ‘het grotere beeld’. Dit moet door de gehele keten op eenduidige wijze worden opgezet.
  - Een hybride benadering van mensen gecombineerd met ICT waardoor de sterke punten van de mens en de techniek worden gecombineerd.

- Om het inlichtingenontwikkelproces optimaal te organiseren is het zinvol dat alle inlichtingen- en veiligheidsdiensten gebruik maken van een eenduidige classificatie van waarschijnlijkheid, ernst en suspicious signs fases (ieder gericht binnen haar eigen taakveld, verantwoordelijkheden en bevoegdheden) om daarmee eenduidig te interpreteren en te combineren producten te ontwikkelen.

- In voorkomende en geoorloofde gevallen is het voor een effectieve combinatie van inlichtingenbestanden van verschillende inlichtingendiensten nuttig dat deze in hun bestanden de elementen uit het gehanteerde datamodel uit dit onderzoek kunnen verwerken. Het is van belang dat de informatiearchitectuur van de diverse diensten daarop wordt afgestemd.

6 Referenties

[1] Nota ‘Nieuw stelsel bewaken en beveiligen’, Brief aan de Voorzitter der Staten-Generaal: (d.d. 20 juni 2003, OOV/BC2003/68622) van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Justitie (TK-stuk, nr. 28974).

[2] Martrin C. Libicki, Shari Lawrence Pfleeger, Collecting the dots, problem formulation and solution elements, ISBN 0-8330-3561, Rand Science and Technology, Santa Monica, United States, Januari 2004.

7 Ondertekening

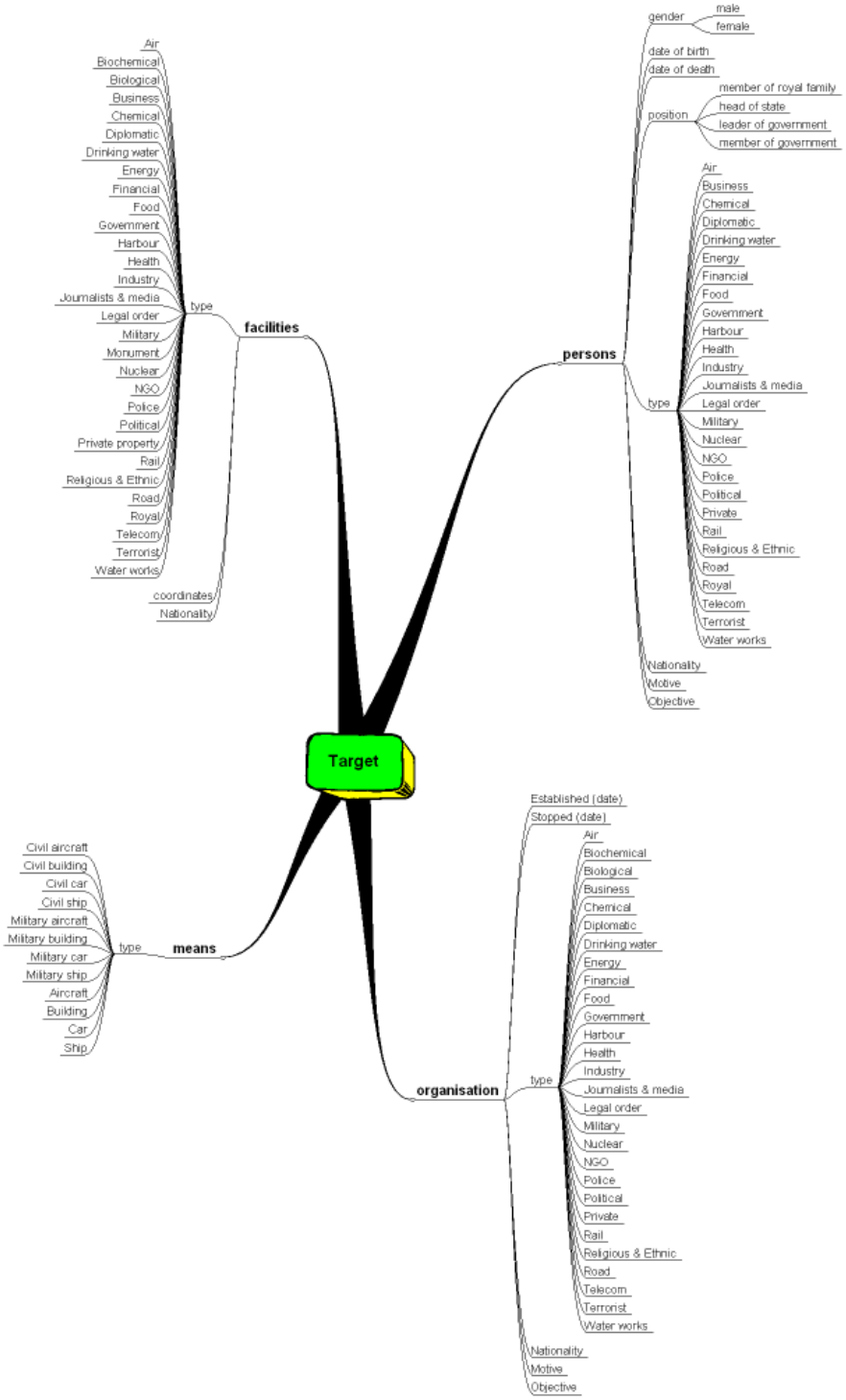
Den Haag, juli 2006

J.G.M. Rademaker
Projectleider

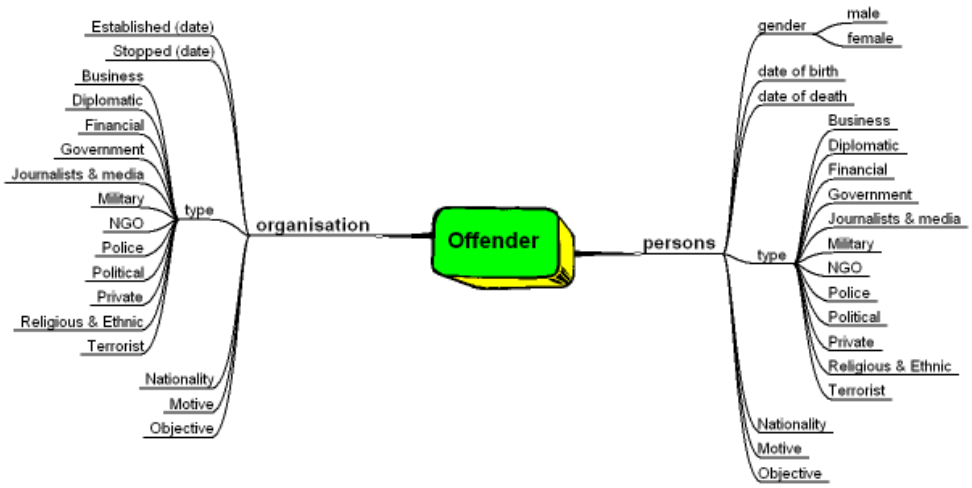
A Datamodel sub-templates

A.1 Templates

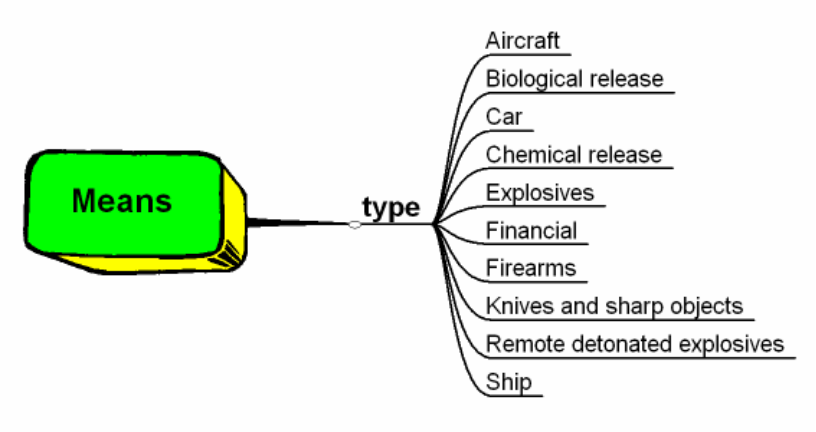
Template Target



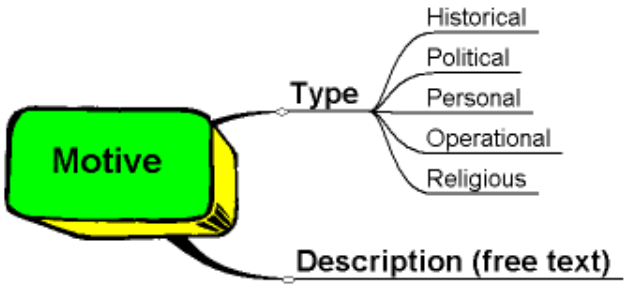
Template Offender



Template Means



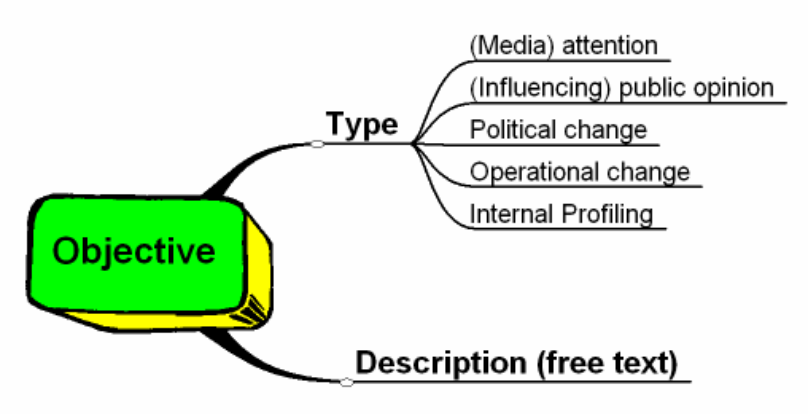
Template Motive



Typen motives
Historische motives zijn in verband gebracht met historische incidenten of 'trauma's' van nationale, politieke of religieuze groepen, zoals deportaties of genocide. Politieke motives zijn in verband gebracht met politieke doelen of bepaalde nationale, politieke of religieuze groepen. Persoonlijke zijn in verband gebracht met persoonlijke stimulansen om (te helpen bij) de organisatie of uitvoering van een 'gewelddadige actie.

Deze stimulansen variëren van persoonlijke trauma's of wraakgevoelens tot en met allerlei verdraaide denkbeelden die ertoe kunnen leiden dat een persoon een 'terroristische' daad uitvoert. Operationele motives zijn in verband gebracht met het algemene proces van de organisatie van een individuele 'terroristische' aanval, een 'campagne of een anti-terroristische activiteit van een overheidsorgaan. Deze motives zijn niet direct in verband gebracht met historische, politieke of persoonlijke motives van de 'terrorist', maar primair met de operationele aspecten van (de bestrijding van) gewelddadige actie.

Template Objective

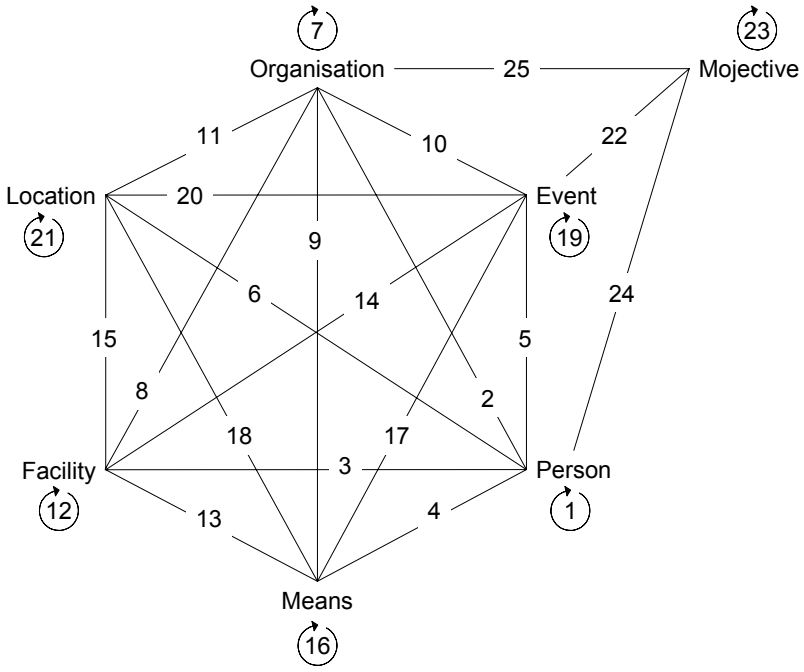


Typen objectives
De typen objectives variëren van nogal directe objectives zoals politieke en operationele verandering en beïnvloeding van de publieke opinie, tot meer indirecte doelen zoals (media) aandacht in het algemeen en interne profilering binnen de eigen groep en beweging.

B Relaties en suspicious signs fases

B.1 Relaties

Figuur B.1 hierna geeft alle mogelijk geachte relaties weer tussen de verschillende topics. Ook tussen de topics zelf bestaan relaties.



Figuur B.1 Schematisch diagram met relaties.

Verschillende soorten relaties tussen topic typen
Onderstaande tabel geeft de relaties weer, genummerd van 1 t/m 23 uit figuur B.1. De relaties tussen topics zijn gelegd van topic links naar topic rechts.
Voorbeeld: Person → Person: Mr. X → Commands → Mr. Y kan ook gemodelleerd worden als Mr. Y → Commanded by → Mr. X. In de tabel is alleen de relatie 'Commands' opgenomen.

1: Person → Person	2: Person → Org.	3: Person → Facility	4: Person → Means	5: Person → Event	6: Person → Location
Family of[2]	Associated with	Owns	Owns	Target of	Lives in
Commands	Commands	Buys	Uses	Caused	Died in
On unfriendly terms with	Member of	Uses	Provides	Claimed	Born in
On friendly terms with	On unfriendly terms with	Possible target for	Produces	Accused of	Related to
Inspired by	On friendly terms with	Related to	Related to	Sentenced	

[2] Brother, sister, father, mother, etc.

The same as	Plans			Offended	
Related to	Related to			Participated in	
				Related to	

7: Org. → Org.	8: Org. → Facility	9: Org. → Means	10: Org. → Event	11: Org. → Loc.	12: Facility → Facility
Associated with	Owns	Owns	Target of	Situated in	Part of
Commands	Buys	Uses	Caused	Established in	Related to
Preceeded	Uses	Controls	Claimed	Related to	
Friend of	Possible target for	Provides	Accused of		
Enemy of	Related to	Produces	Sentenced		
Supports		Related to	Plans		
In conflict with			Disapproves		
The same as			Related to		
On unfriendly terms with					
On friendly terms with					
Related to					

13: Facility → Means	14: Facility → Event	15: Facility → Location	16: Means → Means	17: Means → Event	18: Means → Location
Related to	Related to	Located in	Part of	Used in	Located in
		Related to	Related to	Related to	Related to

19: Event → Event	20: Event → Location	21: Location → Location	22. Mojective → Event	23. Mojective → Mojective	24. Mojective → Person	25. Mojective → Org.
Preceded	Happened in	Related to	Caused	Related to	Has	Has
Caused	Related to		Related to		Related to	Related to
Related to						

C Typeringen voor intelligence

De volgende typeringen voor intellignece zijn in gebruik:
SIGINT (deze bestaan uit COMINT en ELINT), HUMINT, IMINT en OSINT.
Minder bekend zijn: ACINT en MASINT

Signals Intelligence (SIGINT)	De algemene term die zowel Communications Intelligence (COMINT) als voor Electronic Intelligence (ELINT) wordt gebruikt wanneer het niet nodig is onderscheid te maken tussen deze twee soorten
Communications Intelligence (COMINT)	Inlichtingen verkregen uit uitzendingen van communicatiemiddelen en verbindingssystemen in het elektromagnetische spectrum door anderen dan de bedoelde ontvangers of gebruikers (OWKL).
Electronic Intelligence (ELINT)	Inlichtingen verkregen uit elektronische niet-radio-uitzendingen door personen of instanties voor wie de uitzendingen niet bestemd zijn. De inlichtingen worden vastgesteld op grond van analyse van de technische karakteristieken van elektromagnetische uitzendingen (geen radio-uitzendingen), bijvoorbeeld radars en raketsystemen alsmede lasers, infrarood apparatuur en alle uitrusting die binnen het elektromagnetische spectrum zenden. (OWKL)
Human Intelligence *(HUMINT)*	Inlichtingen afgeleid van door mensen verzamelde en geleverde gegevens (OWKL).
Imagery Intelligence (*IMINT)*	Inlichtingen die zijn afgeleid uit beelden van fotografische, radar-, electro-optische, infrarode, thermische en multi-spectrale sensoren. Deze sensoren zijn grondgebonden, bevinden zich op of in zee dan wel in vliegende platforms (inbegrepen een satelliet). De informatie die een beeld op zich geeft, dient vaak om inlichtingen verkregen uit een andere bron te bevestigen of aan te vullen. Satellieten, bemande en onbemande vliegtuigen leveren het meeste beeldmateriaal aan. Omdat dit beeldmateriaal veelal op het strategische en operationeel niveau wordt verwerkt, is het momenteel nog niet direct beschikbaar op lagere niveaus.
Open Source Intelligence (OSINT)	Inlichtingen die worden verkregen uit open bronnen zoals radio, televisie, internet, pers, bevolking en andere ongerubriceerde informatie die een beperkte verspreiding heeft of beperkt toegankelijk is (OWKL).
Acoustic Intelligence (ACINT)	Inlichtingen die zijn verkregen met behulp van geluidssensoren.
Measurement and signature intelligence (MASINT)	Wetenschappelijke en technisch informatie die verkregen is door de kwantitatieve en kwalitatieve analyse van gegevens (metrisch, ruimtelijk, golflengten, tijd afhankelijkheid, modulatie, plasma en magnetisme). Deze gegevens worden met speciale sensoren verworven met het doel specifieke kenmerken van zenders te onderkennen en zodoende de identificatie daarvan vast te stellen.

Distributielijst

Onderstaande instanties/personen ontvangen een volledig exemplaar van het rapport.

1	Directeur CCSS, prof. dr. R. de Wijk
2	Adjunct directeur CCSS, ir. R.F.W.M. Willems
3	J.G.M. Rademaker MTL, Projectleider
4/6	Reserve