



Ministerie van Defensie

## Joint Doctrine Publicatie 2 Inlichtingen

Dit is een uitgave van:  
Ministerie van Defensie

Vormgeving:  
Grafische Dienst | Audiovisuele Dienst Defensie | Den Haag

Foto's:  
Audiovisuele Dienst Defensie



Joint Doctrine Publicatie 2

## **Inlichtingen**

## Colofon

Defensiestaf  
Directie Operationeel Beleid, Behoeftestellingen en Plannen  
Afdeling Doctrine

Plein 4  
Postbus 20701  
2500 ES Den Haag

**Contactpersoon** KLTZ E. de Jong  
*DOCTRINEONTWIKKELAAR*  
T 070 316 77 87  
MDTN \*06 501 67787  
doctrine.cds@mindef.nl

**Versie** Definitief  
**Opdrachtgever** CDS  
**Auteur(s)** Dhr. P.A. Brouwer (DIVI)  
Maj M.Scholten (DIVI)

## Voorwoord CDS

Adequate informatie en inlichtingen zijn essentieel voor besluitvorming bij militaire operaties. De militaire functie inlichtingen voorziet in een zo volledig en actueel mogelijk beeld van de situatie en is een randvoorwaarde voor het kunnen functioneren van een militaire eenheid. Inlichtingen komen tot stand via het gericht verzamelen en verwerken van informatie. De commandant geeft richting aan het inlichtingenproces. Zijn belangstelling richt zich niet alleen op de 'klassieke' aspecten vijand, weer en terrein maar ook op informatie over historische, culturele, sociale en religieuze achtergronden van een crisis en de rol en betekenis van alle spelers in het operatiegebied.

De Nederlandse krijgsmacht voert in nationaal en internationaal verband operaties uit. Hierbij is *jointness* de norm en wordt ook steeds vaker in een geïntegreerde benadering met andere niet-militaire partijen opgetreden. Succesvolle samenwerking betekent ook dat processen en procedures op elkaar zijn afgestemd. De Joint Doctrine Publicatie (JDP) Inlichtingen beschrijft de grondbeginselen en principes die ten grondslag liggen aan de inrichting van het functiegebied Inlichtingen en de belangrijkste processen daarbinnen. De publicatie is een gemeenschappelijk uitgangspunt voor de krijgsmacht.

Het belang van tijdige en juiste inlichtingen is van alle tijden. Recente operaties in een complexe operationele omgeving onderstrepen dit belang. De operationele omgeving nu en in de toekomst bevat dreigingen met een hybride karakter waarin geweldsniveaus snel en onvoorspelbaar kunnen wisselen. Dit legt extra nadruk op de anticipatiefunctie van inlichtingen.

Het inlichtingenveld is constant in beweging. De doctrine beschrijft zoveel mogelijk de huidige situatie en relevante ontwikkelingen zijn zo compleet mogelijk verwerkt en beschreven. Nog niet alle discussies, studies en onderzoeken zijn afgerond. Zo is beleid over de aansturing van nationale inlichtingenmiddelen bij operaties in het buitenland nog in ontwikkeling. Nieuwe technologieën en wetenschappelijke inzichten blijven voortdurend invloed uitoefenen op het militaire vakgebied. Hierop wachten zou betekenen dat we de kans verloren laten gaan om nu al van de opgedane kennis en ervaringen te kunnen profiteren.

Ik verzoek u bij de planning, gereedstelling en inzet van personeel en eenheden voor operaties gebruik te maken van de in deze doctrine beschreven inzichten.

DE COMMANDANT DER STRIJDKRACHTEN

P.J.M. van Uhm  
Generaal

## Inhoud

<b>Colofon</b>	<b>3</b>
<b>Voorwoord CDS</b>	<b>4</b>
<b>INLEIDING</b>	<b>9</b>
<b>1 CONTEXT VAN HET INLICHTINGEN EN VEILIGHEIDSDOMEIN</b>	<b>12</b>
<b>1.1 INLEIDING</b>	<b>12</b>
<b>1.2 INLICHTINGEN</b>	<b>12</b>
1.2.1 Doel van inlichtingen	12
1.2.2 De operatieomgeving.	14
1.2.3 Bescherming van inlichtingen	15
1.2.4 Inlichtingencapaciteit	15
<b>1.3 INLICHTINGENONDERSTEUNING VAN DE OPERATIE</b>	<b>17</b>
1.3.1 Strategisch niveau	17
1.3.2 Operationeel niveau	18
1.3.3 Nationale operaties	19
1.3.4 De inlichtingenketen	21
<b>1.4 JURIDISCH KADER</b>	<b>24</b>
<b>1.5 BESCHERMING VAN MILITAIR VERMOGEN</b>	<b>25</b>
1.5.1 Operationele veiligheid	26
1.5.2 Contra-Inlichtingen en Veiligheid(CI&V)	27
<b>1.6 INFORMATIETECHNOLOGIE</b>	<b>27</b>
<b>1.7 ACTUELE ONTWIKKELINGEN</b>	<b>29</b>
1.7.1 Operationele ontwikkelingen	30
1.7.2 Bedreigingen	30
1.7.3 Kwaliteiten	31
1.7.4 Middelen	32
1.7.5 Samenwerking	32
1.7.6 Opleiding en training	32
1.7.7 Processen en procedures	32
<b>1.8 SAMENVATTING</b>	<b>33</b>
<b>2 BEGRIPSVORMING INLICHTINGEN EN VEILIGHEID</b>	<b>34</b>
<b>2.1 INLEIDING</b>	<b>34</b>
<b>2.2 DEFINITIES</b>	<b>34</b>
2.2.1 Definitie van inlichtingen	34
2.2.2 Definitie van Contra-Inlichtingen en Veiligheid	36
2.2.3 Definitie van Veiligheid	36
<b>2.3 GRONDBEGINSELEN</b>	<b>37</b>
2.3.1 Responsiviteit ( <i>Responsiveness</i> )	37

2.3.2	Tijdigheid ( <i>Timeliness</i> )	37
2.3.3	Objectiviteit ( <i>Objectivity</i> )	37
2.3.4	Toegankelijkheid ( <i>Accessibility</i> )	37
2.3.5	Voortdurende beoordeling ( <i>Continuous review</i> )	38
2.3.6	Bronbescherming ( <i>Source protection</i> )	38
2.3.7	Centrale coördinatie ( <i>Centralised co-ordination</i> )	38
2.3.8	Systematische inzet en exploitatie ( <i>Systematic exploitation</i> )	38
<b>2.4</b>	<b>NIVEAUS VAN INLICHTINGEN</b>	38
2.4.1	Inlichtingen op het strategische niveau	39
2.4.2	Inlichtingen op het operationele niveau	40
2.4.3	Inlichtingen op het tactische niveau	40
2.4.4	Inlichtingen op het technische niveau	40
<b>2.5</b>	<b>SOORTEN INLICHTINGEN</b>	42
2.5.1	Basisinlichtingen	42
2.5.2	Actuele inlichtingen	42
2.5.3	Doelinlichtingen	42
2.5.4	Technische Inlichtingen	42
<b>2.6</b>	<b>VERZAMELMETHODEN, -ORGANEN EN BRONNEN</b>	43
2.6.1	Verzamelmethode	44
2.6.2	Verzamelorgaan	46
2.6.3	Bron	46
<b>2.7</b>	<b>SAMENVATTING</b>	47
<b>3</b>	<b>INLICHTINGEN VOOR DE COMMANDOVOERING</b>	48
<b>3.1</b>	<b>INLEIDING</b>	48
<b>3.2</b>	<b>HET INLICHTINGENPROCES</b>	48
3.2.1	De inlichtingencyclus	48
3.2.2	<i>Collection Co-ordination &amp; Information Requirements Management</i>	49
<b>3.3</b>	<b>INITIËREN (DIRECTION)</b>	51
3.3.1	Gebied van inlichtingenverantwoordelijkheid en -belangstelling	51
3.3.2	Bepalen van de inlichtingenbehoefte	52
3.3.3	Uitwerken van de inlichtingenbehoefte	53
3.3.4	Het verzamelplan ( <i>Intelligence Collection Plan; ICP</i> )	54
<b>3.4</b>	<b>VERZAMELEN (COLLECTION)</b>	54
3.4.1	Verzamelorganen	55
3.4.2	De bewerking door verzamelorganen	56
<b>3.5</b>	<b>VERWERKEN (PROCESSING)</b>	57
3.5.1	Registeren ( <i>Collation</i> )	57
3.5.2	Evalueren	57

3.5.3	Analyseren	57
3.5.4	Integreren	58
3.5.5	Interpreteren	58
<b>3.6</b>	<b>VERSPREIDEN (DISSEMINATION)</b>	59
<b>3.7</b>	<b>INLICHTINGENONDERSTEUNING VAN COMMANDOVOERING</b>	60
3.7.1	<i>Intelligence Preparation of the Environment (IPE)</i>	61
3.7.2	<i>Environment Evaluation (EE)</i>	63
3.7.3	<i>Threat Evaluation (TE)</i>	63
3.7.4	<i>Factor Integration (FI)</i>	63
<b>3.8</b>	<b>IPE BIJ DE BESLUITVORMING EN PLANNING</b>	64
3.8.1	Het generieke proces	64
3.8.2	De toepassing bij militaire operaties	65
<b>3.9</b>	<b>SAMENVATTING</b>	68
<b>4</b>	<b>CONTRA-INLICHTINGEN EN VEILIGHEID (CI&amp;V)</b>	70
<b>4.1</b>	<b>INLEIDING</b>	70
<b>4.2</b>	<b>DE DREIGING VAN SSST</b>	70
4.2.1	Directe dreiging	70
4.2.2	Indirecte dreiging	70
<b>4.3</b>	<b>DE BEVEILIGINGSMATREGELEN TEGEN SSST</b>	72
4.3.1	Personele beveiliging	73
4.3.2	Fysieke beveiliging	73
4.3.3	Informatiebeveiliging	73
4.3.4	Industriebeveiliging	74
<b>4.4</b>	<b>INTERNATIONALE AFSPRAKEN</b>	74
<b>4.5</b>	<b>SAMENVATTING</b>	74
<b>Bijlage 1</b>	<b>VERZAMELMETHODEN, -ORGANEN EN BRONNEN</b>	76
<b>Bijlage 2</b>	<b>BRON-, INFORMATIE- EN INLICHTINGENEVALUATIE</b>	84
<b>Bijlage 3</b>	<b>JURIDISCHE ASPECTEN-Wiv 2002</b>	88
<b>Bijlage 4</b>	<b>VERKLARENDE WOORDENLIJST</b>	90
<b>Bijlage 5</b>	<b>LIJST VAN AFKORTINGEN</b>	92

## Inleiding

Inlichtingen is een functie van het militaire optreden die zich richt op het ondersteunen van commandanten op ieder niveau bij hun beeldvorming, oordeelsvorming en besluitvorming tijdens het commandovoeringsproces. De *Joint Doctrine Publicatie 2* “Inlichtingen” (JDP-2) is een leidraad voor de inlichtingenondersteuning van de planning, voorbereiding, uitvoering en afronding van (militaire) operaties op nationaal grondgebied en tijdens expeditionaire inzet. Omdat het functiegebied inlichtingen nauw verbonden is aan contra-inlichtingen en veiligheid, gaat deze publicatie daar ook op in. Operationele ontwikkelingen, zoals een geïntegreerde benadering van hedendaagse en toekomstige veiligheidsproblemen, de toenemende verwevenheid van externe en interne veiligheid en de vervlechting van de traditionele niveaus van het militair optreden, nopen tot de vaststelling van deze doctrine. Verder zijn de geleerde lessen uit expeditionaire operaties richtinggevend. Hierin is ervaring opgedaan met uiteenlopende dreigingen, de complexiteit van de operationele omgeving (onder andere de bevolking in verstedelijkte gebieden) en technologische ontwikkelingen.

De JDP-2 is één van de publicaties in de joint doctrine hiërarchie. De publicatie richt zich primair op commandanten en personeel werkzaam in het operationele domein. Het document biedt een kader aan commandanten voor de aansturing van het inlichtingen- en veiligheidsproces. Hoewel ze richting geeft aan hoofdkwartieren op het operationele niveau, is de publicatie ook van waarde voor commandanten en staven op het strategische en hogere tactische niveau. De JDP-2 is voorts een referentie voor personeel werkzaam binnen het functiegebied ‘Inlichtingen en Veiligheid’ (I&V). De doctrine is de basis voor onderwijs en training en geeft richting aan de ontwikkeling van afgeleide doctrinepublicaties; in die zin beoogt de doctrine ook een startpunt te zijn voor verdere studie van het onderwerp inlichtingen. Voor niet-militaire organisaties is deze doctrine bruikbaar in het kader van informatie en wederzijds begrip.

De JDP-2 vindt haar basis in de doctrinepublicaties van de NAVO en is daardoor sterk verweven met internationale (doctrine)ontwikkelingen. In beginsel is de NAVO-doctrine leidend over een nationale doctrine, in het bijzonder in multinationale operaties. De JDP-2 vormt de basis voor de ontwikkeling van afgeleide en meer gedetailleerde publicaties. Ook geeft de JDP-2 richting aan het schrijven van handboeken en publicaties voor de Operationeel Commando's (OPCO's). Deze publicatie is ontwikkeld op basis van de volgende inhoudelijke uitgangspunten:

- De doctrine is algemeen van aard. Dat betekent dat de JDP-2 de principes, uitgangspunten en randvoorwaarden voor inlichtingen beschrijft.

- De publicatie is beschrijvend, biedt handvatten voor en over inlichtingen, maar is geen procedurehandboek voor een specifieke eenheid, operatie of proces. Daar waar nodig en mogelijk, wordt verwezen naar andere publicaties.
- Nederlandse strijdkrachten opereren veelal in multinationalaal en joint verband; deze publicatie beschouwt multinationaliteit en jointness als de standaard voor de inzet van militair vermogen.

Omdat per organisatiedeel en per niveau de doelstellingen van commandanten en de belangen van opponenten en actoren kunnen variëren, zullen ook de primaire inlichtingenbehoefte op deze niveaus onderling verschillen. De grondslagen, principes en processen zijn in generieke termen echter identiek voor alle inlichtingenfuncties van de krijgsmacht. De JDP-2 beschrijft deze generieke visie op inlichtingen. De publicatie schept een gemeenschappelijk beeld, op basis waarvan de diverse operationele commandanten, binnen hun operationele domein, leidraden en handboeken kunnen ontwikkelen voor het functiegebied I&V.

Na deze inleiding wordt in hoofdstuk 1 de functie inlichtingen in algemene zin gedefinieerd en in context geplaatst. Belangrijke kernbegrippen, zoals informatie en inlichtingen, de operationele omgeving, inlichtingenondersteuning van de militaire operatie, evenals samenwerking en juridische kaders worden beschreven.

Hoofdstuk 2 schetst aan de hand van een begrippenkader en de grondbeginselen van inlichtingen een raamwerk waarin de diverse inlichtingencapaciteiten binnen de functie inlichtingen van het militair optreden zich manifesteren.

In hoofdstuk 3 wordt de relatie tussen de functie inlichtingen en commandovoering beschreven. Dit gebeurt door in het inlichtingenproces de vier stappen van de inlichtingen-cyclus, te weten initiëren, verzamelen, verwerken en verspreiden te verbinden aan het besluitvormingsproces.

In hoofdstuk 4 wordt tot slot de functie van Contra-Inlichtingen en Veiligheid toegelicht. Bij het samenstellen van de JDP-2 is, onder andere, gebruik gemaakt van de volgende publicaties:

- Militair Strategische Visie 2010, Commandant der Strijdkrachten, 2010
- Nederlandse Defensie Doctrine (NDD), Commandant der Strijdkrachten, 2005

- Joint Doctrine Publicatie 5 Commandovoering, Commandant der Strijdkrachten, 2010
- Eindrapport Verkenningen: 'Houvast voor de krijgsmacht van de toekomst', Ministerie van Defensie, 2010
- Defensie Beveiligings Beleid (DBB), Ministerie van Defensie, 2007
- Algemene Beveiligingseisen voor Defensie Opdrachten (ABDO), Ministerie van Defensie, 2006
- *Allied Joint Publication (AJP)- 2, Allied Joint Intelligence, Counter Intelligence and Security Doctrine, 2003*
- *Allied Joint Publication (AJP)- 2.3, Allied Joint Doctrine for Human Intelligence (HUMINT), 2008*
- *Allied Administrative Publication (AAP)- 6, Nato Glossary of Terms and Definitions, 2009*
- *Joint Publication (JP) 2-0 Joint Intelligence, United States, Chairman Joint Chiefs of Staff, 2007*
- Rapport 'Inlichtingen en Veiligheid Defensie: Kwaliteit, Capaciteit en Samenwerking', Onderzoeksgroep Inlichtingen en Veiligheid Defensie ("Commissie Dessens"), 2007

# 1. CONTEXT VAN HET INLICHTINGEN EN VEILIGHEIDSDOMEIN

## 1.1 Inleiding

Dit hoofdstuk gaat in op de algemene aspecten van de functie inlichtingen en plaatst inlichtingen in context.

De inzet van het militaire instrument kan bijdragen aan het bereiken van de politiek-strategische doelstellingen van de Nederlandse overheid. Om tot een goed gefundeerd besluit te komen voor die inzet, is een gedegen inzicht in relevante actoren en factoren, en de invloed die zij uitoefenen op elkaar en de omgeving, een belangrijke voorwaarde. Dit onderwerp wordt beschreven in sectie 1.2.

Militaire operaties kunnen zowel in coalitieverband als nationaal worden uitgevoerd. De eisen die hierbij worden gesteld aan het inlichtingenwerkveld kunnen verschillen. Dit geldt o.a. voor de inrichting van de inlichtingenketen en de samenwerking met andere partners. Deze onderwerpen komen aan de orde in sectie 1.3.

Sectie 1.4. geeft het juridische kader weer waarbinnen de activiteiten van het inlichtingendomein plaatsvinden. In sectie 1.5 wordt de invloed van de onderwerpen *Operations Security* en *Contra-Inlichtingen en Veiligheid* beschreven als onderdeel van bescherming van militair vermogen.

De ontwikkelingen en het gebruik van informatietechnologie voor inlichtingen worden beschreven in sectie 1.6. Als laatste komen in sectie 1.7 de actuele ontwikkelingen, die invloed hebben op het inlichtingendomein, aan de orde.

## 1.2 Inlichtingen

### 1.2.1 Doel van inlichtingen

Zonder informatie geen operatie. Inlichtingen zijn de resultante van kennis, interpretatie en begrip over de activiteiten, mogelijkheden (*capabilities*) en intenties van alle actoren en factoren van invloed die voor de operatie van belang kunnen zijn. De militaire functie inlichtingen voorziet in een zo volledig en actueel mogelijk beeld van de situatie en is een randvoorwaarde voor het effectief kunnen functioneren van een militaire eenheid. Inlichtingen komen tot stand via het gericht verzamelen en verwerken van informatie. De commandant geeft richting aan het inlichtingenproces. Zijn belangstelling richt zich niet alleen op de 'klassieke' aspecten vijand, weer en terrein maar ook op informatie over rol, betekenis en samenstelling van relevante actoren als bevolking, politieke partijen, invloedrijke personen en/of organisaties alsmede historische, culturele, sociale en religieuze aspecten van een crisis en de omgeving.

Het doel van inlichtingen is de ondersteuning van commandanten op ieder niveau bij hun beeldvorming, oordeelsvorming en besluitvorming tijdens het commandovoeringsproces. Een goed beeld van de situatie door gevalideerde inlichtingen vermindert de onzekerheden over de operationele omgeving waarin commandanten met de inzet van de hen ter beschikking staande middelen hun doelen moeten bereiken.

Hoe goed de inlichtingenpositie ook is, een commandant wordt vrijwel altijd geconfronteerd met onzekerheden als gevolg van een informatietekort. Hoewel er in algemene zin veel informatie beschikbaar zal zijn, is niet altijd duidelijk welke informatie relevant is en is de informatie ook niet altijd beschikbaar op het juiste niveau. De relevantie van beschikbare informatie kan snel wijzigen als gevolg van wijzigingen in de geografische ruimte, de interactie tussen de vele actoren, de wijze van optreden van opposanten en de samenstelling van de coalitie in het inzetgebied. De eventuele onzekerheid als gevolg van een verondersteld tekort aan informatie mag echter niet leiden tot het uitstellen of niet nemen van besluiten en daardoor tot operationele verlamming. Daar waar informatie (nog) ontbreekt zullen aannames moeten worden gedaan. Validering van deze aannames daarna is een continu proces. Een juiste balans is essentieel.

Een juist begrip van de operationele omgeving is gebaseerd op informatie en inlichtingen. Informatie is gevraagd en ongevraagd beschikbaar uit een veelheid aan bronnen. Operaties vinden veelal plaats in gebieden met sociaal-culturele omstandigheden die van de onze afwijken, wat een robuuste mix vergt van diverse expertises. Dit vraagt uiteenlopende kwaliteiten op verschillende deelgebieden in het inlichtingenproces, zodat een brede oriëntatie, ook op niet-militair terrein mogelijk wordt. Naast dat specifieke inlichtingen-capaciteiten gericht informatie verzamelen en inlichtingen produceren, is ook veel informatie beschikbaar van actoren die niet specifiek zijn bedoeld voor het verzamelen van informatie. Dit betreft onder andere militairen en militaire eenheden die in het operatiegebied optreden. Daarnaast kunnen niet-militaire actoren zoals internationale organisaties, non-gouvernementele organisaties, universiteiten en denktanks bijdragen aan een beter begrip van de situatie.

Operationeel succes vergt een nauwkeurige afstemming van alle beschikbare middelen en capaciteiten aan de hand van een geïntegreerde en effectgerichte benadering<sup>1</sup>. Naast het fysiek en kinetisch aangrijpen van doelen zullen er vele niet-kinetische activiteiten uitgevoerd worden die zijn gericht op het beïnvloeden van de perceptie van partijen. Dit betreft onder andere *Civil Military Cooperation (CIMIC)*, *Information Operations (InfoOps)* en

<sup>1</sup> Zie JDP-5 Commandovoering, 2010



ondersteuning aan economische en bestuurlijke (weder)opbouw. Om daarin samenhang aan te brengen is een gedegen inzicht in en diepgaande kennis van de operatieomgeving onontbeerlijk. Het beschikken over zo gedetailleerd en actueel mogelijke inlichtingen en informatie vormt hiervoor de basis. Dit leidt vervolgens tot een omgevingsbeeld (*situational awareness*) dat dient te worden gedeeld met relevante spelers. Het gedeelde omgevingsbeeld moet bijdragen aan een diepgaand begrip van de situatie (*understanding*) waarbij een specifieke situatie op een juiste wijze wordt geïnterpreteerd. Begrip is alleen mogelijk door het voortdurend analyseren van de situatie en het contact met de belangrijkste actoren. Het vereist het delen van kennis en inzicht in en gevoel voor individuele groepen en actoren.

### 1.2.2 De operatieomgeving.

De omgeving, waarin commandanten militair vermogen inzetten, kenmerkt zich door een grote hoeveelheid aan actoren en factoren van invloed. Dit zijn actoren en factoren vanuit de fysieke omgeving ('weer en terrein') en vanuit de maatschappelijke omgeving (de 'Human Dimension'). De actoren oefenen invloed uit op elkaar en op de omgeving en veroorzaken daardoor dynamiek.

Crises en conflicten worden gekarakteriseerd door een combinatie van historische, politieke, militaire, sociale, culturele en economische aspecten. Om de operatieomgeving gestructureerd in kaart te brengen, kan gebruik gemaakt worden van een analytisch model of raamwerk. Een dergelijk raamwerk is een hulpmiddel dat verschillende aspecten ordent en dat commandanten en (inlichtingen)staven helpt om inzicht in de omgeving te krijgen. Welk raamwerk gebruikt wordt, hangt af van de situatie maar belangrijk is dat alle actoren die gezamenlijk optreden hetzelfde raamwerk gebruiken. Een voorbeeld van een raamwerk is het binnen de NAVO gebruikte PMESII-model<sup>2</sup> dat de omgeving beschrijft aan de hand van de aspecten politiek, militair, economisch, sociaal, infrastructuur en informatie.

Actoren en partijen in het conflict zijn grofweg in te delen in drie groepen. Allereerst de categorie die, in één of andere vorm van samenwerking, bijdraagt aan het bereiken van de strategische doelstellingen. Dan de tweede categorie die ten opzichte van deze doelstellingen een neutrale positie inneemt, maar die zich actief of passief ophoudt in de operatieomgeving. De derde categorie wordt gevormd door de actoren in de operatieomgeving die zich niet kunnen verenigen met de doelstellingen en zich al dan niet gebruik makend van een vorm van geweld verzetten.

<sup>2</sup> Political, Military, Economic, Social, Infrastructural, Informational (environment)

### 1.2.3 Bescherming van inlichtingen

Inlichtingen zijn waardevol en de waarde hangt af van de exclusiviteit. Eigen inlichtingen dienen beschermd te worden. Dit vereist een juiste toepassing van operationele veiligheidsmaatregelen (*Operations Security*; OPSEC<sup>3</sup>) noodzakelijk voor de veiligheid van de operatie. Dit bepaalt ook deels de nationale geloofwaardigheid en betrouwbaarheid binnen een coalitieverband. Het delen van inlichtingen en informatie op een *need-to-know* of *need-to-share* basis kan operationeel noodzakelijk zijn. Hierbij valt ook te denken aan het delen van inlichtingen en informatie met NGO/IO's<sup>4</sup>, lokale overheden en/of het lokale veiligheidsapparaat. Daarbij mag de veiligheid van eigen troepen niet in gevaar worden gebracht en mogen de inlichtingenbronnen niet worden gecompromitteerd. Het delen van inlichtingen en informatie met niet-militaire organisaties stelt speciale eisen aan de wijze waarop we omgaan met OPSEC. Veiligheidsbewustzijn is mede bepalend voor het behoud van de inlichtingenwaarde. Het delen van inlichtingen en beschikbare informatie is aan regels en procedures onderhevig die door iedereen moeten worden nageleefd.

### 1.2.4 Inlichtingencapaciteit

Inlichtingen zijn essentieel voor besluitvorming en uitvoering. De wijze waarop met beschikbare inlichtingen wordt omgegaan, is onder meer bepalend voor de effectiviteit van de geïntegreerde benadering (*comprehensive approach*). Het expeditionair optreden in wisselend samengestelde coalities vereist een eigen inlichtingenstaf en uitgebreide verzamel- en analysecapaciteit. Deze capaciteit omvat onder meer bemande en onbemande sensoren die zijn gekoppeld in een netwerk. Sensoren kunnen opereren in alle dimensies: maritiem, land, lucht, en ruimte.

De snelheid waarmee informatie wordt verwerkt tot inlichtingen is eveneens bepalend voor de snelheid van besluitvorming en daarmee ook voor de effectiviteit van het optreden. Een geïntegreerde netwerkomgeving gebaseerd op robuuste *Information & Communications Technology* (ICT) draagt hieraan bij door snelle verspreiding van inlichtingen en de mogelijkheid om inlichtingen te delen met verschillende niveaus. Hierdoor ontstaat een gemeenschappelijk omgevingsbeeld dat tot op het laagste niveau beschikbaar behoort te zijn. Inlichtingensystemen dienen dan ook inter-operabel te zijn. Een wereldwijde inzet stelt hoge eisen aan de I&V-capaciteit. Het vakgebied kent een veelzijdig specialisme met eisen op tactisch, operationeel, strategisch en ook economisch, cultureel, bestuurlijk, juridisch,

<sup>3</sup> OPSEC: Het proces dat een militaire operatie of oefening voorziet van de passende veiligheid, door passieve of actieve maatregelen toe te passen, hiermee actoren van invloed kennis te ontzeggen over disposities, mogelijkheden en intenties van eigen troepen.

<sup>4</sup> NGO: Non Gouvernementele Organisatie. IO: International Organization

infrastructureel, medisch en linguïstisch vlak. Betrouwbaarheid en vertrouwelijkheid maken dat elementen van de inlichtingencapaciteit niet zonder meer extern te verkrijgen zijn.

Per organisatiedeel en niveau kan het belang van opposanten en actoren variëren. Bovendien kunnen de doelstellingen van commandanten verschillen en zullen de primaire inlichtingenbehoefes op deze niveaus onderling kunnen verschillen. De processen en procedures echter zijn in generieke termen hetzelfde.

Het I&V-personeel op het tactische en operationele niveau moet daarom, naast specifieke I&V-expertise, beschikken over een gedegen kennis van en ervaring met de operationele inzet van de eigen (*joint*) eenheid. I&V-capaciteit zal moeten voorzien in een optimale invulling van de inlichtingenbehoefte van commandanten op de verschillende niveaus.

Voor de inlichtingenondersteuning van operaties, en bij de gereedstelling hiervoor van personeel en materieel, wordt een inlichtingenketen gevormd. De keten heeft als doel om iedere commandant op zijn niveau in de commandovoeringsketen een samenhangend en zo compleet mogelijk beeld te geven van zijn omgeving. Dit wordt mogelijk gemaakt door de samenwerking tussen, de coördinatie en het overleg met alle inlichtingenelementen die deelnemen aan de keten. Dit gebeurt met betrekking tot enerzijds de interpretatie van alle beschikbare informatie en anderzijds de inzet van alle beschikbare verzamel- en verwerkingscapaciteit.

De inlichtingenketen van Defensie wordt gevormd door de MIVD<sup>6</sup> en de inlichtingenstaf van de CDS (DOPS/J2) en de inlichtingenstaven van de operationele commando's, waaronder A2, N2, G2 en S2<sup>7</sup>, eventueel aangevuld met informatieverwerkende componenten van andere (ook niet-militaire) deelnemers aan de operatie.

De MIVD ondersteunt het inlichtingenproces op meerdere niveaus in de keten en is, mede hierdoor, in staat een onafhankelijk oordeel te geven over het omgevingsbeeld.

<sup>5</sup> De inlichtingen- en veiligheidsketen binnen Defensie is de gestructureerde aaneenschakeling van gelijksoortige entiteiten die zich binnen Defensie bezighouden met de productie van inlichtingen.

<sup>6</sup> De MIVD is rechtstreeks onder de SG geplaatst. Hierdoor wordt gegarandeerd dat de MIVD buiten het directe gereedstellingsproces en operationele proces staat en op basis daarvan te allen tijde een volstrekt onafhankelijk oordeel kan geven over het inlichtingenbeeld.

<sup>7</sup> Bij landeenheden gebruikt men de letter G (Ground) als aanduiding voor een stafsectie in een Generale Staf en de letter S (stafsectie) voor een stafsectie in lagere staven; bij maritieme en luchtmachtstrijdkrachten zijn dit respectievelijk de letters N (Naval) en A (Air). De letter J duidt op een joint stafsectie. Het cijfer 2 duidt de functionaliteit inlichtingen aan. Zie verder de JDP-5 Commandovoering.

Dat laat onverlet dat alle inlichtingenstaven, ieder op eigen niveau, verantwoordelijk blijven voor het inlichtingenbeeld dat wordt geschetst ten behoeve van de eigen commandant. Daarom moet elk element in de keten een onafhankelijk oordeel kunnen geven over het omgevingsbeeld in diverse fasen van het besluitvormingsproces.

## 1.3 INLICHTINGENONDERSTEUNING VAN DE OPERATIE

### 1.3.1 Strategisch niveau

Tot deelname aan militaire operaties wordt besloten op politiek-strategisch niveau. Het besluit om het militaire machtsmiddel in te zetten als bijdrage in crisisbeheersing is de exclusieve verantwoordelijkheid van een regering, ongeacht of deze zelfstandig optreedt of handelt in samenwerking met andere regeringen in een veiligheidsorganisatie zoals de VN, in een bondgenootschap zoals de NAVO of in een ad hoc coalitie. De nationale hoofdrolspelers op dit niveau zijn voornamelijk de minister-president en de ministers van Buitenlandse Zaken en Defensie en hun hoogste adviseurs. Op internationaal niveau worden in overleg met coalitiepartners en in samenhang met andere politiek-strategische doelstellingen, de doelstellingen van een militaire operatie bepaald.

In overleg met de andere spelers op het politiek-strategische niveau geeft de minister van Defensie opdracht aan de MIVD om delen van de wereld, vooral de (potentiële) crisisgebieden, te beschouwen en veranderingen hierin tijdig te onderkennen. Deze beschouwing geeft in eerste instantie een voortdurend algemeen inzicht in de bestaande situatie (*General Awareness*; GA<sup>8</sup>). In tweede instantie worden daartoe aangemerkte gebieden specifiek onderzocht, zodat besluitnemers zich voortdurend bewust zijn van het verloop van de gebeurtenissen in de onderzochte gebieden (*Situational Awareness*; SA). De MIVD presenteert deze beschouwing in de vorm van een dreigingsanalyse, die uiteindelijk bij de besluitvorming over een militaire bijdrage wordt meegewogen. In het besluitvormingsproces dat leidt tot een besluit over deelname aan een militaire operatie geeft de Commandant der Strijdkrachten (CDS) een militair advies over de mogelijkheden en haalbaarheid van de militaire bijdrage.

Militaire operaties kunnen zowel in coalitieverband als nationaal worden uitgevoerd. Bij deelname aan militaire operaties in coalitieverband draagt de CDS zorg voor de planning, voorbereiding en gereedstelling van de Nederlandse bijdrage. Op inlichtingengebied resulteert dit onder andere in richtlijnen voor de inrichting van de operationele inlichtingenketen en de training van het operationele inlichtingenpersoneel.

<sup>8</sup> *General en situational awareness* worden later in dit document nauwkeuriger omschreven in het kader van de besluitvorming van de commandant.



Tevens is hij verantwoordelijk voor de nationale ondersteuning van de Nederlandse militairen ingezet bij internationale operaties.

### 1.3.2 Operationeel niveau

Bij deelname in coalitieverband zullen de militair-strategische doelstellingen van de Nederlandse regering ingebed zijn in de geformuleerde militair-strategische doelstellingen van de coalitie. Deze doelstellingen geven de algemene richting aan voor de campagne. De coalitie stelt ten behoeve van de militaire operatie een *Joint Force Commander* (JFC) aan, die op basis van de militair-strategische doelstellingen zijn operationele doelstellingen formuleert. Deze doelstellingen zijn richtinggevend voor de te plannen operaties. Dit planningsproces gebeurt aan de hand van een operationeel besluitvormingsproces, zoals het binnen de NAVO gebruikte *Operational Planning Process* (OPP). Een OPP bestaat uit meerdere fasen, waarbij elke fase zijn specifieke eisen stelt aan de inbreng van inlichtingen<sup>9</sup>.

De inlichtingen die ter ondersteuning van het besluitvormingsproces worden gebruikt, worden verkregen door het uitvoeren van de zogenaamde *Intelligence Preparation of the Environment* (IPE).

Op basis van de inlichtingendocumenten die zijn gebruikt voor het strategische planningsproces wordt de opbouw van GA en SA op operationeel niveau voortgezet.

<sup>9</sup> De werkwijze bij deze inbreng wordt besproken in Hoofdstuk 3, INLICHTINGEN VOOR DE COMMANDOVOERING.

Met behulp van IPE wordt de bestaande situatie van de operatieomgeving verder inzichtelijk gemaakt. IPE zorgt voor detaillering van de relevante factoren van invloed van het terrein, het weer, het klimaat en de PMESII-dimensies. Op basis van deze beschrijving worden hypothesen opgesteld over te verwachten scenario's in de operatieomgeving. In deze scenario's worden naast de mogelijke activiteiten van gewelddadige actoren, de zogenaamde *Enemy Courses of Action* (ECOA), ook de mogelijke activiteiten van andere (niet-gewelddadige) actoren en groeperingen weergegeven.

De NAVO, de EU en de VN vormen de belangrijkste institutionele kaders voor militaire samenwerking. Dit heeft directe invloed op het gezamenlijk (*combined*) uitvoeren van militaire operaties. Het betekent voor inlichtingstaven dat informatie en inlichtingen met meerdere coalitiepartners gedeeld moeten kunnen worden, wat bijdraagt aan de duidelijkheid en de tijdigheid van het inzicht in de diffuse omgeving. Aangezien bij deze staven vaak sprake is van het gebruik en de verwerking van gevoelige informatie, moeten heldere afspraken worden gemaakt en duidelijke procedures worden gevolgd, waarin is vastgelegd welk materiaal met wie gedeeld mag worden en op welke wijze dit kan gebeuren. Dit laatstvergt de nodige zorgvuldigheid, want er zijn naast de hiervoor genoemde verbanden veel verschillende andere relaties (zowel met militaire als niet-militaire organisaties).

Een intensieve samenwerking binnen het inlichtingenproces op verschillende niveaus is om meerdere redenen noodzakelijk. Ten eerste zijn de traditionele tactische, operationele en strategische niveaus van militair optreden steeds meer met elkaar verweven<sup>10</sup>. Ten tweede is het door o.a. technologische ontwikkelingen, meer en meer mogelijk om het inzetgebied in toenemende mate te voorzien van inlichtingondersteuning vanuit Nederland. Ten derde wordt het uitvoeren van militaire operaties gekenmerkt door samenwerking met andere ministeries en organisaties (*interagency*). Om helderheid te creëren is het nodig dat de betrokken partijen van elkaars methodiek(en) op de hoogte zijn om een integrale werkwijze en beoordeling mogelijk te maken. Om deze afstemming internationaal mogelijk te maken, gebruikt Nederland afspraken die in NAVO-verband zijn gemaakt. De in de volgende hoofdstukken beschreven definities, processen en werkwijzen zijn daarop gebaseerd.

### 1.3.3 Nationale operaties

Onder nationale operaties<sup>11</sup> vallen alle militaire operaties onder Nederlands bevel of gezag. Dit betreft zowel internationale inzet onder nationaal bevel (zoals *Non-Combatant Evacuation Operations* of humanitaire hulpverlening) als nationale inzet in het kader van bijstand en

<sup>10</sup> Zie ook paragraaf 1.3.4: De Inlichtingenketen.

<sup>11</sup> Nationale operaties zijn niet voorbehouden aan het nationale grondgebied. (JDP-5)

steunverlening al dan niet op Nederlands grondgebied. Deze twee soorten operaties verschillen in aansturing (commandovoering) en zijn volledig gescheiden wat betreft de juridische basis, toepasselijk recht en operationele concepten. De grondslag voor de internationale inzet onder nationaal bevel is de Grondwet, waarbij de aansturing plaats vindt door de CDS onder gezag van de Minister van Defensie. De grondslag voor de nationale inzet in het kader van bijstand en steunverlening is de Defensienota en de Nederlandse wet, waarbij de aansturing gebeurt door de CDS onder gezag van de civiele autoriteiten. Hoewel de juridische basis voor de inzet van het militaire instrument bij nationale operaties anders is, zijn de algemene grondslagen, principes en uitgangspunten voor de inlichtingenondersteuning van nationale operaties in beginsel gelijk aan operaties in internationaal verband.



In het geval van inzet in het kader van bijstand en steunverlening kan de samenstelling van de commandovoeringlijn een voornamelijk civiel karakter dragen en andere procedures kennen. Zo zal op nationaal grondgebied de militaire component onder gezag van de civiele autoriteiten optreden. De commandant zal in dat geval zijn *Command and Control (C2)*-proces moeten aanpassen aan de procedures van het hem sturende element, ook op het gebied van inlichtingen. Bij onduidelijkheid over deze procedures kan de militaire commandant in zijn organieke lijn om nadere richtlijnen vragen.

In het geval van een militaire operatie onder nationaal bevel blijven, tenzij anders wordt aangegeven, de normale structuren van toepassing.

Het op nationaal grondgebied gericht verzamelen van informatie is op grond van de Wet Inlichtingen en Veiligheid-2002 (Wiv 2002) enkel voorbehouden aan de Algemene Inlichtingen en Veiligheidsdienst (AIVD) en MIVD<sup>12</sup>. Voor de uitvoering van de eigen taak op het technische niveau is het militaire commandanten wel toegestaan om algemene informatie te verzamelen.

### 1.3.4 De inlichtingenketen

Iedere commandant is op zijn niveau verantwoordelijk voor het behalen van de hem opgedragen doelen. Voor de inlichtingenondersteuning van de operatie beschikt de commandant vanaf een bepaald niveau over een inlichtingenstaf<sup>13</sup>. Deze staf zorgt ervoor dat de commandant tijdig over de voor hem noodzakelijke inlichtingen beschikt. De inlichtingenstaf kan niet in alle gevallen met de beschikbare middelen aan de benodigde informatie komen. Soms doordat de bron voor dit niveau niet toegankelijk is, soms doordat de informatie in het toegewezen gebied van inlichtingenverantwoordelijkheid (*Area of Intelligence Responsibility*; AIR) niet verkrijgbaar is. In dat geval wordt uitgezocht of de benodigde informatie beschikbaar is bij of verkregen kan worden door inlichtingenstaven van de andere niveaus. Deze mogelijkheid ontstaat door gebruik te maken van de inlichtingenketen.

<sup>12</sup> Er is geen eigen bevoegdheid tot de inzet van inlichtingenmiddelen op Nederlands grondgebied door de overige I&V-capaciteit. De Wiv 2002 voorziet alleen in bevoegdheden voor de AIVD en MIVD. In voorkomend geval is voorzien in een strafuitsluitingsgrond voor de AIVD en MIVD van bepaalde in het Wetboek van Strafrecht opgenomen verboden (zie artikel 139b en 139c Wetboek van Strafrecht). Inzet middelen overige I&V-capaciteit nationaal is alleen mogelijk in geval van militaire bijstand ingevolge de Politiewet 1993. Dan geschiedt de inzet op basis van de bevoegdheid (en onder verantwoordelijkheid) van de verzoekende instantie.

<sup>13</sup> Waar in dit document wordt gesproken over een inlichtingenstaf, omvat deze term alle organisatievormen die de staffunctionaliteit inlichtingen van een commandant kunnen vormen, zoals inlichtingensectie, -afdeling, -dienst, -officier.

De inlichtingenketen loopt parallel aan de operationele lijn en wordt gevormd door de verbinding tussen alle inlichtingstaven binnen de coalitie in combinatie met nationale inlichtingstaven. De inlichtingenketen kan ten behoeve van operaties worden uitgebreid en op maat gemaakt met andere instanties die beschikken over de gewenste informatie. Door gebruik te maken van deze keten kunnen de inlichtingstaven onderling informatie en inlichtingen uitwisselen, de inzet van verzamelorganen en het beheer en het gebruik van bronnen coördineren, en onderlinge ondersteuning bieden bij verwerkingsactiviteiten<sup>14</sup>.

De op een bepaald niveau verkregen en beschikbare informatie kan voor meerdere niveaus van belang zijn. Een inlichtingenketen biedt inlichtingstaven de mogelijkheid dat de vereiste informatie voor die niveaus beschikbaar is. Het onderscheid tussen strategische, operationele en tactische niveaus vervaagt, omdat op het tactische niveau verkregen informatie ook strategisch van belang kan zijn en omgekeerd. Daarom loopt de keten op alle niveaus door de inlichtingstaven, vanaf het hoogste niveau naar het laagste niveau en terug. De MIVD ondersteunt hierbij op meerdere niveaus in de keten. Daardoor kan men, met inachtneming van veiligheids- en rubriceringsbeperkingen, optimaal inzicht verkrijgen in elkaars (gevalideerde) informatie, geanalyseerde inlichtingen en in de locaties en de (toekomstige) taken van de verzamelorganen. Hierdoor kan de totale beschikbare inlichtingencapaciteit efficiënt worden ingezet en ontstaat een kwalitatief beter beeld van de operatieomgeving. Immers, binnen de keten kunnen de onderzoeken en conclusies van de hogere niveaus dienen voor de GA en SA van de lagere niveaus, terwijl de onderzoeken en conclusies van de lagere niveaus verdichting en verscherping creëren in het beeld dat de hogere niveaus hebben van hun omgeving.

Als het vanwege de genoemde veiligheids- en rubriceringsbeperkingen onmogelijk is om rechtstreeks toegang te krijgen tot andere dan de eigen informatie, moet een liaison(organisatie) worden opgezet. Deze liaisonfunctie zorgt ervoor dat informatie beschikbaar kan worden gesteld aan de verzoekende commandant. Als de Nederlandse belangen tijdens een operatie groot zijn, kan deze liaisonfunctie zelfs de aard krijgen van concrete ondersteuning van de operationele eenheid door een op maat samengesteld element, voorzien van verzamel- en verwerkingscapaciteit van het strategische niveau ten behoeve van het operationele niveau.

<sup>14</sup> Een beleidsmatige rol voor de inrichting en het goed laten functioneren van de inlichtingenketen is weggelegd voor de Defensie Inlichtingen en Veiligheidsraad (DIVR). De DIVR coördineert de samenhang tussen de inlichtingencapaciteiten ter voorbereiding op eventuele formele besluitvorming binnen de Bestuursstaf. De Raad behandelt, onder voorzitterschap van de Secretaris Generaal, op hoofdlijnen de werking en sturing en de transities binnen de I&V-keten, het afstemmen van prioriteiten bij de inzet van schaarse I&V-capaciteit en de personele en materiële ontwikkelingen, waaronder ontwikkelingen ten aanzien van het verbeteren van de kwaliteit van het personeel en het ondersteunende materieel.

Dit wordt gedaan in de vorm van een *National Intelligence Support Team* (NIST<sup>15</sup>) van de MIVD. Indien rechtstreekse toegang tot elkaars informatie niet mogelijk is, of indien de informatie als zodanig niet voorhanden is, kunnen gerichte vragen worden gesteld in de keten door middel van *Requests For Information* (RFI). Voor een ander niveau is het moeilijk in te schatten wat beoogd wordt met de gevraagde informatie. Hierdoor ontstaat het risico onvolledige of niet ter zake doende informatie toegezonden te krijgen. Daarom is het essentieel dat de gevraagde informatie nauwkeurig wordt omschreven. Verder moet de reden voor de RFI gegeven worden, ook ter beoordeling van de importantie en de prioriteit waarmee deze in behandeling moet worden genomen.

De commandant baseert zijn plannen en besluiten voor een groot deel op de hem ter beschikking staande kennis van, en inzichten in de (operationele) omgeving. Naast feiten vormt de beschrijving van hypothesen en scenario's hierbij een belangrijke bijdrage. De opdrachten aan de ondercommandanten komen voort uit het beeld en begrip dat de hogere commandant heeft van *zijn* omgeving.

Om frictie in de operationele lijn te voorkomen, moeten lagere inlichtingstaven er voor zorgen dat de voor hun niveau en door hen ontwikkelde inlichtingenoperatie past binnen de beschouwing van het hogere niveau. Een uitgangspunt in de ketenbenadering is dus dat inlichtingendocumentatie en conclusies van het hogere niveau richtinggevend zijn voor onderzoeks-, verzamel- en verwerkingsactiviteiten op het lagere niveau. De commandant weegt dit, en de inlichtingenbehoefte van zijn ondercommandanten, mee bij zijn besluit over de inzet van zijn inlichtingencapaciteit. Een gegeven richting van het hogere inlichtingenniveau mag echter niet leiden tot een beperkte beschouwing van de omgeving. De omstandigheden kunnen plaatselijk en tijdelijk belangrijk afwijken van het algemene beeld van het hogere niveau. Dat dwingt de inlichtingstaf, op ieder niveau, tot een kritische beschouwing, om de eigen commandant juist geïnformeerd te houden. Voortdurende terugkoppeling in de keten is noodzakelijk.

Commandanten krijgen voor de uitvoering van militaire operaties een gebied van verantwoordelijkheid toegewezen (*Area of Operational Responsibility*, AOR). De AOR is meestal een geografisch of thematisch afgebakend onderdeel van het operatiegebied van de hogere commandant. Dit heeft tot gevolg dat ook de AIR van de verschillende niveaus deels samenvallen. Hierdoor treden verzamelorganen van verschillende niveaus met hun

<sup>15</sup> De primaire taak van het NIST is het leveren van inlichtingenondersteuning aan de commandant (en staf) van de uitgezonden eenheid. Als secundaire taak dient het verzamelen van informatie ten behoeve van het opbouwen en toetsen van het normbeeld ten aanzien van specifieke operatiegebieden door de MIVD.



sensoren op in hetzelfde geografische gebied en worden informatieopslag- en analyseactiviteiten mogelijk uitgevoerd over dezelfde thema's. Binnen de inlichtingenketen is dus coördinatie vereist op het gebied van het verzamelplan, de inzet van verzamelorganen en bronbeheer.

## 1.4 JURIDISCH KADER

Bij de inzet van inlichtingencapaciteit moet vooraf de juridische context worden gedefinieerd waarbinnen deze inzet kan plaatsvinden. Relevante regelgeving voor het verzamelen van informatie bestaat onder andere uit de Wet op de inlichtingen- en veiligheidsdiensten 2002, het Nederlands strafrecht en het op de militaire operatie van toepassing zijnde internationale juridische kader, dat kan bestaan uit:

- het mandaat, al dan niet neergelegd in een VN Veiligheidsraadresolutie;
- toepasselijke verdragen, waaronder mensenrechtenverdragen, het VN Zeerechtverdrag en verdragen van het Humanitair Oorlogsrecht (HOR)<sup>16</sup>;
- *Rules of Engagement* (ROE).

<sup>16</sup> Formeel is het HOR alleen van toepassing tijdens een gewapend conflict. Ook wanneer het HOR niet van toepassing is, is het beleid van Nederland (en de NAVO) om de beperkingen uit het HOR te hanteren als veilige marge bij het optreden van de Nederlandse krijgsmacht.

Specifieke aanwijzingen aan commandanten voor het inzetten van middelen en het aanwenden van bevoegdheden worden vaak in de vorm van ROE gegoten. Voor het inzetten van inlichtingmiddelen en het aanwenden van daaraan gerelateerde bevoegdheden zijn ROE echter minder geschikt, vanwege de doctrine, systematiek en doelstelling van ROE. Wel kunnen en zullen hiervoor specifieke aanwijzingen en richtlijnen worden uitgevaardigd die, net als ROE dat doen voor geweld en aanverwante zaken, operationele instructies bevatten voor de commandant in dit kader. Door dergelijke aanwijzingen net als ROE door de CDS te laten vaststellen, kunnen zij eveneens dezelfde status binnen het militaire straf- en tuchtrecht verkrijgen als voor ROE het geval is.

Het juridisch aspect speelt ook een rol bij de uitwisseling van gerubriceerde inlichtingen of informatie door de operationele commandant.

## 1.5 BESCHERMING VAN MILITAIR VERMOGEN

Bescherming betreft alle maatregelen en middelen die er op gericht zijn om het effect van bedreigingen tegen het eigen militair vermogen en optreden te voorkomen en/of te minimaliseren. Door bescherming, onder andere door maatregelen in het kader van operationele veiligheid (*operations security*-OPSEC) behoudt men de eigen vrijheid van handelen en de operationele effectiviteit. Hierdoor blijft een succesvolle uitvoering van de opdracht mogelijk. De bescherming van het eigen militair vermogen gebeurt onder andere door het gebruik van actieve en passieve maatregelen die vijandige actoren informatie over disposities, mogelijkheden en intenties van de eigen troepen ontzeggen.

Beveiligingsmaatregelen worden ook genomen om te voorkomen dat anderen inzicht krijgen in de wijze waarop wij informatie hebben verkregen. Dit om onze capaciteiten, maar ook om de bron waaruit deze informatie voortkomt, te beschermen. Het Defensie Beveiligings Beleid (DBB) beschrijft de maatregelen die moeten worden genomen om informatie te beschermen. Deze maatregelen dienen met zorg te worden toegepast. Een te lage beveiligingsgraad levert het gevaar op van compromittatie. Maar een te hoge beveiligingsgraad veroorzaakt het gevaar dat de gebruiker niet kan beschikken over de voor hem noodzakelijke informatie.

Er zal een balans gevonden moeten worden tussen de bescherming en de beschikbaarheid van informatie. Het delen van relevante informatie tussen de betrokken partijen (militair en niet-militair), is essentieel voor *situational awareness* en een gemeenschappelijk begrip. Bescherming, maar ook het niet willen delen van de informatie (informatie is macht) kunnen de toegang tot informatie beperken. Hoewel er altijd omstandigheden zullen zijn die het delen van informatie niet toestaan, dient de *wil* om te delen centraal te staan. Beveiliging van informatie moet zich richten op de wijze waarop informatie kan worden gewaarborgd zonder de effectiviteit van de ondersteuning aan te tasten. Daarbij vormt

risicomangement een integraal onderdeel van informatiebeveiliging. De uitdaging ligt hierbij in het vinden van (technische) oplossingen die betaalbaar en werkbaar zijn, met een voor de organisatie acceptabel risico.

De inlichtingenstaf is ervoor verantwoordelijk dat inlichtingen beschikbaar worden gesteld aan de gebruikers. Dit kan door daar waar nodig de producten zodanig te ontdoen van informatie, dat een hoge rubricering niet meer vereist is (*sanitization*). Ook kan rubricering vaak van tijdelijke aard zijn omdat de informatie een in tijd beperkte waarde heeft. Voor het beschikbaar stellen van gerubriceerde informatie is toestemming van de steller nodig.

### 1.5.1 Operationele veiligheid

Actoren in de operatieomgeving trachten informatie te verkrijgen over onze (geplande) operatie(s) of acties en over onze wijze van optreden. Om dit te voorkomen wordt OPSEC toegepast.

In het OPSEC-proces wordt eerst vastgesteld welke informatie de actoren inzicht kan verschaffen over onze operatie en ons optreden. Vervolgens wordt vastgesteld welke actoren gebruik zouden kunnen maken van deze informatie, op welke wijze zij dit kunnen doen en welke middelen zij hiervoor gebruiken. Dan wordt bezien welke elementen van een geplande operatie of actie belangrijke informatie kunnen tonen of vrij kunnen geven, de zogenaamde OPSEC-indicatoren. Van deze OPSEC-indicatoren wordt onderzocht of zij door de vastgestelde actoren kunnen worden onderkend. Daarbij moet er rekening mee worden gehouden dat het onderkennen van de OPSEC-indicatoren niet alleen gebeurt door directe waarneming, maar ook door analyse. Bij deze stap worden de kwetsbaarheden bepaald. Met dit resultaat wordt vastgesteld welke OPSEC-maatregelen nodig zijn om de vastgestelde kwetsbaarheden te neutraliseren. Vervolgens wordt een risicoanalyse uitgevoerd om te kunnen bepalen welke OPSEC-maatregelen moeten worden geïmplementeerd. Deze maatregelen worden vastgelegd in een OPSEC-plan.

Het OPSEC-proces wordt tijdens de oordeelvorming door de gehele staf uitgevoerd en wordt voor iedere planmogelijkheid uitgewerkt. De bijdrage van de inlichtingenstaf aan het OPSEC-proces en -plan bestaat vooral uit het uitvoeren van de stap waarin wordt vastgesteld welke actoren belang hebben bij het verkrijgen van de informatie en de wijze waarop en de middelen waarmee zij dit kunnen doen. Op basis van de hierbij verkregen informatie ontwikkelt de inlichtingenstaf scenario's die worden gebruikt bij het onderzoek naar de door de actoren te onderkennen OPSEC-indicatoren.

### 1.5.2 Contra-Inlichtingen en Veiligheid(CI&V)

De dreiging tegen defensiepersoneel, - middelen en - activiteiten<sup>17</sup> die veroorzaakt wordt door spionage, sabotage, subversie en terrorisme (afgekort tot SSST)<sup>18</sup> valt onder Contra-Inlichtingen. De maatregelen die nodig zijn om de door CI gedefinieerde dreiging het hoofd te bieden, vormen het aspect Veiligheid (V). In het verleden ging deze dreiging voornamelijk uit van (potentieel) vijandelijke inlichtingen- en veiligheidsdiensten, die tevens als taak hadden zoveel mogelijk inlichtingen over bondgenootschappelijke en Nederlandse territoriale kwetsbaarheden in kaart te brengen. Hierdoor werd deze dreiging, waaronder industriële spionage, het werkveld van de CI. Door de toegenomen belangstelling voor andere potentiële veroorzakers van de SSST-dreiging, is het werkkerrein van CI&V uitgebreid. De dreiging komt niet alleen meer van buitenlandse inlichtingen- en veiligheidsdiensten, maar komt ook van andere - niet noodzakelijk staatsgebonden - organisaties.

## 1.6 INFORMATIETECHNOLOGIE

De hoeveelheid informatie die beschikbaar is en wordt verzameld in hedendaagse operaties is groot. Dit is enerzijds het gevolg van een veel bredere dan alleen maar vijand gerichte oriëntatie, maar anderzijds ook het gevolg van de toepassing van nieuwe informatie- en communicatietechnologieën (ICT). Goede ICT ondersteuning is essentieel in het inlichtingssysteem. De veelheid aan informatie moet namelijk worden opgeslagen, geordend, verwerkt en verspreid. Daarnaast is het tempo waarmee deze activiteiten worden uitgevoerd hoog. Een goede ordening is van wezenlijk belang om de noodzakelijke informatie te kunnen terugvinden en bij elkaar te brengen daar waar nodig. Voor alle inlichtingen geldt dat kleine puzzelstukjes bij elkaar een plaatje maken waarmee commandanten en eenheden in staat worden gesteld voldoende *situational awareness* op te bouwen om de activiteiten daarop af te stemmen. Het is daarom cruciaal om de juiste informatie te kunnen terugvinden als het nodig is.

Het gebruik van ICT ondersteunt de inlichtingenstaf tijdens het bepalen en uitwerken van de inlichtingenbehoefte door: (1) het vaststellen van de al beschikbare informatie, (2) geautomatiseerde verwerking bij de presentatie van bekende informatie uit de operatie-

<sup>17</sup> Onder activiteiten worden niet alleen militaire operaties verstaan, maar ook oefeningen, havenbezoeken, strategisch transport, etc.

<sup>18</sup> In sommige discussies binnen de NAVO wordt de dreiging soms uitgebreid met "Georganiseerde Misdad (*Organized Crime*)" waardoor het acroniem TESSOC (*Terror, Espionage, Sabotage, Subversion and Organized Crime*) ontstaat. Georganiseerde misdaad speelt als (f)actor van invloed in het gehele spectrum van de operatieomgeving en moet daarom integraal beschouwd worden.



omgeving, (3) het opbouwen van scenario's en hypotheses door modellering en simulatie en (4) het coördineren van de werkzaamheden die voortvloeien uit het synchroniseren van het verzamelpaan.

Gedurende het verzamelen is ondersteuning door informatietechnologie nodig bij de opslag en voorbewerking van sensorinformatie tot antwoorden op vragen uit het *Intelligence Collection Plan* (ICP; zie 3.3.4) en bij de snelle overdracht van de daaruit gegenereerde informatie aan de inlichtingenstaf. Applicaties voor statistische verwerking van omvangrijke datasets en niet-tekstuele informatie zijn daarbij een waardevol instrument.

De ondersteuning van de verwerkingsfase door informatietechnologie bestaat uit het bieden van snelle en accurate opslag- en terugzoekmogelijkheden, het vaststellen van de waardering bij evaluatiecriteria, informatievergelijking en -selectie, hypothesetoetsing en -opbouw en uit de vergelijking hiervan.

Inlichtingenproducten bestaan vaak uit visuele of grafische presentaties. ICT ondersteuning biedt de mogelijkheden om informatie en inlichtingen toegankelijk te maken en te delen tussen eenheden maar ook tussen verschillende niveaus. Eenheden en staven die beschikking hebben over het betreffende inlichtingensysteem, kunnen toegang hebben tot, of kunnen kennis nemen van, elkaars inlichtingen.

De beschikbaarheid van informatie op verschillende niveaus draagt bij aan een betere gezamenlijke *situational awareness*. Verder kan door ICT ondersteuning informatie snel verspreid worden naar gebruikers. Dit vereist echter adequate datatransmissiecapaciteit. Omdat informatie binnen de operationele eenheid en met andere partijen moet worden uitgewisseld, is een grote mate van standaardisatie van de gebruikte systemen met voldoende capaciteit vereist.

ICT ondersteuning is noodzakelijk en biedt vele mogelijkheden om het inlichtingenproces te ondersteunen. De sleutel van goede benutting daarvan ligt in de menselijke factor. De omvang en de complexiteit van de informatiestromen binnen de informatievoorziening (IV) van een inlichtingenorganisatie en de staven, vereisen informatiemanagement (IM). Binnen de inlichtingenketen, staven en eenheden dienen hierover afspraken te worden gemaakt en gebruikers en bedieners van systemen dienen voortdurend oog te houden voor de juiste toepassing van informatiemanagement. Dit moet geborgd zijn om te voorkomen dat in de veelheid aan informatie de inlichtingenwaarde verloren gaat.

Daarnaast is van belang te realiseren dat het ook altijd de menselijke analysecapaciteit is die moet maken dat informatie inlichtingenwaarde kan krijgen. ICT systemen zullen nooit kunnen voorzien in de interpretatie en analyse die nodig is om te komen van informatie tot inlichtingen. ICT ondersteuning is noodzakelijk voor opslag, ordening en verwerking van grote hoeveelheden informatie en inlichtingen, maar succesvolle toepassing is afhankelijk van door mensen uitgevoerde informatiemanagement en analyse.

## 1.7 ACTUELE ONTWIKKELINGEN

De komende decennia kunnen worden gekenmerkt als een periode van fundamentele onzekerheid. Onderzoek toont aan dat Nederland in het algemeen en de krijgsmacht in het bijzonder zullen worden geconfronteerd met een groot aantal trends en ontwikkelingen die van invloed kunnen zijn op de veiligheidssituatie. De invloed die dit kan hebben op het functiegebied I&V wordt hieronder beschreven bij "operationele ontwikkelingen". De resultaten van onderzoek worden ondersteund door waarnemingen en recente ontwikkelingen in het functiegebied I&V. De ontwikkelingen zijn ingezet naar aanleiding van de lessen die zijn opgedaan tijdens de expeditionaire inzet van de krijgsmacht.

### 1.7.1 Operationele ontwikkelingen

De fundamenteel onzekere omgeving heeft zijn invloed op de uitvoering van militaire operaties. Anticipatie neemt aan belang toe. Anticiperen op de dynamiek vraagt van de commandant inzicht in de omgeving. Het functiegebied I&V wint aan belang. De mogelijke operaties en taken die voortvloeien uit de anticipatiefunctie zijn verkenningsoperaties,



informatie verzamelen, analyse van informatie, scenario-ontwikkeling en -analyse en informatieoperaties<sup>19</sup>.

### 1.7.2 Bedreigingen

De bedreigingen die zich in verschillende denkbare scenario's voordoen, zijn sociale onrust, georganiseerde criminaliteit en terroristische activiteiten, fenomenen die voornamelijk plaatsvinden in een grotendeels geurbaniseerde omgeving. Een grootschalig symmetrisch militair optreden is alleen te verwachten in een scenario waarin de mondiale samenleving zich ontwikkelt tot een multipolaire omgeving, waarin verschillende machtsblokken tot stand komen. Het gebruik van nucleaire massavernietigingswapens, maar ook het gebruik van biologische en chemische wapens zal vooral zichtbaar zijn als terroristisch instrument<sup>20</sup>.



<sup>19</sup> Eindrapport project Verkenningen.

<sup>20</sup> Resolutie 1540 Veiligheidsraad, het *Proliferation Security Initiative*, het *Global Threat Reduction Initiative*, diverse Clingendael publicaties en Tussenrapport project Verkenningen, versie V1.0.0 dd 03 juni 2009

Deze bedreigingen rechtvaardigen een verschuiving in aandacht, zeker voor het functiegebied I&V, naar een meer *People-Centric*<sup>21</sup> benadering. Dit betekent ook een gedegen inzicht in doelstellingen, werkwijze en middelen van opposenten en *Non-State Actors* (NSA). Mogelijke wijzigingen in modus operandi van opposenten moeten blijvend gevolgd worden. Wijzigingen kunnen zich voordoen als opposenten gebruikmaken van de nieuwste ontwikkelingen op technologisch gebied.

### 1.7.3 Kwaliteiten

Om met een *People-Centric* benadering inzicht te hebben in een fundamenteel onzekere omgeving en tijdig over relevante inlichtingen en informatie te beschikken, is een voortdurend contact met en kennis over de bevolking noodzakelijk. Daarvoor dient de krijgsmacht te beschikken over capaciteiten voor algemene *overt Human Intelligence* (HUMINT) (zie hoofdstuk 2, paragraaf 2.6.1), relevante taalkennis, kennis over cultureel-antropologische



<sup>21</sup> *People centric* benadering: Het doel van de militaire bijdrage binnen de *Comprehensive Approach* is het creëren van een veilige omgeving, waarbinnen de andere processen van staatsvorming kunnen plaatsvinden. Staatsvorming heeft alleen een kans van slagen als de bevolking hiermee een aantrekkelijk alternatief wordt geboden. Dit plaatst de bevolking centraal in de operatie.

achtergronden en historische kenmerken en specifieke kwaliteiten op het gebied van andere HUMINT-technieken met speciaal hiertoe opgeleid personeel. Bij deze laatste categorie kwaliteiten wordt onderscheid gemaakt tussen ondervraagactiviteiten, het omgaan met bronnen en algemene communicatietechnieken. Om snel en adequaat te kunnen reageren op kansen en bedreigingen zijn alle bekwaamheden nodig tot op een zo laag mogelijk niveau.

#### 1.7.4 Middelen

Om het omgevingsbewustzijn van commandanten, staven en eenheden voortdurend op peil te houden, is een continue inlichtingenoperatie noodzakelijk. De uitvoering van deze operatie in een complexe en dynamische omgeving vereist een juiste mix aan technologisch hoogwaardige en menselijke sensoren, een snelle en robuuste technologische opslag- en verwerkingscapaciteit en een breed spectrum aan analysecapaciteiten. Voldoende voortzettingsvermogen en instandhoudingscapaciteit dienen beschikbaar te zijn om inzet langdurig te kunnen ondersteunen.

#### 1.7.5 Samenwerking

Om de effectiviteit van de militaire operatie en de (technologische) onderzoeken, ontwikkelingen en toepassingen te optimaliseren is samenwerking in de breedste zin van het woord een uitgangspunt. Om dit te bewerkstelligen is de samenwerking binnen de krijgsmacht tussen de krijgsmachtdelen (*joint*) en tussen de krijgsmachten binnen coalities (*combined*) vanzelfsprekend en wordt samenwerking met andere organisaties (*interagency*) en het bedrijfsleven verbeterd. Hiervoor worden betrouwbare en veilige procedures afgesproken.

#### 1.7.6 Opleiding en training

Optimale benutting van kansen en het onderkennen en weerstaan van bedreigingen in een fundamenteel onzekere omgeving vergen een gedegen voorbereiding op de operatie. Hiervoor moet een gefundeerd opleidings- en trainingsmodel worden opgezet. Dit model bevat, door modellering en simulatie gebouwde, opgestelde hypothesen en scenario's over de complexe omgeving met zijn actoren.

#### 1.7.7 Processen en procedures

De in het functiegebied I&V bekende en geldende processen en procedures hebben al gedurende lange tijd hun waarde bewezen. Diverse werkwijzen zijn op grond van militaire ontwikkelingen aangepast aan de eisen van de tijd. De toegepaste technieken worden voortdurend op hun waarde en bruikbaarheid getoetst aan de zich openbarende werkelijkheid. Naast recentelijk geïntroduceerde technieken zoals *Sensitive Site Exploitation*, *Weapon*

*Intelligence Teams*, forensische technieken, DNA-technieken en documentatie-exploitatietechnieken, worden nieuwe onderzoeks- en analysetechnieken ontwikkeld en worden de waardevolle bestaande technieken van partners of civiele instanties op hun bruikbaarheid onderzocht.

## 1.8 SAMENVATTING

Het doel van inlichtingen is de ondersteuning van commandanten op ieder niveau bij hun beeldvorming, oordeelvorming en besluitvorming over de omgeving waarin zij effecten beogen te bereiken met de inzet van de hen ter beschikking staande middelen. Inlichtingen beschrijven hiervoor alle actoren en factoren die in deze omgeving een rol spelen, in onderlinge samenhang. De inlichtingenondersteuning vindt vaak plaats in (internationale) samenwerkingsverbanden.

Militaire operaties worden uitgevoerd in een zeer complexe omgeving. Dit stelt hoge eisen aan de duidelijkheid en tijdigheid van het te schetsen beeld van de omgeving en het hiervan afgeleide dreigingsbeeld. Dit heeft zijn effect op de wijze waarop de militaire operaties moeten worden ondersteund met inlichtingen.

Een goed functionerend inlichtingenproces en deugdelijke procedures, zoals de inlichtingencyclus (IC) en de inlichtingenvoorbereiding van de operationele omgeving, uitgevoerd door een overzichtelijke en effectieve inlichtingenorganisatie, maken de ondersteuning mogelijk. Het vaststellen en het beschrijven van een aantal specifieke kenmerken van de dreiging (spionage, sabotage, subversie en terrorisme en georganiseerde misdaad) en de hierbij behorende tegenmaatregelen, zijn de verantwoordelijkheid van Contra-Inlichtingen en Veiligheid. De uitvoering van het gehele proces is gebaat bij een duidelijkheid verschaffend juridisch kader.

## 2 BEGRIPSVORMING INLICHTINGEN EN VEILIGHEID

### 2.1 Inleiding

Doordat de werkzaamheden binnen het functiegebied I&V veelvuldig plaatsvinden in een *joint, combined* en/of *interagency* omgeving en zelfs in samenwerking met private organisaties, is het van belang om binnen deze mogelijke samenwerkingsverbanden eenheid van opvatting over de gebruikte terminologie te creëren. Voordat wordt ingegaan op inhoudelijke processen en procedures wordt daarom in dit hoofdstuk aandacht besteed aan de definitie van inlichtingen (met daarbij de beschrijving van het domein van inlichtingen), het verschil tussen informatie en inlichtingen, een aantal grondbeginselen, eigenschappen, basisprincipes en de gebruikte terminologie.

### 2.2 DEFINITIES

#### 2.2.1 Definitie van inlichtingen

Ten behoeve van de duidelijkheid over het huidige en toekomstige werkgebied van inlichtingen is het geboden om het gebied te definiëren en inzicht te verschaffen in het domein van dit werkgebied<sup>22</sup>. Als basis hiervoor dient de definitie, beschreven in de AAP-6. Uit zorgvuldigheid en gemakshalve wordt hier de definitie uit het NAVO-document letterlijk weergegeven, waarna de betekenis ervan voor het werkgebied wordt omschreven: Intelligence is “*The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity.*”

Het begrip inlichtingen kent in het militaire taalgebruik drie betekenissen. Het begrip wordt ten eerste toegepast op het proces, dat van een behoefte aan kennis tot het product leidt en als resultaat voorziet in deze behoefte, ten tweede op het product zelf, en ten derde op het organisatie-element dat dit proces uitvoert en zorg draagt voor het genoemde product.

Het is goed om te realiseren dat niet-militaire actoren mogelijk een andere begripsomschrijving van inlichtingen kunnen hanteren en dat bij samenwerking met hen de eventueel verschillende definities op elkaar worden afgestemd.

In het dagelijks taalgebruik worden de termen data, gegevens, informatie en inlichtingen vaak door elkaar gebruikt.

<sup>22</sup> Als gevolg van de omstandigheden en omgevingsfactoren waaronder operaties worden uitgevoerd is discussie ontstaan over het werkgebied dat onder verantwoordelijkheid van de staffunctionaliteit inlichtingen valt. De hier aangegeven beschrijving is geheel gebaseerd op de NAVO definitie en dient als richtlijn voor het uitvoeren van inlichtingenactiviteiten.



Op nationaal niveau stelt de Wiv-2002 strikte voorwaarden en ook binnen de NAVO werken de partners, binnen de militaire context, met afgebakende betekenissen.

Data en gegevens vormen niet meer dan rudimentaire informatiebouwstenen en bestaan meestal uit eenvoudige feiten en statistieken. Door aan data betekenis toe te kennen en ze te plaatsen in een bepaalde context, wat gedaan kan worden door de mens of door een geautomatiseerd systeem, ontstaat informatie. Door de data en informatie in relatie te brengen met de actoren en factoren die van invloed zijn (op de uitvoering van een opdracht) in een specifieke operationele omgeving, ontstaan inlichtingen.

De eerder genoemde definitie van inlichtingen benoemt ook de reikwijdte van het werkteerrein van (militaire) inlichtingen. Het werkteerrein omvat vreemde mogendheden, vijandige of in aanleg vijandige strijdkrachten of elementen en gebieden waarin (mogelijk) operaties plaats (gaan) vinden. De afbakening van het fenomeen “vreemde mogendheden” gebeurt op politiek-strategisch niveau door nationale besluitvorming (zie paragraaf 1.3.1) evenals wat (in aanleg) vijandige strijdkrachten en (potentiële) operatiegebieden zijn. Vijandige elementen (personen, groeperingen, organisaties) laten zich minder eenvoudig op strategisch niveau definiëren en kunnen vaak pas worden herleid en nauwkeurig beschreven als het operatiegebied al is vastgesteld.

Wereldwijd opererende vijandige elementen zijn vaak niet gebonden aan een specifiek geografisch grondgebied. Ze worden daarom eerder thematisch benaderd. Een diepgaand begrip van vijandige strijdkrachten of elementen is alleen goed mogelijk als hun doelstellingen, bestaansredenen, mogelijke doctrine en werkwijzen in de context geplaatst worden van andere actoren en factoren in hun omgeving. Dit vergt een gedegen inzicht in deze actoren en factoren<sup>23</sup>.

### 2.2.2 Definitie van Contra-Inlichtingen en Veiligheid

Ook voor de afbakening van het werkveld van Contra-Inlichtingen is een definitie van kracht. De definitie<sup>24</sup> luidt:

*Counter-Intelligence are “Those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in espionage, sabotage, subversion or terrorism.”* De definitie omvat de activiteiten van de Contra-Inlichtingen- en Veiligheidsfuncties (zie 1.5.2).

### 2.2.3 Definitie van Veiligheid

Binnen het werkkterrein CI&V wordt de term “veiligheid” met regelmaat gebruikt. Het begrip dient echter in zijn context te worden beschouwd. Daarvoor zijn drie definities<sup>25</sup> van kracht die ieder een ander perspectief van het begrip belichten. De eerste definieert veiligheid als toestand, de tweede als geheel aan maatregelen en de derde als organisatievorm. Deze drie bestaansvormen van veiligheid worden in sectie 4.3 verder besproken.

Security is “*the condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorized disclosure.*”

Security is “*the measures necessary to achieve protection against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorized disclosure.*”

Security is “*the organizations responsible for protecting against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorized disclosure.*”

<sup>23</sup> Zie Hoofdstuk 3: INLICHTINGEN VOOR DE COMMANDOVOERING en de toekomstige afgeleide publicatie over de inlichtingenvoorbereiding van de operationele omgeving dat naar verwachting in 2011 verschijnt.

<sup>24</sup> AAP-6

<sup>25</sup> AAP-6

## 2.3 GRONDBEGINSELEN

Om de effectiviteit en efficiëntie van het I&V-systeem zo groot mogelijk te maken worden binnen de NAVO acht grondbeginselen gehanteerd<sup>26</sup>. Zij hebben betrekking op de bruikbaarheid van de I&V-producten, het zorgvuldige beheer van het systeem en de doelmatige inzet van verzamelorganen en bronnen.

### 2.3.1 Responsiviteit (*Responsiveness*)

De inlichtingenstaf moet voortdurend alert zijn en in staat zijn om de commandant te ondersteunen met een goed inlichtingenbeeld. Dit gebeurt door het beschikbaar stellen van door hem gevraagde inlichtingen, maar zeker ook door met ongevraagde informatie tijdig zijn aandacht te richten op zaken die zijn aandacht vereisen. Dit houdt in dat de inlichtingenstaf inzicht moet hebben in de langetermijnvisie van de commandant, zijn oogmerk en de actuele onderwerpen waarop hij zijn aandacht wenst te richten.

### 2.3.2 Tijdigheid (*Timeliness*)

Inlichtingen moeten om bruikbaar te zijn zo vroeg mogelijk, maar in ieder geval op tijd, aangeleverd worden aan de behoeftesteller. Dit grondbeginsel is ook geldig voor de aansturing van bronnen en organen om bij veranderende situaties ten behoeve van effectiviteit en efficiëntie direct bij te kunnen sturen.

De inlichtingenstaf moet hier een zorgvuldige tijdsplanning hanteren, waarbij kennis van de beslismomenten, de tijd die nodig is om tot het beslismoment te komen en de tijd die nodig is om de inlichtingenoperatie te sturen benodigde voorwaarden zijn.

### 2.3.3 Objectiviteit (*Objectivity*)

De kwaliteit van inlichtingen valt of staat met de objectieve wijze waarop naar gegevens en informatie wordt gekeken. Vooringenomen meningen en standpunten geven een verkeerd beeld van de werkelijkheid. Vooral is het van belang de beschikbare gegevens en informatie in de context van de omgeving te plaatsen om hieraan de juiste betekenis te kunnen toekennen.

### 2.3.4 Toegankelijkheid (*Accessibility*)

Gegevens, informatie en inlichtingen moeten toegankelijk zijn. Inlichtingenpersoneel, dat uiteindelijk de inlichtingen moet produceren, moet snel materiaal kunnen vergelijken en de gebruikers van inlichtingen moeten eenvoudig bij de benodigde producten kunnen komen.

<sup>26</sup> AJP-2, “Joint Intelligence, CI & Security” (02 Feb 2004) paragraph 1301 a to h

Deze toegankelijkheid wordt mogelijk gemaakt door standaardprocedures, informatiesystemen en databanken. Koppelingen binnen de inlichtingenketen en met de eenheden, formaties en krijgsmachtdelen vergroten de toegankelijkheid nog verder. Dit grondbeginsel wint in de huidige en toekomstige inzetscenario's aanmerkelijk aan belang.

### 2.3.5 Voortdurende beoordeling (*Continuous review*)

Inlichtingen zijn zelden onveranderlijk en ze moeten daarom continu worden beoordeeld op hun geldigheid en zo nodig worden herzien. Nieuwe informatie en een zich ontwikkelende situatie worden hierbij meegenomen.

### 2.3.6 Bronbescherming (*Source protection*)

Alle informatie- en inlichtingenbronnen moeten beschermd worden tegen compromittatie. Die bescherming heeft als doel de veiligheid van de bron te garanderen en (de toegang tot) de informatie van de bron veilig te stellen.

### 2.3.7 Centrale coördinatie (*Centralised co-ordination*)

Om te voorkomen dat overbodige inlichtingenspanningen worden geleverd moet afstemming plaatsvinden tussen taken en verantwoordelijkheden. Dit kan gebeuren door geografische afbakening (bij overlappende gebieden van verantwoordelijkheid), thematische afbakening en zorgvuldig bronbeheer. Centrale coördinatie is, binnen de inlichtingenketen, een van de hoofdtaken van de inlichtingstaven.

### 2.3.8 Systematische inzet en exploitatie (*Systematic exploitation*)

Het doel is om met de beschikbare middelen een zo compleet mogelijk beeld te vormen. Bronnen en verzamelorganen hebben hun specifieke, meestal van elkaar verschillende, kenmerken. Een systematisch gebruik en een systematische inzet vergen een goede kennis van hun mogelijkheden en beperkingen.

## 2.4 NIVEAUS VAN INLICHTINGEN

Bij de overweging, planning en uitvoering van militaire operaties worden vijf niveaus gehanteerd. Hieraan gekoppeld kent het functiegebied I&V een identieke indeling. Het politiek-strategisch niveau en het militair-strategisch niveau worden ondersteund met strategische inlichtingen. Het operationele, tactische en technische niveau met achtereenvolgens operationele, tactische en technische<sup>27</sup> inlichtingen. Door de behoefte aan dezelfde inlichtingen op verschillende niveaus en door het toenemend gebruik van ICT in een

<sup>27</sup> Deze categorie Technische inlichtingen betreft het technische niveau van militair optreden. De term technische inlichtingen kan ook betrekking hebben op techniek. Dit laatste wordt in de volgende sectie beschreven.

genetwerkte omgeving vloeien deze niveaus in elkaar over, waardoor het onderscheid tussen deze niveaus vervaagt. Daarom wordt gebruik gemaakt van de inlichtingenketen die de samenwerking tussen de niveaus garandeert.

### 2.4.1 Inlichtingen op het strategische niveau

Op het politiek-strategische niveau zijn strategische inlichtingen benodigd voor de toepassing van machtsmiddelen op het gebied van politieke, diplomatieke, economische en militaire zaken. Deze toepassing vindt plaats op nationaal en internationaal niveau. Hiertoe wordt de internationale situatie door de MIVD voortdurend beoordeeld aan de hand van vooraf bepaalde criteria en zijn indicatoren vastgesteld waarmee dit niveau tijdig kan worden geïnformeerd (het zogenaamde *Indicator and Warning* systeem).

Strategische inlichtingen dienen verder om politieke besluitvorming over een eventuele inzet van militaire middelen te ondersteunen en de besluitvorming hierover te kunnen evalueren. Ook worden ze op dit niveau gebruikt om de regering de mogelijkheid te geven de voortgang van een missie te bewaken en bij eventuele (politiek) onwenselijke gevolgen tijdig maatregelen te nemen om de Nederlandse militaire inzet bij te kunnen sturen.



Voor het militair-strategische niveau dienen inlichtingen onder andere om de bronnen van instabiliteit en/of conflict en de militaire dreiging in de diverse relevant geachte inzetgebieden in kaart te brengen, de inzet te kunnen beoordelen, bij te sturen en te evalueren. Dit draagt mede bij aan de instandhouding van een op zijn taak berekende krijgsmacht. In het nationale militaire planningsproces, voor een mogelijke deelname aan een internationale troepenmacht, moeten inlichtingen bijdragen aan het vaststellen van de haalbaarheid van de beoogde effecten die de Nederlandse bijdrage moet kunnen bereiken. De keuze van de in te brengen middelen zal mede op grond daarvan worden bepaald.

#### 2.4.2 Inlichtingen op het operationele niveau

Operationele inlichtingen worden verworven op basis van enerzijds het beeld dat voor het strategische niveau geschetst is en anderzijds de behoefte van de operationele commandant. Ze worden gebruikt bij de planning en uitvoering van campagnes en operaties op het operationele niveau. Enerzijds geven ze de CDS inzicht in de omgevingsfactoren die benodigd zijn voor de planning, gereedstelling en uitvoering van (de Nederlandse bijdrage aan) militaire operaties. Anderzijds worden operationele inlichtingen gebruikt door de operationele (internationale) commandant om de operaties in een aangegeven campagne te plannen en uit te voeren. De instrumenten die hij hiervoor gebruikt zijn *operational art* en *operational design*. De essentie hierbij is om met operationele inlichtingen vast te stellen wat de *Centers of Gravity* (CoG)<sup>28</sup> van de operatieomgeving en eventuele opponenten zijn.

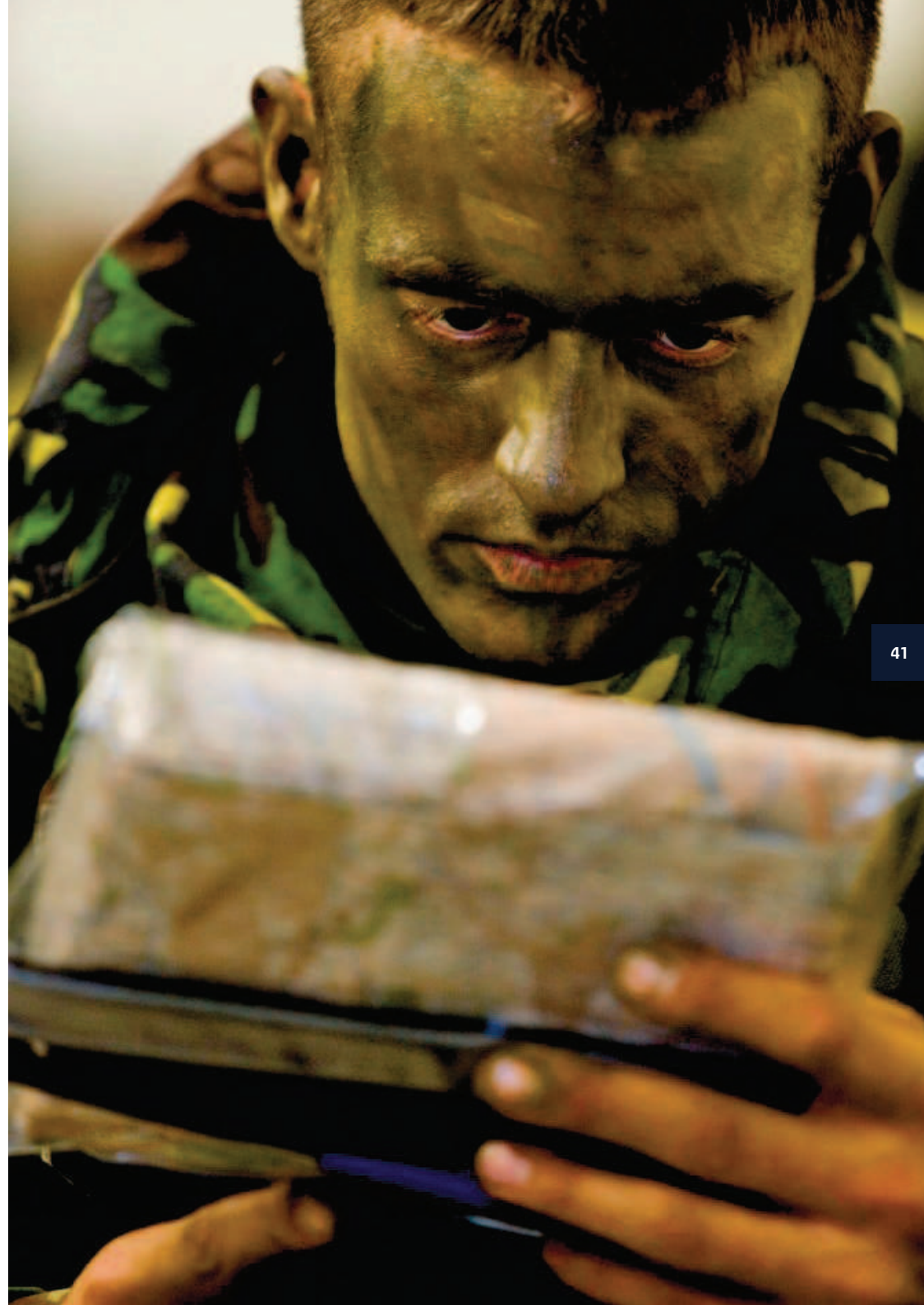
#### 2.4.3 Inlichtingen op het tactische niveau

Op het tactische niveau wordt leiding gegeven aan de militairen en eenheden die in direct contact komen met de partijen in het conflict. Tactische inlichtingen zijn van belang bij de ondersteuning van te ontplooiën activiteiten van deze militairen en eenheden. Kenmerken van tactische inlichtingen zijn de directe toepasbaarheid (*actionable intel*), de tijdsgevoelighed en de accuratesse, omdat op basis hiervan vaak in korte tijd beslissingen moeten worden genomen. Zij bieden de commandant de gelegenheid om in het hem toegewezen operatiegebied zijn kansen, bedreigingen en risico's goed in te schatten.

#### 2.4.4 Inlichtingen op het technische niveau

Het technische niveau van optreden is het uitvoerende optreden van militairen en eenheden die in direct contact (kunnen) komen met de actoren in het conflict. Inlichtingen benodigd op dit niveau betreffen het hele spectrum van inlichtingen: van de strategische doelstellingen van de actoren tot en met de wijze van inzet en het optreden van kleine

<sup>28</sup> *Center of Gravity* (CoG): de karakteristieken, capaciteiten of locaties waaraan een natie, alliantie, militaire eenheid, groepering of andere soort opponent haar vrijheid van handelen, fysieke kracht of wil om te strijden ontleent (*hub of all power*).



eenheden<sup>29</sup> van de actoren om in een bepaalde samenhang en volgorde het (tactisch) doel van de actoren te bereiken. Bij dit laatste gaat het o.a. om de daadwerkelijke (gevechts)-technieken en -tactieken (*Techniques, Tactics and Procedures, TTP*) van de actoren, veelal met een specifiek (wapen)stelsel of een andere effectenbrenger. Het technische niveau van optreden dient niet te worden verward met Technische Inlichtingen (zie hiervoor paragraaf 2.5.4).

## 2.5 SOORTEN INLICHTINGEN

Er zijn vier soorten inlichtingen, die in te delen zijn naar hun aard. Alle vier kunnen ze worden gebruikt op ieder van het voorgaande beschreven niveau.

### 2.5.1 Basisinlichtingen

Basisinlichtingen zijn inlichtingen en gevalideerde informatie over elk denkbaar onderwerp. Zij dienen als basis voor het verwerken van nieuw beschikbaar komende informatie of inlichtingen.

### 2.5.2 Actuele inlichtingen

Actuele inlichtingen geven de huidige toestand of ontwikkelingen weer. Deze inlichtingen kunnen meer gedetailleerder zijn dan basisinlichtingen en vanwege hun actualiteit zijn zij meer tijdkritisch van aard.

### 2.5.3 Doelinlichtingen

Doelinlichtingen worden gegenereerd door het benutten van relevante basisinlichtingen en actuele inlichtingen en zij ondersteunen de commandant in zijn doelkeuze en wijze van doelbestrijding. Zij voorzien in een definitie van (delen van) het doel of doelencomplex, het relatieve belang daarvan voor het eigen optreden en dat van de opponent, een bepaling van de locatie van dit (deel van) het doel(-encomplex) en de kwetsbaarheden ervan. Tevens kunnen zij na een eventuele doelbestrijding dienen voor effectmeting (*Measurement of Effects; MoE*).

### 2.5.4 Technische Inlichtingen

Technische inlichtingen betreffen technische ontwikkelingen, mogelijkheden en operationele capaciteiten van materieel, die een militaire toepassing hebben of zouden kunnen hebben.

<sup>29</sup> Soms zelfs individuele militairen of (wapen)systemen.

## 2.6 VERZAMELMETHODEN, -ORGANEN EN BRONNEN

Inlichtingen kunnen, onafhankelijk van de indeling naar niveau, soort of doel, ook worden ingedeeld naar de bron en/of de methode van verzamelen. In het inlichtingenproces zal altijd worden getracht gebruik te maken van verschillende soorten bronnen, verzamelorganen en zo mogelijk verzamelmethode om zo door onderlinge aanvulling en overlapping de betrouwbaarheid van de inlichtingen te vergroten en de kans op misleiding zo klein mogelijk te maken. Een eenvoudige verzamelmethode levert informatie (INF) aan. De informatie die is verkregen door verschillende verzamelmethode wordt gecombineerd om voor de commandant bruikbare inlichtingen (INT<sup>30</sup>) te verkrijgen<sup>31</sup>. In enkele gevallen is men in staat om met de toepassing van één specifieke methode direct inlichtingen te genereren, veelal voor direct gebruik op het tactische niveau.



<sup>30</sup> In de internationale gemeenschap wordt voor alle verzamelmethode doorgaans het woord *Intelligence* en de afkorting INT gebruikt. Ter voorkoming van verwarring wordt dat in dit document ook gedaan.

<sup>31</sup> Zie sectie 3.5 VERWERKEN.

In deze paragraaf worden de meest voorkomende methoden om informatie te verzamelen, het verzamelorgaan<sup>32</sup> en de bron gedefinieerd. Een meer uitgebreide toelichting is weer-gegeven in bijlage 1.

### 2.6.1 Verzamelmethoden

- *Acoustic Intelligence* (ACINT). ACINT betreft inlichtingen afgeleid uit informatie van en over akoestische bronnen (geluidsspectrum).
- *Geospatial Intelligence* (GEOINT). GEOINT produceert inlichtingen die afgeleid zijn van de analyse van georuimtelijke informatie (*geospatial information*; GEOINF<sup>33</sup>) en beeldmateriaal (zie IMINT), om fysieke kenmerken en geografisch gerelateerde activiteiten te beschrijven, te duiden en visueel uit te beelden.
- *Human Intelligence* (HUMINT). HUMINT is een categorie inlichtingen die wordt verkregen uit alle vormen van informatie welke is verzameld of verstrekt door menselijke bronnen.
- *Imagery Intelligence* (IMINT). IMINT wordt verkregen door de analyse en interpretatie van beeldmateriaal.
- *Measurement and Signature Intelligence* (MASINT). MASINT verkrijgt inlichtingen uit wetenschappelijke en technische informatie door kwantitatieve en kwalitatieve analyse van gegevens<sup>34</sup>, afkomstig van sensoren die de identificerende en onderscheidende kenmerken van een doel, (stralings)bron of zender kunnen vaststellen, om te voorzien in diens omvang en identificatie. Bij MASINT worden ook forensische onderzoeksmethoden toegepast<sup>35</sup>.

<sup>32</sup> Sommige middelen waarmee informatie wordt verzameld, kunnen ook voor offensieve doeleinden worden ingezet. Die kwaliteiten en procedures vallen onder operatiën en worden hier niet beschreven.

<sup>33</sup> GEOINF beschrijft de fysieke omgeving en omvat data afkomstig van aeronautische, geografische, hydrografische, oceanografische en meteorologische disciplines. Deze data wordt geleverd door (of door tussenkomst van) CLAS Dienst Geografie KL (geografische data), CZSK Dienst der Hydrografie (hydrografische en oceanografische data) en CLSK Joint Meteo Groep (meteorologische en aeronautische data)

<sup>34</sup> Het handelt hier om metrische-, hoek-, ruimtelijke-, golflengte-, tijd-, modulatie-, plasma- en hydro-magnetische gegevens.

<sup>35</sup> Forensisch onderzoek is geen verzamelmethode, maar kent technieken die steeds vaker benut worden in het verzamelen van informatie bij de uitvoering van operaties. Vanwege de aard van die onderzoeksmethoden is het onderwerp opgenomen bij MASINT.

- *Medical Intelligence* (MEDINT). MEDINT is gebaseerd op medische, biomedische, epidemiologische, milieu-/omgevingsinformatie en overige informatie gerelateerd aan humane factoren en/of diergezondheidsfactoren.
- *Open Source Intelligence* (OSINT). OSINT betreft inlichtingen die worden verkregen uit informatie uit publiekelijk toegankelijke bronnen zoals radio, televisie, internet, pers en andere ongerubriceerde informatie.
- *Signals Intelligence* (SIGINT). SIGINT is de generieke term om inlichtingen te beschrijven die worden verkregen uit informatie vanuit het elektromagnetische spectrum. Het omvat *communications intelligence* (COMINT) en *electronic intelligence* (ELINT). *Computer Network Exploitation* (CNE) vormt een onderdeel van *Computer Networks Operations* (CNO). De NAVO beschouwt in haar doctrine CNO als een deel van *Information Operations* en dan meer specifiek als deel van Elektronische Oorlogvoering (EOV). Hierbij maakt CNE deel uit van COMINT.





### 2.6.2 Verzamelorgaan

Een verzamelorgaan is een organisatie of een persoon die betrokken is bij het verzamelen van informatie. Het moet beschikken over de juiste sensor, het platform, de verzamelgelegenheid en de verwerkingscapaciteit. Verder is een verzamelorgaan in staat om informatie in een geschikt formaat aan te leveren.

### 2.6.3 Bron

Een bron is een persoon, voorwerp, zaak of gebeurtenis waaraan informatie kan worden ontleend. Praktisch gezien zijn dit personen, media, documenten, literatuur en de werkelijkheid (directe waarneming). Bronnen kunnen worden ingedeeld in gecontroleerde, ongecontroleerde en gelegheidsbronnen.

## 2.7 SAMENVATTING

In de vorige paragrafen is een uiteenzetting gegeven van de grondbeginselen en de niveaus en soorten van inlichtingen. Sommige algemene termen zijn in dit hoofdstuk nog niet verklaard, zoals GA en SA, *Indicator and Warning (I&W)* en 'voorspellend vermogen'. Voor de duidelijkheid zal deze terminologie worden verklaard in het verband, waarin ze in de volgende hoofdstukken worden geïntroduceerd.



## 3 INLICHTINGEN VOOR DE COMMANDOVOERING

### 3.1 INLEIDING

Commandovoering omvat het leiden en besturen van een militaire organisatie om haar doelstellingen te realiseren<sup>36</sup>. Het inlichtingenproces wordt aangestuurd vanuit de commandovoering en ondersteunt de hoofdelementen van commandovoering: besluitvorming, bevelvoering en leiderschap. Centraal in het inlichtingenproces staat de inlichtingencyclus die bestaat uit de fasen initiëren, verzamelen, verwerken en verspreiden. Dit hoofdstuk beschrijft hoe het inlichtingenproces de commandovoering van de commandant ondersteunt.

### 3.2 HET INLICHTINGENPROCES

Het inlichtingenproces maakt, samen met het doelbestrijdingsproces (*Targeting*), integraal onderdeel uit van het besluitvormingsproces. Het inlichtingenproces levert niet alleen inlichtingen voor doelbestrijding- en besluitvormingsprocessen, maar ontvangt hieruit ook informatie. Het proces levert inlichtingen aan de commandant en de overige behoefte-stellers voor alle niveaus en functies van militair optreden.

#### 3.2.1 De inlichtingencyclus

In deze sectie wordt het inlichtingenproces uitgewerkt aan de hand van een model, dat de inlichtingencyclus wordt genoemd. In de cyclus worden de deelprocessen met hun onderlinge relaties beschreven en ook de methode die wordt gehanteerd om het inlichtingenproces te beheersen. De inlichtingencyclus kent vier fasen<sup>37</sup> – initiëren, verzamelen, verwerken en verspreiden – die hierna zullen worden beschreven.

De start van de cyclus wordt gekenmerkt door een behoefte<sup>38</sup> aan inlichtingen (het stellen van een vraag) en wordt afgerond met het aanleveren van het gewenste product (het geven van het antwoord). Hiertussen zijn de eerder genoemde fasen duidelijk te herkennen en afgebakend, waarbij iedere fase zijn eigen onderverdeling van stappen en activiteiten kent. De systematiek van de inlichtingencyclus is voor de inlichtingenstaven op alle niveaus gelijk. Alleen de aard van de vragen en antwoorden zal per niveau verschillen.

Het inlichtingenproces wordt ondersteund door het managementproces van de cyclus, het *Collection Co-ordination and Information Requirements Management*

<sup>36</sup> Zie JDP-5 "Commandovoering".

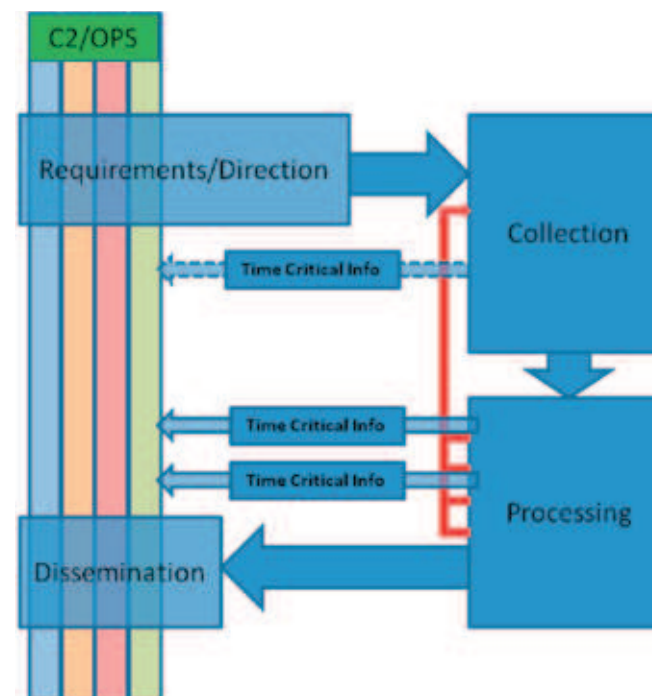
<sup>37</sup> Internationaal wordt er discussie gevoerd over het aantal fasen, waarbij het aantal in de discussie varieert van vier, vijf of zes of in een enkel geval nog meer. Bij het vastleggen van dit hoofdstuk was nog geen uitzicht op de mogelijke uitkomst van de discussie, waardoor om redenen van eenvoud, en de definitie in AAP-6, in de beschrijving is uitgegaan van vier fasen.

<sup>38</sup> Ten onrechte wordt "behoefte" wel eens gelijkgesteld met "actieve vraagstelling door commandant en/of andere behoefte-stellers". Dit is hier slechts een klein onderdeel van. Inlichtingenbehoefte kan impliciet zijn verwoord in het oogmerk van de commandant, of in zijn visie en beschouwingen op de operatieomgeving en op komende of lopende operaties.

(CCIRM). De CCIRM-functie omvat het proces van coördinatie en voortgangscntrole op de informatieverzamelactiviteiten en het management van de informatiebehoefte van de commandant.

#### 3.2.2 *Collection Co-ordination & Information Requirements Management*

CCIRM omvat het proces van coördinatie en voortgangscntrole van alle verzamel- en verwerkingsactiviteiten<sup>40</sup> in de inlichtingencyclus en houdt toezicht op een tijdige verspreiding van de inlichtingen. Het moet een doelmatige uitvoering van het inlichtingenproces garanderen. CCIRM bevat twee componenten: ten eerste het beheer van de informatie-



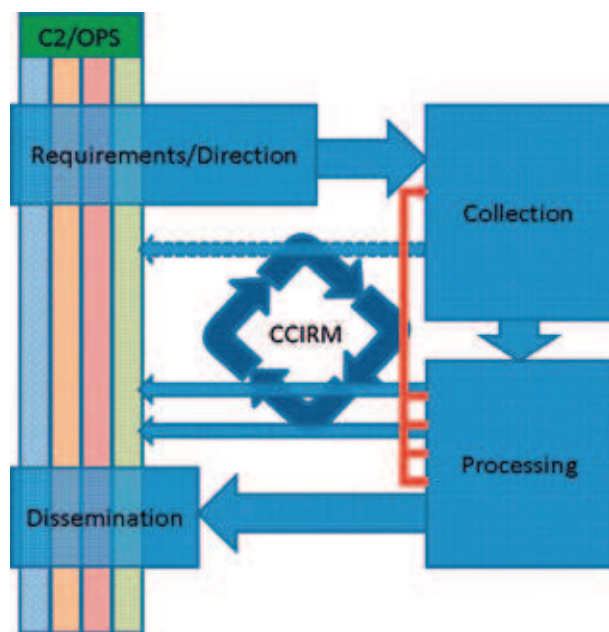
Figuur 1 Inlichtingencyclus

<sup>39</sup> De definitie van inlichtingen en informatie is beschreven in paragraaf 2.2.1. Op basis hiervan wordt de letter "I" in CCIRM voluit "Information". De AJP-2 wordt in 2010 herzien. Hierbij is dit onderwerp in bespreking.

<sup>40</sup> Verzamel- en verwerkingsactiviteiten beperken zich niet alleen tot de verzamel- en verwerkingsfase van de inlichtingencyclus, maar vangen al aan tijdens het initiëren bij de controle op het reeds beschikbaar zijn van informatie.

behoefte (*Information Requirements Management*<sup>41</sup>) en het toezicht erop en ten tweede de coördinatie van de verzamelactiviteiten (*Collection Co-ordination*).

CCIRM begint bij het uitwerken van de inlichtingenbehoefte (zie paragraaf 3.3.3), waarbij eerst moet worden vastgesteld of informatie al beschikbaar is. Tevens wordt hier vastgesteld welke informatie onder verantwoordelijkheid van de eigen operationele commandant kan worden verzameld (organieke en onder bevel gestelde verzamelorganen en eenheden) en welke moet worden verkregen door activiteiten van andere inlichtingenstaven en verzamelorganen. Verder valt het beheer<sup>42</sup> van het verzamelplan (*Intelligence Collection Plan of ICP*), zie 3.3.4, onder CCIRM.



Figuur 2 CCIRM

<sup>41</sup> Hier moet duidelijk onderscheid gemaakt worden tussen *Information Management* en *Information Requirements Management*. Het eerste betreft het management van alle informatiestromen binnen een staf, een verantwoordelijkheid van de Chef Staf en het tweede betreft het management van de informatiebehoefte binnen de inlichtingenstaf en de inlichtingenketen ten behoeve van de productie van inlichtingen.

<sup>42</sup> Beheer ICP: invoegen van aanvullende vragen in relatie tot bestaande behoefte, verwijderen van beantwoorde vragen, toezicht houden op tijdcriteria.

CCIRM ziet toe op de juiste opslag van de informatie en vormt het communicatiekanaal met externen (andere inlichtingenstaven) voor het coördineren van verzamelinspanningen, bronbeheer en informatie-uitwisseling (het versturen en beantwoorden van *Requests for Information*; RFI). Voor het uitwisselen van informatie moeten bepaalde regels uit het DBB in acht worden genomen<sup>43</sup>.

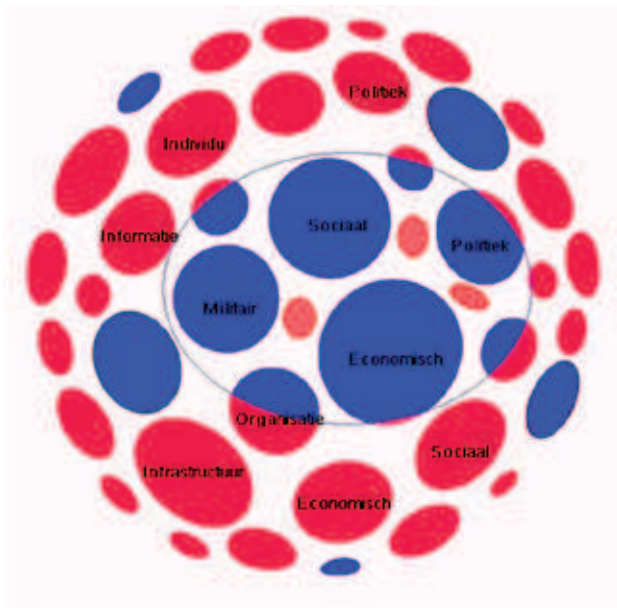
### 3.3 INITIËREN (DIRECTION)

Initiëren is de fase van de inlichtingencyclus waarin de commandant richting geeft aan de inlichtingenstaf. Hij doet dit door het vaststellen van wederzijdse verantwoordelijkheden, door zijn ervaring en achtergrondkennis, door zijn eigen perceptie van de omgeving en door zijn interesses. In de initiatiefase wordt bovendien de inlichtingenbehoefte geformuleerd zodat opdrachten en verzoeken tot verzamelen kunnen worden gedaan. De processtap initiëren kan plaatsvinden op het hoogste niveau, waarop de regering toezicht wil kunnen houden op gebieden waarin mogelijk bepaalde machtsmiddelen kunnen worden ingezet, tot en met het laagste niveau waar een individuele militair zich afvraagt hoe zijn directe omgeving eruit ziet. Verder zal in dit document slechts gesproken worden over die niveaus waarop de commandant beschikt over een inlichtingenstaf.

#### 3.3.1 Gebied van inlichtingenverantwoordelijkheid en -belangstelling

Om de verantwoordelijkheden voor het verzamelen van informatie af te bakenen zullen er een gebied van inlichtingenverantwoordelijkheid (*Area of Intelligence Responsibility*; AIR) en een gebied van inlichtingenbelangstelling (*Area of Intelligence Interest*; AII) worden vastgesteld. Ongeacht het niveau, waarop de inlichtingenactiviteiten worden uitgevoerd, zal de commandant altijd definiëren in welk geografisch of thematisch gebied de voorgenomen operaties of activiteiten plaats zullen vinden, het operatiegebied (*Area of Operations*; AO) genoemd. Gerelateerd aan dit operatiegebied wordt vastgesteld welke actoren en factoren van invloed zijn op de operatie (AIR) of dat mogelijk kunnen worden (AII) en in welke omgeving (wederom geografisch en thematisch) deze (f)actoren actief zijn. De commandant stelt de AIR en AII vast en draagt de inlichtingenstaf op om daarin hun activiteiten te ontplooiën. Voor de uitvoering van de inlichtingentaken zal ook de inzet van middelen en informatie van de nevenschikte- en hogere niveaus worden gevraagd.

<sup>43</sup> Zie ook paragraaf 4.3.3. "Informatiebeveiliging".



Figuur 3 AIR en AII

### 3.3.2 Bepalen van de inlichtingenbehoefte

Voor zijn besluitvorming heeft de commandant behoefte aan informatie. De behoefte gaat uit naar informatie over bevolking, relevante actoren, intenties, (potentiële) tegenstanders en voorts over alle functies van militair optreden. De noodzakelijke informatie is de zogenaamde *Commanders Critical Information Requirements* (CCIR<sup>44</sup>). De informatie over de actoren en factoren van invloed uit de omgeving waarin hij zijn missie, operatie of opdracht uit gaat voeren, wordt inlichtingen (*Intelligence Requirements*; IR) genoemd. Aan de formulering van de inlichtingenbehoefte kunnen verschillende motieven ten grondslag liggen. De behoefte kan voortvloeien uit de wens om tot een algemeen besef (GA) te komen van de aard van zijn omgeving, dan wel uit de wens om een meer concreet bewustzijn van de gebeurtenissen - en de betekenis daarvan - in die omgeving (SA) te krijgen. Daarnaast kan het ook gaan om specifieke vragen gerelateerd aan komende of lopende operaties. Aan sommige behoeften

<sup>44</sup> Zie ook paragraaf 4.3.3. "Informatiebeveiliging".

kent hij een hoge prioriteit toe en die worden kernvragen (*Priority Intelligence Requirements*; PIR) genoemd. Het overgrote deel van zijn inlichtingenbehoefte stelt hij vast op basis van zijn beschouwing van de operatieomgeving, waarin de actoren en factoren van invloed een rol spelen, evenals op basis van de hierin voorkomende dynamiek.

De beschrijving van de operatieomgeving wordt hem gepresenteerd door de inlichtingenstaf. Verderop in het hoofdstuk wordt de *Intelligence Preparation of the Environment* toegelicht als werkwijze om de operatieomgeving te beschrijven. Het grootste belang van deze beschrijving wordt gevormd door de kansen, bedreigingen en risico's, die de commandant hieruit kan afleiden.

Daarnaast kan de commandant opdracht van zijn hogere commandant krijgen om vanuit zijn operatiegebied actief informatie of inlichtingen te genereren ten behoeve van de GA, SA en besluitvorming van de hogere commandant.

Om bij het bepalen van de inlichtingenbehoefte een adviserende rol te kunnen spelen, moet de inlichtingenstaf ten eerste beschikken over inzicht in de operatie en het oogmerk van de commandant en ten tweede over kennis van de hierbij gebruikte technieken, procedures en middelen.

### 3.3.3 Uitwerken van de inlichtingenbehoefte

Zodra de inlichtingenbehoefte van de commandant bekend is, moet deze vertaald worden naar uitvoerbare verzamelopdrachten en/of verzoeken voor de verschillende bronnen en verzamelorganen<sup>45</sup>. Dit houdt in dat de opdracht of vraag, desnoods opgedeeld in meerdere deelvragen, wordt voorzien van waarneembare en herkenbare indicatoren<sup>46</sup>, die in tijd en ruimte begrensd worden.

Op basis van deze indicatoren stelt de inlichtingenstaf vast, welke verzamelorganen en bronnen in staat zijn de gestelde vraag tijdig te beantwoorden. Voordat deze vragen omgezet worden in opdrachten en verzoeken gaat de inlichtingenstaf eerst na of de gevraagde informatie of inlichtingen niet al beschikbaar zijn bij het eigen personeel of in bestaande databases.

<sup>45</sup> Hierbij wordt niet alleen gekeken naar verzamelorganen in de eigen organisatie of bronnen binnen het eigen gebied van inlichtingenverantwoordelijkheid, maar naar alle bij de campagne betrokken eenheden en (inlichtingen)elementen.

<sup>46</sup> Een indicator is een waarneembare aanwijzing dat een (verwachte) gebeurtenis of activiteit plaats gaat vinden, plaats vindt of plaats heeft gevonden.

Om de uitwerking van de inlichtingenbehoefte adequaat te laten verlopen, is kennis van de kenmerken en mogelijkheden en beperkingen van de verzamelorganen en bronnen evenals de werking van eventuele databases, een vereiste voor de inlichtingenstaf.

#### 3.3.4 Het verzamelplan (*Intelligence Collection Plan; ICP*)<sup>47</sup>

Zodra de inlichtingenbehoefte van de commandant is uitgewerkt, ontstaat een overzicht van de nog te beantwoorden vragen en van de middelen die beschikbaar zijn om dit te doen. Vervolgens worden mogelijkheden ontwikkeld om de gewenste informatie te verkrijgen, waarbij de synchronisatie van behoefte en beschikbare capaciteit cruciaal is. Om uit de ontwikkelde mogelijkheden de beste keuze te kunnen maken, worden criteria geformuleerd en gehanteerd, zo mogelijk op basis van de grondbeginselen. De belangrijkste hiervan zullen altijd de prioriteitstelling van de commandant zijn en criteria die te maken hebben met effectiviteit (bijvoorbeeld tijdigheid en objectiviteit) en met efficiëntie. Daarbij prevaleert effectiviteit boven efficiëntie. Een andere belangrijke factor is dat sommige cruciale informatie snel beschikbaar moet komen en bevestigd moet worden, waardoor gekozen kan worden voor de inzet van meerdere organen om dezelfde informatie te verzamelen. Op basis van de gekozen mogelijkheid wordt vastgesteld welke ondersteuning en *enablers* nodig zijn om de uitvoering hiervan mogelijk te maken. Deze elementen vormen uiteindelijk het verzamelplan (*Intelligence Collection Plan; ICP*).

Met behulp van het ICP worden opdrachten verstrekt aan alle onder bevel staande verzamelorganen en operationele eenheden<sup>48</sup> (*Intelligence Collection Orders; ICO's*) en verzoeken gedaan aan andere inlichtingenstaven met *Requests for Information (RFI)*.

### 3.4 VERZAMELEN (COLLECTION)

De verzamelfase vangt aan na het verstrekken van de verzamelopdrachten of -verzoeken en heeft als resultaat het leveren van informatie of mogelijk al van inlichtingen aan de verwerkingsfase. Daarnaast is het mogelijk als (tijdkritische) omstandigheden daarom vragen, direct vanuit deze fase (on)gevalideerde informatie te verstrekken. De ontvanger van een verzamelopdracht stelt met behulp van een besluitvormingsmodel vast hoe de verzamelcapaciteit effectief kan worden ingezet.

<sup>47</sup> Door de definitie van inlichtingen en de definitie van informatie is hier sprake van een plan om informatie te verzamelen. De Engelse term *Intelligence Collection Plan* staat op dit moment binnen de NAVO bij het samenstellen van de AJP-2 ter discussie.

<sup>48</sup> Operationele eenheden zijn, door hun aanwezigheid in het gebied, een waardevolle bron en mogelijk verzamelorgaan. Volledigheidshalve wordt hier opgemerkt, dat de door de inlichtingenstaf verstrekte opdrachten worden gegeven namens de commandant.



Aan de hand van het hiermee ontwikkelde plan worden de sensoren ingezet.

De verzamelfase kent een aantal verzamelmethode waarmee bronnen worden geëxploiteerd op basis van hun kenmerken. De verzamelorganen die deze methodes toepassen, dragen zorg voor de verstrekking van de verworven informatie conform de eisen vermeld in de verzamelopdracht. Dit houdt in dat de informatie in ieder geval tijdig wordt aangeleverd, maar zo nodig ook wordt voorbereid. Aan deze voorbereiding zal in de laatste paragraaf van de verzamelfase aandacht worden besteed.

#### 3.4.1 Verzamelorganen

Een verzamelorgaan is een organisatie of een persoon die betrokken is bij het verzamelen van informatie. Het verzamelorgaan moet beschikken over de juiste sensor<sup>49</sup>, het platform, de verzamelgelegenheid en de verwerkingscapaciteit. Verder is een verzamelorgaan in staat om informatie in een geschikt formaat aan te leveren. Verzamelorganen met een eigen organieke verwerkingscapaciteit kunnen *single-source* inlichtingen leveren; verzamelorganen zonder verwerkingscapaciteit kunnen dit niet. Verzamelorganen gebruiken de bronnen en verzamelmethode die genoemd zijn in sectie 2.6<sup>50</sup>.

<sup>49</sup> In het ICP kunnen als sensor aangemerkt worden: elementen van verzamelorganen, (elementen van) verkenningseenheden, (elementen van) reguliere eenheden met een verkenningsoopdracht, reguliere eenheden tijdens hun normale taakuitvoering en alle personen behorend tot de eigen eenheid tijdens hun normale taakuitvoering.

<sup>50</sup> Voor een uitgebreide beschrijving zie bijlage 1.

### 3.4.2 De bewerking door verzamelorganen

Tijdens en na de uitvoering van de verzamelactiviteiten door de sensoren van de verzamelorganen, kan het mogelijk zijn dat de in het ICP van de inlichtingenstaf gestelde vragen direct beantwoord kunnen worden. In dit geval worden de resultaten onmiddellijk door het verzamelorgaan aan de eenheden gerapporteerd, zodat zij direct kunnen bijdragen aan de *situational awareness* van de commandant. Gelijktijdig zullen de resultaten aan de inlichtingenstaf worden aangeboden waarna de verwerkingsfase van de inlichtingencyclus begint.

Als gevolg van het hoogtechnologische en/of zeer specialistische karakter van de hedendaagse sensor is het aannemelijk dat de sensorinformatie eerst door specialistisch personeel moet worden beoordeeld, voordat de vraag uit het verzamelplan kan worden beantwoord. Om de vraag te kunnen beantwoorden, zal het verzamelorgaan de sensorinformatie moeten analyseren. Dit doet het nadat de informatie is opgeslagen (registreren) en de inhoud op waarde is beoordeeld (evalueren). Dit betekent dat het verzamelorgaan stappen uitvoert, die later bij de verwerkingsfase worden toegelicht.

Dit betekent niet dat het verzamelorgaan delen van het verwerkingsproces van de inlichtingenstaf overneemt. De inlichtingenstaf zal het verwerkingsproces starten conform het gestelde in de volgende paragraaf, met dien verstande dat dit gebeurt met de door de verzamelorganen aangeleverde antwoorden op de vragen.

## 3.5 VERWERKEN (PROCESSING)

De fase van het verwerken begint zodra de antwoorden (de resultaten van de verzamelopdrachten, verzoeken en RFI) van verzamelorganen, eenheden en andere inlichtingenstaven binnen komen. Deze antwoorden worden verwerkt tot inlichtingenproducten die voldoen aan de gestelde eisen van de behoeftesteller, waarna zij kunnen worden verspreid. De stappen van deze fase - registreren, evalueren, analyseren, integreren en interpreteren - worden aansluitend doorlopen. Gelijktijdige uitvoering van de stappen is sneller, maar meestal minder volledig. Voor gelijktijdige uitvoering kan worden gekozen bij het verwerken van tijdkritische inlichtingenbehoeften, waarbij de beschrijvende analytische conclusies vaak belangrijker zijn dan de verklarende en/of beschouwende (en dus voorspellende) analyseproducten.

### 3.5.1 Registeren (*Collation*)

Registratie is een noodzakelijke en veelomvattende activiteit, waaraan hoge eisen worden gesteld. De grote hoeveelheid informatie die ontvangen wordt, moet op de juiste wijze worden opgeslagen. Met elkaar verband houdende informatie dient eerst te worden gegroepeerd en vergeleken voordat verdere verwerking plaatsvindt. Hierbij is het gebruik van geautomatiseerde informatieverwerkende systemen een vereiste.

### 3.5.2 Evalueren

Voordat de opgeslagen informatie voor analyse kan worden gebruikt, moeten eerst de betrouwbaarheid van de bron en de geloofwaardigheid van de informatie vastgesteld worden. De criteria hiervoor zijn opgenomen in bijlage 2.

### 3.5.3 Analyseren

Nadat de informatie is vergeleken met gelijksoortige informatie die al beschikbaar is én de bron- en de informatie-evaluatie zijn uitgevoerd, wordt de informatie onderworpen aan een kritische beschouwing. Dit heeft als doel de relevante feiten, omstandigheden en gebeurtenissen vast te kunnen stellen. De veelheid aan factoren en actoren in de operatieomgeving dwingt tot de inzet van materiedeskundig personeel dat de informatie in de juiste context kan verklaren.





#### 3.5.4 Integreren

De geanalyseerde informatie wordt vergeleken met eerder verkregen inlichtingen en informatie, waaronder de ontwikkelde hypothesen.<sup>51</sup> Zo nodig worden nieuwe hypothesen ontwikkeld, die voor de analyse een mogelijke context kunnen bieden. Om uitgangspunten, criteria en ontwikkelingen uit de hypothesen te kunnen bevestigen of ontkennen, worden vragen ontwikkeld om in het ICP te worden ingevoerd.

#### 3.5.5 Interpreteren

Op basis van de beschikbare informatie worden de hypothesen met elkaar vergeleken en in volgorde van waarschijnlijkheid (interpretatie) geplaatst. Hiermee worden mogelijke toekomstige ontwikkelingen beschreven, die kunnen worden gebruikt om het lopende of het geplande optreden te toetsen of de richting van een operatie bij te sturen. In de praktijk zijn de overgangen tussen de diverse stappen vaak minder zichtbaar, aangezien zij elkaar wederzijds blijven beïnvloeden, doordat nieuw ontwikkelde hypothesen of ontstane gebeurtenissen aanleiding kunnen geven tot een terugblik of heroverweging in het proces.

<sup>51</sup> Belangrijke hypothesen worden al ontwikkeld bij de derde stap van IPE (zie sectie 3.7: INLICHTINGENONDERSTEUNING VAN COMMANDOVOERING)

### 3.6 VERSPREIDEN (DISSEMINATION)

De laatste fase van de inlichtingencyclus betreft verspreiden. Verspreiden is het overdragen van inlichtingen aan de commandant en andere behoeftezoekers en wel tijdig, in de juiste vorm en op elke geschikte manier. Dit is een verantwoordelijkheid van de inlichtingenstaf. De verspreiding kan op actieve of op passieve wijze plaatsvinden. Bij actieve verspreiding (*information push*) zorgt de inlichtingenstaf ervoor dat de gevraagde producten bij de behoeftezoeker terechtkomen. Bij passieve verspreiding (*information pull*) legt de inlichtingenstaf producten vast in voor gebruikers toegankelijke opslagmedia, waaruit de gebruiker zelf de voor hem noodzakelijke informatie en inlichtingen haalt. De inlichtingenstaf zorgt ervoor dat de daar aanwezige informatie en inlichtingen actueel blijven. Door deze twee principes te combineren (*smart pull*) kunnen actuele gegevens en informatie over de actoren en factoren van invloed uit de operatieomgeving door derden worden gebruikt, waardoor de inlichtingenstaf efficiënt kan worden ingezet.

De in de verwerkingsfase geproduceerde inlichtingen worden voorafgaand aan de verspreiding in een zodanige presentatievorm opgesteld, dat de behoeftezoeker optimaal profijt haalt uit deze inlichtingen. De vier meest voorkomende presentatievormen zijn: mondeling (bij deelname aan overlegfora, briefings), schriftelijk (in de vorm van diverse (periodieke) rapportages), grafisch (overzichtskaarten, foto's, video) en in de vorm van data (matrices, geografische posities).

Bij het ter beschikking stellen van de inlichtingenproducten geeft de inlichtingenstaf een inschatting van het vertrouwen dat hij heeft in de conclusies die in het product worden gepresenteerd (*confidence level*). Ten eerste geeft dit een indicatie van het gewicht dat moet worden toegekend aan de inhoud. Ten tweede kan van het inlichtingenproduct worden aangegeven welke informatie-elementen ten grondslag hebben gelegen aan de toegekende waarschijnlijkheid of onwaarschijnlijkheid van de gepresenteerde conclusie. Door zijn invloed op deze informatie-elementen uit te oefenen, stelt dit de commandant in staat om de (on)waarschijnlijkheid toe of af te laten nemen.<sup>52</sup> Tevens wordt aan de inlichtingenproducten een waarschijnlijkheidsindicatie toegevoegd. Hiervoor wordt een gestandaardiseerde methodiek toegepast waarbij de dreiging en de dreigingindicatoren worden geclassificeerd. De tabellen die hierbij gehanteerd worden, zijn opgenomen in bijlage 2.

<sup>52</sup> Zie bijlage 2, Confidence Levels

Ten behoeve van de verspreiding van inlichtingenproducten buiten de eigen inlichtingketen moeten regels opgesteld worden die voldoen aan beveiligingsregels (*disclosure procedures*) waarin niet alleen de verspreiding naar coalitiegenoten is geregeld, maar ook de verspreiding naar andere organisaties.

Binnen alle fasen van de inlichtingencyclus, zo ook in het deelproces Verspreiden, zijn terugkoppelmomenten vast te stellen bij de overdracht van deelproducten en opdrachten en verzoeken (productevaluatie). De belangrijkste terugkoppelcriteria zijn bruikbaarheid, nauwkeurigheid, compleetheid en tijdigheid, en op sommige momenten in het proces, objectiviteit.

Tussen deze overdrachtmomenten wordt de wijze van uitvoeren van de activiteiten geëvalueerd (procesevaluatie).

Deze terugkoppelmomenten dienen tevens voor het vastleggen van *lessons identified*, *lessons noted* en de implementatie van *lessons learned*.

## 3.7 INLICHTINGENONDERSTEUNING VAN COMMANDOVOERING

De operatieomgeving is voortdurend onderhevig aan al dan niet mensgestuurde veranderingen die kansen kunnen bieden of risico's en bedreigingen kunnen veroorzaken in relatie tot de gewenste eindsituatie. Voor de operationele planning en besluitvorming moeten commandanten op de hoogte zijn van de bestaande toestand en van de te verwachten ontwikkelingen in hun gebied van verantwoordelijkheid. Zodra dat beeld van de omgeving voldoende duidelijk is, wordt vastgesteld voor welke onderdelen van de bestaande toestand en dynamiek het wenselijk is deze te beïnvloeden. Vervolgens wordt bepaald op welke wijze de gewenste beïnvloeding moet plaatsvinden. Voortdurend wordt bewaakt of er zich in de bestaande toestand of verwachte dynamiek wijzigingen voordoen die van invloed (kunnen) zijn op de te plannen, geplande of in uitvoering zijnde besluiten. Uiteindelijk wordt getoetst of met de beïnvloeding de gewenste eindsituatie is of wordt bereikt. De wijze waarop deze operationele omgeving inzichtelijk wordt gemaakt, wordt beschreven in de volgende paragrafen. Hierin komen IPE en de toepassing daarvan voor het operationele niveau aan de orde.



### 3.7.1 Intelligence Preparation of the Environment (IPE)

IPE is een werkmethode waarmee op effectieve wijze de operatieomgeving voor de commandant in kaart gebracht kan worden. De uitkomsten van het onderzoek geven de commandant inzicht in de kansen en mogelijkheden die de operatieomgeving hem biedt en de risico's en bedreigingen die hij hierin met zijn missie of operatie loopt. Daarom worden alle actoren en factoren van de operatieomgeving in beschouwing genomen, de manieren waarop zij elkaar mogelijk kunnen beïnvloeden en welke mogelijke ontwikkelingen zich in die omgeving voor kunnen doen.

Aan de hand van de conclusies van IPE is de commandant in staat doelen te formuleren waarop hij zijn vermogen wil concentreren en te bepalen met welke middelen hij dit wil doen. Daarnaast vormt het de basis voor het vaststellen van zijn beschermingsmaatregelen om de risico's en bedreigingen te verminderen.

Om het onderzoek zorgvuldig te laten verlopen en de commandant adequaat op de hoogte te kunnen stellen, moeten grote hoeveelheden basisinformatie en -inlichtingen worden verwerkt in statistieken, overzichten, matrices en andere (visuele) ondersteuningsmiddelen (*mapping the environment*).



Deze basisinformatie en -inlichtingen omvatten alle mogelijke segmenten van de operatie-omgeving en kunnen worden beschreven volgens de eerder genoemde PMESII-factoren. De op deze wijze gecreëerde databases, overzichten en ondersteuningsmiddelen kunnen naast het ondersteunen van de besluitvorming, planning en doelbestrijding tevens worden benut voor diverse deeloperaties, deelprocessen en functies zoals *Civil Military Cooperation* (CIMIC) en *Information Operations* (Infoops).

Om structuur in de grote hoeveelheid data en informatie te brengen en deze logisch te verwerken tot inlichtingen waarmee de commandant en overige behoeftezoekers kunnen werken, is IPE ingericht in drie stappen, waarbij elke stap wordt afgesloten met het formuleren van (sub)conclusies die bijdragen aan het inzicht van de commandant. Daarnaast ondersteunt de laatste stap het voorspellend vermogen van het inlichtingenproces, door hypothesen (scenario's en *Enemy Courses of Action*) te ontwikkelen die richting geven aan vervolgonderzoek. Aangezien met deze laatste stap een belangrijk deel van de inlichtingenbehoefte van de commandant wordt geformuleerd, wordt IPE afgerond in de stap

“Bepalen van de inlichtingenbehoefte” in de inlichtingencyclus. De drie stappen van IPE worden in de volgende paragrafen kort beschreven<sup>53</sup>.

Voorafgaand aan het uitvoeren van IPE wordt vastgesteld wat het AIR en het AII zijn (zowel geografisch als thematisch), wat het oogmerk is van de commandant, zijn visie op de operatie en wat de hieruit voortvloeiende inlichtingenbehoefte is.

### 3.7.2 *Environment Evaluation* (EE)

De EE richt zich op de inventarisatie, evaluatie en analyse van de geografische, hydrografische, meteorologische en oceanografische elementen (de fysische omgevingsfactoren) en de elementen van de Human Dimension inbegrepen de historische achtergronden van de operatieomgeving (de niet-fysische factoren). De EE moet leiden tot (sub)conclusies over de invloed en effecten die de onderzoekscategorieën hebben op het eigen optreden en op dat van de andere actoren. Een belangrijke subconclusie is het vaststellen welke elementen van de *Human Dimension* tot de groep van mogelijk gewelddadige actoren behoren.

De analyse en de beschrijving van het omgevingsbeeld vinden plaats door bestudering van de aanwezige actoren, factoren, processen en onderlinge verbanden binnen de context van de dynamische omgeving. De omgevingsanalyse is dus meer dan alleen het opnoemen van feiten en factoren van invloed, en moet nadrukkelijk ingaan op de wijze waarop deze factoren kunnen worden beïnvloed. De in NAVO veel gebruikte vorm voor het beschrijven van de omgevingsfactoren is het PMESII- model dat de omgeving analyseert aan de hand van de aspecten politiek, militair, economisch, sociaal, infrastructuur en informatie.

### 3.7.3 *Threat Evaluation* (TE)

De TE richt zich op de inventarisatie, evaluatie en analyse van alle beschikbare relevante informatie over mogelijk gewelddadige actoren die de uitvoering van de opdracht bedreigen. Daarbij wordt in het bijzonder gekeken naar de dispositie, capaciteiten, intenties en mogelijk te onderkennen modus operandi.

### 3.7.4 *Factor Integration* (FI)

In deze stap wordt, op basis van de (sub)conclusies van de EE en de TE, de dynamiek in de omgeving vertaald naar omgevings- en dreigingsscenario's.

<sup>53</sup> IPE zal in detail worden uitgewerkt in een inlichtingenbulletin "*Intelligence Preparation of the Environment*" dat verschijnt in 2011; dit bulletin kan in een later stadium als JDP-2.x.x., conform de doctrinehiërarchie, worden gepubliceerd.



De verschillende manieren waarop actoren zich in een omgeving zullen gedragen worden (*F*actor *I*ntegrated *S*cenario's genoemd). De wijze waarop mogelijk gewelddadige actoren kunnen of zullen optreden binnen deze omgevings- en dreigingsscenario's wordt *Enemy Course of Action* (ECOA) genoemd.

Bij scenario- en hypothesebouw worden logische, voorstelbare maar zeer zeker ook minder waarschijnlijke toekomstbeelden geschetst. Er kunnen twee soorten scenario's worden onderscheiden. Enerzijds de richtinggevende scenario's die alleen grove lijnen beschrijven naar een bepaald toekomstbeeld. Deze scenario's kunnen worden getoetst aan actuele inlichtingen. Op deze manier is het mogelijk tijdig te anticiperen op ontwikkelingen (*early warning*). Anderzijds zijn er de volledig uitgewerkte scenario's. Zij hebben een veel grotere mate van detaillering en kunnen daarom toegepast worden in de daadwerkelijke planning, uitvoering en bijsturing van (inlichtingen)operaties.

### 3.8 IPE BIJ DE BESLUITVORMING EN PLANNING

In deze paragraaf wordt gesproken over de wijze waarop de planning en besluitvorming worden ondersteund met inlichtingen door de toepassing van IPE. Eerst zal de generieke en de daarvan afgeleide militaire besluitvorming kort worden toegelicht. Vervolgens wordt per fase beschreven welke activiteiten uit IPE dit proces ondersteunen.

#### 3.8.1 Het generieke proces

Het generieke planningsproces bestaat uit de fasen doelbepaling, beeldvorming, oordeelsvorming en besluitvorming, waarna uitvoering en bijsturing plaatsvindt.

De doelbepaling betreft de keuze van het te bereiken doel. Als de keuze is bepaald, moet worden vastgesteld of het doel kan worden gerealiseerd en onder welke voorwaarden. Hierbij moet worden aangegeven binnen welke termijn, tegen welke prijs en met welke beschikbare middelen dit moet gebeuren.

De beeldvorming betreft de beeldopbouw van relevante aspecten van de situatie waarbinnen het doel moet worden bereikt, waarbij het beeld met betrekking tot de eigen sterke en zwakke punten en de mogelijke kansen en bedreigingen voortdurend dient te worden geactualiseerd.

De oordeelsvorming betreft de ontwikkeling en beoordeling van de mogelijkheden die leiden tot het bereiken van het doel. In deze fase wordt nagegaan welke mogelijkheden, gelet op de beschikbare middelen, binnen de gestelde tijd kunnen leiden tot het bereiken van het geformuleerde doel.

Eerst worden de effecten die kunnen bijdragen aan de realisatie van de doelstelling onderkend. Vervolgens wordt nagegaan welke acties nodig zijn om die effecten te bereiken en daarna wordt geïnventariseerd welke middelen daarvoor nodig zijn. Per mogelijkheid wordt getracht te voorspellen wat de reactie zal zijn op zowel elke afzonderlijke voorgestelde actie als op alle acties samen. Vervolgens identificeert men per mogelijkheid de voordelen, nadelen en risico's, evenals het beslag op de beschikbare middelen. Bij de besluitvorming wordt op basis van de analyse tijdens de beeldvorming en oordeelsvorming die mogelijkheid gekozen die het meest geschikt lijkt om het probleem op te lossen. Dit gebeurt door de commandant of de functionaris die binnen de organisatie belast is met de leiding en de autoriteit heeft om besluiten te nemen.

#### 3.8.2 De toepassing bij militaire operaties

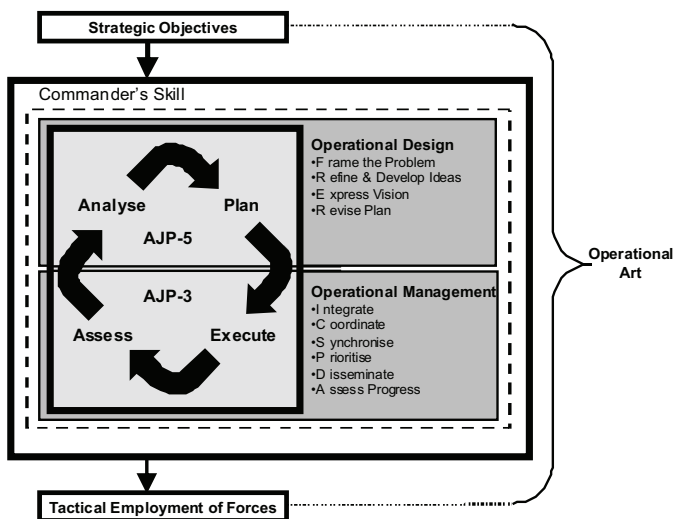
Militaire besluitvorming<sup>54</sup> vindt plaats binnen het bredere kader van *operational art*<sup>55</sup> en wordt gerealiseerd door een combinatie van capaciteiten van een commandant en de door de staf ondersteunde processen *operational design* en *operational management*.

*Operational design* formuleert het probleem en de dieper liggende oorzaken in de juiste context en ontwikkelt en verfijnt vervolgens de operationele ideeën van de commandant om de basis voor gedetailleerde en uitvoerbare plannen te leveren.

In de operatieomgeving wordt het probleem veroorzaakt door de diverse factoren en actoren (de drijvende krachten; *drivers*). De doelstellingen, intenties en modus operandi van de betrokken actoren verergeren of verminderen het probleem. Door het toepassen van de stappen EE en TE uit IPE worden de actoren met hun doelstellingen, intenties en modus operandi in de context van de operatieomgeving geplaatst en ontstaat een juist beeld voor de commandant en zijn probleemdefinitie. Vanuit de probleemdefinitie worden de doelen geformuleerd.

<sup>54</sup> Het NAVO OPP, beschreven in *Allied Joint Publication (AJP)-5 for operational planning*, dient als grondslag voor het besluitvormingsproces op operationeel en hoger tactisch niveau. Als primair planningsinstrument dienen de *Allied Command Operations (ACO) Guidelines for Operational Planning (GOP)*. Hierin zijn alle relevante aspecten van operationele planning beschreven. Het ACO GOP geeft richtlijnen over de in beschouwing te nemen planningsfactoren bij de ontwikkeling van een operationeel plan, en bevat de standaard structuur en inhoud van dit plan. Het GOP wordt in 2011 vervangen door de *Comprehensive Operations Planning Directive*.

<sup>55</sup> Zie JDP-5 Commandvoering, 2010.



omgevingsfactoren moeten voldoen en of die criteria eventuele bijsturing of stopzetting van de uitvoering van het plan nodig maken.<sup>56</sup> Deze criteria worden voorzien van indicatoren en opgenomen in het ICP.

*Operational management* integreert, coördineert en synchroniseert alle beschikbare middelen en capaciteiten en stelt prioriteiten bij de uitvoering van een operatie. Ook beoordeelt het voortdurend de voortgang ervan. De reacties vanuit de operatieomgeving hebben onvermijdelijk effect op het eigen optreden. Het evalueren van de voortgang van de operatie en het vervolgens snel reageren (om het plan zodanig te wijzigen dat de beoogde effecten onder de gewijzigde omstandigheden nog steeds kunnen worden gehaald) is daarom een belangrijke manier waarop een commandant een operatie leidt.



<sup>56</sup> Go, no-go en abort-criteria

Zodra de doelen zijn gedefinieerd wordt met een meer diepgaand onderzoek tijdens de EE en de TE een nauwkeurigere beschrijving van de doelen geformuleerd, zoals de locatie waar het doel zich bevindt, met eventueel het tijdstip waarop dit doel zich daar bevindt, de sterke punten en kwetsbaarheden van het doel evenals welke activiteit het op een bepaald moment onderneemt.

Gelijktijdig wordt nagegaan welke effecten bij kunnen dragen aan de realisatie van de doelstelling waarna wordt vastgesteld welke acties nodig zijn. Op basis hiervan worden mogelijkheden ontwikkeld en beoordeeld. Deze mogelijkheden worden op uitvoerbaarheid getoetst aan de operatieomgeving en er wordt bekeken wat vanuit de operatieomgeving de reacties kunnen zijn op de afzonderlijke voorgestelde acties en op alle acties samen. Per mogelijkheid wordt bekeken wat de voor- en nadelen, kansen en risico's en het beslag op eigen middelen zijn.

Om de ontwikkelde mogelijkheden aan de operatieomgeving te kunnen toetsen en de reacties hieruit te kunnen voorspellen, worden met behulp van de stap *Factor Integration* (op basis van de conclusies uit de EE en de TE) scenario's en hypotheses ontwikkeld, waarbinnen mogelijke bewegingen en activiteiten worden aangegeven van doel(f)actoren en (f)actoren in de omgeving die door neveneffecten kunnen worden getroffen (*collateral damage*). Per ontwikkeld plan wordt vastgelegd wat in de operatieomgeving de criteria zijn waaraan de

De ondersteuning van dit proces vergt toezicht op en beoordeling van de activiteiten en bewegingen van de actoren en factoren van invloed. De in de planningsfase ontwikkelde scenario's en hypothesen, evenals de criteria die bijsturing of stopzetting van het plan beogen, zijn hierbij leidend. De commandant en de staf dienen voor hun *awareness* continu van de situatie op de hoogte te worden gehouden. Als de waargenomen activiteiten en bewegingen niet meer voldoen aan de gestelde voorwaarden en het plan zodoende niet verder uitgevoerd of bijgestuurd kan worden, vindt operational *re-design* plaats.

Operational design vindt gedurende de gehele operatie plaats, waar nodig bijgestuurd door wijzigingen in de strategische richtlijnen. Het operational design wordt nooit als een afgeronde fase beschouwd, omdat de situatie altijd kan wijzigen. Daarom vormen periodieke heroverweging en verfijning de vaste elementen van een continue operational *re-design* wanneer een situatie daadwerkelijk wijzigt.

Naast veranderingen in de strategische richtlijnen kunnen ook een toename of een afname van het vermogen van de drijvende krachten, of het zich ontwikkelen van nieuwe drijvende krachten, de oorzaak zijn van veranderingen in de dynamiek, en daardoor een heroverweging van het probleem noodzakelijk maken.

### 3.9 SAMENVATTING

Voor een goede GA en SA en een soepele planning en aansturing van de lopende of komende operatie(s) is een goed beeld van de operatieomgeving een eerste vereiste. Het inlichtingenproces speelt hierin een doorslaggevende rol. Dit proces wordt uitgevoerd door de toepassing van de inlichtingencyclus: een uit vier fasen opgebouwd model dat zorg draagt voor het tijdig aanleveren van relevante inlichtingen over deze operatieomgeving aan de commandant en de overige behoeftestellers. Een nauwkeurige formulering van de inlichtingenbehoefte is de start van een effectieve inlichtingencyclus.

De inlichtingencyclus wordt ondersteund door *Collection Co-ordination and Information Requirements Management*. Dit subproces vormt de basis voor een effectieve en efficiënte inrichting van het verzamelplan. Aan de hand van dit plan worden door de verzamelorganen met hun specifieke verzamelmethode doelgericht gegevens en informatie verzameld. De verkregen informatie wordt in de verwerkingsfase omgezet in relevante inlichtingen door middel van een grondige analyse waarbij de informatie in zijn operationele context wordt geplaatst. De op deze wijze geproduceerde inlichtingen worden met behulp van snelle en accurate overdrachtsmethodes in de meest wenselijke presentatievorm aangeboden aan de commandant en de overige behoeftestellers.

Voor de praktische toepassing van de inlichtingencyclus zijn diverse werkprocedures vastgesteld, die in de internationale omgeving breed worden gedragen. Deze werkprocedures zijn afgestemd op de commandovoeringsprocessen waaraan zij moeten bijdragen, zoals het *Operational Planning Process* en diverse besluitvormingsmodellen op tactisch niveau. De inlichtingenstaf is op zijn niveau verantwoordelijk voor het aanleveren van de inlichtingen die de commandant nodig heeft voor zijn besluitvormings- en *targeting* proces en zijn te nemen veiligheidsmaatregelen. Informatie ten behoeve van de inlichtingenproductie verwerft de staf deels door inzet van eigen middelen in de AIR, maar ook van andere schakels uit de inlichtingenketen. Daarnaast wordt in de keten de inzet van verzamelactiviteiten gecoördineerd en verwerkingscapaciteit uitgewisseld. Informatieuitwisseling in de keten zorgt voor de opbouw en een verdichting van de GA en SA.

Door de toepassing van IPE wordt een grondige bestudering van de operatieomgeving uitgevoerd. Door de drie onderzoekscomponenten (*human dimension*, weer en terrein) te inventariseren, te evalueren en te analyseren en de uitkomsten hiervan te beschouwen in hun historische context, is de inlichtingenstaf in staat conclusies te trekken over de invloeden van de actoren en factoren in de operatieomgeving. Hiermee worden scenario's ontwikkeld en hypothesen opgesteld om een voorspellend vermogen te genereren. Met de conclusies en scenario's wordt de commandant in staat gesteld de kansen en de risico's voor zijn optreden vast te stellen. Daarnaast geven de uitkomsten van IPE ook voor een groot deel richting aan het samenstellen van het ICP.

Op het operationele niveau vinden *operational design* en *operational management* plaats om een optimale uitvoering van een militaire operatie te bewerkstelligen. In iedere fase van deze processen bestaat een specifieke inlichtingenbehoefte, waarin met behulp van IPE wordt voorzien.

## 4 CONTRA-INLICHTINGEN EN VEILIGHEID (CI&V)

### 4.1 INLEIDING

Contra-Inlichtingen en Veiligheid (CI&V) omvat de aspecten van dreiging tegen defensiepersoneel, defensiemiddelen en activiteiten die veroorzaakt worden door spionage, sabotage, subversie en terrorisme (SSST). CI benadert deze aspecten met dezelfde processen en procedures die ook worden gevolgd bij de inlichtingenondersteuning van besluitvorming voor operaties<sup>57</sup>. CI wordt toegepast vanaf politiek-strategisch niveau tot de laagste niveaus binnen de krijgsmacht. Op ieder niveau wordt vastgesteld waartegen de activiteiten van vijandige SSST zich kunnen richten. De hierbij geformuleerde SSST-doelen variëren van elementen die van belang zijn voor het functioneren van de Nederlandse samenleving als geheel, tot elementen van de krijgsmacht zelf die afscherming en bescherming vereisen. Op basis hiervan wordt door de commandanten de CI-inlichtingenbehoefte gesteld, waarna de CI een inlichtingencyclus doorloopt.

Uiteindelijk volgen hieruit adviezen aan de commandanten over te nemen beschermings- en beveiligingsmaatregelen, welke uitmonden in te nemen maatregelen die de veiligheid (V) optimaliseren.

In dit hoofdstuk wordt eerst ingegaan op het vaststellen van de CI-dreiging, vervolgens op de hieraan gekoppelde veiligheid (V) en ten slotte op de internationale afspraken.

### 4.2 DE DREIGING VAN SSST

De dreiging van SSST is onder te verdelen in een directe en een indirecte dreiging. De dreiging bestaat voornamelijk uit *Foreign<sup>58</sup> Intelligence Services* (FIS), groeperingen en/of individuen van subversieve, terroristische en/of criminele organisaties, *Special Forces* van een tegenstander, surveillance en verkenningen door IMINT- en/of SIGINT- verzamelorganen en bestaat uit individuen zonder vastgestelde doelen. De inlichtingenvergaring over vijandige SSST gebeurt met dezelfde onderzoeks- en analysemethoden als de generieke inlichtingenvergaring. De SSST-dreiging richt zich op personen, fysieke infrastructuur, informatie (systemen) en industrie.

<sup>57</sup> Waar in dit hoofdstuk wordt gesproken over operaties worden ook andere activiteiten bedoeld, zoals oefeningen, oefenreizen, havenbezoeken, logistiek transport, etc.

<sup>58</sup> Er wordt dus niet gesproken over vijandelijke (*hostile*) inlichtingendiensten.

#### 4.2.1 Directe dreiging

Directe dreiging bestaat uit het voorbereiden en uitvoeren van gerichte activiteiten door tegenstanders, met inbegrip van hun sympathisanten, tegen een duidelijk te definiëren doel. Hieronder wordt verstaan een onderdeel van de eigen organisatie, zoals een persoon, een eenheid of een opdracht. Bij het uitvoeren van operaties zal de tegenstander zijn eigen inlichtingensysteem gebruiken voor informatie- en inlichtingenvergaring ten behoeve van militaire operaties, offensieve informatieoperaties, sabotage en spionage.

Tegen directe dreiging kan een commandant OPSEC-maatregelen nemen.

#### 4.2.2 Indirecte dreiging

De indirecte dreiging wordt gevormd doordat (potentiële) tegenstanders een inlichtingenbeeld opbouwen en door de gerichte beïnvloeding van de moraal, de loyaliteit of de betrouwbaarheid van individuen in onze samenleving.

Deze dreiging wordt gevormd door:



*spionage* (inlichtingenvergaring door bijvoorbeeld het hacken van computers of overt HUMINT-activiteiten);

*subversie* (door het openlijk verspreiden van tendentieuze informatie (propaganda), het toebrengen van imagoschade, het heimelijk beïnvloeden van bestaande organisaties die (mogelijk) deloyaal zijn, het infiltreren in lokale organisaties en het werven van deloyale personen als bronnen of agenten);

*sabotage* (het vernielen of het vernietigen van essentieel materieel, zoals kritieke infrastructuur en aanvoerlijnen, maar ook het lekprikken van banden van militaire voertuigen op een kazerne en het vernielen van de cockpit van een vliegtuig);

*terrorisme* (zoals zelfmoordaanslagen in combinatie met het gebruik van *Improvised Explosive Devices*) en;

*georganiseerde misdaad*.

Georganiseerde misdaad kan naast zijn verwevenheid met de andere SSST-elementen op zichzelf al een destabiliserend effect hebben. Indien tegen de georganiseerde misdaad actief wordt opgetreden, zal dit over het algemeen een verantwoordelijkheid zijn voor de *Host Nation Government* en de lokale politie.

## 4.3 DE BEVEILIGINGSMAATREGELEN TEGEN SSST

Iedere commandant is op zijn niveau verantwoordelijk voor CI&V. Dit houdt in dat hij ervoor moet zorgen dat de CI-dreiging wordt vastgesteld, dat beveiligingsmaatregelen tegen deze dreiging worden afgewogen en dat de vastgestelde maatregelen worden uitgevoerd. Door de Beveiligingsautoriteit (BA) zijn voor de SSST-dreiging tegen personen, fysieke infrastructuur, informatie(systemen) en industrie maatregelen vastgelegd in het Defensie Beveiligingsbeleid (DBB). Het doel van het DBB is het helpen waarborgen van de betrouwbaarheid van de bedrijfsprocessen van het ministerie van Defensie voor een ongestoorde uitoefening van zijn taken.<sup>59</sup> De uitvoering van dit beleid ligt zowel bij de MIVD (o.a. opstellen van dreigingsanalyses en voorstellen doen voor te nemen maatregelen) als bij de beveiligingscoördinatoren (BC'n) van de Operationele Commando's (o.a. de uitvoering en de controle op de naleving van de vastgestelde maatregelen en beveiligingsplannen,

en rapporteren over de toestand van de beveiliging en incidenten).<sup>60</sup> De CDS draagt de eindverantwoordelijkheid voor de coördinatie met en tussen de OPCO's, het stellen van prioriteiten in de toewijzing van beveiligingsmiddelen en het opstellen en vaststellen van de beveiligingsparagraaf in de operatieplannen en de implementatie hiervan. Voor de aandachtsgebieden komen de maatregelen op het volgende neer:

### 4.3.1 Personele beveiliging

Personele beveiliging betreft het geheel van maatregelen om het militaire en burgerpersoneel van Defensie te beschermen tegen invloeden die hun betrouwbaarheid (kunnen) ondermijnen. Tevens stellen deze maatregelen zeker dat het personeel de toegewezen taken loyaal zal uitvoeren. Enkele van deze maatregelen zijn het veiligheidsonderzoek, het instellen van veiligheidsmachtigingniveaus (VMN) voor bepaalde functies en de afgifte van de Verklaring van Geen Bezwaar (VGB). Ook andere internationale organisaties waarbij Nederlands personeel werkzaam kan zijn, stellen eisen op het gebied van personele veiligheid (bijvoorbeeld NAVO, EU, VN en eventueel andere samenwerkingsverbanden). Een onzorgvuldig gebruik van moderne communicatievormen op het internet (*cyberspace*) vormt een risico voor de privacy van defensiepersoneel en de bedrijfsvoering van de defensieorganisatie. Het internetgebruik heeft een nauwe relatie met de informatiebeveiliging. De Veiligheidsfunctie vervult een belangrijke rol in het beheersen van deze bedreiging.

### 4.3.2 Fysieke beveiliging

De fysieke beveiliging betreft het nemen van actieve en passieve beveiligingsmaatregelen voor terreinen, militaire installaties, gebouwen of faciliteiten waar te beschermen belangen voor de defensieorganisatie aanwezig zijn. Deze maatregelen zijn onderverdeeld in organisatorische, bouwkundige en elektronische beveiligingsmaatregelen (OBE-maatregelen).

### 4.3.3 Informatiebeveiliging

Informatiebeveiliging bestaat uit de beveiliging van informatie en IT-diensten (inclusief verbindingbeveiliging). Hierbij gaat het erom het verlies of de compromittatie van informatie, in welke vorm dan ook, te voorkomen. En om de beschikbaarheid, integriteit en exclusiviteit (vertrouwelijkheid) te waarborgen van informatie die verwerkt, opgeslagen of getransporteerd wordt met behulp van IT-diensten.

<sup>59</sup> Bron: Defensie Beveiligings Beleid dd. 15 maart 2007

<sup>60</sup> In de CDS Aanwijzing 200 (MIVD ondersteuning op het gebied van CI&V bij vredesoperaties) heeft de CDS richtlijnen neergelegd voor de ondersteuning door de MIVD op het gebied van CI&V.

#### 4.3.4 Industriebeveiliging

Industriebeveiliging is de samenstelling van beschermende maatregelen en procedures om schade te voorkomen aan de belangen van de staat en/of zijn bondgenoten, waaronder het voorkomen van misbruik van bijzondere (gerubriceerde) informatie, die zich buiten de defensieorganisatie bevindt. In de ABDO-regeling<sup>61</sup> wordt verder aangegeven hoe dit toegepast moet worden.

### 4.4 INTERNATIONALE AFSPRAKEN

Ondanks het feit dat de CI&V-taak een nationale verantwoordelijkheid is, hebben de NAVO-lidstaten de verplichting om vooraf overeengekomen informatie te delen. Daarnaast zijn de lidstaten overeengekomen dat de *host nations* primair verantwoordelijk zijn voor NAVO-installaties op hun grondgebied. Alleen de militaire installaties van *de Strategic Commands Allied Command Operations (ACO)* en *Allied Command Transformation (ACT)* beschikken over een gezamenlijke CI-organisatie: de *Allied Command Counter Intelligence (ACCI)*<sup>62</sup>. Tijdens *Out-of-Area (OOA)* operaties kan de CI-verantwoordelijkheid worden gedelegeerd aan de NAVO-Commandant ter plaatse, die daarvoor beschikt over een ACCI-detachement. Dit detachement en de ter plaatse aanwezige CI-diensten werken tijdens OOA-operaties binnen het zogenaamde *Combined Forces CI concept (CFCI)*. Nationale wetgeving van de *Host Nation* en internationale verdragen mogen hierbij niet worden geschonden.

Bij niet-NAVO operaties worden er op CI&V-gebied aparte afspraken gemaakt. Bij multinationale operaties wordt dit gedaan met de aan de operatie deelnemende landen. Bij nationale operaties gebeurt dit met de deelnemende organisaties.

### 4.5 SAMENVATTING

Het werkveld van CI&V betreft de dreiging die uitgaat van SSST en de daartegen te nemen maatregelen. De dreiging kan direct en indirect zijn en wordt vastgesteld door CI.

De hiertegen te nemen veiligheidsmaatregelen (V) zijn door de BA vastgelegd in het DBB en voor uitvoering opgedragen aan de MIVD en de Beveiligingscoördinatoren van de Operationele Commando's en defensieonderdelen.

Deze maatregelen zijn ingedeeld in vier categorieën, te weten; personele beveiliging, fysieke beveiliging, informatie beveiliging en industriebeveiliging.

CI&V is een nationale verantwoordelijkheid. Binnen deze verantwoordelijkheid zijn de NAVO-lidstaten overeengekomen dat voor NAVO-installaties op hun grondgebied de *host nation* verantwoordelijk is. Voor militaire installaties van ACO en ACT en voor operaties buiten het verdragsgebied is het ACCI verantwoordelijk voor CI.

<sup>61</sup> Algemene Beveiligingsseisen voor Defensie Opdrachten

<sup>62</sup> Het ACCI is gevestigd te Mons (BE) binnen het hoofdkwartier van SHAPE.

# Bijlage 1 VERZAMELMETHODEN, -ORGANEN EN BRONNEN

## VERZAMELMETHODEN

### **Acoustic Intelligence (ACINT)**

ACINT zijn inlichtingen die zijn verkregen uit het verzamelen en verwerken van akoestische uitstralingen in het geluidsspectrum. ACINT kan gebruik maken van twee type bronnen. Ten eerste van bronnen die onbedoeld signalen uitstralen en geruis veroorzaken en ten tweede van bronnen die opzettelijke geluiden veroorzaken ten behoeve van communicatie, navigatie en/of lokalisatie (actieve uitzendingen). De akoestische analyse is zowel gericht op het detecteren, lokaliseren, classificeren en waar mogelijk identificeren van de bron als op het verkrijgen van technische inlichtingen.

ACINT-analyse gebeurt veelal real-time tijdens militaire operaties (t.b.v. *situational awareness*), maar ook tijdens een uitgebreidere analyse achteraf (veelal in Nederland) t.b.v. technische inlichtingen. Nederlandse verzamelcapaciteiten zijn beperkt tot het gebruik van mobiele sensoren bij militaire eenheden. Sommige andere landen maken daarnaast ook gebruik van statische sensoren zoals b.v. *Integrated Underwater Surveillance System* (IUSS) en *Unmanned Ground Stations* (UGS). Vlootseenheden en maritieme helikopters verkrijgen de ruwe akoestische informatie vooral met passieve akoestische sensoren of sonarapparatuur. Bij landoptreden en in de lucht, worden andere sensoren gebruikt. Dit gebruik wordt *Battlefield Acoustics* genoemd.

De interpretatie van akoestische informatie kan tactische inlichtingen opleveren over de gedragingen, de modus operandi en de tactische intentie van het onderschepte doel. ACINT wordt met name gebruikt op het operationele en tactische niveau. ACINT van passief geluid heeft ook strategische waarde omdat het, veelal blijvende, kwetsbaarheden van de opponent aantoonde.

### **Geospatial Intelligence (GEOINT)**

GEOINT produceert inlichtingen die afgeleid zijn van de analyse van georuimtelijke informatie (GEOINF) en beeldmateriaal (IMINT), om fysische kenmerken en geografisch gerelateerde activiteiten te beschrijven, te duiden en visueel uit te beelden. Door IMINT, GEOINF evenals overige inlichtingen te georefereren en in een GIS<sup>63</sup>-applicatie te verwerken, kunnen met behulp van speciale (geo/GIS) analysetechnieken patronen in gedragingen van personen en/of groepen en socio-economische activiteiten worden vastgesteld en vierdimensionaal worden gevisualiseerd. Deze visualisaties zijn GEOINT-

producten. GEOINT omvat een scala aan producten die variëren van eenvoudige rapporten tot zeer complexe - vierdimensionale - overzichten. Een *Go, No-Go layer* bijvoorbeeld kan een GEOINT-product zijn; en als input voor IPE dienen<sup>64</sup>.

### **Human Intelligence (HUMINT)**

HUMINT betreft inlichtingen die zijn afgeleid van door mensen verzamelde en geleverde informatie. Het verkrijgen van de benodigde informatie kan plaatsvinden door directe waarneming, zoals verkenning of observatie, debriefing en ondervraging en door meer indirecte methoden, zoals het gebruikmaken van gerekruteerde bronnen. Naast de HUMINT-activiteiten, uitgevoerd door speciaal hiervoor opgeleid personeel, kan ieder lid van het defensiepersoneel bij dragen aan HUMINT.

HUMINT ontleent grote waarde aan zijn vermogen informatie te verwerven die niet met technische middelen kunnen worden verkregen. HUMINT wordt in de regel verkregen door de inzet van speciaal opgeleid personeel, maar elk willekeurig personeelslid dat waarnemingen verricht of gesprekken met anderen voert, verwerft informatie. Indien gerapporteerd levert dit een grote hoeveelheid informatie op welke in een operatie bijdraagt aan de opbouw, instandhouding en verdichting van *situational awareness*. Bijzondere waarnemingen en gespreksinhoud kunnen zelfs direct bruikbare informatie opleveren.

Een categorie speciaal opgeleid personeel wordt gevormd door individuen en eenheden die verkenningen of surveillance uitvoeren, met het oogmerk informatie te vergaren. Deze categorie wordt gevormd door verkenningseenheden of reguliere eenheden met verkenning- of surveillanceopdrachten. Verkenningen en surveillance kunnen openlijk of discreet worden uitgevoerd.

Een volgende categorie (in het dagelijkse gebruik wordt de term HUMINT voor deze groep gebruikt) bestaat uit speciaal opgeleid personeel om gerekruteerde bronnen aan te sturen of gelegenheidsbronnen te bevragen en ondervragingen uit te voeren (*source operations*). Daarnaast worden door HUMINT-personeel *debriefings* verricht op het eigen personeel, vluchtelingen of personeel dat terugkeert uit een omgeving met een mogelijk hoge inlichtingenwaarde.

<sup>63</sup> GIS: Geografisch Informatie Systeem.

<sup>64</sup> Het verzamelen van GEOINF en het uitvoeren van GEOINT ten behoeve van expeditionaire operaties wordt bij CZSK ook wel aangeduid met de term *Rapid Environmental Assessment* (REA).



HUMINT-activiteiten kunnen worden onderverdeeld in openlijke (*overt*), discrete (*discrete*) en afgeschermd (*covert*) activiteiten. Er zijn voorwaarden verbonden aan de uitvoeringsvormen van HUMINT-activiteiten. Dit leidt er toe dat er onderscheid gemaakt moet worden in de opleidingseisen en de toepassing van methoden, technieken en het juridisch kader.

De openlijke activiteiten kunnen zichtbaar en herkenbaar worden uitgevoerd. Iedere militair die in gesprek komt met derden kan *overt* HUMINT toepassen.

*Discrete* HUMINT-activiteiten worden onopvallend en discreet uitgevoerd door hiervoor opgeleid en getraind personeel, omdat de gezochte informatie gevoelig kan zijn en zodoende de veiligheid van zowel de contactpersoon als de informatieverzamelaar kan aangaan. Tot deze categorie worden de leden van het *Field HUMINT Team* (FHT) gerekend, maar ook ondervragers die met gedetineerde personen spreken.

De afgeschermd (*covert*) manier van inwinnen van informatie wordt heimelijk uitgevoerd door daartoe aangewezen en bevoegde personen. Vanwege de hoge risico's wordt veel aandacht besteed aan de operationele veiligheid. Afgeschermd operaties vinden plaats onder nationale verantwoordelijkheid in opdracht van de minister en worden uitsluitend uitgevoerd door bevoegd personeel van de MIVD. Het personeel heeft daarbij de mogelijkheid om geüniformeerd of in burger op te treden.

### **Imagery Intelligence (IMINT)**

IMINT betreft inlichtingen die worden verkregen door de analyse en interpretatie van beeldmateriaal. Het voor IMINT gebruikte beeldmateriaal kan conventioneel (film, *hardcopy*) of elektronisch (digitaal, *softcopy*) geproduceerd zijn. Dit materiaal kan met behulp van diverse sensoren worden verkregen.

De sensoren bevinden zich op diverse platforms. Veelvoorkomende sensoren zijn: optisch, electro-optisch, infrarood, multi-spectraal, laser of radar. Optische sensoren zijn relatief eenvoudig te bedienen en kunnen door veel platforms (waaronder de mens) worden meegevoerd. Electro-optische sensoren kunnen een hoge mate van detail verwerken, maar zijn minder goed bruikbaar bij duisternis of slecht zicht. Infrarood geeft beeld van contrasten in temperatuurverschillen en is goed bruikbaar bij slecht zicht. Multi-spectraal sensoren bouwen beelden op aan de hand van verschillen in materiaalsoorten. Indien gevoelig genoeg, is de sensor in staat vluchtige materiaalsoorten in kaart te brengen, zoals chemische emissies, atmosferische veranderingen en elektromagnetische propagatie-karakteristieken.

Radar vormt beelden aan de hand van teruggekaatste energie. Laser is door de reflectie van verzonden pulsen in staat zeer nauwkeurig afstanden tot het doel vast te stellen. Hiermee kan onder andere adequaat elevatie worden bepaald en kunnen afstanden worden gemeten en daardoor kan de laser driedimensionale beelden opbouwen.

De producten worden niet alleen gebruikt bij de verwerking tot inlichtingen, maar kunnen ook inzicht geven in terreinomstandigheden bij de voorbereiding van een operatie of een actie.

### **Measurement and Signature Intelligence (MASINT)**

MASINT verkrijgt inlichtingen uit wetenschappelijke en technische informatie door kwantitatieve en kwalitatieve analyse van gegevens, afkomstig van sensoren die de identificerende en onderscheidende kenmerken van een doel, (stralings)bron of zender kunnen vaststellen, om te voorzien in diens omvang en identificatie. Bij MASINT worden ook forensische onderzoeksmethoden toegepast. Het "*measurement*"-deel van MASINT betreft de feitelijke metingen van parameters van een gebeurtenis of voorwerp. Het "*signature*"-deel is het product van meerdere metingen over langere tijd en onder verschillende omstandigheden. *Signatures* worden gebruikt om doelprofielen te ontwikkelen.

De bronnen die de gegevens aan kunnen leveren zijn sensoren die ook bij andere verzamelmethode worden ingezet, zoals de elektro-optische, radar, laser, multi-spectrale of geofysische data (IMINT), maar ook akoestische en seismische (ACINT), of elektro-magnetische en radiofrequentie data (SIGINT).

Forensisch onderzoek is sporenonderzoek dat gedaan wordt ten behoeve van het strafrechtelijk onderzoek. Het helpt bij het opsporen van de daders of de oorzaken van (mogelijke) misdrijven op basis van bewijsvoering. Van de vele onderzoeksgebieden die de forensische wetenschap kent, zijn de bekendste die gebruikt kunnen worden bij het verzamelen van informatie voor militaire operaties: de biometrie, dactyloscopie<sup>65</sup>, DNA-onderzoek, digitale sporen, documentonderzoek en ballistiek.

<sup>65</sup> Het zichtbaar maken, vergelijken en identificeren van vingerafdrukken

### **Medical Intelligence (MEDINT)**

MEDINT verkrijgt inlichtingen uit medische, biomedische, epidemiologische, milieu-/omgevingsinformatie en overige informatie gerelateerd aan humane factoren en/of diegezondheidsfactoren. MEDINT ondersteunt de besluitvorming, planning en voorbereiding voorafgaand en tijdens een operatie. Het geeft de commandant inzicht in de gezondheidsrisico's die van invloed kunnen zijn op de inzetbaarheid en de gevechtskracht. Dit moet resulteren in het nemen van de juiste beschermingsmaatregelen op gezondheidstechnisch gebied. Een onderdeel hiervan wordt gevormd door de identificatie en beoordeling van de medische infrastructuur in en nabij het missiegebied. Een analyse van de gezondheidstoestand van actoren van invloed en de door hen te gebruiken medische infrastructuur kan inzicht geven in hun vermogenstoestand en capaciteit tot behoud van dit vermogen. Gebaseerd op deze kennis kan de omgeving worden beïnvloed<sup>66</sup>.

Tevens kan deze analyse, in combinatie met de kennis van medische logistieke stromen in (de omgeving van) het operatiegebied, leiden tot inzicht in mogelijke intenties en mogelijke *Courses of Action* van actoren van invloed.<sup>67</sup>

De benodigde informatie wordt verkregen door medische *Information Requirements* en indicatoren vast te stellen en deze op te nemen in het ICP. Om deze vast te stellen en om medische informatie te kunnen analyseren en interpreteren is specifieke medische kennis nodig. Als deze kennis niet in een operationele staf aanwezig is, moet liaison worden uitgebracht met een geneeskundige staf. De meeste informatie wordt verkregen uit OSINT en uit internationale (NAVO) netwerken.

Om tot medische inlichtingen te komen, wordt de inlichtingencyclus toegepast. De door de commandant gestelde behoefte wordt omgezet naar medische *Information Requirements* met indicatoren. Deze zullen veelal te maken hebben met factoren van invloed op de gezondheid (en dus inzetbaarheid) van het personeel, zoals de in het missiegebied voorkomende endemische ziekten, hygiëneaspecten en klimaat- en milieufactoren.

<sup>66</sup> Het ter beschikking stellen van medische kennis en middelen kan, met name onder de bevolking, een positief effect hebben op de houding en het gedrag vanuit de omgeving op de operatie.

<sup>67</sup> Om te kunnen komen tot een beschouwing over intenties en *courses of action* van actoren van invloed is een uitgebreide medische informatie verzamel- en verwerkingscapaciteit nodig.

Daarnaast wordt informatie over inzetgebieden verzameld op het gebied van medische infrastructuur, nabijheid van havens/luchthavens, wegomstandigheden, etc. Deze informatie kan van belang zijn voor het bepalen van de benodigde medische evacuatieketen.

De gezondheidstoestand van actoren van invloed en de kwaliteit van de door hen te gebruiken medische infrastructuur kunnen van invloed zijn op de besluitvorming van de commandant. Enerzijds kan het de doelselectie beïnvloeden en anderzijds de wijze waarop hij het doel wenst te beïnvloeden. Dit onderzoek, gecombineerd met informatie over medische logistieke stromen, kan mogelijk inzicht verschaffen in intenties en *Courses of Action* van actoren van invloed.

Voor het vaststellen van medische IR's en indicatoren en het analyseren van de binnengekomen informatie is medische achtergrondkennis noodzakelijk. Hiervoor kan personeel met deze kennis worden opgenomen in de inlichtingenstaf van de operationele commandant, dan wel een liaison worden ingericht tussen de inlichtingenstaf en de medische staf.

Het verzamelen van medische informatie gebeurt bij voorkeur door personeel met medische kennis. In sommige gevallen is het mogelijk voor het verzamelen niet-medische verzamelorganen in te zetten. Bijvoorbeeld als de locatie waar de informatie verkregen kan worden zich buiten bereik van eerdergenoemd personeel bevindt. Tevens kan dit voorkomen als de IR's en indicatoren zodanig niet-medisch kunnen worden omschreven, dat dit in het reguliere verzamelproces kan worden uitgevoerd.

Delen van de benodigde informatie voor medische inlichtingen worden verkregen uit open bronnen (OSINT) en kunnen door eigen verzamelorganen en bronnen worden verkregen. Sommige informatie valt buiten het bereik van de eigen verzamelcapaciteit en kan middels RFI worden verkregen uit NAVO-middelen (o.a. NAVO *Medical Intelligence Expert Team* vallend onder COMEDS), overige nationale en internationale relaties van de DMG en/of overige medische staven (bijv. OPCO's, DOPS). Het verspreiden van de medische inlichtingen vindt plaats door de producten op te nemen in de bestaande verspreidingsmethoden.

### **Open Source Intelligence (OSINT)**

OSINT betreft inlichtingen die worden verkregen uit informatie uit publiekelijk toegankelijke bronnen zoals radio, televisie, internet, pers en andere ongerubriceerde

informatie. In toenemende mate wordt bij de verspreiding van informatie naast de traditionele bronnen (radio, televisie, pers etc.) gebruik gemaakt van (semi-) ongestructureerde informatiebronnen (bijvoorbeeld *chat-sites* en *weblogs*). De van deze laatste bronnen afkomstige informatie moet eerst worden voorbereid (*pre-processing*) voordat het verder verwerkt kan worden. Doorgaans is het verzamelorgaan dat de informatie aanlevert ook belast met de uitvoering van de bewerking. OSINT vormt een belangrijke aanvulling op andere methoden met name tijdens de analyse van de elementen van de *Environment Evaluation*. Het maakt voor de fysische omgevingsfactoren gebruik van openbare geografische, hydrografische, meteorologische en oceanografische studies en informatie en voor de *Human Dimension* van sociologische, demografische, culturele en etnologische studies en informatie. OSINT is de primaire bron voor basisinlichtingen.

### **Signals Intelligence (SIGINT)**

SIGINT is de generieke term om inlichtingen te beschrijven die worden verkregen uit informatie vanuit het elektromagnetische spectrum. Het omvat *communications intelligence* (COMINT) en *electronic intelligence* (ELINT). Met COMINT worden elektromagnetische tekst of spraakcommunicatiesignalen geïntercepteerd, gelokaliseerd en geanalyseerd, van communicatiemiddelen en verbindingssystemen in het elektromagnetisch spectrum door anderen dan de bedoelde ontvangers of gebruikers. Hierbij wordt de inhoud van het bericht beoordeeld (*communications-internal*) en de zenderkarakteristieken worden onderzocht waarmee het bericht wordt verzonden (*communications-external*), zoals frequentie, modulatie, codering, stemherkenning, etc.

ELINT betreft inlichtingen verkregen uit elektromagnetische niet-radio-uitzendingen door personen of instanties voor wie de uitzendingen niet zijn bestemd. Met ELINT worden elektromagnetische niet-communicatieve transmissies geïntercepteerd en gelokaliseerd, waarbij door analyse van de signalen de parameters worden gemeten en vastgelegd voor identificatie van bijvoorbeeld radar-, laser- en *non-imagery* infraroodsystemen.

*Computer Network Exploitation* (CNE) vormt een onderdeel van *Computer Networks Operations* (CNO). Met behulp van CNE wordt toegang verkregen tot programmatuur en gegevens die zich op computernetwerken bevinden. De NAVO beschouwt in haar doctrine CNO als een deel van *Information Operations* en dan meer specifiek als deel van Elektronische Oorlogvoering (EOV). Hierbij maakt CNE deel uit van COMINT.

### **Verzamelorganen**

Met verzamelorganen worden organisaties of personen aangeduid die betrokken zijn bij het verzamelen van informatie. Verzamelorganen passen een bepaalde verzamelmethode toe. Verzamelorganen met een eigen organieke verwerkingscapaciteit kunnen *single-source* inlichtingen leveren; verzamelorganen zonder verwerkingscapaciteit kunnen dit niet. Voor de meeste bronnen dient een voorbereiding (*pre-processing*) te worden uitgevoerd om de informatie geschikt te maken voor verdere verwerking. Doorgaans is het verzamelorgaan dat de informatie aanlevert ook belast met de uitvoering van de voorbereiding.

### **Bronnen**

Een bron is een persoon, voorwerp, zaak of gebeurtenis waaraan informatie kan worden ontleend. Gecontroleerde bronnen kunnen bestaan uit eigen personeel, eenheden en sensoren van eigen verzamelorganen. Ongecontroleerde bronnen zijn geselecteerde personen of organisaties die op grond van hun kennis of positie informatie zouden kunnen leveren, maar hiertoe niet kunnen worden verplicht. Zulke bronnen kunnen zijn *key leaders*, *powerbrokers* of functionarissen behorend tot (semi)overheids- of politieke organisaties, maar ook de diverse media. Een andere groep wordt gevormd door eventueel te ondervragen personeel, buitgemaakte documenten en stukken materieel. Gelegenheidsbronnen kunnen, zoals het woord al aangeeft, bij gelegenheid informatie leveren, zoals vluchtelingen, *walk-ins*<sup>68</sup> en overlopers.

Een aparte categorie die bij alle bronsoorten kan worden ingedeeld, zijn materiedeskundigen. Zij zijn terug te vinden bij (inter)nationale overheidsorganisaties- of bij private organisaties en bedrijven, zoals universiteiten en scholen. Het vaststellen van de waarde van een bron wordt beschreven in de volgende bijlage.

<sup>68</sup> Personen, die zich bij militaire instanties melden en informatie aanbieden.

## Bijlage 2 BRON-, INFORMATIE- EN INLICHTINGENEVALUATIE

De besluitvorming van de commandant en het vaststellen van de doelstellingen en de uitvoering van operaties kunnen afhankelijk zijn van de wetenschap dat inlichtingen zijn gebaseerd op feiten of op aannames. De inlichtingenstaf geeft bij de presentatie van de beschrijving over de operatieomgeving een waardeoordeel over de feitelijkheid van zijn conclusies. Dit waardeoordeel is gebaseerd op de evaluatie van de bron en de geleverde informatie, in principe aan de hand van de in STANAG 2511 vastgelegde normen. Deze normen kunnen door de JFC anders worden bepaald.

### Evaluatie van de bron

De bronevaluatie in een rapport is samengesteld uit meerdere delen. De evaluatie beschrijft zowel de historische ervaring met de bron zelf, de directe kennis van de bron over de geleverde informatie en het inzicht van de bron in de geleverde informatie. Een vierde element is de nabijheid van de bron ten opzichte van de informatie. Het vijfde element van bronevaluatie is de toepasselijkheid van de informatie (de relatie tussen de aard van de bron en de aard van de informatie).

### Evaluatie van de informatie

De door de bron geleverde informatie wordt afzonderlijk geëvalueerd. Allereerst wordt de geloofwaardigheid van de informatie geschat, waarbij rekening moet worden gehouden met al dan niet bewuste misleiding. Vervolgens wordt bekeken of de geleverde informatie redelijkerwijs aansluit bij andere informatie over het onderwerp. Die verwachting is vooral gebaseerd op de kennis die de analist over het onderwerp heeft.

#### Waardering van de bron

Code	Waardering	Verklaring
A	Volledig betrouwbaar	Geen twijfel aan echtheid, geloofwaardigheid of kennis. De bron is voorheen altijd betrouwbaar gebleken.
B	Doorgaans betrouwbaar	Geringe twijfel aan echtheid, geloofwaardigheid of kennis. De bron heeft voorheen meestal geldige informatie geleverd.

C	Redelijk betrouwbaar	Twijfel aan echtheid, geloofwaardigheid of kennis. De bron heeft voorheen wel geldige informatie geleverd.
D	Gewoonlijk niet betrouwbaar	Aanzienlijke twijfel aan echtheid, geloofwaardigheid of kennis. De bron heeft voorheen wel geldige informatie geleverd.
E	Onbetrouwbaar	Gebrek aan echtheid, geloofwaardigheid en kennis. De bron heeft voorheen geen, of geen geldige informatie geleverd.
F	Geen oordeel	Geen referentie voor waardeoordeel aanwezig.

#### Waardering van de informatie

Code	Waardering	Verklaring
1	Bevestigd	Bevestigd door andere, onafhankelijke bronnen; logisch samenhangend, in overeenstemming met andere informatie over hetzelfde onderwerp.
2	Waarschijnlijk correct	Niet bevestigd, logisch samenhangend, in overeenstemming met andere informatie over het onderwerp.
3	Mogelijk correct	Niet bevestigd, redelijk samenhangend, komt deels overeen met andere informatie over het onderwerp.
4	Twijfelachtig	Niet bevestigd, mogelijk maar niet logisch, geen andere informatie over het onderwerp.
5	Onwaarschijnlijk	Niet bevestigd, omsamenhangend, in tegenspraak met andere informatie over het onderwerp.
6	Geen oordeel	Geen referentie voor waardeoordeel aanwezig.

### Confidence Levels, evaluatie van de inlichtingen

De inlichtingenstaf kent aan iedere analytische conclusie van een inlichtingenproduct een indicator toe voor de mate van vertrouwen die hij heeft in de juistheid van de conclusie, het *Confidence Level*. Met behulp van deze indicatoren worden de conclusies op een consequente manier voorgelegd aan de besluitvormers.

Deze *Confidence Levels* zijn feitelijk de verwoording van zowel de evaluatie van de bron en diens informatie en van de ervaring, de intuïtie en het oordeel van de analist. Soms worden gangbare termen als “(zeer) waarschijnlijk”, “mogelijk” en “(zeer) onwaarschijnlijk” gekoppeld aan percentages tussen 0% en 100% om de mate van vertrouwen te kwantificeren.<sup>69</sup> Historisch psychologisch onderzoek heeft uitgewezen dat groepen mensen een ongeveer gelijke waardebeleving hebben bij de genoemde steekwoorden.

Description of Probability or Confidence	Synonyms	Percentage
Highly Likely	Highly Probable We are convinced Virtually Certain Almost Certain High Confidence High Likelihood	> 90% 60 – 90%
Likely	Probable We estimate Chances are good High-Moderate Confidence Greater than 60% Likelihood	
Even Chance	Chances are slightly greater (or less) than Even (Chances are about Even Moderate Confidence Possible	40 – 60%
Unlikely	Probably not Not Likely	10 – 40%

69 <http://www.dcdc-strategictrends.org.uk/viewdoc.aspx?doc=1>

	Improbable We believe ... not Low Confidence Possible but not Likely	
Highly Unlikely	Highly Improbable Nearly Impossible Only a slight Chance Highly Doubtful	< 10%

### Dreigingsniveaus<sup>70</sup>:

De Afdeling Inlichtingen van de MIVD hanteert een gestandaardiseerde systematiek, op basis van het begrip dreiging (\*) en dreigingsfactoren (\*\*), voor de bepaling van dreigingsniveaus. Hierbij wordt de dreiging bepaald aan de hand van de dreigingsfactoren *intentie, capaciteit / mogelijkheden* en *activiteit*.

Dreigingsniveau	Intentie		Middelen		Activiteit
Hoog	Sterk	en	Aanzienlijken		Hoog
Significant	Sterk	en	Aanzienlijk	en	Matig
Matig	Sterk	en	Beperkt	en	Matig
Matig	Beperkt	en	Aanzienlijk	en	Matig
Laag	Beperkt	en	Beperkt	en	Gering
Verwaarloosbaar	Geen	en	A/B/G	en	Geen
Onbekend	Onbekend	en/of	Onbekend	en/of	Onbekend

Dreigingsniveau	Mate van waarschijnlijkheid
Hoog	Bevestigd; er is sprake van een <b>acute</b> dreiging
Significant	Waarschijnlijk
Matig	Mogelijk
Matig	Mogelijk
Laag	Onwaarschijnlijk
Verwaarloosbaar	Zeër onwaarschijnlijk

(\*) Dreiging: “Een gevaar voor de levens van personen, voor de uitvoering van de missie, voor eigen en/of bondgenootschappelijke eenheden of, in een breder kader, de belangen van het Koninkrijk”.

(\*\*) *Samenstellende delen*.

70 Bron: MIVD: Handboek Inlichtingen voor de analist, DIS2009021353, (2009), p. 97.

## Bijlage 3 JURIDISCHE ASPECTEN – Wiv 2002

Alle inlichtingenvergaring dient te worden uitgevoerd in overeenstemming met nationale en internationale wetgeving (onder andere de Wet op de Inlichtingen- en Veiligheidsdiensten van 2002 - Wiv 2002). Enkele zaken zijn in het bijzonder relevant:

- De Wiv-2002 is formeel slechts van toepassing op activiteiten van de MIVD in Nederland en heeft daarom geen extraterritoriale werking. Ook is de Wiv-2002 niet van toepassing op andere I&V onderdelen van Defensie dan de MIVD.
- Wel heeft de Wiv-2002 ten aanzien van het optreden van de MIVD in het buitenland in principe een analoge werking.

### **Optreden in operatiegebieden in het kader van een militaire operatie**

Ten aanzien van het optreden van inlichtingenvergarende niet-MIVD onderdelen in een operatiegebied is het op de militaire operatie van toepassing zijnde internationale juridische kader grondslag biedend en kaderstellend.

Ook ten aanzien van het optreden van de MIVD in operatiegebieden in het kader van een militaire operatie is het op de militaire operatie van toepassing zijnde internationale juridische kader primair grondslag biedend en kaderstellend. De Wiv 2002 wordt daar waar mogelijk analoog toegepast voor zover dit (de omstandigheden van het operatiegebied in ogenschouw nemend) in de rede ligt.

### **Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv-2002)**

Alle verzamelactiviteiten, vooral HUMINT en SIGINT, zijn onderworpen aan strikte procedures en toezicht in overeenstemming met de artikelen en uitvoeringsbepalingen van de Wiv-2002, die een wettelijke basis verschaft voor het gebruik van onderzoekstechnieken.

### **Humanitair Oorlogsrecht**

Het HOR, zoals onder meer beschreven in de Verdragen van Genève met de daarbij behorende aanvullende protocollen, is kaderstellend voor het rechtsregime tijdens militaire operaties in het buitenland. Het doel van het HOR is een balans te realiseren tussen militaire noodzaak (de realiteit van geweldgebruik) en humaniteit (onnodig leed te voorkomen). Het HOR kent hiertoe bevoegdheden en beperkingen. De bevoegdheden betreffen voornamelijk het recht van combattanten om deel te nemen aan de vijandelijkheden. De beperkingen betreffen voornamelijk de regel aangaande de methoden en middelen van oorlogvoering en regels die toezien op bescherming van personen en goederen.

Het HOR is formeel van toepassing zodra er sprake is van een 'gewapend' conflict. Of daarvan sprake is, is een feitelijke kwalificatie, die niet afhankelijk is van (politieke) standpunten van strijdende partijen. Ook wanneer het HOR formeel niet van toepassing is, is het NAVO en Nederlands beleid om de beperkingen uit het HOR te hanteren als veilige marge bij het optreden van de Nederlandse krijgsmacht. Daarmee wordt voorkomen dat onduidelijkheid zou ontstaan over de bevoegdheden, afhankelijk van de soms mogelijk wisselende status van een vredesmacht in een conflictgebied.

### **Rules of Engagement (ROE)**

Voor alle militaire operaties gelden ROE. Nadat een staat een rechtsgrondslag heeft om buiten haar grondgebied op te treden, zullen voor de in te zetten militaire eenheden een heldere opdracht, een oogmerk en ROE moeten worden geformuleerd. ROE dienen altijd binnen de grenzen van het toepasselijke recht, waaronder het HOR, te blijven. ROE zijn richtlijnen voor commandanten ten aanzien van de aard en wijze van gebruik van militair vermogen binnen de politieke en juridische kaders. Ze worden ontworpen om te verzekeren dat politieke autoriteiten het gebruik van dit vermogen kunnen beheersen. ROE informeren commandanten over beperkingen of vrijheden bij het uitvoeren van hun toegewezen taken; ze zijn geen middel om specifieke taken toe te wijzen. ROE verschaffen ruimte voor het gebruik van militair vermogen; ze verplichten er niet toe. Commandanten mogen vigerende ROE altijd inperken voor ondercommandanten; zelfstandig uitbreiden mag nooit.

ROE zijn over het algemeen niet specifiek toegesneden op het verzamelen van informatie en vormen hiervoor ook niet het geëigende middel. Dit neemt niet weg dat de ROE wel meer algemene bevoegdheden of beperkingen bevatten die ook moeten worden gerespecteerd, zoals de mogelijkheid om middelen van elektronische oorlogvoering in te zetten of in geval van geografische beperkingen. De inlichtingenstaf moet zich bewust zijn van de ROE en vooral van de beperkingen die zij opleveren voor het verzamelen van informatie en de manier waarop dit het ICP kan beïnvloeden.

## Bijlage 4 VERKLARENDE WOORDENLIJST

### **Collection Co-ordination and Information Requirements Management (CCIRM)**

CCIRM is het geheel van activiteiten die zorgen voor het op doelmatige wijze verzamelen van de noodzakelijke informatie.

### **Commanders Critical Information Requirements (CCIR)**

Informatie over activiteiten van eigen eenheden en van actoren van invloed en de informatie uit en van de operatieomgeving, die de commandant kritisch acht voor het onderhouden van *Situational Awareness*, voor het plannen van komende activiteiten en ter ondersteuning van tijdige en goed onderbouwde besluitvorming.

### **Gebied van inlichtingenbelangstelling (Area of Intelligence Interest; AII)**

Geografisch of thematisch gebied dat die (f)actoren van invloed omvat, die in de ( nabije) toekomst hun invloed op de operatie kunnen doen gelden.

### **Gebied van inlichtingenverantwoordelijkheid (Area of Intelligence Responsibility; AIR)**

Geografisch of thematisch gebied dat die (f)actoren van invloed omvat die hun invloed op de operatie kunnen doen gelden. Het AIR wordt opgedragen aan de inlichtingenstaf om daarin zijn activiteiten te ontplooiën.

### **Indicatoren (Indicators)**

Informatie die de intentie of het vermogen tot handelen van een mogelijke actor of groep van actoren weergeeft om een *Course of Action* (CoA) te volgen of te wijzigen. De indicator uit zich in waarneembaar gedrag. Indicatoren zijn gegevens, activiteiten of het is een toestand die met doelopsporingsmiddelen, verzamelorganen of bronnen kan worden onderkend.

### **Inlichtingenbehoefte (Intelligence Requirements (IR))**

De behoefte van de commandant aan informatie betreffende (f)actoren in de operatieomgeving om de invloeden en dreiging daarvan op de uitvoering van de operatie vast te stellen, te bewaken en of kansen en gevaren te onderkennen.

### **Inlichtingenoperatie**

De planning, coördinatie, sturing van de activiteiten van doelopsporingsmiddelen, verzamelorganen, overige subeenheden en verwerkingselementen om in het kader van de lopende of komende operatie, binnen het gebied van inlichtingenverantwoordelijkheid, (doel)informatie te verwerven en om actuele inlichtingen te produceren.

### **Priority Intelligence Requirements (PIR; kernvragen)**

De essentiële inlichtingenbehoefte. Dat deel van de inlichtingenbehoefte waaraan de commandant een prioriteit heeft toegekend omdat de beantwoording van de eruit voortvloeiende vragen essentieel is voor zijn besluitvorming en bevelvoering.

### **Requests for Information (RFI)**

Een verzoek om informatie van de inlichtingenstaf aan andere inlichtingenstaven of speciale inlichtingenelementen of agencies.

## Bijlage 5 LIJST VAN AFKORTINGEN

Afkorting	Betekenis	Afkorting	Betekenis
AAP	Allied Administrative Publication	GEOINF	Geospatial Information
ACCI	Allied Command Counter Intelligence	GEOINT	Geospatial Intelligence
ACINT	Acoustic Intelligence	HUMINT	Human Intelligence
ACO	Allied Command Operations	I&V	Inlichtingen en Veiligheid
ACT	Allied Command Transformations	I&W	Indicators & Warning
All	Area of Intelligence Interest	ICP	Intelligence Collection Plan
AIR	Area of Intelligence Responsibility	ICT	Information & Communications Technology
AO	Area of Operations	IMINT	Imagery Intelligence
AOR	Area of Operational Responsibility	IR	Intelligence Requirement
BA	Beveiligings Autoriteit	JDP	Joint Doctrine Publicatie
BC	Beveiligings Coördinator (OPCO)	JFC	Joint Forces Command
C-	Commandant van ...	KMAR	Koninklijke Marechaussee
CCIR	Commanders Critical Information Requirements	LDP	Landmacht Doctrine Publicatie
CCIRM	Collection Co-ordination and Information Requirements Management	LMO	Leidraad Maritiem Optreden
CDS	Commandant der Strijdkrachten	MASINT	Measurement and Signature Intelligence
CI	Counter Intelligence	MEDINT	Medical Intelligence
CI & V	Contra-Inlichtingen en Veiligheid	MIVD	Militaire Inlichtingen- en Veiligheids Dienst
CIMIC	Civil-Military Co-operation	MV	Militaire Veiligheid
CLAS	Commando Landstrijdkrachten	MvD	Minister van Defensie
CLSK	Commando Luchstrijdkrachten	NAVO	Noord-Atlantische Verdrags Organisatie
CNE	Computer Network Exploitation	NDD	Nederlandse Defensie Doctrine
COA	Course Of Action	NIST	National Intelligence Support Team
COG	Centre Of Gravity	OA	Operations Area
COMEDS	Committee of the chiefs of military medical services in NATO.	OBE	Organisatorisch, Bouwkundig en Elektronisch
COMINT	Communications Intelligence	OPCO	Operationeel Commando
CZSK	Commando Zeestrijdkrachten	OPP	Operationeel Planning Proces
DBB	Defensie Beveiligings Beleid	OPSEC	Operations Security
DMG	Directie Militaire Gezondheidszorg	OSINT	Open Source Intelligence
DNA	Desoxyribonucleïnezuur	PIR	Priority Intelligence Requirement
ECoA	Enemy Course of Action	PMESII	Political, Military, Economic, Social, Infrastructural, Informational (environment)
EE	Environment Evaluation	REA	Rapid Environmental Assessment
ELINT	Electronic Intelligence	RFI	Request For Information
EOV	Elektronische Oorlogvoering	SA	Situational Awareness
FHT	Field HUMINT Team	SIGINT	Signals Intelligence
FI	Factor Integration	SSST	Spionage, Sabotage, Subversie en Terrorisme
FIS	Factor Integrated Scenario	TE	Threat Evaluation
FIS	Foreign Intelligence Services		



TTP	Tactics, Techniques and Procedures
VGB	Verklaring van Geen Bezwaar
VMN	Veiligheids Machtiging Niveau
Wiv-2002	Wet op de Inlichtingen- en Veiligheids Diensten van 2002

