

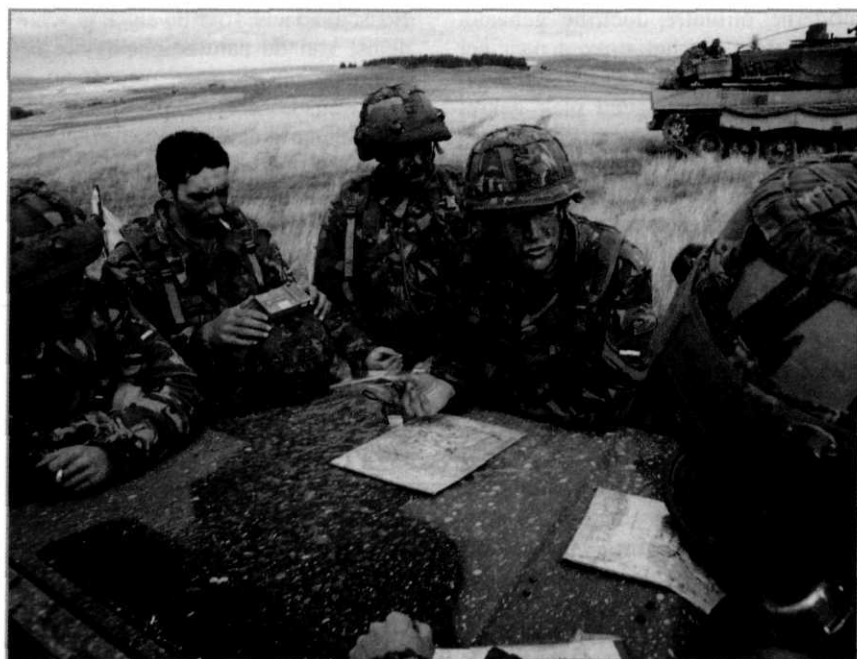
# Psychologische perspectieven op Informatie Operaties

dr. H.J. Griffioen-Young, drs. H.J.W. Janssen en prof. dr. A.W.K. Gaillard\*

## Inleiding

Een commandant in het veld krijgt een melding dat de vijand vanuit het noorden zal aanvallen. Deze informatie is echter tegenstrijdig met eerdere berichten dat de vijand vanuit westelijke richting komt. Wat gelooft de commandant? Moet hij de nieuwe informatie negeren, omdat de melding wellicht een poging tot misleiding is? Of moet hij deze informatie serieus nemen en zijn besluitvorming erop aanpassen? Tegenstrijdige informatie maakt een commandant onzeker en ondermijnt de commandovoering. Dit voorbeeld laat zien hoe door de manipulatie van informatie de daadkracht aangetast kan worden, en benadrukt het belang van *Informatie Operaties* in het moderne militaire optreden.

Informatie Operaties (Info Ops) zijn activiteiten gericht op het beïnvloeden van beslissers ter ondersteuning van politieke en militaire doelstellingen door de informatie, besluitvormingsprocessen, commandovoerings-



## Besluitvorming in het veld

middelen en ondersteunende communicatie en informatiesystemen van een opponent aan te grijpen en gelijktijdig de eigen informatie, processen en systemen te benutten en te beschermen. Er zijn twee vormen van Info Ops: defensieve en offensieve, afhankelijk van de aard van de betreffende activiteiten (Beleidskader *Information Operations*, 2001).<sup>1</sup>

Het doel van offensieve Info Ops is het besluitvormingsproces van de tegenstander te beïnvloeden door zijn informatiesystemen en -stromen te verstoren of te manipuleren. Bij defensieve Info Ops gaat het om het beschermen van de eigen informatie-

systemen, zodat het eigen besluitvormingsproces niet verstoord kan worden door de tegenstander. Wanneer we meer inzicht hebben in offensieve Info Ops, weten we ook beter hoe we ons tegen Info Ops van de tegenstander kunnen beschermen.

In dit artikel beschrijven we allereerst de offensieve mogelijkheden van Info Ops, waarbij het met name gaat om de gevolgen van het manipuleren van informatie. Vervolgens gaan we in op de defensieve kant van Info Ops. Hierbij beschrijven we hoe gemanipuleerde informatie kan worden herkend en hoe schadelijke effecten kunnen worden beperkt. Tot slot illustre-

\* De auteurs zijn werkzaam bij TNO Technische Menskunde als wetenschappelijk onderzoeker.

<sup>1</sup> De Engelstalige definitie van de NAVO luidt: 'Information Operations are actions taken to influence decision-makers in support of political and military objectives by affecting other's information, information based processes, command and control capabilities and supporting communication and information systems while exploiting and protecting one's own. There are two categories of Info Ops: defensive Info Ops and offensive Info Ops, depending upon the nature of the actions involved' (MC-422).

ren we dit met de resultaten van een onderzoek dat door ons werd uitgevoerd.

## **Informatiemanipulatie**

Om politieke en militaire doelstellingen te bereiken, proberen we het gedrag van de tegenstander te sturen in een gewenste richting. Het gaat vooral om het beïnvloeden van het denken en handelen van personen die beslissingen nemen. Daarvoor is het belangrijk te weten hoe mensen informatie verwerken, hoe zij beïnvloed kunnen worden en wat de zwakke plekken in het besluitvormingsproces zijn.

Figuur 1, dat bekend staat als de Lasswell-formule (1948) geeft weer welke factoren bijdragen aan het succes van een beïnvloedingspoging. Het beïnvloeden van mensen wordt gezien als

een vorm van communicatie waarin vier factoren worden onderscheiden: bron, boodschap, medium en ontvanger. We kunnen de factoren opsommen met de vraag wie zegt wat op welke wijze tegen wie?

De mate van beïnvloeding wordt bepaald door een ingewikkeld samenspel tussen de verschillende factoren. Zo kan één factor een bepaald effect hebben in combinatie met een tweede factor, maar een totaal ander effect in combinatie met een derde. Mensen die bijvoorbeeld zeer betrokken zijn bij een onderwerp laten zich niet overtuigen door irrelevante kenmerken van de persoon die de boodschap brengt, zoals zijn aantrekkelijkheid, maar wel door sterke argumenten. Anderzijds laten mensen die niet zo betrokken zijn bij het onderwerp zich juist wel overtuigen door kenmerken zoals aantrekkelijkheid van de bron. In dit geval is het dan ook meer een

kwestie van een mooi verhaal in plaats van een goed verhaal (Petty, Cacioppo & Goldman, 1981; Griffioen-Young, 2000; Janssen & Griffioen-Young, 2001).

Info Ops is gericht op het bemoeilijken van de besluitvorming van de tegenstander door de informatie waarover de tegenstander beschikt te manipuleren. Dit kan op de volgende manieren:

### **Informatie verwijderen**

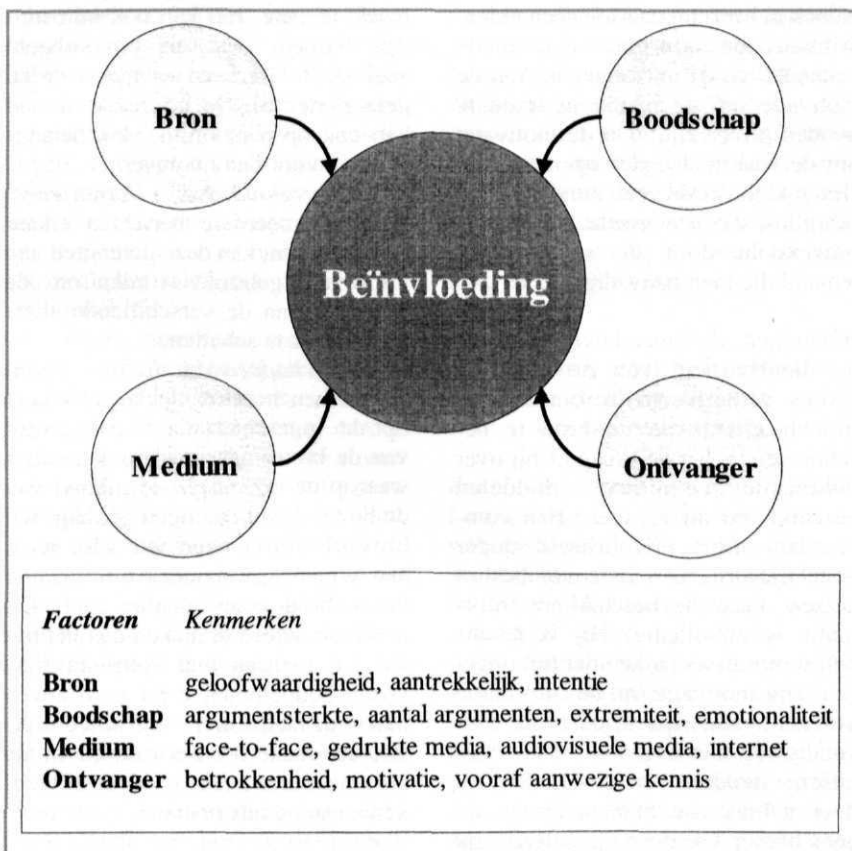
Het verwijderen van essentiële informatie verstoort het besluitvormingsproces en kan leiden tot verkeerde beslissingen. Wanneer informatie onvolledig is, kan men geen goed beeld van de situatie vormen en wordt het nemen van een goede beslissing ernstig bemoeilijkt.

### **Informatie toevoegen**

Het toevoegen van informatie kan het besluitvormingsproces op twee manieren verstoren. Ten eerste kan onjuiste informatie de ontvanger op het verkeerde been zetten en leiden tot verkeerde beslissingen. Ten tweede kan men zoveel informatie toevoegen dat *information overload* ontstaat: door de grote hoeveelheid informatie kunnen mensen het niet meer onthouden en verwerken, waardoor essentiële informatie over het hoofd wordt gezien, of er aanzienlijk meer tijd en mankracht nodig is om alle informatie te verwerken.

### **Informatie wijzigen**

Men kan de bron, de ontvanger en de inhoud van de boodschap wijzigen. Informatie van een bron met veel aanzien vindt men vaak betrouwbaarder en belangrijker dan informatie van een bron met weinig aanzien. Dus door het wijzigen van de bron kan men ervoor zorgen dat de ontvanger de informatie anders beoordeelt, en meer prioriteit geeft. Ook kan men ervoor zorgen dat informatie niet bij de juiste ontvanger aankomt. Als een willekeurige operator de informatie krijgt die eigenlijk voor de commandant bedoeld is, kan de inhoud ervan verloren gaan, omdat de operator de



**Fig 1. Beïnvloedingsmodel**

informatie niet begrijpt, of niet weet voor wie de informatie bedoeld is. Tot slot kan men de inhoud van een boodschap wijzigen, zodat er een onjuist beeld van de situatie ontstaat.

### Waar of niet waar?

Het nemen van juiste beslissingen is essentieel voor het succes van een militaire operatie. Verkeerde beslissingen kunnen ingrijpende consequenties hebben voor de betrokkenen, de uit te voeren operatie en zelfs de politieke verhoudingen. Wanneer informatie binnenkomt is het vaststellen van de juistheid ervan daarom van groot belang. Maar hoe maken wij een onderscheid tussen leugens en de waarheid?

#### Voordeel of nadeel van de twijfel?

Wanneer we eenmaal weten dat iemand liegt of dat bepaalde informatie onwaar is, zijn we beter in staat met die persoon of de onjuiste informatie om te gaan. Helaas is het in de praktijk vaak moeilijk leugenaars en leugens te herkennen. Onder normale omstandigheden gaan wij er vanuit dat mensen de waarheid spreken. Als wij dit niet zouden doen, zou de omgang met anderen nagenoeg onmogelijk worden. Immers, als we bij alles wat we te horen krijgen ons moeten afvragen of het wel of niet waar is, kunnen we nauwelijks nog functioneren. Het ervan uitgaan dat anderen altijd de waarheid vertellen heet het *waarheidsvooroordeel*. Met name als wij een persoonlijke band hebben met iemand, of als iemand veel aanzien of een hoge positie heeft, zijn we geneigd die persoon zonder meer te geloven.

Het omgekeerde bestaat echter ook. Het *leugenvooroordeel* is het fenomeen dat men zonder meer aanneemt dat iemand liegt. Vooral als we eenmaal twijfelen aan iemands betrouwbaarheid, zijn we geneigd te denken dat alle informatie van deze persoon onwaar is. Zowel bij het waarheids- als leugenvooroordeel wordt binnenkomende informatie

niet meer kritisch beoordeeld, maar krijgt a priori het label waar of onwaar.

In de meeste gevallen zullen mensen uitgaan van het waarheidsvooroordeel. Als iemand geen reden heeft om aan de betrouwbaarheid van de bron te twijfelen, zal hij het waarheidsvooroordeel blijven gebruiken, ook wanneer er signalen zijn dat dit niet verstandig is. Wanneer een informant altijd juiste informatie doorspeelt, zal de commandant daarop vertrouwen zolang hij geen reden heeft om aan te nemen dat de informatie onjuist is. Wanneer de informant inmiddels is omgekocht door de tegenstander en onjuiste informatie doorspeelt, zal de commandant nog lange tijd uitgaan van de juistheid ervan.

Ook wanneer een ontvanger niet gemotiveerd is om aan de betrouwbaarheid van de bron te twijfelen, zal hij aannemen dat de informatie waar is, ook al heeft hij daartoe geen reden. Wanneer de informant een goede bekende van de ontvanger is, kan de motivatie om de relatie in stand te houden groter zijn, dan de motivatie om de waarheid onder ogen te zien. Het lijkt daarom veel minder waarschijnlijk dat een goede bekende is omgekocht door de vijand, dan iemand die men nauwelijks kent.

Bovendien, als iemand twijfelt aan de betrouwbaarheid van de bron en tevens gemotiveerd is om de betrouwbaarheid van de bron te beschouwen, is het de vraag of hij over voldoende cognitieve middelen beschikt om dit te doen. Een commandant moet bijvoorbeeld onder hoge tijdsdruk een risicovol besluit nemen, maar de beschikbare informatie is onvolledig. Hij is tevens belast met zoveel taken dat hij, ongeacht zijn motivatie om de informatie kritisch te beoordelen, daarvoor eenvoudigweg niet over voldoende cognitieve middelen beschikt. Als hij door gebrek aan mankracht en tijd geen beroep kan doen op anderen, zal hij geneigd zijn terug te vallen op zijn vooroordelen.

#### Inschatten van de waarheid

Naast een inschatting van de betrouwbaarheid van de bron, moet ook een inschatting worden gemaakt van het waarheidsgehalte van de informatie. Om te beoordelen of informatie waar is, gebruiken wij verschillende aanwijzingen die als ezelsbruggetjes fungeren. Enkele voorbeelden.

- *De vergelijking met situaties uit het verleden.* Wanneer de informatie in de huidige situatie gelijk is aan ervaringen uit het verleden, wordt de kans dat de huidige informatie waar is, groter geacht.
- *Aannemelijkheid.* Schijnbaar aannemelijke informatie zal veel minder snel kritisch worden beoordeeld.
- *Saillantie.* Informatie die goed in het geheugen blijft hangen (ofwel saillant is) krijgt meer geloofwaardigheid. Deze saillantie kan door verschillende mechanismen worden veroorzaakt. Het kan de eerste informatie zijn die iemand krijgt, of juist de meest recente. Het kan ook inhoudelijk extreem zijn (als bijvoorbeeld veel slachtoffers en ravage worden gerapporteerd). De informatieinhoud kan ook op persoonlijk vlak belangrijk zijn voor de ontvanger.
- *Aanwezigheid van alternatieven.* Wanneer meerdere berichten elkaar tegenspreken, kan deze diversiteit aan informatie gebruikt worden om de waarheid van de verschillende alternatieven in te schatten.
- *Eigenschappen van de bron.* Bronkenmerken hebben niet alleen effect op de ingeschatte betrouwbaarheid van de bron, maar ook op de manier waarop de ontvanger de inhoud van de boodschap beoordeelt. Zo zijn wij bijvoorbeeld geneigd iets voor waar aan te nemen, wanneer wij inschatten dat de bron juiste intenties heeft. Dit heeft niet alleen te maken met het feit dat wij mensen met (vermoedelijk) goede bedoelingen meer vertrouwen dan mensen met (vermoedelijk) slechte, maar het vertrouwen in de bron geeft een zeker gewicht of betekenis aan de informatie.

#### Vertrouwen

Omdat je niet altijd kunt weten of

iemand de waarheid spreekt, komt de beoordeling van een persoon en de informatie die hij verstrekt vaak neer op vertrouwen. Vertrouwen verwijst naar de verwachting dat iemand anderen niet opzettelijk zal benadelen. Dus wanneer je iemand vertrouwt, verwacht je dat hij handelt in jouw belang, en er niet op uit is jou te misleiden ten gunste van zichzelf. Vertrouwen wordt volgens Sniezek en Van Swol (2001) bepaald door de volgende factoren.

- *Onzekerheid van de ontvanger over zijn eigen kennis.* Iemand met weinig kennis over een bepaald onderwerp, is afhankelijk en daarom genoodzaakt te vertrouwen op informatie van anderen. Omdat een commandant in het veld niet zijn eigen inlichtingen kan verzamelen moet hij wel vertrouwen op anderen.

- *Aanwijzingen met betrekking tot de expertise van de informatiebron.* Aanwijzingen over de expertise van de informatiebron geven aan of deze kennis van zaken heeft. Het beroep dat iemand uitoefent of de hoeveelheid ervaring die iemand heeft, zijn wat dat betreft vrij expliciete aanwijzingen. Zo wordt een commandant geacht kennis te hebben van militaire operaties. Sommige aanwijzingen zijn daarentegen wat minder expliciet, zoals het zelfvertrouwen van de informatiebron.

- *De relatie tussen de ontvanger en de bron.* Men is geneigd elkaar meer te vertrouwen naarmate men elkaar beter kent of wanneer men al eerder heeft samengewerkt. Een informant waar men al vaker informatie van heeft gekregen en die goed bevallen is, zal men meer vertrouwen dan een nieuwe informant. En een vriend die informatie heeft zal men eerder vertrouwen, dan een onbekende die anoniem informatie doorspeelt.

Vertrouwen hangt dus af van kenmerken van de ontvanger, kenmerken van de informatiebron en hun onderlinge verhouding. Hoewel deze bevindingen op zich niet heel opzienbarend zijn, is met name de wijze waarop deze factoren met elkaar samenhan-

gen interessant, ook voor het moderne militair optreden (Janssen, Griffioen-Young & Van der Kleij, 2001).

Bij besluitvorming speelt het verzamelen, beheren en uitwisselen van informatie immers een grote rol en inzicht in de wijze waarop dit beïnvloed wordt door vertrouwen in de informatiebron, is van grote waarde voor Info Ops.

Gebrek aan vertrouwen kan ertoe leiden dat men informatie van een goede bekende of naaste collega verkiest boven informatie van een minder bekende bron, die objectief gezien over betere informatie beschikt. Dit gebeurt ook in besluitvormingsteams binnen de krijgsmacht. Uit gesprekken met militaire deskundigen blijkt dat men relatief veel waarde hecht aan informatie die men krijgt via het netwerk van vrienden en naaste collega's. Dit gaat soms ten koste van de informatie die wordt verstrekt via de officiële bronnen, zoals inlichtingendiensten. Dat kan leiden tot verkeerde beslissingen met grote consequenties. In het kader van Info Ops zouden ondersteuningsconcepten kunnen worden ontwikkeld om deze processen te herkennen en zich tegen de gevaren ervan te behoeden. Hiervoor is meer en specifiek inzicht nodig in de rol van vertrouwen bij informatieverwerking en besluitvorming.

### **Effecten van zekerheid en deskundigheid op beïnvloeding**

Zoals besproken zijn verschillende factoren bepalend voor het vertrouwen dat iemand in een ander heeft en de inschatting van het waarheidsgehalte van informatie. Uit de eerder genoemde interviews kwam naar voren dat men bij de besluitvorming vaak in de verkeerde persoon vertrouwen heeft. Naar aanleiding hiervan deed TNO Technische Menskunde onderzoek naar hoe mensen bepalen wie zij kunnen vertrouwen en van wie zij informatie aannemen. Daartoe is in een laboratoriumomgeving de invloed van de volgende factoren on-

derzocht: de *expertise* van de informatiebron, de *zekerheid* waarmee de bron deze informatie presenteert aan de ontvanger en de mate van *risico* verbonden aan de beslissing.

Om dit te onderzoeken hebben wij een studie uitgevoerd waaraan 108 studenten deelnamen die twintig meerkeuzevragen moesten beantwoorden over de krijgsmacht. Dit onderwerp werd gekozen, omdat verwacht werd dat studenten hiervan niet bijzonder veel kennis hebben. Dat was belangrijk, omdat het we de expertise van de zogenaamde adviseur dan beter konden manipuleren, zoals verderop duidelijk zal worden.

Ieder proefpersoon werd verteld dat hij moest samenwerken met een ander proefpersoon, en dat ze konden communiceren via computers met een directe verbinding. De ene proefpersoon kreeg de rol van beslisser en moest de vragen beantwoorden. Hierbij kon hij desgewenst gebruikmaken van het advies van de andere proefpersoon, die de rol van adviseur had. Echter, deze andere proefpersoon bestond niet en werd door ons gesimuleerd door middel van vooraf geformuleerde antwoorden op de computer.

Om deskundigheid te manipuleren werd de proefpersonen verteld dat de adviseur veel meer wist over de krijgsmacht dan zijzelf (hoge expertisecnditie), of dat de adviseur ongeveer evenveel wist (lage expertisecnditie). Om zekerheid te manipuleren, gaf de adviseur zijn adviezen met veel overtuiging ('ik weet zeker dat het A is'; hoge zekerheidsconditie) of met weinig overtuiging ('ik weet het niet zeker, maar ik denk dat het A is'; lage zekerheidsconditie). De risicomaniplatie bestond in de hoge risicoconditie uit de mogelijkheid om een financiële bonus te verdienen door het geven van goede antwoorden. In de lage risicoconditie had het geven van goede of foute antwoorden geen financiële consequenties voor de proefpersonen. In totaal waren er dus acht condities: 2 (expertise: hoog, laag) x 2 (zekerheid: hoog, laag) x 2 (risico: hoog, laag).

Om antwoord te geven op onze onderzoeksvragen hebben wij gekeken naar drie zaken. Ten eerste: om te beoordelen in hoeverre mensen zich door de expertise en zekerheid van de adviseur lieten beïnvloeden, hebben wij het aantal overgenomen adviezen met elkaar vergeleken. Dit aantal kan variëren van 0 tot 20. Ten tweede: om het vertrouwen in de adviseur te beoordelen, hebben wij proefpersonen gevraagd hoeveel vertrouwen zij in hun adviseur hadden op een 9-puntsschaal (1 = weinig vertrouwen, 9 = veel vertrouwen). Als indirecte aanwijzing voor vertrouwen hebben wij, na het beantwoorden van iedere vraag in de taak, tevens aan de proefpersonen gevraagd hoe zeker zij waren van hun antwoord (1 = zeer onzeker, 9 = zeer zeker).

Uit figuur 2 is af te leiden dat proefpersonen zich sneller laten beïnvloeden wanneer het risico hoog is dan wanneer het risico laag is. Bovendien laten proefpersonen zich sneller beïnvloeden door adviseurs die met veel zekerheid hun advies overbrengen dan door adviseurs die aarzelend hun advies geven. De expertise van de adviseur heeft geen invloed op het aantal overgenomen adviezen.

Figuur 3 laat zien dat proefpersonen meer vertrouwen hebben in adviseurs met een hoge expertise dan met een lage expertise. Proefpersonen hebben

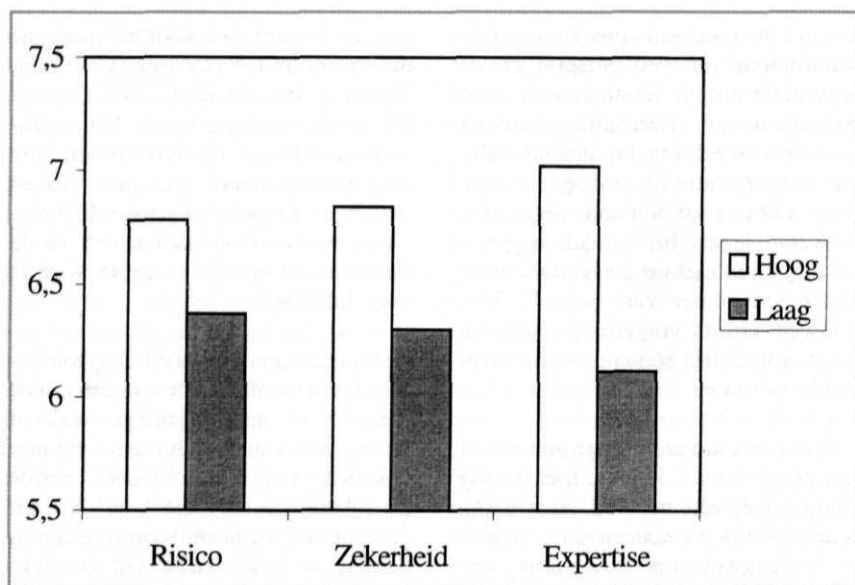


Fig 3. Vertrouwen in de adviseur per conditie

niet meer vertrouwen in hun adviseur wanneer deze veel zekerheid uitstraalt dan wanneer deze weinig zekerheid uitstraalt. Het risico dat met de beslissing gepaard ging was ook nauwelijks van invloed op de mate van vertrouwen.

Een vergelijkbaar patroon zien wij in figuur 4, dat de responszekerheid toont. Responszekerheid is de mate waarin de proefpersoon zeker is van zijn antwoord. Proefpersonen zijn zekerder van hun antwoord als ze advies hebben gekregen van een adviseur met een hoge zekerheid of exper-

tise. Het risico dat met de beslissing gepaard ging was nauwelijks van invloed op de responszekerheid.

Samenvattend kunnen we stellen dat proefpersonen aangeven meer vertrouwen te hebben in adviseurs met veel expertise, en zekerder te zijn van hun antwoorden wanneer zij een advies krijgen van een adviseur met veel expertise. Tegelijkertijd zien we echter dat als het erop aankomt, de expertise van de adviseur er in het besluitvormingsproces eigenlijk niet toe doet. Proefpersonen lieten zich namelijk niet vaker beïnvloeden door adviseurs met een veel expertise. Sterker nog, als het erop aan komt, laten proefpersonen zich beïnvloeden door enerzijds de mate van risico die aan de beslissing verbonden is en anderzijds de zekerheid waarmee de adviseur zijn advies overbrengt. Wij kunnen daarom het volgende stellen: mensen laten zich beïnvloeden door de risico's die verbonden zijn aan een beslissing en de zekerheid waarmee een advies wordt gebracht, ongeacht de expertise van de bron. Mensen geven echter wel aan meer te vertrouwen op adviseurs met veel expertise.

Dit onderzoek laat duidelijk zien dat men bij het nemen van risicovolle beslissingen niet altijd gebruik maakt

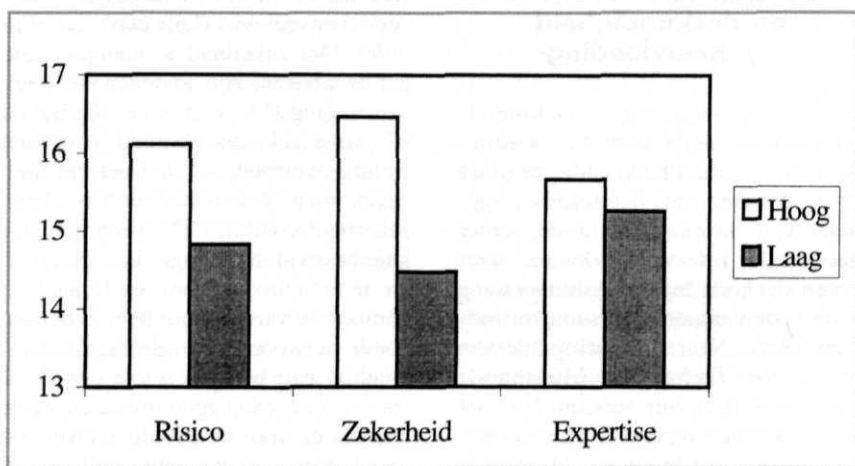


Fig 2. Het aantal overgenomen adviezen per conditie

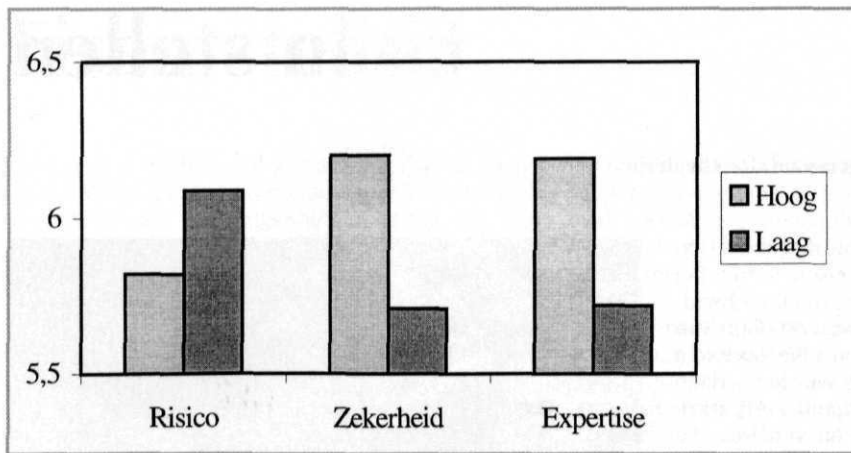


Fig 4. Responszekerheid per conditie

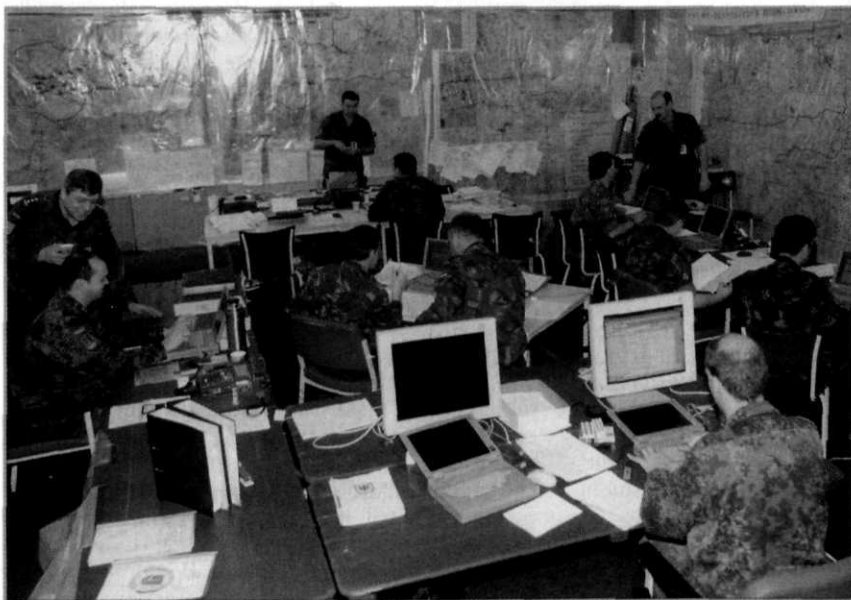
van de beste informatie. Een bron met veel expertise kan de juiste informatie verschaffen, maar kan vervolgens worden overtroffen door een bron met meer overtuigingskracht. Indien we risicovolle besluitvorming willen verbeteren, dienen we ons niet alleen te richten op het verzamelen, beheren en uitwisselen van informatie, maar ook op de psychologische processen die bepalen hoe commandanten met informatie omgegaan. Deze kennis is van grote waarde voor zowel defensieve als offensieve Info Ops. Vanuit defensief oogpunt gaat het om het geven van advies of ondersteuning bij besluitvorming om dergelijke proces-

sen te herkennen en negatieve effecten ervan te voorkomen. Vanuit offensief oogpunt gaat het om het verstoren van besluitvorming van de tegenstander, niet alleen door manipulatie van de informatie zelf, maar ook de manipulatie van de informatiebron.

### Conclusie

In een maatschappij waarin steeds meer informatie steeds sneller wordt uitgewisseld, is het essentieel op trends vooruit te lopen. Dit is niet alleen van belang voor innoverende organisaties, maar ook voor de krijgs-

macht. Wat betekenen deze ontwikkelingen voor het verloop van militaire operaties? Hoe kunnen wij ons beschermen tegen offensieve Info Ops van de tegenstander en nadelige effecten tegengaan? Kennis van psychologische processen van informatieverwerking en besluitvorming is hierbij van wezenlijk belang. Want ook al beschikken commandanten over de meest geavanceerde informatiesystemen, het daadwerkelijk nemen van een beslissing is uiteindelijk mensenwerk. In risicovolle situaties spelen naast rationele argumenten ook minder doordachte processen, zoals intuïties en emoties, een rol. Dit hoeft op zich geen slechte zaak te zijn, maar inzicht in deze processen, en bescherming tegen mogelijke nadelige effecten, is van groot belang om de kwaliteit van besluitvorming te waarborgen en optimaliseren.



Gebruik van informatie bij besluitvorming

### Literatuur

- Beleidskader Information Operations (Info Ops), juli 2001.
- Griffioen-Young, H.J. *How to compose a PsyOps message: The effects of involvement and information source on persuasion* (Rapport TM-00-A025). Soesterberg: TNO Technische Menskunde, 2000.
- Janssen, H.J.W., & Griffioen-Young, H.J. *How to compose a PsyOps message. Part III: The effects of medium and emotionality on persuasion* (Rapport TM-01-A046). Soesterberg: TNO Technische Menskunde, 2001.
- Janssen, H.J.W., Griffioen-Young, H.J., & Kleij, R. van der. *Risicovolle besluitvorming in teams: De invloed van onzekerheid en onbetrouwbaarheid* (Rapport TM-01-A060). Soesterberg: TNO Technische Menskunde, 2001.
- Lasswell, H.D. The structure and function of communication in society. In L. Bryson (Ed.), *The communication of ideas: Religion and civilization series* (pp. 37-51). New York: Harper & Row, 1948.
- Petty, R.E., Cacioppo, J.T., & Goldman, R. Personal involvement as a determinant of argument-based persuasion. *Journal of Personality and Social Psychology*, 4, 847-855, 1981.
- Sniezek, J.A., & van Swol, L.M. Trust, confidence and expertise in a Judge-Advisor System. *Organizational Behavior and Human Decision Processes*, 84, 288-307, 2001.