

BOB DE GRAAFF

# DATA EN DREIGING

STAP IN DE WERELD VAN INTELLIGENCE

**Boom**

AMSTERDAM

Vormgeving: Bart van den Tooren

© 2019 Bob de Graaff

Behoudens de in of krachtens de Auteurswet van 1912 gestelde uitzonderingen mag niets uit deze uitgave worden vervoelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch door fotokopieën, opnamen of enig andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

*No part of this book may be reproduced in any way whatsoever  
without the written permission of the publisher.*

ISBN 9789461058720

NUR 680

WWW.BOOMGESCHIEDENIS.NL

WWW.BUA.NL

# INHOUD

## 9 Inleiding

### 13 1. Wat is intelligence?

- 13 Vergaring van afgeschermd informatie
- 15 Niet alle informatie is intelligence
- 17 In een competitieve omgeving
- 17 Dreigingen
- 21 Waardering van informatie
- 21 Succes of falen: intelligence versus denial en deception
- 22 Definitie
- 23 De Britten en Amerikanen: twee verschillende culturen
- 24 Inlichtingen in termen van activiteit en organisatie

### 29 2. Inlichtingen verzamelen

- 29 Inleiding
- 30 Voor wie of wat?
- 34 Behoeftestelling
- 38 Verzamelen
  - 38 Humint
    - 38 Algemeen
    - 39 Agenten
    - 47 Targeting
    - 48 Motieven
    - 56 De benadering, ontwikkeling en rekrutering
    - 59 De relatie runner-agent
    - 63 Voor- en nadelen
  - 65 Sigint
  - 72 Imint en geoint
  - 77 Masint
  - 79 Osint
  - 82 Cyberint en socmint
  - 86 Intelligence liaison

### **93 3. Bewerken, waarderen en analyseren**

- 93 Bewerken
- 94 Waarderen
- 98 Analyse
  - 98 ‘Het belangrijkste aspect van intelligence’
  - 99 Van gegeven naar verhaal
  - 101 Methode en expertise
  - 102 Het persoonlijkheidstype van analisten
- 104 Kunst of wetenschap?
- 105 Slow en fast thinking
- 107 Data- of conceptgestuurd
- 109 Een empirische of een constructivistische benadering
- 110 Het product
- 112 Kritiek op de inlichtingencirkel

### **117 4. Wat gebeurt er met intelligence?**

- 117 Inleiding
- 118 Disseminatie: de achilleshiel van het inlichtingenproces
  - 120 Op zoek naar het beoogde effect
  - 121 Een scheidingsmuur of niet?
  - 123 Rapporteurs en besluitvormers: twee stammen
  - 126 Overtuigen
  - 128 Politisering
- 129 Covert action: de niet zo stille optie
- 135 Contra-inlichtingen
  - 137 Defensief
  - 140 Offensief
  - 142 Militair
  - 143 Vallen contra-inlichtingen onder intelligence?
- 144 Internationale samenwerking
- 145 Intelligence failures
  - 149 Redenen voor intelligence failures
    - 149 Misleiding
    - 149 Fouten of gebreken in de aansturing
  - 150 De inlichtingenverzameling
  - 151 De bewerking
  - 151 De analyse
  - 157 Disseminatie
  - 158 Verschuivende inzichten
- 162 ‘Oplossingen’

## **165 5. Verantwoording, recht, toezicht en ethiek**

- 166 Wetgeving
- 170 Toezicht
- 177 Ethiek
- 181 Deontologie
- 182 Deugdethiek
- 183 Realistische ethiek
- 183 Utilitaristische ethiek
- 185 *Gesinnungs- en Verantwortungsethik*
- 186 Situationele ethiek
- 187 Virtue by proxy
- 188 Leer van de rechtvaardige intelligence
- 192 Casussen en codes

## **195 6. De toekomst van intelligence**

- 195 De eerste intelligencerevolutie: van privaat naar staat
- 197 De tweede intelligencerevolutie: blijvende  
schaalvergroting, bureaucrativering en professionalisering
- 200 Een derde intelligencerevolutie?
- 202 Politiek-maatschappelijke ontwikkelingen
- 209 Technologische ontwikkelingen
- 212 Veranderingen in organisatie
- 212 Van schaken naar snelschaken
- 213 Van producenten en consumenten naar prosumenten
- 215 Omgaan met kritiek uit de waardeomgeving
- 216 En wat als iedereen een inlichtingendienst wordt?
- 218 Tot slot

- 220 Noten
- 234 Lijst van figuren
- 235 Afkortingen
- 238 Literatuur
- 260 Personenregister

# INLEIDING

Het aardse bestaan van de mens is altijd gekenmerkt geweest door onzekerheden. De natuur kon hem voor verrassingen plaats in de vorm van overstromingen, windhozen, orkanen, aardbevingen of vulkaanuitbarstingen. Dat waren rampen die ‘van boven kwamen’ of zoals het in het Engels heet: *God-made disasters*. De mens kon zich ertegen proberen te beveiligen door terpen aan te leggen, dijken te bouwen of betere bouwmaterialen te gebruiken. Deze vorm van beveiliging wordt aangeduid met het Engelse woord *safety*. Maar het kon ook gebeuren dat de ene mens de andere mens rampspoed bereidde. Hij kon de ander overvallen, zijn dijk doorsteken of met pokken besmette koeienkadavers over de muur van de tegenstander in de belegerde stad katapulteren. Zo bezorgde de ene mens de andere mens *man-made disasters* en de vorm van beveiliging daartegen heet in het Engels *security*.

Het feit dat andere mensen iemand onaangenaam konden verrassen, vormde een bedreiging van het bestaan. Het zorgde voor onzekerheid. In een antiek verleden vatten mensen deze onzekerheid op als een gegeven van het leven. Voorspoed en onheil waren het (nood)lot van de mensen. Zij hadden daar zelf uiteindelijk geen invloed op. De goden bezorgden de mensen niet uitsluitend *God-made disasters*, maar bepaalden ook welke *man-made disasters* iemand in zijn leven tegenkwam. Al probeerden de mensen zelfstandig te handelen, in feite waren zij marionetten die gemanoeuvreerd werden door de goden, die soms hun onderlinge ruzies in hemelse sferen botvierden via de mensen op aarde.

Niet wetend wat hem te wachten stond probeerde de mens zicht te krijgen op zijn toekomst. In het verleden (en ook nu nog) zocht en zoekt hij daarom zijn toevlucht tot orakels of waarzeggers die beweren de gave te hebben zaken te kunnen voorzien. Het waren niet alleen goedwillenden die beangstigd waren voor toekomstige bedreigingen die hun heil zochten in voorspellingen. Ook zij die van plan waren anderen te overvallen, bijvoorbeeld met hun legers, wendden zich tot orakels of priesters om te vragen of deze op grond van hun relaties met hogere machten konden voorzeggen wanneer het moment gunstig zou zijn voor hun aanval of wat het gevolg zou zijn van hun actie. Met de juiste informatie, die uiteraard verborgen moest blijven voor de tegenstander, kon een voordeel worden behaald. Er kon een beter gefundeerde beslissing mee worden genomen. Dus een informatievoorsprong kon leiden tot een besluitvormingsvoordeel.

Die pogingen onzekerheid te reduceren om aldus bedreigingen te kunnen keren en kansen op succes (*opportunities*) aan te geven heeft, naarmate de mens de directe invloed van de goden op het aardse bestaan minder aanvaardde, een steeds belangrijker plaats ingenomen in het bestaan van volken. Koningen en legeraanvoerders gingen zich bedienen van spionage om te weten te komen waar vijandelijke legers zich bevonden en hoe die verrast konden worden. Ze stuurden verkenners vooruit om vijandelijke posities waar te nemen of ze onderschepten boodschappen van de tegenstander. Spionage heeft altijd die twee vormen gekend: waarneming en onderschepping van communicatie. Spionage vormde de ogen en de oren van degenen die strategische, operationele of tactische beslissingen moesten nemen. Dit betekende dat de wijze van spioneren veranderde naarmate er nieuwe mogelijkheden van waarneming en communiceren kwamen. Van verre kijker tot satelliet en van brief tot versleuteld e-mailbericht - het had allemaal invloed op de wijze van spioneren of, op zijn Engels, *intelligence*.

Intelligence is niet alleen gericht op externe tegenstanders. Uit onzekerheid over de vraag wat eigen onderdanen, eigen soldaten of bondgenoten in hun schild voerden hebben vorsten en legeraanvoerders door de eeuwen heen ook altijd willen weten wat voor potentiële rampspoed hun van die kant te wachten stond. Meer nog dan om de capaciteiten (*capabilities*) van deze mogelijke tegenstanders ging het daarbij om hun intenties. De wensdroom van machthebbers is altijd geweest om door te dringen in het hoofd van degenen die volgens hen kwaadwillend waren. Daartoe moest intelligence binnendringen in de persoonlijke levenssfeer van degenen die binnen het bereik van de macht waren en als het om de verhouding tussen een overheid en haar onderdanen of burgers ging, lag repressie dus steeds op de loer.

Dit boek biedt een inleiding in de wereld van intelligence, een begrip dat om redenen die nog aan bod zullen komen, de voorkeur verdient boven de term spionage. Het gaat daarbij primair om *security*, niet om *safety*. Uitgangspunt van intelligence is steeds een antwoord te bieden op onzekerheid, hetzij om bedreigingen weg te nemen of te reduceren, hetzij om gebruik te maken van *opportunities*. Mensen die zich met intelligence bezighouden, hebben echter geen glazen bol. Volledige

zekerheid kunnen zij niet bieden. Zij konden dat vroeger niet en ze kunnen het nog steeds niet. Niettemin heeft zich in de loop der tijden niet alleen in de wijze waarop inlichtingen worden verzameld, maar ook in de manier waarop die worden geïnterpreteerd en geanalyseerd grote veranderingen voorgedaan. Achterliggend doel was steeds de onzekerheid te reduceren of ten minste beheersbaar te maken. Het is een activiteit die gedoemd is gebrekkig te zijn, omdat nu eenmaal niets zo onzeker is als de toekomst. Dit neemt niet weg dat er inmiddels een hele industrie bestaat die zich toelegt op intelligence. Het is allang niet meer een zaak van alleen vorsten, legeraanvoerders of nationale overheden. Zoals in dit boek duidelijk zal worden, is intelligence zelfs een zaak waar in de huidige samenleving ieder individu zich bewust of onbewust mee bezighoudt.

De tijd dat onderwijs over intelligence buiten het kader van inlichtingen- en veiligheidsdiensten zelf een vorm van intelligence vergde is voorbij. Er bestaan tal van meer of minder omvangrijke Engelstalige inleidingen inzake intelligence. Over het algemeen staat de praktijk van de officiële Amerikaanse en/of Britse inlichtingendiensten hierin centraal. Het is mijn ervaring dat mensen op het Europese vasteland hieraan wel algemene beginselen kunnen ontleen, maar in deze literatuur vaak onvoldoende houvast vinden voor de praktijk waarmee zij meestal te maken hebben of krijgen. Inlichtingenculturen zijn vaak bepaald door de nationale geschiedenis, de geopolitieke ligging van het eigen land en het nationale staatsbestel.

Deze Nederlandstalige introductie in het fenomeen intelligence probeert zo veel mogelijk algemene noties over intelligence te verstrekken. Het boek is daardoor minder gekoppeld aan de Amerikaanse of Britse praktijk, al zullen Engelse uitdrukkingen uit het intelligencejargon, tekenend voor de Angelsaksische dominantie van het vakgebied, helaas onvermijdelijk zijn en al zullen de voorbeelden vaak aan de Britse en Amerikaanse praktijk worden ontleend, omdat die nu eenmaal nog steeds beter beschreven is.

Dit boek richt zich op iedereen die meer over intelligence wil weten. Om te beginnen de nieuwsgierige leek, die er het nieuws beter door wil volgen, waarin intelligence tegenwoordig een veelbesproken en vaak beschreven verschijnsel is. Het is ook geschikt voor de beoefenaar van intelligence die het allemaal nog eens op een rijtje gezet wil zien of met enige distantie wil bekijken hoe zijn dagdagelijkse bezigheden passen binnen het bredere fenomeen en hoe zijn vakgebied zich heeft ontwikkeld en nog steeds verder ontwikkelt. En ten slotte is het niet in de laatste plaats bedoeld voor degenen die te maken krijgen met de producten van intelligence, de mensen die beslissingen nemen op basis van intelligence en hopen dat het hun door de intelligence geboden informatievoordeel zal leiden tot een voordeel in de besluitvorming ten opzichte van andere actoren. Hopelijk zal dit boek het mogelijk maken de werking van het steeds meer alomtegenwoordige verschijnsel intelligence beter te begrijpen en op waarde te schatten.

Dit boek is niet bedoeld als training in de zogeheten verwervings- of analysemethoden van intelligence. Het is geen *how to*-boek. Het is primair bedoeld als reflectie

op de processen van intelligence en wil op die manier verstandiger handelen in de praktijk mogelijk maken. Idealiter helpt dit boek beoefenaren van intelligence dus *reflective practitioners* te worden, die met de hier geboden inzichten gewapend zijn voor de praktijk van vandaag en morgen.

Het boek telt zes hoofdstukken. In het eerste komen de definitie en de organisatie van intelligence aan de orde. Het tweede en derde hoofdstuk behandelen een aantal belangrijke activiteiten uit de zogeheten inlichtingencirkel: de vergaring, de bewerking, de evaluatie en de analyse van gegevens. Het vierde hoofdstuk gaat in op de vraag wat er geschiedt met de geanalyseerde informatie: wat gebeurt er wanneer die wordt aangeboden aan de zogeheten consumenten van intelligence, ook wel afnemers genoemd? En wanneer is een inlichtingenproduct een succes en wanneer veroorzaakt het een zogeheten *intelligence failure*? Tevens worden hier de belangrijkste principes van contra-inlichtingen en *covert action* beschreven. In hoofdstuk vijf staan de juridische en ethische aspecten van intelligence centraal, alsmede het toezicht en de controle op het inlichtingenproces. Het zesde en laatste hoofdstuk heeft de toekomst van intelligence als onderwerp. Een van de zaken die dit boek wil duidelijk maken is dat intelligence tegenwoordig een transitie ondergaat, waardoor werkwijzen die de afgelopen eeuw gebruikelijk waren ter discussie komen te staan. Dit slothoofdstuk werpt een blik vooruit. Kort samengevat komen achtereenvolgens de vragen aan de orde: wat, hoe, waartoe, met welke restricties en waarheen?

Dit boek is onderdeel van het Intelligence Lab, een initiatief van de afdeling Geschiedenis van Internationale Betrekkingen van de Universiteit Utrecht en Boom uitgevers Amsterdam. Het Intelligence Lab is een platform voor blended learning rondom het thema intelligence. Bekijk alle activiteiten op [www.intelligencelabs.nl](http://www.intelligencelabs.nl).

# 1. WAT IS INTELLIGENCE?

## VERGARING VAN AFGESCHERME INFORMATIE

Wat is intelligence? En waarom spreek ik over intelligence en niet over inlichtingen of over spionage? Definitiekwesties zijn altijd lastig. Er bestaan honderden definities van begrippen als religie, democratie, geweld, imperialisme, fascisme of terrorisme. En ook het aantal definities van intelligence is legio. Bovendien kan de definitie van intelligence door de tijd heen nog veranderen, zoals later in dit boek nog zal blijken. Iedere auteur moet daarom met zijn lezer afspraken maken over wat hij onder het centrale begrip, in dit geval intelligence, verstaat. Laat ik een praktisch voorbeeld nemen aan de hand waarvan ik kan laten zien hoe ik intelligence voorlopig afbaken.

Stel dat ik in de gangen van een voetbalclub rondzwerf, terwijl de trainer achter gesloten deuren in het kleedlokaal met het eerste elftal het tactisch plan bespreekt voor de wedstrijd tegen de belangrijkste rivaal, die enkele dagen later, op zondag, zal plaatsvinden. Laten we zeggen dat het gaat om de club Blauw-Zwart, die de cruciale wedstrijd tegen aartsrivaal Rood-Wit gaat spelen. Door de dunne scheidingswand waar ik tegen aanleun, kan ik alles verstaan van het strijdplan dat de trainer van Blauw-Zwart in de kleedkamer tegenover zijn spelers uiteenzet. Nadat de bespreking is afgelopen, blijft de deur van het kleedlokaal openstaan en door de opening zie ik het papier hangen waarop hij met cirkeltjes en pijltjes het plan uiteen heeft gezet. Ik maak een foto van het papier met de opstellingen en loopacties van de spelers en teken op wat ik heb gehoord.

Beschik ik nu over intelligence?

Dat hangt ervan af. Om te beginnen was de bespreking niet voor mij bedoeld. Niet voor niets ging de deur van de kleedkamer dicht toen de trainer het tactische plan besprak. Het was eigenlijk ook niet de bedoeling dat ik de tekening met het plan had gezien. Er was dus in beginsel sprake van informatie die had moeten worden afgeschermd. Inlichtingen- en veiligheidsdiensten (op het onderscheid tussen beide kom ik nog terug) baseren zich niet uitsluitend op afgeschermd of geheime informatie. Ten tijde van de Koude Oorlog gaven veel auteurs aan dat slechts twintig procent van de gegevens waarmee zulke diensten werkten geheim was en tachtig procent openbaar. Tegenwoordig valt te lezen dat zelfs nog maar vier of vijf procent geheim is.<sup>1</sup> De rest wordt verkregen uit zogeheten open bronnen. Niettemin wordt dat beperkte deel aan afgeschermd of geheime informatie nog steeds als een wezenlijk bestanddeel van intelligence gezien: 'Intelligence is a game between hidiers and finders.'<sup>2</sup>

Officiële inlichtingen- en veiligheidsdiensten, zoals in Nederland de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), staan bijzondere, bij de wet vastgelegde bevoegdheden ter beschikking om bij die afgeschermd informatie te mogen komen. Medewerkers of agenten van deze diensten mogen, als aan bepaalde streng gereuleerde voorwaarden is voldaan, bijvoorbeeld inbreken in afgesloten gebouwen of computers hacken. Deze diensten zien hun bijzondere bevoegdheden daarom als een toegevoegde waarde, die hen onderscheidt van andere overheidsinstellingen, die niet zo verregaand mogen ingrijpen in de persoonlijke levenssfeer van burgers.

Merk op dat ik liever dan over geheime informatie spreek over afgeschermd of af te schermen informatie, in de woorden van de Britse inlichtingenexpert David Omand: 'information others want to stop one from having'.<sup>3</sup> Stel: je hebt als zestienjarige ooit een foto of filmpje van jezelf op het internet gezet, waar je later spijt van hebt gekregen. Misschien was je gedeeltelijk ontkleed of zichtbaar aangeschoten. Ondanks verwoede pogingen is het je niet gelukt die afbeelding van het internet te doen verdwijnen. Enkele jaren later solliciteer je op een baan en je bent bang dat de werkgever, of een door hem ingehuurd bureau, bij een zoekactie op het internet je foto of filmpje zal zien. De kans dat je de begeerde baan zult krijgen, acht je in dat geval klein. De foto of het filmpje staat op het voor iedereen toegankelijke internet en is niet geheim. Nu zijn er gespecialiseerde bureaus die er soms in slagen zulke door de oorspronkelijke maker ongewenste informatie toch van het internet af te krijgen of ervoor kunnen zorgen dat deze informatie pas bij bijvoorbeeld het honderdeneerste resultaat verschijnt bij een zoekactie. Je kunt dan de hulp van zo'n bureau inroepen in de hoop dat je nieuwe werkgever niet verder zal kijken dan het honderdste resultaat. Er is dan dus geen sprake van geheime informatie (het internet is openbaar), maar wel van afgeschermd informatie, althans je hebt een poging tot afscherming gedaan. En net zoals jij zo'n poging doet, zo zou Blauw-Zwart er goed aan hebben gedaan om zijn informatie, zowel de bespreking als het papier met aantekeningen, af te schermen.

## NIET ALLE INFORMATIE IS INTELLIGENCE

Stel dat ik de informatie die ik na afloop van de voetbaltraining van het eerste elftal van Blauw-Zwart opsla in mijn geheugen en op zondag naar de wedstrijd tegen Rood-Wit ga kijken. Is er dan sprake van intelligence? Nee. Intelligence wordt altijd verzameld of vergaard ten behoeve van iemand die er 'iets mee kan', de zogeheten afnemer, klant of inlichtingenconsument, die met behulp van de aangeleverde informatie een besluit kan nemen of beleid kan maken. We zeggen daarom wel dat intelligence een vorm van beleidsondersteuning is. In een statelijke context wil dit zeggen, zoals Sherman Kent, de grondlegger van de Amerikaanse inlichtingenanalyse, het omschreef: 'Intelligence... is kennis die onze hooggeplaatste burgers en militairen moeten hebben om het nationale welzijn veilig te stellen.'<sup>4</sup>

Als ik de informatie over het strijdplan van Blauw-Zwart niet zou geven aan de coach van Rood-Wit, de tegenstander van aanstaande zondag, maar aan zijn collega van een team dat in een heel andere divisie uitkomt, is er evenmin sprake van intelligence. Die coach heeft namelijk op zich niets aan die informatie. Intelligence dient (beleids)relevant te zijn voor de afnemer, en wel in hoge mate. Intelligence behoort niet tot de afdeling irrelevante weetjes. Bij intelligence gaat het om informatie waarvan het ontbreken de besluitvormer - figuurlijk of letterlijk - buikpijn of slapeloze nachten bezorgt.

Dat intelligence in dienst staat van beleid en besluiten heeft belangrijke gevolgen. Beleidsmakers en besluitvormers kunnen acties ondernemen zonder zich iets aan te trekken van de intelligence die hun wordt aangeleverd. Dit kan structurele vormen aannemen. Zo zei voormalig CIA-hoofd James Woolsey over zijn 'relatie' met president Bill Clinton: 'I didn't have a bad relationship with the President, I just didn't have one at all.'<sup>5</sup> En bij een andere gelegenheid maakte Woolsey de wrange grap: 'Remember the guy who in 1994 crashed his plane onto the White House lawn? That was me trying to get an appointment to see President Clinton.'<sup>6</sup> Besluitvormers trekken zich dus soms niets aan van de informatie die inlichtingenmensen hun bieden. Omgekeerd kunnen mensen in de sfeer van intelligence echter niet buiten besluitvormers of beleidsmakers. Zonder intelligenceconsumenten hebben intelligenceproducenten geen bestaansrecht. Deze (scheve) verhouding, die nog vaak aan bod zal komen, is kenmerkend voor het inlichtingenbedrijf zoals we dat tot op de dag van vandaag kennen.

Een belangrijke voorwaarde om informatie intelligence te laten zijn is dus dat het om afgeschermd informatie gaat of informatie die vanuit het oogpunt van de 'auteur' van de informatie, of het nu gaat om een sollicitant of om voetbalclub Blauw-Zwart, afgeschermd had moeten worden. We kunnen dus nu reeds zeggen dat niet alle informatie intelligence is. Intelligence is een deelverzameling van informatie. We kunnen met behulp van nog meer randvoorwaarden die deelverzameling nog kleiner maken ten opzichte van de totale informatie.

Verbeeld je dat ik de informatie op maandag, de dag na de wedstrijd, aan de coach van de tegenstander, Rood-Wit, geef, is er dan sprake van intelligence? Nee, om in-

telligence te zijn moet informatie de afnemer zodanig tijdig bereiken dat hij er nog iets mee kan doen: intelligence moet *actionable* zijn. Zelfs informatie die nog vóór de wedstrijd komt, maar heel kort tevoren, is niet echt bruikbaar. De coach zal niet een kwartier voor aanvang van de wedstrijd, op basis van nieuwe informatie over de tegenstander, plotseling een strijdplan dat hij de afgelopen dagen uitvoerig met zijn spelers heeft besproken volledig omgooien. De kans op verwarring bij zijn spelers is dan te groot. De intelligence is in dat geval niet langer *actionable*. Komt intelligence te laat, dan is het over het algemeen voer voor geschiedschrijvers, niet voor inlichtingenanalisten. In het voetbalvoorbeeld kan de coach er namelijk niets meer mee.

Er is een sterke analogie tussen inlichtingenmensen en historici. Er wordt wel gezegd dat als je in het boek *Writing History* van de historicus en tevens peetvader van de inlichtingenanalyse Sherman Kent het woord 'historian' vervangt door 'intelligence officer' je een prima handleiding voor de inlichtingenanalist hebt.<sup>7</sup> Er is echter een wezenlijk verschil tussen beiden, en dat is dat de historicus per definitie achterom kijkt, naar het verleden, en de inlichtingenman of -vrouw naar voren kijkt, naar de toekomst. Informatie die de dag na een bewuste gebeurtenis komt, is te laat voor inlichtingenmensen en wellicht interessant voor geschiedschrijvers.

Als intelligence te laat komt, is het letterlijk: *game over*. Dit kan zeer pijnlijke gevolgen hebben, zoals enkele voorbeelden kunnen illustreren. Tijdens de Jom Kippoeroorlog van 1973 maakte een Amerikaanse KH-8-satelliet geweldige foto's van het conflict. In die tijd werden de foto's echter nog na zes weken als een cassette naar de aarde gezonden, met als gevolg dat de foto's pas arriveerden toen de oorlog voorbij was.<sup>8</sup> In oktober 1983 onderschepte de NSA radioverkeer tussen Teheran en de Iraanse ambassade in Damascus omtrent een op handen zijnde bomaanslag in Libanon. De berichten werden echter pas gedecodeerd enkele weken nadat 243 Amerikaanse mariniers de dood hadden gevonden in Beiroet bij de aanslag met een autobom.<sup>9</sup> In juli 1995 vielen Bosnisch-Servische legereenheden de Bosnische moslimenclave Srebrenica aan, waar ter bescherming een Nederlands bataljon - Dutchbat - onder VN-vlag was gestationeerd. In de nasleep vermoordden Bosnisch-Servische militairen ongeveer achtduizend moslimmannen. Bosnische regeringsautoriteiten hadden berichten van Servische legereenheden over de voorgenomen executies van mannen uit de enclave Srebrenica onderschept, maar die werden pas maanden later uitgeluisterd en hadden dus geen betekenis meer voor het lot van die mannen. Hoogstens konden deze *intercepts* (onderschepte berichten) later bij het Joegoslaviëtribunaal nog worden gebruikt bij de berechting van de daders. Hetzelfde gold voor luchtfoto's die in die tijd vanuit Amerikaanse vliegtuigen waren gemaakt van executieplaatsen, maar waarvan de interpretatie pas geschiedde nadat de terechtstellingen hadden plaatsgevonden.

Hiermee hebben we een aantal voorwaarden behandeld waarom het gaat wil er sprake zijn van intelligence. Het moet gaan om althans ten dele afgeschermd informatie, die beleidsrelevant is en tijdig de afnemer bereikt opdat die daarop actie kan ondernemen. En de intelligence is informatie die een rol speelt in een compe-

tatieve omgeving, een omgeving waarin meerdere partijen hun doelen proberen te resulteren ten koste van elkaar.

## IN EEN COMPETITIEVE OMGEVING

Intelligence kan zich voordoen in alle sectoren van de maatschappij. Naast statelijke intelligence zijn er tal van vormen van niet-statale intelligence, bijvoorbeeld van de kant van het bedrijfsleven (*business intelligence* of *competitive intelligence*), criminele bendes, terroristische organisaties en ja, voetbalclubs. En dus zijn er ook allerlei verschillende afnemers: regeringen, individuele ministers, militaire commandanten, bendeleiders of voetbaltrainers. Een voorwaarde voor het gebruik van intelligence is dat er sprake is van competitie. Tussen clubs die in verschillende divisies spelen is er in beginsel geen sprake van competitie en is er dan ook geen intelligence nodig. Als de relatie met mijn echtgenote goed is, is er geen sprake van competitie en zal zij mij hartelijk ontvangen na een lange werkdag. Mocht zij - terecht of ten onrechte - het idee krijgen dat er iemand anders is tot wie ik mij aangetrokken voel, dan is er sprake van competitie en ontstaat de behoefte aan intelligence. Zij gaat mij vragen waarom en met wie ik moest overwerken, misschien snuffelt zij in mijn jaszakken, agenda of mobiele telefoon en in het ergste geval schakelt zij een privé-detective in om mijn gangen na te gaan.

Laten we ervan uitgaan dat de relatie met mijn partner goed is en ik intussen dankzij mijn oplettendheid bij Blauw-Zwart een informatievoordeel heb bereikt dat, indien ik mijn informatie tijdig aan de coach van Rood-Wit verstrek, kan worden omgezet in een besluitvormingsvoordeel. Met mijn informatie kan de trainer van Rood-Wit besluiten om met een versterkt middenveld te gaan spelen, met een libero of misschien met een extra spits, terwijl hij dat aanvankelijk, zonder mijn informatie, niet van plan was geweest. Misschien doet hij dat omdat hij dankzij mijn informatie geattendeerd is op tactische zetten die zijn collega van Blauw-Zwart in petto heeft die hij niet had verwacht. Intelligence dient dus vaak om (vervelende) verrassingen te voorkomen.

## DREIGINGEN

Vervelende verrassingen worden gezien als dreigingen. Zulke vervelende verrassingen kunnen worden veroorzaakt door mensen, bijvoorbeeld in de vorm van een terroristische aanslag of door een cyberhack. Er bestaan ook verrassingen in de vorm van 'acts of God': vulkaanuitbarstingen, aardbevingen, overstromingen en dergelijke. Tot voor kort richtten westerse inlichtingen- en veiligheidsdiensten zich uitsluitend op de eerste categorie, de man-made-disasters, die werden gezien als een security-risico en niet op de tweede, de safety-vraagstukken. Tegenwoordig wordt het onderscheid minder scherp gemaakt en hanteren diverse westerse diensten een benadering die rekening houdt met beide typen veiligheidsrisico's, de zogeheten *all-hazards*-benadering. Daar zijn twee belangrijke redenen voor. Ten eerste hangen de twee soorten catastrofes soms samen. Zo

kunnen de gevolgen van klimaatverandering, zoals verwoestijning, opdroging of juist watersnood leiden tot security-risico's, zoals migratiestromen of politiek geweld. Ten tweede is soms niet direct duidelijk of er sprake is van een security- of van een safety-kwestie. Als een trein van een brug stort, kan dat zijn door een mechanisch defect, maar het kan ook gebeuren omdat de trein bewust tot ontsporing is gebracht. Als er brand is in een metrobus, kan dat veroorzaakt zijn door kortsluiting, maar er kan ook sprake zijn van een terroristische aanslag. Dat wordt pas na verloop van tijd duidelijk. Omdat dit gevolgen kan hebben voor de hulpverlening (denk aan de mogelijkheid van secundaire aanslagen) en omdat sporen omtrent de daders zo snel mogelijk veilig gesteld moeten worden, is het in zo'n geval vaak het beste het eerst uit te gaan van het donkerste scenario, dat van een bewuste menselijke daad.

Intelligence is dikwijls bedoeld om tijdig dreigingen te onderscheiden. In een simpele formule geldt: dreiging = *capability* x intenties. Een potentiële tegenstander die de intentie heeft een atoomwapen te gebruiken, maar in de verste verte niet in staat is zo'n wapen te ontwikkelen of aan te schaffen, vormt geen nucleaire dreiging. In dit geval is immers de *capability* of het vermogen nul, en elke vermenigvuldiging met het getal nul eindigt op nul. Zo zal een tegenstander die wel beschikt over atoomwapens, maar heeft uitgesproken deze nooit maar dan ook nooit als eerste te zullen gebruiken, ook nooit een bedreiging vormen zolang niet een ander atoomwapen gebruikt. In dit geval is namelijk de intentie nul en dus de dreiging eveneens. Er zijn overigens complexere formules voor dreiging mogelijk, waarbij bijvoorbeeld ook de mate van activiteit van een potentiële opponent wordt meegewogen.

In de inlichtingenwereld zal niet uitsluitend worden vastgesteld of er sprake is van een dreiging en hoe groot die is, maar ook van het risico dat een dreiging zich manifesteert. De grootte van het risico wordt vaak gezien als de uitkomst van de verwachte impact van een dreiging maal de kans dat de dreiging zich voordoet, waarbij ook nog eens de kwetsbaarheid dan wel de weerbaarheid van het doelwit in beschouwing kan worden genomen: risico = impact x kans x kwetsbaarheid. De kans dat een potentiële terrorist iemand onverhoeds met een mes neersteekt, is groter dan dat hij een atoomwapen gebruikt. Wanneer hij dit laatste doet, zal echter de maatschappelijke impact van zijn daad vele malen groter zijn dan bij het gebruik van een mes als steekwapen. De vraag of intelligence zich vooral moet richten op waarschijnlijke dreigingen met een geringe impact of op onwaarschijnlijke dreigingen met een grote impact, is in de eerste plaats een zaak van de zogeheten behoeftesteller, waarover dadelijk meer. Wanneer niet duidelijk is wat de te verwachten impact van een dreiging is en evenmin iets gezegd kan worden over de waarschijnlijkheid dat die zich manifesteert, is er sprake van onzekerheid. In dat opzicht bestaat het werk van inlichtingendiensten als instrument ter vermindering van onzekerheid in een vertaling van onzekerheid naar dreiging en van dreiging naar risico: onzekerheid (= kans op verrassing) > dreiging > risico.

Nu bestaat er een onderscheid tussen gekende en ongekende dreigingen. Het zou de trainer van Rood-Wit bekend kunnen zijn dat zijn opponent van Blauw-Zwart nu eens met een 4-4-2-systeem speelt en dan weer met een 4-3-3-formatie. Misschien heeft hij me er wel speciaal op uitgestuurd om erachter te komen welk van de systemen Blauw-Zwart gaat gebruiken. In dat geval is er sprake van een gekende dreiging. Het kan ook zijn dat de trainer van Blauw-Zwart een tactisch meesterbrein is dat bij elke wedstrijd een onverwachte vondst op de grasmat legt en dat de trainer van Rood-Wit mij juist naar de vijandelijke kleedkamer heeft gestuurd om zo'n konijn uit de hoge hoed vóór te zijn. In dat geval is er sprake van een ongekende dreiging, waarvan de trainer van Rood-Wit zich bewust is. Het is een zogeheten gekende ongekende dreiging. De feitelijk aanwezige informatie noemen we kennis (in dit geval: ongekend); de vraag of we beseffen of kennis wel of niet aanwezig is, duiden we aan als metakennis (in dit geval: gekend). Dus in de samenstelling 'gekende ongekende dreiging' behoort 'gekend' tot de metakennis en 'ongekend' tot het domein van kennis.

Ook een ongekende ongekende dreiging is voorstelbaar. Blauw-Zwart heeft misschien onlangs een sterspeler aangekocht, maar algemeen wordt aangenomen dat hij voor de wedstrijd van aanstaande zondag nog niet speelgerechtigd is, omdat zijn werkvergunning nog niet rond is. Als ik er door mijn spionage bij de kleedkamer van Blauw-Zwart achter kom dat, zonder dat zijn nieuwe club dit bekendgemaakt heeft, hij wel speelgerechtigd is en zijn trainer van plan is hem op te stellen, dan ben ik gestuit op een ongekende ongekende dreiging, een zogeheten *unknown unknown*, in het jargon ook wel een *unk unk* genoemd. We kennen dus de volgende dreigingen: de gekende dreiging (*known known*), de gekende ongekende dreiging (*known unknown*) en de ongekende ongekende dreiging (*unknown unknown*). Ten slotte is er nog een vierde type verrassing of dreiging denkbaar, namelijk een waarvan ik wel op de hoogte ben, maar waarvan ik me niet realiseer dat ik die ken (*unknown known*). Van dit laatste was mogelijkterwijs sprake bij de Amerikaanse inlichtingengemeenschap voorafgaand aan de aanslagen van 11 september 2001, toen in totaal negentien kapers vier vliegtuigen overnamen om daarmee belangrijke gebouwen in de Verenigde Staten binnen te vliegen, wat in drie van de vier gevallen lukte. Voorafgaand aan deze aanslagen beschikten de gezamenlijke Amerikaanse inlichtingendiensten bijvoorbeeld over een computer die toebehoorde aan de man die waarschijnlijk de twintigste kaper had moeten worden, over informatie over Arabieren die hun visumtermijn hadden overschreden, over informatie dat bepaalde Arabieren verdachte geldtransacties in de Verenigde Staten hadden verricht en over berichten dat er Arabieren waren geweest die vlieglessen hadden genomen, maar hadden meegedeeld dat ze niet hoefden te leren hoe ze moesten opstijgen of landen. Die informatie was dus wel voorhanden, maar was om uiteenlopende redenen niet tijdig bijeengebracht, of, zoals de Amerikanen zeiden: *we didn't connect the dots*.

**Figuur 1. Vier typen dreigingen, geordend op basis van kennis**

		Kennis	
		Gekend	Ongekend
Metakennis	Gekend	Gekend gekend (Known known)	Gekend ongekend (Known unknown)
	Ongekend	Ongekend gekend (Unknown known)	Ongekend ongekend (Unknown unknown)

Mensen in de sfeer van intelligence houden zich met alle vier de typen dreigingen bezig. Het zal duidelijk zijn dat het ene type dreiging lastiger te detecteren is dan het andere. Natuurlijk vreest iedereen in het bijzonder de ongekende ongekende dreiging, zeker als het daarbij gaat om een gebeurtenis waarvan het weliswaar zeer onwaarschijnlijk is dat die zal plaatsvinden, maar die een grote impact zou hebben als het toch zou gebeuren. Denk bijvoorbeeld aan een terroristische aanslag met een massavernietigingswapen. Zal men die tijdig op het spoor komen of doet zo'n terroristische aanslag zich totaal onverwacht voor? Is dat het geval, dan is de kans groot dat de inlichtingen- en veiligheidsdiensten zal worden aangewreven. Er wordt dan gesproken van een *intelligence failure*, waarover meer in hoofdstuk 4.

Aan de andere kant hoeven inlichtingen- en veiligheidsdiensten niets of weinig te doen als het gaat om een dreiging waarvan de besluitvormers voortdurend alle ins en outs kennen. Wanneer er sprake is van zekerheid, is intelligence namelijk niet nodig. Besluitvormers doen slechts een beroep op intelligence wanneer zij zich onzeker voelen. Inlichtingendiensten moeten door het achterhalen van niet gemakkelijk verkrijgbare informatie de onzekerheid bij de besluitvormers wegnemen of in elk geval reduceren of beheersbaar maken. We kennen nu dus twee voorwaarden waaronder intelligence niet nodig zal zijn: ten eerste bij het ontbreken van competitie en ten tweede bij volkomen zekerheid aan de zijde van de besluitvormers. Van zo'n situatie is bijvoorbeeld sprake als de dreiging voorbij is. Wanneer de wedstrijd tegen Blauw-Zwart achter de rug is, heeft de coach van Rood-Wit geen behoefte meer aan het strijdplan van de tegenstander, tenzij hij heel erg houdt van bespiegelingen achteraf of historische interesses heeft. Anders gezegd: post mortem, als het lijk er al is, is intelligence niet nodig. Wanneer er een lijk wordt gevonden, wordt normaliter de politie ingeschakeld, niet een inlichtingen- of veiligheidsdienst. Rechercheurs gaan achteraf, na het delict, op zoek naar technische aanwijzingen of motieven die de dader kunnen verraden, die als bewijzen door een rechter of een