EDITORIAAL

Nota bene

De Militaire Spectator kan en mag niet aan het verschijnen van de nieuwe defensienota voorbij gaan. Wij hebben enkele auteurs benaderd met het verzoek de eigen visie op de defensienota te geven. Op deze wijze maakt de lezer kennis met meningen vanuit verschillende invalshoeken. Wij zijn de auteurs dankbaar voor hun bereidwilligheid om hun gedachten en opvattingen met ons te delen.

Precies drie jaar geleden droeg het editoriaal de titel 'visie gevraagd'.[1] Er werd gewezen op drie verschijnselen die in het bijzonder aandacht vroegen. Ten eerste de effecten van het verdwijnen van een zekere voorspelbaarheid in de internationale arena. Ten tweede wat kan worden geduid als *the transformation of war*. Het lijkt er meer en meer op dat het conventionele interstatelijke conflict een achterhaald concept is. Geweld lijkt steeds meer een zaak van andere partijen en groeperingen te worden. Ten slotte de effecten van technologische ontwikkelingen. In het verlengde daarvan werd geconstateerd dat veiligheid een zodanig complex begrip lijkt te zijn geworden dat het de aandacht van meer ministeries vraagt dan die van Buitenlandse Zaken en Defensie. Het lijkt logisch dat ook Algemene Zaken, Economische Zaken, Justitie, Financiën en Binnenlandse Zaken aan een integrale benadering gaan bijdragen.
Eenzelfde logica, aldus de boodschap uit 1997, pleit ervoor ook binnen internationale kaders als NAVO en Europese Unie na te gaan of veiligheid niet vanuit een te eng perspectief wordt benaderd. Deze boodschap is nog steeds relevant. Het voorbeeld *Information Operations* moge dit verduidelijken.

1 MS **166** (1997) 1-97, blz. 2-3.
2 Lezing tijdens het symposium 'Information Operations' aan de KMA te Breda. De tekst is opgenomen in de *Netherlands Annual Review of Military Studies 1999*: 'Information Operations'.

Generaal-majoor Gardeta van de *International Military Staff, NATO Headquarters* gaf bij een lezing begin december aan dat dit thema van kritiek belang is voor de lidstaten.[2] Information Operations kunnen het functioneren van de staat beïnvloeden. Dat informatie een essentieel middel is en dus een belangrijk doel kan zijn, is een oude wijsheid. Inlichtingen en veiligheidsdiensten ontlenen er hun bestaansrecht aan. Dat informatie een wapen kan zijn, is ook niet nieuw. De NAVO heeft niet voor niets sinds 1995 een *Command and Control Warfare Policy* (C2W). Deze ligt vast in de MC-348. Het doel van C2W is duidelijk:

> *to deny information to, influence, degrade or destroy an adversary's command and control capability while protecting against similar actions.*

De NAVO heeft de nodige ervaring met het toepassen van dit concept bij het uitvoeren van operaties. Tegelijkertijd moet worden geconstateerd dat de wereld complexer is geworden. Crisis en conflict komen veelal niet uit de lucht vallen. Daarnaast is veelal – zeker in de aanloop naar een dergelijke situatie – minder duidelijk wie vriend, tegenstander of belangstellende toeschouwer is. Informatie speelt dus een belangrijke rol, ook in wat wel als 'alledag' wordt geduid. De media vormen daarbij de brug tussen boodschappen en ontvangers. Hun invloed moet niet overschat, noch minder onderschat worden.

De andere kant van de technologie-medaille is dat staten, bondgenootschappen en anderen voor het opslaan, behandelen, gebruiken en verspreiden van informatie afhankelijk zijn geworden van energie, computers en verbindingen. Ten slotte wordt meer en meer duidelijk dat besluitvorming in de internationale arena een spel is waarin vele spelers van invloed kunnen zijn. Overigens leiden deze bevindingen niet alleen tot het onderkennen van risico's. Er liggen in deze bevindingen ook kansen. Gegeven het vorenstaande zou immers ook kunnen worden gezocht naar wegen om informatie te gebruiken om conflicten te voorkomen of om een crisis te de-escaleren. Dit alles bracht de NAVO tot het formuleren van een *Information Operations Policy*. De NAVO-council stemde in januari 1999 met dit document, de MC-422, in. Dergelijke operaties worden gedefinieerd als:

actions taken to influence decision-makers in support of political and military objectives by affecting others information, information based processes; Command and Control Systems and Command Information Systems while exploiting and protecting one's own information and/or information systems.

Waartegen is bescherming nodig? Een opponent kan het bondgenootschap, al dan niet direct, raken door mediacampagnes, psychologische oorlogvoering, elektronische oorlogvoering, misleiding, fysiek geweld en het aangrijpen van *netwerken en verbindingen*. Omgekeerd staat ook het bondgenootschap in theorie dezelfde instrumenten ter beschikking. Het zal niet verbazen dat het document nadrukkelijk vaststelt dat het bondgenoodschap afstand neemt van valse propaganda en leugens. Men is zich bewust van de oude waarheid: al is de leugen nog zo snel, de waarheid achterhaalt haar wel. Information Operations omvatten dus zowel de continue besluitvorming binnen het bondgenootschap, het politieke consultatieproces, de militair-strategische werkelijkheid én de dialoog met de omgeving. C2W is de militaire toepassing van Information Operations tegen een of meer feitelijke tegenstanders. In de komende periode gaat men zich op de nadere consequenties bezinnen.

Belangrijk onderdeel van het concept is overigens *Information Assurance*. Hoe stellen we zeker dat de nationale, internationale en bondgenootschappelijke informatie-infrastructuren worden beschermd? Hoe beveiligen we vitale informatie in databanken en computersystemen? Op dit gebied zijn er beduidend meer vragen dan antwoorden. Robert Ayers schetst dit probleem tijdens een in 1998 door het *Royal United Services Institute for Defence Studies* (RUSI) georganiseerde conferentie.[3] Hij was in 1995 directeur *Information System Security* programma van het Amerikaanse *Department of Defence*. In 1992 begon hij met het controleren van de veiligheid van defensiesystemen. Eind 1995 waren er 18.000 systemen getest. In 88 procent van de gevallen verkreeg men controle over het systeem; de eigenaar had als het ware het beheer over het systeem verloren. In 96 procent werd niet ontdekt dat een ander 'in control' was. Wat nog meer verbaasde: de 4 procent die ontdekte dat er iets niet klopte, reageerde niet of nauwelijks. Ayers komt tot de conclusie dat slechts één op de 500 acties tegen computersystemen wordt gerapporteerd.

Gegeven het feit dat er 1995 555 acties 'van buiten defensie' werden gerapporteerd zouden er 250.000 acties kunnen hebben plaatsgevonden.

In 1995 vond in de VS de oefening 'Global 95' plaats. Het scenario omvatte een systematische aanval op de nationale informatie-infrastructuur. Doelwit waren telefoonsystemen, digitale netwerken, *air traffic control*, spoorwegen, en de olievoorziening. De belangrijkste les was wel dat er geen enkele structuur bestond waarin overheid en bedrijfsleven met elkaar konden overleggen over de problemen, de effecten en mogelijke oplossingen. De overheid heeft allang haar greep op de informatie-infrastructuur losgelaten. Het beveiligen ervan wordt daarmee tot een complex probleem en dit geldt voor alle moderne westerse landen.

Ayers gaf aan hoe hij een informatieoorlog met de VS zou voeren. Hij zou het met één miljoen dollar kunnen doen. Hij zou naar de Universiteit van Californië gaan en de tien beste computerdeskundigen onder de studenten aantrekken. Hij zou ze 100.000 dollar per jaar geven en opdracht geven om met zestig voorstellen te komen om de nationale infrastructuur aan te grijpen. Het zou hen waarschijnlijk slechts ongeveer acht uur werk kosten. Zoiets zou iedereen kunnen bedenken.

De *Defensienota 2000* geeft aan dat het besef van kwetsbaarheid bestaat: 'gegeven de grote afhankelijkheid van Informatie- en Communicatietechnologie (ICT) kan immers niet worden uitgesloten dat in de toekomst wordt getracht Defensie juist op dit terrein te treffen'. Dit is waar; de veiligheid kan echter ook op heel andere manieren in het geding raken. Niet alleen defensie is een mogelijk doel. Ook de energievoorziening, de financiële wereld, handel, verkeer en transport en de telecommunicatie kunnen tot doel worden. Veiligheid wordt meer en meer een zaak van allen. De boodschap van januari 1997 is voor herhaling vatbaar.

[3] Robert Ayers. 'The New threat: Information Warfare', RUSI-Journal, oktober 1998, blz. 23-27.