Information Warfare

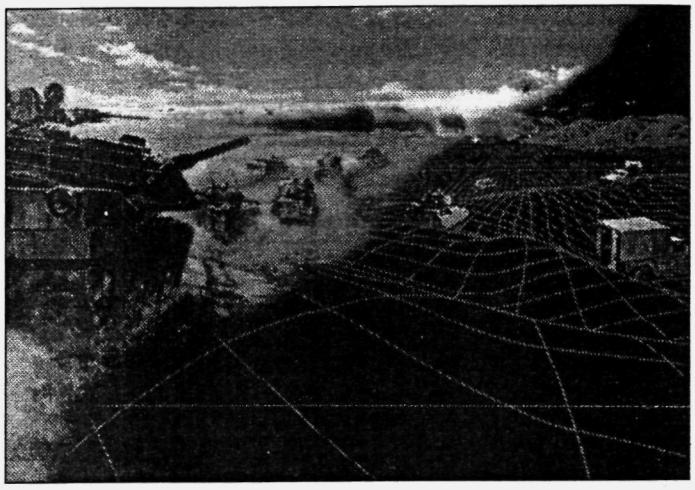
drs. ing. C.W. d'Huy

De tijden dat Defensie zich opmaakte om met massale middelen de veronderstelde dreiging uit het oosten tegen te gaan zijn voorbij. Deze wijze van optreden stond ook wel bekend als attritie-oorlogvoering waarin getracht werd de vijandelijke eenheden tijdens het gevecht meer te laten 'slijten' dan de eigen eenheden. Dit resulteerde met name in een wapenwedloop waarin men met aantallen (hoeveelheden tanks, artilleriestukken, soldaten et cetera) versus kwaliteit (precisie en vernietigingsvermogen) elkaar probeerde te imponeren. In de huidige geo-politieke situatie is dit niet langer wenselijk. De enorme kosten die gepaard gaan met de instandhouding van een grote strijdkracht alsmede de sociaal-maatschappelijke implicaties die dit met zich meebrengt hebben geleid tot een herbezinning van de manier van oorlogvoering [4].

Van oudsher is het ter beschikking hebben van informatie over het weer, het terrein, de vijand en de eigen organisatie van essentieel belang geweest. Nu de slagkracht niet langer primair ontleend kan worden aan de omvang van de strijdmacht, is het goed om te onderzoeken hoe de informatieverzorging binnen de eigen troepen verbeterd kan worden en hoe we die van de vijand op een voor hem nadelige wijze kunnen beïnvloeden (1). Alle activiteiten die gericht zijn op het verkrijgen en behouden van een informatievoorsprong op de vijand kunnen worden samengevat onder de term 'Information Warfare'. In dit artikel zal in vogelvlucht nader worden ingegaan op de manier waarop informatieverzorging een rol speelt in Information Warfare.

Informatieverzorging

Informatieverzorging kan worden gedefinieerd als: 'het doelgericht verwerven, verwerken, vastleggen, presenteren, distribueren en transporteren van informatie'. De informatieverzorging ondersteunt de besluitvorming en bevelvoering van een commandant en is bepalend voor de kwaliteit daarvan.
Wanneer men in militaire zin spreekt over de verbetering van de informatieverzorging dan richt deze zich op twee doelen: ten eerste het verbeteren van de zogenaamde 'Situational Awareness', en ten tweede het verbeteren van de relatie 'Sensor-to-Shooter'.
Situational Awareness (SA) houdt in het bewust zijn van de eigen positie, rol en status in relatie tot eigen, vijandelijke en neutrale eenheden in het operatiegebied. Een goede SA is een zeer belangrijke component die een effectieve, doelmatige en niet te vergeten veilige (2) inzet van militaire eenheden te verwezenlijken. Het keer op keer inschatten van de situatie in een operatiegebied vormt de basis voor alle activiteiten die men in dat gebied wil gaan ontplooien. Dit kan uiteenlopen van het plannen van een operatie door een brigadecommandant tot het al dan niet aangaan van het gevecht door de individuele soldaat. Voor het verkrijgen van SA is verwerving van informatie over het slagveld en alles wat zich daarop beweegt en afspeelt essentieel. Hoe kunnen we nu de SA proberen te verbeteren? In min of meer willekeurige volgorde kan aandacht besteed worden aan de volgende onderwerpen.



Figuur 1: Het gedigitaliseerde slagveld (© TRW)

De kwantiteit van informatie

De waarschijnlijk meest voor de hand liggende methode is het verwerven van meer informatie (het breder maken van de informatiebasis) dan waarover men reeds beschikt. Indien het volume van de informatie groeit dient men er echter wel rekening mee te houden dat het overzicht over de informatie verloren kan raken. In de praktijk wordt deze kwantitatieve aanpak vaak sterk begrensd door de schaarse middelen die voor het verwerven van informatie te beschikking staan. Bovendien, de groei van de informatiestroom wordt eveneens begrensd door de fysieke bandbreedte van de communicatiemedia waarover men de beschikking heeft (telefoon, radio's et cetera).

De kwaliteit van informatie

Een tweede methode richt zich op de verwerving van kwalitatief betere informatie (verdieping van de informatiebasis). De behoefte tot betere informatie vloeit voort uit de observatie dat informatie vaak te globaal (mate van detail), onnauwkeurig (precisie) of onzeker (geldigheid) is.

De actualiteit van informatie

Het gebeurt helaas nog te vaak dat informatie te laat (na het beslissingsmoment) arriveert. Het gevolg is dat men met incomplete en/of verouderde gegevens moet werken, hetgeen mogelijkerwijs de kwaliteit van een beslissing nadelig beïnvloedt.
Gerelateerd aan het tijdig kunnen beschikken over informatie is het sneller of vaker (verversingsfrequentie) verwerven van informatie waardoor het beslissingsmoment in de tijd naar voren gebracht kan worden.

De beschikbaarheid van informatie

Informatie is vaak wel in een organisatie aanwezig maar niet altijd op de plek waar zij nodig is. Voor een deel wordt dit veroorzaakt doordat er geen adequaat mechanisme is om informatie

binnen de eigen organisatie te distribueren (repliceren). Het tegenovergestelde: alle informatie naar iedereen repliceren is om begrijpelijke redenen niet gewenst; een mechanisme voor het filteren van informatie is dus nauw gerelateerd aan het repliceren.

De functionaliteit van informatie

Zelfs indien alle informatie aanwezig is, is het nog steeds zaak dat men in staat moet zijn om op een begrijpelijke en eenduidige wijze met deze informatie te kunnen interacteren. Juist op het gebied van de mens-machine-interface valt voor de meeste militaire (informatie)systemen vaak nog veel te verbeteren.
Een meer geavanceerde methode is het afleiden van nieuwe informatie uit de reeds bestaande gegevens. Informatiecorrelatie, informatieaggregatie en informatiefusie zijn hierbij de te gebruiken technieken om nieuwe informatie af te leiden. Een fictief voorbeeld hierbij is dat wanneer men vier maal een tank heeft waargenomen binnen een bepaald gebied men vermoedelijk te maken heeft met een tankpeloton.
Opgestelde hypotheses, gemaakte aannames en conclusies, en daadwerkelijk observaties moeten constant met elkaar in verband gebracht worden. Het gebruik van kennistechnologie (onder meer truth-maintenance algoritmes) bij de bouw van systemen die tot informatiecorrelatie, -aggregatie en -fusie in staat zijn ligt dan ook voor de hand.

De prijs van informatie

Een interessante vraag is welke prijs men bereid is te betalen voor de verwerving van bepaalde informatie. Uit puur economische (bijvoorbeeld de prijs van een bepaald type sensor) en/of militair tactische redenen (gebruik van schaarse middelen en tijd) zal men vaak genoodzaakt zijn om af te zien van de mogelijke vergaring van bepaalde informatie. De verbetering van de geschetste kosten-batenverhouding is één van de belangrijkste aandachtspunten van de Nederlandse krijgsmacht. De wens om zoveel mogelijk 'commercial off the shelf' hardware en software te gebruiken begint dan ook binnen Defensie gemeengoed te worden.

Verbeteren relatie Sensor-Decider-Shooter

Nu de krijgsmacht in omvang sterk afneemt, zal op het moment suprême nog beter gebruik gemaakt moeten worden van de steeds schaarser wordende middelen. Er zal gestreefd moeten worden naar een situatie waarin zoals de Amerikanen het omschrijven: 'Every sensor is sensing, every decider is deciding, every shooter is shooting, and every supporter is supporting'. Een dergelijke situatie zal echter de meeste vruchten afwerpen wanneer de informatieverzorging optimaal is. De hierboven beschreven Situational Awareness vormt hierbij een belangrijke component in de besluitvorming maar minstens zo belangrijk is de rol die informatietechnologie speelt in de bevelvoering (de aansturing van de eenheden). Het accuraat en in 'near real time' kunnen aansturen van eenheden middels een efficiënte informatieverzorging is uiteindelijk van doorslaggevend belang voor het effectief uitvoeren van een operatie.

Middelen

Welke middelen staan nu tot onze beschikking om het slagveld te informatiseren? Allereerst hebben we te maken met een scala van communicatiemiddelen. Voorbeelden hiervan zijn: zogenaamde combat net radio's, straalzenders en satellietcommunicatie. Belangrijke parameters hiervan zijn het bereik, de bandbreedte en de geschiktheid voor datacommunicatie. Momenteel is het gebruik van deze verbindingsmiddelen sterk gelieerd aan de eenheid die ze gebruikt en zijn ze onderling meestal niet interoperabel. Met name voor datacommunicatie is dit laatste een vervelende eigenschap. Met het streven naar een tactisch internet waar het voor de gebruiker transparant is welk verbindingsmiddel gebruikt wordt tracht men daar iets aan te doen.
Ten tweede komen er steeds meer sensoren tot de beschikking van de militair. Voorbeelden hiervan zijn: allerlei navigatiemiddelen als het elektronische kompas en het Global Positioning System (GPS); waarnemingsmiddelen als warmtebeeld- en daglichtcamera's, slagveldradars, combat identification devices en laser-afstandsmeters. Veel van deze systemen zijn in principe ontworpen als stand-alone/gesloten componenten; ze bestaan in zowel digitale als analoge varianten en de wijze waarop ze met de buitenwereld kunnen communiceren (interfaces) is vaak beperkt.

Ten derde krijgt de hedendaagse militair op elk niveau te maken met diverse computerhardware en software die het werk zouden moeten vereenvoudigen en/of ondersteunen. Dit betekent in ieder geval de introductie van basiskantoorautomatisering in een legergroene omgeving (het kantoor te velde). Maar ook het gebruik van meer geavanceerde beslissingsondersteunende programmatuur als (geografische) gegevensanalyse (GIS), planningstools en de al eerder genoemde informatiefusiesoftware.
Al deze middelen zullen op verschillende plekken op het slagveld verschijnen: in bunkers, in commandoposten, in voertuigen, op het wapensysteem of gedragen door de individuele soldaat. Met andere woorden: voor de hogere eenheden zal meer sprake zijn van een gemilitariseerde kantooromgeving, voor de lagere eenheden van 'embedded systems'.
Dit betekent dat men name in dit laatste geval de omgeving een sterke invloed zal hebben op de mogelijkheden en fysieke verschijningsvormen van de middelen. Het naadloos op elkaar afstemmen van alle hierboven genoemde middelen (interoperabiliteit en integratie) is dé belangrijkste ontwikkeling in de militaire informatieverzorging van dit moment en wordt samengevat onder de titel: Digitalisatie van het slagveld. Hierbij is van belang dat de middelen niet alleen hardware-technisch gezien op elkaar afgestemd zijn maar ook moeten ze conceptueel de zelfde taal spreken; de ontwikkeling van een algemeen geaccepteerd corporate datamodel is daarbij het middel.

Counter measures

In het voorgaande is de nadruk met name gelegd op het verkrijgen van een optimale 'Situational Awareness' bij de eigen eenheden. Het is echter ook interessant om te onderzoeken hoe we die bij de tegenpartij op een nadelige manier kunnen beïnvloeden. Hierbij kunnen we twee verschijningsvormen van Information Warfare onderscheiden: Command & Control warfare (C2W), en defensive Intelligence-based Warfare (IBW) [1], [2].

Command & Control warfare

C2W richt zich met name op het raken van 'het hoofd' (commandoposten en beslissingscentra), en 'de nek' (communicatienetwerken) van de vijandelijke eenheden. Voor beide doelstellingen bedient men zich in algemene zin van de volgende technieken:

- Jamming (door radioverbindingen en netwerken te storen wordt de communicatie bemoeilijkt);
- Spoofing (men breekt in op een communicatiekanaal en doet zich voor als een bevriende partij. Echter door op dit kanaal eveneens moeilijk van echt te onderscheiden maar onjuiste informatie te verspreiden probeert men de tegenstander op het verkeerde been te zetten);
- Offensive hacking (hieronder verstaat men allerlei technieken die uit de zelfkant van de informatietechnologie afkomstig zijn. Hiertoe behoren onder meer virussen (en in het bijzonder de zogenaamde 'logic bomb') en 'chipping' [3]. Dit laatste betreft het aanbrengen van booby-traps op computerchips die mogelijkerwijs in wapensystemen gebruikt zouden kunnen worden. Onder normale omstandigheden werkt zo'n chip normaal, echter wanneer deze naar de mening van de aanbrenger van de booby-trap verkeerd wordt gebruikt dan vernietigt hij zichzelf.
- Vernieling (een zeer voor de hand liggende techniek is het met een hoge precisie fysiek uitschakelen van communicatienetwerken en commandoposten (surgical strike). Hiervoor kan men conventionele middelen gebruiken (bijvoorbeeld smart weapons) maar ook meer geavanceerde als de EMP-bom (elektromagnetische puls) en de HERF-gun (High Energy Radio Frequency). In beide gevallen wordt een zeer sterke puls opgewekt die (alle) elektronische componenten in de omgeving laat doorbranden. De HERF-gun wordt gericht op een uit te schakelen object, een EMP-bom daarentegen is vele malen krachtiger en kan een groot gebied bestrijken.

Defensive Intelligence-based warfare

Defensive IBW richt zich op de negatieve beïnvloeding van de vijandelijke informatievergaring. Dit betekent dat men zich ondermeer bezig houdt met het opsporen van de vijandelijke sensoren. Als bekend is waar welke sensoren geplaatst zijn dan kan men er rekening mee houden (denk hierbij bijvoorbeeld aan het ontwijken van vijandelijke radarstations door vliegtuigen). Wanneer de positie van een sensor bekend is dan kan men deze ook trachten uit te schakelen. Een voorbeeld hiervan is de zogenaamde 'anti radiation missile' die gebruikt wordt om vijandelijke radarsystemen uit te schakelen. Daarnaast is het mogelijk om de sensoren te storen (bijvoorbeeld door middel van een 'radar jammer'), minder nauwkeurig te maken (door middel van Stealth-technieken), of te overvoeren met informatie ('clutter'). Een laatste vorm van Defensive IBW betreft alles wat de maken heeft met de versluiering van eigen activiteiten en misleiding van de tegenstander. Het gebruik van 'decoys' voor wapensystemen (bijvoorbeeld nep SCUD-raketten) en commandoposten in de golfoorlog is daarbij illustratief.

Counter-Counter measures

Ook in information warfare geldt regeren is vooruit zien. Met andere woorden ook de vijand kan zich van information warfare counter measures bedienen en dus zullen we daar op moeten reageren. Men zal er tenminste voor moeten zorgen dat alle sensoren en commandoposten moeilijk te vinden zijn. Dit betekent dat zij voldoende gecamoufleerd (optisch) dienen te zijn en zo min mogelijk ongewenste infrarode en elektromagnetische uitstraling veroorzaken (isolatie- en zogenaamde TEMPEST-maatregelen). Actieve sensoren daarentegen moeten juist enige mate van straling uitzenden willen ze überhaupt kunnen werken (bijvoorbeeld radar). Deze emissies moeten zo kort mogelijk gehouden worden (korte detectietijd), over een zo groot mogelijk deel van het spectrum verspreid zijn (moeilijk te storen) en zelf gebruikmaken van misleidingstechnieken (chirping en sputtering).

Natuurlijk wordt er ook van allerlei beveiligingstechnieken gebruik gemaakt. We kunnen hierbij denken aan beveiliging met betrekking tot toegang tot bepaalde ruimten, toegang tot computerapparatuur, toegang tot informatie (cryptografie en 'file access'), toegang tot netwerken en toegang tot communicatiemedia. De landmacht maakt momenteel al gebruik van combat net radio's die een aantal keer per seconde over een brede band van radiofrequentie veranderen ('frequency hopping') en daardoor moeilijk te storen zijn. Omdat ze met een betrekkelijk hoog vermogen uitzenden zijn ze wel met relatief eenvoudige middelen op te sporen. Een meer geavanceerde vorm van spread spectrum communicatie ontstaat wanneer tegelijkertijd met een laag vermogen over meerdere frequenties wordt uitgezonden. Per gebruikte frequentie is het vermogen zo laag dat het signaal nauwelijks van de achtergrondruis te onderscheiden is, alleen alle gebruikte frequenties tezamen maken het mogelijk het originele signaal te decoderen. Per gebruiker wordt via een code de te gebruiken frequenties vastgelegd (Code Division Multiple Access). Het mogelijk meest tot de verbeelding sprekend is stealth-communicatie. Bij deze communicatietechniek wordt op een frequentie van 60 gigahertz uitgezonden. Communicatie bij dergelijke hoge frequenties is zeer moeilijk opspoorbaar; het signaal dooft namelijk zeer snel uit en heeft dus een beperkte dracht.

'Welke prijs is men bereid te betalen voor verwerving van bepaalde informatie?'

Naast al deze min of meer high-tech maatregelen zijn er ook enkele eenvoudigere benaderingen te volgen. Allereerst kunnen we zoveel sensoren inzetten dat de vijand deze onmogelijk allemaal kan uitschakelen ('too many sensors to kill'). Daarnaast zijn uiteraard ook traditionele beschermingstechnieken (bijvoorbeeld bepantsering) te gebruiken. Ook het verhogen van de mobiliteit van de kwetsbare systemen verlaagt de kans op uitschakeling. Verder kan er ook een economische benadering gevolgd worden waarin de kosten van het uitschakelen van een sensor die van de sensor zelf vele malen overtreffen ('too cheap a sensor to kill'). Gelukkig kunnen we wat betreft counter-counter measures dankbaar gebruik maken van ontwikkelingen uit de civiele hoek. Met name de bescherming van allerlei financiële (informatie)systemen uit de bank- en aandelenwereld tegen natuurrampen en/of ongewenst gebruik door derden, vertoont een verrassende gelijkenis met die van de militaire informatieverzorging.

Conclusies

Information Warfare is onlosmakelijk verbonden met oorlogsvoering in het algemeen. Dit is niet een nieuw fenomeen van de moderne tijd; het verzamelen van inlichtingen over de vijand en zijn mogelijke activiteiten is bijvoorbeeld altijd al belangrijk geweest. Nu we als gevolg van de veranderde geo-politieke situatie de slagkracht niet langer meer kunnen ontlenen aan de

omvang van de strijdmacht moeten we ons meer en meer gaan richten op andere manieren om deze te verbeteren.
Middelen ter verbetering van de informatieverzorging gericht op het bereiken van een optimale 'situational awareness' vormen daarbij één manier. Met deze middelen moet men echter ook de mogelijke tegenmaatregelen en tegen-tegenmaatregelen in beschouwing nemen. Op deze drie gebieden staan we slechts aan het begin van wat er technisch mogelijk is en kunnen we mogelijkerwijs getuigen zijn van een nieuwe wedloop: 'de slagveldinformatiseringswedloop'.

Referenties

[1] Libicki, M., What is Information Warfare, Institute for National Strategic Studies, USA.
[2] Information Warfare, Fact sheet 95-20, US Air Force, Doctrine Division Office.
[3] Washington, D.W., Onward Cyber Soldiers, TIME Magazine, August 21, 1995, Volume 146, No 8.
[4] Toffler, A. & H., War and anti War, Survival at the dawn of the 21st century, Little, Brown 1993

Noten

(1) Een andere maar wel hieraan gerelateerde trend is de ontwikkeling van precisie / intelligente wapensystemen (zogenaamde intelligent munitions en smart weapons).
(2) Broedermoord (fratricide) wordt vaak veroorzaakt door de onzekerheid of men met een vriend of vijand te maken heeft. Denk hierbij ook aan een van Murphy's laws of combat: 'Friendly fire isn't'.

Cees d'Huy is werkzaam bij TNO Defensieonderzoek Fysisch en Elektronisch Laboratorium, divisie Command & control en simulatie, en momenteel gedetacheerd bij het projectteam Battlefield Management Systemen onder regie van de Landmachtstaf.

Battlefield Digitization

Drs. R.J.M. Groen

Onder digitalisatie wordt het geheel van maatregelen verstaan om het tijdig toepassen van informatietechnologie (IT) ter verhoging van de operationele effectiviteit van krijgsmachtdelen mogelijk te maken. Digitalisatie moet er toe leiden dat commandanten, staven en uitvoerders tijdig worden voorzien van essentiële informatie. Op de niveaus brigade en hoger wordt hier in voorzien door invoering van een stafinformatiesysteem. Op de niveaus eskadron of compagnie en lager is sprake van meer taakgerichte systemen, bijvoorbeeld ter ondersteuning van verkenning, artillerie, cavalerie en dergelijke.

Deze systemen worden algemeen aangeduid als Battlefield Management Systems (BMS). In een BMS vindt ook verwerking van sensor- en voertuig(platform)informatie plaats. Hierbij kan bijvoorbeeld gedacht worden aan plaatsbepalingsapparatuur (GPS) en laserafstandsmeters, maar ook voertuigsensoren die gegevens leveren over brandstofvoorraad, bandenspanning, wapenstatus en munitievoorraad.
Voor het bataljonsniveau dat zich daartussen bevindt, lijkt het vanwege het meer 'verbonden' karakter van dit niveau, voor de hand liggend dat daar eerder behoefte bestaat aan een stafinformatiesysteem, dan aan een BMS.
Ook de enkele soldaat zal niet ontkomen aan digitalisatie. Op dit moment zijn al laboratoriumversies beschikbaar van 'wearable computers', waarbij de harde schijf, de batterij en de verwerkingseenheid in een riem worden verwerkt, en de gegevens via een zogenaamde heads-up-display aan haar of hem worden getoond. Het gebruik van 'palmtop' computers is in de civiele wereld al ingeburgerd, het gebruik van dergelijke systemen door de militair zal niet lang meer op zich laten wachten.
Van groot belang is dat al deze systemen verticaal én horizontaal naadloos op elkaar aansluiten, waardoor een zo compleet mogelijk omgevingsbeeld (Situational Awareness) ontstaat.

Internationale ontwikkelingen

Een van de belangrijkste buitenlandse ontwikkelingen op het gebied van digitalisatie van het gevechtsveld vindt plaats in de Verenigde Staten. In de US Army wordt een complete brigade in het kader van het 'Task Force XXI advanced warfighting experiment' (kortweg TFXXI) gedigitaliseerd. Hierbij wordt gebruik gemaakt van verschillende bestaande en nieuw ontwikkelde hardware en software, die inmiddels onder de verzamelnaam 'Appliqué' bekend is geworden. Een en ander is onder leiding van hoofdaannemer TRW ontwikkeld. De Appliqué-systemen kenmerken zich doordat zij allen voorzien zijn van dezelfde grafische gebruikers interface, ongeacht waar in de organisatie de systemen worden ingezet. De beschikbare applicaties verschillen per taakstelling van de eenheid. Ook wat betreft de hardware wordt onderscheid gemaakt ten behoeve van de specifieke omgevingseisen. In een tank wordt gemilitariseerde hardware gebruikt, in tenten kan volstaan worden met 'ruggedised' apparatuur, terwijl in kantoor-shelters vaak civiele apparatuur voldoet.
TFXXI is tevens de eerste grote veldtest van een speciaal voor smalbandige verbindingen ontwikkeld berichtenformaat. Dit bit-georiënteerde formaat is efficiënter dan de tot nog toe gangbare karakter-georiënteerde formaten, iets dat van cruciaal belang is in omstandigheden waar de verbindingen worden gerealiseerd door Combat Net Radio's en waardoor de capaciteit vaak beperkt is tot maximaal 1000 bps. Ook de gebruikte netwerkprotocollen zijn aan specifieke militaire omstandigheden en eisen aangepast, maar wel zo dat het netwerk zich 'aan de buitenkant' laat zien als een standaard IP-netwerk, waar standaard