Toespraak van de minister van Defensie, J.S.J. Hillen, ter gelegenheid van het NLDA Cyber Symposium op 27 juni 2012 te Breda. Let op: Alleen gesproken woord geldt!

De zwaardmacht in het digitale domein

Op 1 november 1911 wierp de Italiaanse piloot Giulio Gavotti vier bommen op Turkse stellingen in Libië. Hij voerde daarmee de eerste luchtaanval in de geschiedenis uit. Een nieuw domein voor oorlogvoering was geboren.

Niet dat iedereen dit onmiddellijk door had. In hetzelfde jaar verkondigde Ferdinand Foch, de latere Franse maarschalk in de Eerste Wereldoorlog, nog dat "vliegen leuk is als sport maar als oorlogswapen waardeloos."

Drie decennia later, in de Tweede Oorlog, bleek echter de dodelijke effectiviteit van het luchtwapen en kreeg Foch ongelijk. Of zoals Erwin Rommel, de Duitse generaal, aan het einde van die oorlog verzuchtte:

"Iemand die, zelfs met de modernste wapens, tegen een vijand moet vechten die over volledige controle van het luchtruim beschikt, vecht als een wilde tegen moderne Europese eenheden, met dezelfde beperkingen en dezelfde kans op succes."

En nu is er dus weer een nieuw domein ontstaan voor militair optreden. Een domein dat door de mens is gecreëerd. Naast het land, de lucht, de zee en de ruimte, is *cyber* het inmiddels vijfde domein voor militair optreden.

Dit digitale domein en de toepassing van digitale middelen als wapen of als inlichtingeninstrument zijn sterk in ontwikkeling. Waar gaat deze ontwikkeling heen? En wat betekent zij voor de Nederlandse krijgsmacht?

Het is terecht dat de Nederlandse Defensieacademie aan deze vragen een hele dag wijdt. Ik voorspel u: er zullen nog vele dagen als deze volgen. Want honderd jaar na 1911 staan we naar mijn overtuiging aan het begin van opnieuw een belangrijke verandering in het militaire optreden. Een ontwikkeling die *the face of battle*, zoals de Brit John Keegan het uitdrukte, de komende decennia zal veranderen.

Laat ik met het positieve beginnen.

Het internet is een enorme verrijking voor de samenleving gebleken en een motor voor economische groei. Digitale middelen maken mogelijk wat vroeger nog onbereikbaar leek.

Defensie wil optimaal van deze mogelijkheden gebruik maken. De digitale technologie stelt de krijgsmacht in staat haar taken doeltreffender en doelmatiger uit te voeren. Zo functioneren vrijwel alle wapensystemen dankzij het gebruik van ICT-componenten. Ook de commandovoering en de logistieke ondersteuning leunen zwaar op digitale systemen. De krijgsmacht is bijna net zo afhankelijk van ICT als Bol.com. Zonder digitale middelen kan zowel onze samenleving als onze krijgsmacht nauwelijks meer functioneren. Zij zijn van levensbelang geworden.

Ook de opkomst van het digitale domein is overigens niet door iedereen op waarde geschat. Zo voorspelde Thomas Watson, bestuursvoorzitter van IBM, in 1943 dat er een wereldmarkt voor misschien vijf computers zou zijn.

Wat ook opvalt – en nu kom ik bij de keerzijde van het digitale fenomeen– is een gebrek aan bewustzijn over de risico's die zijn verbonden aan de explosieve groei van computernetwerken. Bij de ontwikkeling van hardware en software en het inrichten van netwerken werd – en wordt – nauwelijks aandacht besteed aan beveiliging. En dit terwijl het eerste computervirus al in 1971 het licht zag.

De aandacht voor bescherming van netwerken hield, kortom, geen gelijke tred met de groei van het digitale domein.

Pas de laatste jaren is sprake van een inhaalslag. *Cyber security* staat nu volop in de aandacht.

En terecht, want de digitale dreiging is reëel. Deze dreiging kan een ICT-afhankelijke samenleving als de onze op tal van manieren ontregelen. Niet alleen in technische zin: denk aan het uitvallen van het bancaire systeem. Maar ook in psychologische zin: denk aan de angst, de paniek en wellicht de toegeeflijkheid jegens de agressor die kan optreden als onze digitale systemen op grote schaal worden gesaboteerd. De gevolgen van een aanval zullen zich niet tot het digitale domein beperken maar ook verregaande gevolgen hebben voor de samenleving als geheel.

Tegen deze dreiging moet onze samenleving zich wapenen. Dat geldt ook voor de krijgsmacht. De Stuxnet en Flame aanvallen hebben duidelijk gemaakt dat ook in het digitale domein conflicten kunnen worden uitgevochten en dat de impact hiervan groot kan zijn.

Veel is nog onduidelijk over de aard van digitale conflicten. Hoe zullen staten en niet-statelijke actoren van het digitale domein gebruik maken om hun politiek doelen te verwezenlijken? Hoe zullen de cyber wapens van de toekomst er uit zien? Het is nog speculeren.

We kunnen het ons echter niet veroorloven lijdzaam af te wachten en maar te zien wat anderen bedenken. Vrijwel alles wat iemand zich kan verbeelden, zo leert de geschiedenis, zal vroeg of laat ook worden gemaakt. Denk maar aan de fantasievolle verhalen van Jules Verne.

Zo zullen ook digitale wapens waarschijnlijk sneller dan we verwachten hun opwachting maken als vast bestanddeel van militaire arsenalen. Defensie moet over verbeeldingskracht beschikken, zowel om de mogelijkheden die het digitale domein biedt met beide handen aan te grijpen als om zich te wapenen tegen wat komen gaat.

Maar wat betekent het om de zwaardmacht in *cyber space* te zijn? Hoe moet de krijgsmacht haar bijzondere taken en verantwoordelijkheden in het digitale domein vervullen?

De digitale uitdaging is, zoveel staat vast, ook in militair opzicht grensverleggend. In de fysieke wereld zijn grenzen over het algemeen duidelijk gedefinieerd, zijn de dreigingen en de tegenstanders over het algemeen goed in kaart te brengen.

In het digitale domein is dit allemaal een stuk minder duidelijk.

In dit domein is niet sprake van een afgebakend militair operatiegebied.

Evenmin is sprake van fysiek geweld.

En *toch* is het voorstelbaar dat door het verstoren van digitale systemen hele samenlevingen ontregeld raken of militaire doelen worden uitgeschakeld.

Het is van groot belang Defensie klaar te stomen voor deze nieuwe werkelijkheid, waarin de virtuele en de reële wereld in elkaar overvloeien.

Vandaag zal ik de Tweede Kamer daarom de defensiestrategie voor het militaire opereren in het digitale domein doen toekomen. De Defensie Cyber Strategie geeft de komende jaren richting, samenhang en focus aan de ontwikkeling van het militaire vermogen in het digitale domein.

In de strategie worden zes speerpunten genoemd. Aan de hand van deze speerpunten zal Defensie haar doelstellingen in het digitale domein verwezenlijken. Ik loop met u deze speerpunten kort even langs.

Integrale aanpak

Het eerste speerpunt betreft de totstandkoming van een integrale aanpak. Wegens het wijdvertakte en veelvormige karakter van het digitale domein, is centrale coördinatie nodig van alle activiteiten die aan het militaire optreden in het digitale domein zijn verbonden.

Ons uitgangspunt is dat de cybercapaciteiten van Defensie volledig geïntegreerd moeten worden in ons militair optreden. De kracht van digitale capaciteiten ligt in de mogelijkheden die deze bieden dit optreden langs alle lijnen en in alle domeinen te ondersteunen en te versterken.

Defensie zal geen afzonderlijk krijgsmachtdeel oprichten voor het optreden in het digitale domein. De operationele cybercapaciteiten zullen in 2014 wel worden ondergebracht in het Defensie Cyber Commando bij de landstrijdkrachten.

Defensief

Ons tweede speerpunt is de versterking van de digitale weerbaarheid van Defensie, de defensieve kant dus. De digitale zelfverdediging behelst de bescherming van netwerken, het monitoren en analyseren van dataverkeer, het onderkennen van digitale aanvallen en de reactie hierop.

Het Joint Informatievoorzieningscommando-in-oprichting (JIVC) en DefCERT hebben hierin een zeer belangrijke rol.

Maar hier rust ook een verantwoordelijkheid op de schouders van iedere defensiemedewerker. De belangrijkste kwetsbaarheid die kan leiden tot het verlies of het compromitteren van informatie komt namelijk voort uit onopzettelijk handelen door medewerkers, zoals ondeskundig of onzorgvuldig gebruik van ICT-middelen. Elke defensiemedewerker moet zich bewust worden van de risico's die aan het gebruik van digitale middelen verbonden zijn.

Offensief
Het derde speerpunt springt wellicht het meest in het oog: de ontwikkeling van het militaire vermogen om cyber operations uit te voeren.

Als zwaardmacht moet de krijgsmacht naar mijn overtuiging ook in het digitale domein offensief kunnen optreden. Het uitschakelen van een tegenstander blijft de bijzondere taak van de krijgsmacht. Ook in het digitale domein. Kennis van offensieve methoden en technieken is bovendien noodzakelijk voor het versterken van de digitale weerbaarheid.

Bij een *cyber attack* denkt men vaak nog aan de eenzame hacker die op zijn zolderkamer het netwerk van het Pentagon plat weet te leggen. Het digitale domein als asymmetrische arena waar David Goliath precies tussen de ogen weet te raken. Dit spreekt tot de verbeelding maar heeft waarschijnlijk weinig met de toekomstige realiteit te maken. Stuxnet en Flame zijn technologisch zeer complex en zijn daardoor zeer kostbaar. Niet iets dat een enthousiaste amateur in een avond in elkaar zet.

De ontwikkeling van offensieve operationele capaciteiten bevindt zich nog in de kinderschoenen. Er is nog veel onduidelijk over de aard van deze capaciteiten, de mogelijkheden die ze een commandant kunnen bieden en de effecten die ermee kunnen worden bereikt.

Bij het ontwikkelen van de offensieve operationele capaciteiten van de krijgsmacht zal gebruik worden gemaakt van kennis en capaciteit van de MIVD. De Commandant der Strijdkrachten kan de offensieve middelen op grond van een mandaat van de regering in een militaire operatie inzetten. De wettelijk vereiste scheiding tussen de taken en de verantwoordelijkheden van de Commandant der Strijdkrachten en de MIVD blijft daarbij onaangetast. Het al genoemde Defensie Cyber Commando draagt zorg voor de gereedstelling van offensieve cybercapaciteiten.

Inlichtingen

Ik noemde de MIVD al. De versterking van de inlichtingenpositie in het digitale domein, is ons vierde speerpunt.

Informatie is van levensbelang voor de krijgsmacht. Door de opkomst van het digitale domein en de toenemende onderlinge verbondenheid van systemen, zijn de mogelijkheden tot het vergaren van informatie enorm toegenomen. Het bezitten van een hoogwaardige inlichtingenpositie in het digitale domein is nodig voor zowel de bescherming van de eigen infrastructuur als het uitvoeren van operaties.

Een complexe uitdaging vormt de attributie van aanvallen. Als niet kan worden vastgesteld waar een aanval vandaan komt, is het nauwelijks mogelijk daarop te reageren. Voor de inlichtingendiensten is hier een belangrijke taak weggelegd.

Zij moeten inzicht hebben in zowel de technische dreiging als in de intenties van aanvallers. Ook zullen zij over het vermogen moeten beschikken om pogingen tot digitale spionage te verstoren en te stoppen.

Adaptief en innovatief

Om op de genoemde terreinen in het digitale domein – defensief, offensief *en* inlichtingen – succesvol te zijn, is meer nodig: de versterking van de kennispositie en van het innovatieve vermogen van Defensie in het digitale domein. Dit vormt dan ook het vijfde speerpunt in onze aanpak. De instelling van een cyberleerstoel bij de NLDA in 2014, die onder meer de volkenrechtelijke aspecten zal onderzoeken, maakt hiervan uiteraard deel uit. Maar ook de werving en het behoud van gekwalificeerd personeel zijn nadrukkelijk met dit speerpunt verbonden.

De snelheid waarmee ontwikkelingen in het digitale domein zich voltrekken, stelt zeer hoge eisen aan het aanpassingsvermogen en de innovatieve kracht van Defensie. Zij moet in het digitale domein in staat zijn snel nieuwe technologie in te voeren en korte innovatiecycli te doorlopen.

Defensie zal dan ook investeren in digitale technologie en onderzoek. Het Defensie Cyber Expertise Centrum wordt de plek waar de kennis wordt samengebracht. Voor onderzoek en ontwikkeling, maar ook voor opleiding, training en oefening zal Defensie beschikken over een 'cyber laboratorium' en een testomgeving.

Een bijzondere uitdaging voor Defensie vormt het aantrekken en behouden van gekwalificeerd personeel dat ook kan functioneren in een militaire omgeving. Om de noodzakelijke kennis, kunde en vaardigheden in huis te halen en te behouden wordt specifiek aandacht besteed aan personeelsbeleid en opleidingen. Specifieke loopbaanpatronen voor 'digitale soldaten' zijn daarbij zeker denkbaar.

Onze krijgsmacht stelt zich nadrukkelijk open voor mensen die digitale kennis in huis hebben, maar waar de overheid nog te weinig gebruik van maakt: de 'white hat hacker'-community, oftewel de bonafide hackers. Zij wijzen ons vaak op lekken. Daar moeten we niet boos om worden, maar gebruik van maken, want zo maken we elkaar sterker. Waarom zou een 'white hat hacker' zich niet willen inzetten om te helpen bij de verdediging van zijn eigen land? Zeker als hij daarvoor niet eens door de modder hoeft te kruipen, maar achter zijn computer kan blijven zitten.

Samenwerking

De intensivering van de samenwerking in nationaal en internationaal verband is, tot slot, ons zesde speerpunt.

In het digitale domein treden publieke en private, civiele en militaire en nationale en internationale actoren tegelijkertijd op. Een gezamenlijke aanpak is noodzakelijk.

Voor Defensie is het van belang om in het kader van de National Cyber Security Strategie nauw samen te werken met publieke en private partijen. Als beheerder van hoogwaardige digitale netwerken en systemen is Defensie zowel nationaal als internationaal een belangrijke partner.

In internationaal verband zal Defensie samenwerking zoeken met landen die een vergelijkbare aanpak voorstaan en die wat ontwikkeling betreft op vergelijkbaar niveau opereren. Doel van de samenwerking is in eerste instantie gericht op het uitwisselen van kennis. Daarna kan worden bezien of er mogelijkheden zijn tot het gezamenlijk ontwikkelen van capaciteiten.

Op de recente top in Chicago heeft ook de NAVO aangekondigd de weerbaarheid van de eigen netwerken en systemen en die van bondgenoten te versterken. Het is niet aannemelijk dat in NAVO-verband gemeenschappelijke cybercapaciteiten worden ontwikkeld. Het bondgenootschap moet echter wel een visie ontwikkelen over de inzet van cybercapaciteiten bij gezamenlijke operaties.

Tot slot

Het belang van het digitale domein en de snelheid waarmee dit zich ontwikkelt, stelt ons voor grote uitdagingen. De Nederlandse krijgsmacht trekt hier de noodzakelijke conclusies uit en wil in het digitale domein de vooraanstaande rol spelen die bij ons land past.

Defensie moet een volwaardige cybercapaciteit ontwikkelen. Hier geldt misschien nog meer dan elders dat stilstand achteruitgang is. Het tempo waarin het digitale domein zich ontwikkelt zal dan tot gevolg hebben dat we zeer snel tegen een achterstand aanlopen.

Dat is de uitdaging waar we nu voor staan. De Defensie Cyber Strategie die ik de Tweede Kamer zojuist heb toegestuurd, fungeert daarbij als leidraad bij het verwezenlijken van onze doelstellingen.

Ik ben vandaag begonnen met de eerste luchtaanval van de Italiaanse piloot Giulio Gavotti in 1911. Nog voordat het vliegtuig was uitgevonden voorspelde de Britse science fiction schrijver H.G. Wells al dat "wanneer luchtoverwicht is verkregen door een van de strijdende legers, de oorlog een conflict wordt tussen een ziende krijgsmacht en één die blind is." Het zou mij niet verbazen wanneer deze voorspelling wordt vertaald naar het digitale domein, deze binnen afzienbare termijn ook uitkomt.

En dan is het nu het moment om het allemaal officieel te maken door de strategie aan de Kamer aan te bieden. Uiteraard doe ik dat digitaal.