Voordracht Cyber
Genm Sander Schnitger
KVBK, 21 november 2011

Introductie
Ruim 125 jaar geleden, op 10 maart 1876, sprak Graham Bell tegen zijn assistent de historische woorden: *"Mr. Watson, come here. I want to see you*." Watson, die in een andere kamer van het huis verbleef, kwam direct. Dit experiment betekende de geboorte van een nieuw – maar onbedoeld tijdperk. Een *nieuw* tijdperk omdat met de legendarische woorden van Graham Bell de telefoon geboren was, en Bell vervolgens de Bell Telephone Company oprichtte die later uit zou groeien tot een van 's werelds grootste bedrijven: de American Telephone and Telegraph Company (AT&T). En *onbedoeld* omdat Bell eigenlijk onderzoek verrichte naar het zichtbaar maken van geluidsgolven ten behoeve van doven en slechthorenden.

Zo'n onverwacht neveneffect doet zich wel vaker voor. In 1969 ontwikkelde DARPA, de Defence Advanced Reseach Projects Agency, de voorloper van het huidige internet ten behoeve van onder andere militaire communicatie. Wij weten inmiddels niet alleen dat internet zijn weg ook naar de civiele maatschappij heeft gevonden, maar ook dat de symbiose tussen telefoon en internet op dit moment in uw binnenzak past: de *smart phone*.

Ik wil de Koninklijke Vereniging ter Beoefening van de Krijgswetenschappen danken voor de gelegenheid die mij geboden is om de relatie tussen deze stukjes geschiedenis en toekomstige uitdagingen van de krijgsmacht te leggen. Na een korte inleiding wil ik beknopt de huidige situatie in cyberspace schetsen. Aansluitend zal ik ingaan op de rol van de krijgsmacht in cyberspace en een aantal voor ons liggende uitdagingen belichten. Ten slotte zal ik aangeven welke activiteiten Defensie de komende periode op dit gebied zal ontplooien.

Inleiding
Wij maken dagelijks gebruik van computers, *tablets*, internet en *smart phones*. Wij zijn in ons dagelijks leven, in ieder geval de jongeren en zij die zich jong voelen, volledig afhankelijk van deze technologie. Technologie die allang niet meer als nieuw of eng wordt ervaren. We betalen en bankieren via internet op elektronische wijze, reserveren een hotel op weekendjeweg.nl, onderhouden contacten met collega's op LinkedIn, solliciteren en beleggen online en melden de laatste vertraging op het spoor via Twitter. Het gevolg is dat al onze privé- en mogelijk ook bedrijfsinformatie zit opgesloten in onze telefoon en is opgeslagen in *the cloud*. Heel veel, vaak schijnbaar onschuldige informatie die interessant is voor criminelen en andere malafide figuren. Herinnert u zich Sandra Bullock nog in de film *The Net,* een film uit 1995! *Identity Theft* als de ultieme identiteitscrisis?

Dagelijks worden we geconfronteerd met berichten over gehackte websites en verlies van privacy gevoelige gegevens. De motieven van waaruit wordt gehandeld en de methoden die worden gehanteerd variëren. Soms gaat het om cyber criminaliteit met geldelijk gewin als doel, zoals bij het sturen van *spam mails* om medicijnen te verkopen of *phishing emails* om uw wachtwoorden te achterhalen (zoals onlangs op ons eigen Defensie Intranet bekend werd gemaakt), dan weer om activisten die willen protesteren door het wijzigen van websites of door websites onbereikbaar te maken door *denial of service* aanvallen vanuit *botnets* te lanceren, zoals naar aanleiding van WikiLeaks met *Cablegate* vanaf het gerubriceerde Amerikaans *SIPRNet*, speciaal opgezet voor de Amerikaanse defensieorganisatie. Van weer een andere orde is de nog vers in het geheugen liggende DigiNotar *hack*, waarbij internet veiligheidscertificaten zijn buitgemaakt. Kennelijk wilden criminelen de buitgemaakte certificaten gebruiken als opstap voor andere illegale vervolgacties.

Ernstiger was het StuxNet virus, een softwareprogramma dat specifiek is ontworpen om de besturing van ultracentrifuges in een Iraanse nucleaire opwerkingsfabriek aan te vallen. StuxNet moet speciaal ontwikkeld zijn om een specifiek deel van het nucleaire verrijkingsproces te verstoren. Een proces dat – voor zover we nu weten – *stand alone*, dus niet verbonden met internet, werd aangestuurd. De in StuxNet verpakte software wijzigde de aansturing van de ultracentrifuges en veroorzaakte daarmee een afwijking in het vereiste toerental van die centrifuges. Als gevolg hiervan verliep de nucleaire opwerking niet optimaal. Twee bijkomstigheden zijn vermeldenswaard. Ten eerste moet de StuxNet-software precies *compatible* zijn geweest met de meest recente softwareconfiguratie – inclusief de laatste updates – van de Siemens hard- en sofware die Iran gebruikte. Ten tweede ging het – zoals gezegd – om *stand alone* apparatuur, en moet het StuxNet de zogeheten *airgap* met een USB, bijvoorbeeld via een *update* vanaf een andere computer of met een geïnfecteerde USB stick, via een menselijke hand hebben overbrugd.

Interessant is bovendien de constatering dat er nu dus *malware* met een specifiek doel is ontworpen en vervolgens als wapen is ingezet. StuxNet heeft gebruik gemaakt van minimaal 4 *zero-day exploits*, unieke kwetsbaarheden in software die nog niet eerder waren ontdekt. De conclusie ligt dan ook voor de

hand dat StuxNet door een grote groep ontwikkelaars (*hackers*) gedurende een langere periode is ontwikkeld en uitgewerkt. Bovendien moeten de ontwikkelaars over eerste klas informatie hebben beschikt over de exacte hard- en software configuraties van de Iraanse apparatuur. Waarschijnlijk heeft StuxNet dan ook vele miljoenen gekost.

We zien hier echter nog een ander leermoment: de StuxNet aanval ging gepaard met een enorme *collateral damage*. Het virus heeft zich namelijk wereldwijd verspreid en moest uit duizenden, zo niet miljoenen systemen worden verwijderd. Er bestaat namelijk geen TomTom voor het internet en een virus verspreid zich door zichzelf continue te vermenigvuldigen en te kopiëren naar andere systemen. StuxNet heeft ons vier lessen geleerd:

- geautomatiseerde systemen kunnen zeer specifiek worden aangevallen en malware kan dus als wapen worden ingezet;
- *airgaps* kunnen en zullen dus worden overbrugd en geïsoleerde *stand alone* systemen zijn niet zo veilig als we altijd dachten;
- de ontwikkeling van dergelijke wapens kost (nu nog) erg veel geld;
- de inzet ervan kan aanzienlijke ongewenste neveneffecten veroorzaken.

Hieronder kom ik op deze geleerde lessen terug. Als eerste wil ik echter kort de huidige situatie in cyberspace schetsen.

<u>Huidige situatie</u>
Alle middelen die we tegenwoordig gebruiken als wereldburger, gebruiken we ook als militair. Daarnaast zien we dat al onze wapensystemen, van jachtvliegtuigen tot fregatten, van gepantserde wielvoertuigen tot helikopters, al onze communicatie en informatiesystemen, radars, sensoren en commandovoeringsystemen, gebruik maken van *cyberspace*. Dat maakt ons enorm kwetsbaar. En tegen deze kwetsbaarheid moeten we ons wapenen. Tegelijkertijd biedt deze situatie ook ruimte voor initiatief, voor nieuwe acties en reacties, nieuwe technieken en modi operandi in aanvulling op het bestaande operationele vermogen. Ik licht dit toe.

We weten dat potentiële opponenten – van *hackers* tot vijandelijke strijdkrachten – ook actief zijn in *cyberspace* en daarin net zo kwetsbaar zijn als wij. Soms gebruikt onze tegenstander slechts een eenvoudige mobiele telefoon voor communicatie of het laten exploderen van een *Improvised Explosive Device*, soms alleen een internetcafé, maar in veel gevallen gebruikt hij dezelfde geavanceerde middelen die wij hebben. Van deze kwetsbaarheid moeten we – uiteraard binnen de grenzen van de juridische kaders – gebruik maken. Allereerst door inlichtingen te verzamelen over zijn kwetsbaarheden: Wat voor soort systemen – hardware en software - gebruikt hij? Ten tweede door in zijn systemen op zoek te gaan naar vitale informatie. Ten derde door zo nodig informatie te wijzigen of te vernietigen en, ten vierde, door de tegenstander – in ruimere zin – via *cyberspace* aan te pakken. Bijvoorbeeld door zijn toegang naar internet tijdelijk te blokkeren, door zijn *Command&Control* systemen te verstoren of door de radar van de luchtverdedigingssystemen onklaar te maken. *Cyber Ops* komt daarmee overigens vaak in de buurt van Elektronische Oorlogsvoering.

Natuurlijk is het moeilijk om een cyber aanval te lanceren op een Taliban strijder met een Kalasjnikov, maar als we ons concentreren op het te bereiken effect wordt het al weer wat overzichtelijker. Zijn berichtenverkeer kunnen we onderscheppen, en bovenal: zijn commandant maakt wél gebruik van telefoons en internet. En de commandanten daarboven voeren een mediastrategie via internet en *Youtube* en ga zo maar door. Bedreigingen dus, maar er zijn ook contouren van kansen zichtbaar. En er is een rol weggelegd voor de krijgsmacht.

<u>De rol van de krijgsmacht</u>
De bijdrage van Defensie vloeit voort uit de bepalingen over de krijgsmacht in de Grondwet. Artikel 97 van de Grondwet stelt dat er een krijgsmacht is "ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde." Deze doelen zijn bewust abstract beschreven om zo het hoofd te kunnen bieden aan nieuwe bedreigingen als terrorisme, aan nieuw materieel en nieuwe inzetmethoden, aan gecombineerde trainingsmissies of aan de beveiliging van de koopvaardij voor de kusten van verre, warme landen.

De krijgsmacht heeft dus niet alleen de ruimte en het mandaat om op nieuwe dreigingen als in het cyberdomein bedacht te zijn, maar moet zich ook voorbereiden op passende antwoorden.
Aangezien cyber overal is en we in toenemende mate de Generaal direct verbinden met de Korporaal, moeten cyberoperaties op elk niveau worden uitgevoerd. Defensie moet in de toekomst niet alleen in *cyberspace* kunnen verdedigen, maar ook inlichtingen kunnen verzamelen en– *last but not least* – in staat zijn het initiatief te grijpen, door aanvallen te lanceren.

Cyber is dus een dreiging en een kans. Cyber is een wapen, maar ook het terrein, het is de infrastructuur, maar ook de *modus operandi*. Het kan naast zee, land, lucht en ruimte gezien worden als het vijfde domein. Het is een domein, omdat je erin kunt opereren *zonder* de andere domeinen te gebruiken. Wat we ons vooral moeten realiseren, is dat we niet meer kunnen functioneren zonder gebruik te maken van *cyberspace*. Cyber is, totdat we de coördinatie en synchronisatie tot stand hebben gebracht, vooral ondersteunend aan de andere domeinen. Tegelijkertijd betekent opereren in cyber niet dat geweld wordt aangedaan aan het joint optreden. Het is nu nog vooral een additionele capaciteit, een *enabler*. Cyber is daarmee nu al een operationeel vermogen en heeft een werkelijk onbegrensd potentieel. Maar dit potentieel waarmaken vereist een andere manier van denken, nieuwe paradigma's.

Met het voorgaande in gedachte heeft Defensie de volgende, weliswaar ambitieuze, visie gedefinieerd:

Defensie heeft in 2015 een robuuste Cybercapaciteit. Deze capaciteit is in staat de ICT middelen van Defensie te verdedigen tegen aanvallen en verstoringen van buitenaf. De Cybercapaciteit draagt met behulp van inlichtingen en offensieve operaties in Cyberspace bij aan het totale operationele vermogen van de krijgsmacht en versterkt het geïntegreerd optreden van de krijgsmacht in alle dimensies. Deze robuuste capaciteit is bovendien relevant voor civiele autoriteiten en ondersteunt deze indien nodig in het kader van ICMS. Defensie is een betrouwbare en innovatieve kennispartner ten aanzien van Cyber.

Zoals gemeld in de beleidsbrief *Defensie na de kredietcrisis* zal Defensie daarom 50 miljoen euro investeren om de bestaande capaciteiten aanzienlijk te versterken en nieuwe te ontwikkelen. Defensie moet daartoe fors investeren in kennis, inlichtingen, defensieve *en* offensieve capaciteiten. De operationele cybercapaciteit gaat daarmee het totale operationele vermogen van de krijgsmacht vergroten en het geïntegreerd optreden van de krijgsmacht in alle dimensies versterken. Zo ontstaat niet alleen de noodzakelijke Cybercapaciteit. Ook wordt het reguliere optreden van de krijgsmacht ondersteund. En, zoals in de visie aangegeven, ondersteunt Defensie hiermee ook de ambities van het Kabinet zoals verwoord in de *Nationale Cyber Security Strategie*. Bij de uitvoering daarvan staan wij voor meerdere uitdagingen. Op een aantal daarvan ga ik nader in.

<u>Uitdagingen</u>
Allereerst het probleem van *attributie*. Dat begint al bij de vraag hoe je weet dat je wordt of bent aangevallen. Mits je dat al weet - en laten we daar gemakshalve van uitgaan - hoe weet je dan wie je aanvalt. En: Hoe weet je in cyberspace zeker dat degene die je aanvalt ook degene is voor wie hij zich voordoet? Een aanvaller kan een staat of een door een staat gesponsorde organisatie zijn, maar ook een terrorist, een crimineel of de veertienjarige buurjongen die zijn eerste *hack*-ervaring op wil doen. Een aanval kan worden aangestuurd vanuit een land op het zuidelijk halfrond, maar vanuit een server komen die op het grondgebied van een Navo partner staat. Als je als militair wilt, kunt en mag reageren, moet je wel precies weten waar het om gaat: was het een *act of war* of een criminele daad? Je zult, met andere woorden, ook iets moeten weten over de intentie van de aanvallende partij. Niet in de laatste plaats omdat de intentie mede bepalend voor de wijze van reageren zal zijn. Op criminele acties zal justitie reageren, op aanvallen met desastreuze gevolgen zijn wellicht ook anderen aan zet.

Een tweede uitdaging is het gebruik van de *offensieve capaciteit*. Wat bedoelen we daar precies mee? We onderscheiden drie mogelijkheden:

- een offensieve reactie na een aanval door de tegenstander (juridische gezien is dat overigens een defensieve actie);
- een proactieve actie om een onmiddellijke dreiging van een vijandelijke aanval te voorkomen;
- een offensieve actie die op zichzelf staat, en waarbij wij het initiatief nemen. Bij deze laatste kun je nog onderscheid maken tussen een actie in het kader van een lopende operatie of een actie voorafgaande aan een operatie.

Daarnaast bestaat er uiteraard een grote variëteit aan offensieve technieken, aan modi operandi. Voorbeelden zijn het veranderen of verwijderen van info in een vijandelijk commandovoeringssysteem, het onklaar maken van hoogtemeters in vliegtuigen, maar ook het 'planten' van besmette USB sticks, zoals bij StuxNet.

De derde uitdaging ligt in de eerder genoemde *collateral damage*. Hoe gaan we daar mee om? Is het acceptabel dat de inzet van een cyberwapen vele miljoenen euro's schade aan civiele systemen genereerd? Ligt die vraag anders, als er slechts enkele tonnen schade ontstaat, maar wel een vitale sector langdurig ontregeld is? En: wat *is* eigenlijk *collateral damage*? Is dat alleen de directe onbedoelde, maar voorziene nevenschade, zoals de stroomuitval in een ziekenhuis na een aanval op een elektriciteitscentrale? Of ook de indirecte, soms na-ijlende, en niet voorziene nevenschade, zoals de noodstroomvoorziening die niet werkt waardoor patiënten overlijden?

Deze drie uitdagingen, hangen nauw samen met en vloeien voor een belangrijk deel voort uit een vierde uitdaging: hoe steekt *het juridische raamwerk* voor cyberoperaties in elkaar?

Dit raamwerk bestaat uit twee delen: de rechtsbasis voor de operaties en de rechtsregimes tijdens de operaties. Het afgelopen voorjaar hebt u hierover kunnen lezen in de Militaire Spectator. Primair is er de vraag wanneer en op welke basis Nederland de krijgsmacht in kan zetten. Die vraag ligt op het politiek strategische niveau en is niet alleen op expeditionaire inzet van toepassing, maar ook op nationale operaties.

Voor expeditionaire operaties is het geweldsverbod in artikel 2 van het VN Handvest het startpunt. Dit verbiedt namelijk het gebruik van interstatelijk of transnationaal militair geweld. Een eerste knelpunt is dan ook de vraag of onze cyberactiviteiten allemaal onder dit verbod vallen. Dit is ook een van de vragen die momenteel door de Adviesraad Internationale Vraagstukken wordt uitgewerkt.
Als onze cyberacties onder dit geweldsverbod vallen, dan is een operatie rechtmatig als – en ik citeer het huidige regeerakkoord op dit punt van het volkenrecht - een "adequaat volkenrechtelijk mandaat" beschikbaar is. Anders gezegd, Nederland zal:

- alleen met toestemming van een andere staat een eventuele cyber-opponent mogen aanpakken;
- dan wel met een mandaat van de VN Veiligheidsraad;
- in het uiterste geval een beroep doen of zelfverdediging.

Tot zover niets nieuws. Dit zijn immers de standaard regels die voor alle expeditionaire missies gelden. Of niet? Het is bijvoorbeeld niet glashelder in welke gevallen zelfverdediging na een vijandelijke cyberaanval is toegestaan. Die cyberaanval moet dan namelijk als een "gewapende aanval" in de zin van het VN Handvest worden aangemerkt. En ook hier is de vergelijking met terrorisme bruikbaar: de terreur aanval van *9/11* is indertijd als een "gewapende aanval" getypeerd en daardoor konden de VS en bondgenoten (waaronder Nederland) hun reactie op zelfverdediging baseren.
Ook deze cruciale vraag – wanneer is een cyber aanval een gewapende aanval? – maakt onderdeel uit van de adviesaanvraag aan de AIV.

Het tweede deel van het juridische raamwerk bestaat uit rechtsregimes die voorschrijven hoe – nadat daartoe is besloten op politiek-strategisch niveau – operaties op de lagere niveaus moeten worden uitgevoerd. Het gaat daarbij onder andere om het vaststellen van de *Rules of Engagement*, de begrenzing die aan een eventueel VN-mandaat wordt ontleend, maar ook om zaken als mensenrechten en in een aantal gevallen ook het Humanitair Oorlogsrecht. Ook in deze laatste kwestie zal de AIV advies uitbrengen. En ook in dit geval gaat het om cruciale antwoorden. Welke schade moet je wel en niet laten meewegen in een *collateral damage estim*ate van een voorgestane cyberaanval? Hoe is de positie van neutrale staten – op wiens grondgebied zich immers servers of ICT verbindingen kunnen bevinden – in het oorlogsrecht geregeld?

Als we over de rechtsregimes spreken, moeten we niet vergeten dat binnenlandse operaties ook tot de mogelijkheden behoren. Zo zal bijvoorbeeld de Wet op de inlichtingen en veiligheidsdiensten wellicht aan de stand van de huidige (en toekomstige) techniek moeten worden aangepast. We zullen alle mogelijkheden én onmogelijkheden moeten inventariseren, willen we binnen de grenzen van de wet aan onze derde hoofdtaak – het ondersteunen van civiele autoriteiten – vorm kunnen geven.

De antwoorden op al deze impliciete en expliciete vragen zullen direct van invloed zijn op het instrumentarium en de modi operandi van onze eigen cyberactiviteiten. Een deel van deze vragen is op dit moment al in onderzoek, maar er is nog veel werk te doen!

<u>Ontwikkelingen binnen Defensie</u>
Om de schaarse middelen binnen Defensie optimaal te kunnen inzetten, is centrale sturing en coördinatie nodig van de activiteiten die aan *cyberoperations* zijn verbonden. Recentelijk is kolonel Hans Folmer aangetreden als commandant *Taskforce Cyber* en hij richt in januari 2012 deze taskforce op. De commandant *Taskforce Cyber* is verantwoordelijk voor de coördinatie van alle cybertaken binnen Defensie en treedt op als cyber aanspreekpunt voor Defensie. De coördinatie van de beleidsontwikkeling komt bij de Hoofddirectie Beleid te liggen. Uitgangspunt blijft dat de betrokken organisatieonderdelen de eigen verantwoordelijkheden behouden.

Op de middenlange termijn (tot 2015) ligt de prioriteit voor Defensie bij het oprichten van een *Defensie Cyber Commando,* een *Defensie Cyber Expertise Centrum* en het versterken van de nationale en internationale samenwerking.

Het *Defensie Cyber Commando* (DCC) wordt verantwoordelijk voor *cyberoperations* binnen Defensie. Op dit niveau vindt ook de verbinding tussen de verschillende cybervermogens en de betrokken defensieonderdelen plaats, nationaal en internationaal. Het DCC draagt zo bij aan de betrouwbare werking van Defensie netwerken en systemen, uitvoering van militaire (cyber)operaties, en het verzekeren van de vrijheid van handelen in *cyberspace* voor Nederland en haar bondgenoten. In het operationele domein is waarschijnlijk een belangrijke, uitvoerende rol weggelegd voor het Commando Landstrijdkrachten.

Defensie is zelf verantwoordelijk voor de beschikbaarheid van de eigen communicatie systemen en netwerken. Het is essentieel dat we erop kunnen vertrouwen dat informatie in onze systemen betrouwbaar is en dat onze systemen betrouwbaar zijn. De beveiliging van onze netwerken – zowel de bedrijfsvoeringnetwerken zoals MULAN, als de operationele netwerken zoals TITAAN - wordt uitgevoerd door het *Defensie Computer Emergency Response Team* (DefCERT) dat onderdeel is van de Bedrijfsgroep IVENT. DefCERT heeft afgelopen jaar *Initial Operational Capability* bereikt en moet eind volgend jaar volledig operationeel zijn, dat wil zeggen 24 uur per dag en zeven dagen per week alle defensienetwerken beschermen. DefCERT zal binnenkort een convenant afsluiten met GovCERT.NL, waarin de intensieve samenwerking tussen beiden wordt afgesproken. Deze betreft zowel informatie-uitwisseling als (personele) ondersteuning bij calamiteiten.

Tot voor kort waren we in de veronderstelling dat de kwetsbaarheid van geïsoleerde netwerken en wapensystemen zeer beperkt was. Ten eerste omdat een virus het doel alleen via een *airgap* kon bereiken en die overbruggen onwaarschijnlijk was. Ten tweede omdat veel software specifiek ontworpen is voor een specifiek systeem. Nu zien we dat ook in specifieke systemen commercieel gebruikelijke software wordt gebruikt. StuxNet heeft echter laten zien dat ook geïsoleerde en specifieke systemen kwetsbaar zijn. We moeten voorkomen dat een volgende keer de SMART-L radar op Hr.Ms. Tromp wordt getroffen. Dit vraagt dus onze specifieke aandacht. Alhoewel het aanvallen van geïsoleerde systemen erg complex is en veel geld kost, moet Defensie de bescherming van wapen-, regel- en IV-systemen en haar netwerken verder versterken.

Defensie moet ook in het digitale domein beschikken over een goede inlichtingenpositie en zorgen een goede *situational awareness* over dreigingen in het digitale domein. Het inlichtingenvermogen wordt door de MIVD gerealiseerd. Binnen de MIVD is daarom een taakgroep opgericht om de cyber inlichtingencapaciteit te vergroten. Daarnaast werkt de MIVD samen met de AIVD en draagt bij aan het opstellen van het Cybersecuritybeeld Nederland.

De krijgsmacht moet ook in het digitale domein tegenstanders uit kunnen schakelen door hun middelen onschadelijk te maken. Het is daartoe noodzakelijk dat Defensie beschikt over de kennis en capaciteiten om offensieve handelingen in het digitale domein te verrichten, zowel op strategisch, operationeel als tactisch niveau. Momenteel vindt gedachtevorming plaats over een offensieve capaciteit. In 2012 zal een *Defensie Cyber Doctrine* worden opgesteld. In deze doctrine zal worden beschreven hoe we met gebruik van *cyberspace* en in *cyberspace* zullen optreden en hoe dit in de planningprocessen moet worden verwerkt. Voor de goede orde, onder offensief versta ik:
- een offensieve reactie na een aanval;
- een proactieve actie ter voorkoming van een onmiddellijke dreiging;
- een op zich zelf staande aanval (al dan niet binnen een grotere operatie).

Ook wordt onderzocht welke mogelijkheden er zijn om een pool van cyberreservisten te creëren. Daartoe vindt overleg plaats met het bedrijfsleven en universiteiten. Een dergelijk systeem functioneert al in Estland. In Nederland hebben zich al *hackers* aangeboden die de overheid graag willen helpen (REALCert).

Het *Defensie Cyber Expertise Centrum* (DCEC) is een zogeheten *shared service center* voor *cyberoperations* dat het strategische, tactische en operationele kennis- en vaardighedenpeil van Defensie voor militaire *cyberoperations* op het gewenste niveau moet brengen. Dit gebeurt enerzijds door het ontwikkelen en samenbrengen van (strategische, beleidsmatige en technologische) kennis (kennisontwikkeling) en anderzijds door opleiding, training en oefening, zowel met als zonder 'live' cybercomponent (kennisverspreiding). Op dit moment worden twee elementen uitgewerkt.

Ten eerste zal er een krijgsmachtbreed *Opleidings- en Trainingscentrum Cyberdefence* worden ontwikkeld. Het vergroten van de bewustwording bij het personeel over de cyberdreiging heeft prioriteit. Als eerste stap wordt een interactieve oefenomgeving ontwikkeld bestaande uit *e-learning* modules en een simulatie- en een kennisbank. Deze oefenomgeving is toegespitst op het hogere niveau (vanaf Ikol) en is begin 2012 beschikbaar.

Ten tweede zal per 1 januari 2012 aan de NLDA een *Universitair Hoofddocent (UHD) Cyber* worden aangesteld. Deze zal zijn of haar aandacht richten op de operationeel-juridische aspecten van cyber en op de oprichting van een multidisciplinaire onderzoeksgroep binnen de Faculteit Militaire Wetenschappen. Per 1 januari 2014 zal een leerstoel cyber worden ingesteld.

Samenwerken

Defensie staat niet alleen aan het Cyberfront. Ook op nationaal niveau en in interdepartementaal verband wordt hard aan de weg getimmerd. Cyber is een *gezamenlijke* verantwoordelijkheid. Ik heb al aangegeven dat het Defensie cyberprogramma bijdraagt aan de ambitie van het kabinet zoals verwoord in de in maart gepubliceerde *Nationale Cyber Security Strategie*. Samenwerking staat hierin centraal. De minister van Veiligheid en Justitie heeft een coördinerende taak, maar alle ministeries houden hun eigen verantwoordelijkheden. Defensie heeft daarbij vanuit artikel 97 Grondwet een taak die zich niet alleen beperkt tot expeditionaire missies, maar ook nationale operaties bestrijkt.

Per 1 januari 2012 wordt het *Nationaal Cyber Security Centrum* (NCSC) opgericht. Defensie participeert bij de totstandkoming van dit centrum, een defensievertegenwoordiger (MIVD) heeft zitting in de kwartiermakergroep. Vanaf 1 januari 2012 zal er een permanente liaison door de *Taskforce Cyber* worden uitgebracht. DefCERT heeft een convenant met GovCERT over de uitwisseling van informatie en het versterken van elkaar in geval van een incident of crisis. Dit zijn geen loze woorden, maar absolute noodzaak en al in de praktijk gebracht. Tijdens de DigiNotar crisis heeft personeel van DefCERT gewerkt op de locatie van GovCERT.

Defensie draagt ook bij aan het tot stand komen van het *Cybersecuritybeeld Nederland*. Dit rapport geeft een beeld van de actuele cyberdreiging in Nederland en zal voor het kerstreces aan de Tweede Kamer worden aangeboden. Het zal informatie bevatten over actoren en mogelijke dreigingen en biedt private en publieke partijen de mogelijkheid tijdig te reageren.

Ook zullen ministeries samenwerken op het gebied van onderzoek. Onderzoeksvragen worden afgestemd teneinde duplicatie te voorkomen en resultaten zijn voor allen beschikbaar. Hierbij wordt ook samengewerkt met universiteiten, kenniscentra en het bedrijfsleven.

Natuurlijk zal ook aansluiting worden gezocht bij de ontwikkelingen binnen NATO en EU. In NATO verband wordt momenteel gewerkt aan een actieplan om de bescherming van eigen netwerken te verbeteren en met NC3A wordt samengewerkt in de ontwikkeling van cyber instrumenten. Ook bilateraal zijn er contacten met diverse partners. Doel van de samenwerking is in alle gevallen het efficiënt gebruik maken van de beperkte beschikbare middelen en het voorkomen van doublures.

Afsluiting

Cyberoperaties zijn geen *science fiction* meer. Via Cyber kunnen en moeten wij ons beschermen. Cyber biedt mogelijkheden om tegenstanders in hun bewegingen te belemmeren (contra-mobiliteit) en is een operationeel vermogen waarmee we eigen mobiliteit genereren. Ik zie daarin een interessante analogie met de drieledige taak die het Wapen der Genie typeert bij de Landmacht:

- bescherming bieden;
- mobiliteit ten eigen faveure genereren;
- contra-mobiliteit (hindernissen) ten nadele van de tegenstander creëren.

De samenleving en ook Defensie zijn afhankelijk van Cyber en ICT en dus kwetsbaar voor cyberaanvallen. De mogelijkheden die cyber biedt aan een tegenstander zijn enerzijds een bedreiging voor ons operationeel vermogen. Anderzijds is cyber een kans. Defensie ontwikkelt daarom een operationele cybercapaciteit. Het digitale domein vormt daarmee naast Land, Zee, Lucht en Ruimte, een nieuw operationeel domein voor de krijgsmacht. Defensie kan in de toekomst operaties in andere domeinen ondersteunen en versterken door inlichtingenvergaring en offensieve operaties in c*yberspace*. Ook buiten Defensie, in binnen- en buitenland, zowel in het publieke als in het private domein, wordt gewerkt aan het ontwikkelen en verstevigen van cybercapaciteit. Defensie zet daarom in op nationale en internationale samenwerking op dit terrein. Indien nodig zal Defensie in de toekomst zijn cybercapaciteiten in het kader van de civiel-militaire samenwerking beschikbaar stellen.

Ik realiseer mij als geen ander dat ik u meer vragen dan antwoorden heb voorgehouden. Ik sta daarom zondermeer open voor zowel uw visionaire vergezichten en uw overzichtelijke oneliners.