Van zwaard naar joystick. De rol van Defensie in de digitale frontlinie.

Toespraak van de minister van Defensie, J.S.J. Hillen, ter gelegenheid van de conferentie Cyber Operaties van het Koninklijk Instituut van Ingenieurs op 13 april 2011 te Amsterdam.

Let op: Alleen gesproken woord geldt!

Geachte dames en heren,

Begin deze week ben ik langs de troepen gegaan om een toelichting te geven op de enorme bezuinigingen bij de krijgsmacht.

Want bij dergelijke forse ingrepen, die haaks staan op de indrukwekkende prestaties van het personeel, moet je elkaar recht in de ogen kijken.
Dat heb ik dan ook samen met de Commandant der Strijdkrachten gedaan.
Het waren moeilijke maar ook heel waardevolle ontmoetingen.

De belangrijkste vraag die de militairen en burgers van Defensie hebben, is deze: wat is de gedachte áchter deze bezuiniging?

Het antwoord op deze vraag geeft ook meteen richting aan mijn voordracht van vandaag.

Want de bezuinigingen zijn niet alléén ingegeven door de noodzaak te moeten schrappen.
We vormen de krijgsmacht ook om.
We maken de krijgsmacht klaar voor de toekomst.

Wie door zijn oogharen kijkt, ziet de komende jaren de contouren van een nieuwe krijgsmacht ontstaan.
Een krijgsmacht die de komende tijd een kolossale verbouwing ondergaat.
Maar ook een krijgsmacht die over drie jaar weer goed op orde is.
Met voldoende munitie, gevechtslaarzen, brandstof en afdoende mogelijkheden voor training en opleiding.

Wie door zijn oogharen kijkt, ziet de contouren ontstaan van een krijgsmacht die een nieuwe koers inslaat.
Onze krijgsmacht krijgt naast het zwaard nadrukkelijker ook toetsenbord en joystick in de hand.

Hier komen we meteen op het onderwerp van vandaag: Cyber Operations.

Of het nu gaat om *cyber security*, *cyber defense*, *cyber crime* of *cyber warfare*; de kranten en internet staan er vol mee.
Terecht, want de dreiging is reëel.

Het is technisch mogelijk om de luchtverdediging van landen met een cyberaanval uit te schakelen.
Daarna kan men ongehinderd het luchtruim binnenvliegen.
Na zo'n aanval kun je dus niets meer. Je bent als land in feite weerloos geworden.

Ik bekijk het onderwerp Cyber Operations dan ook als pregnant, eigenstandig militair vraagstuk.

Dames en heren,

Asymmetrische oorlogsvoering neemt toe.
We zien steeds vaker dat kleine groepen die het opnemen tegen grote staten.
Met maximale ontregeling als doel.

Ik verwacht dat deze ontwikkeling doorzet.
De ontwikkeling naar het verzwakken en ontregelen van de tegenstander.
Zonder zwaar geschut.
Zonder fysieke aanwezigheid.

We hebben het dan nog steeds wel over oorlog en gewapend conflict.

Maar niet meer uitgevochten met vooral bommen en granaten.

Veel meer uitgevochten door acties gericht op het ontwrichten van de samenleving.

Wat denkt u dat er gebeurt als in Nederland

- **De stoplichten uitvallen.**
- **De treinen niet meer rijden (☺ die ervaring hebben we al)**
- **Supermarkten niet meer kunnen worden bevoorraad?**
- **Het licht uitvalt?**
- **Er geen schoon water meer uit de kraan komt?**
- **Het geldverkeer plat ligt?**

Ik garandeer u dat wij binnen de kortste keren hier een grote chaos hebben.

Waar kwaadwillenden vervolgens misbruik van maken.

Hoewel geen direct bloed wordt vergoten, is zo'n aanval dus wel degelijk gewelddadig en gevaarlijk.

Wij moeten daarom een beter beeld krijgen van de digitale wapens die het grondgebied van Nederland kunnen bedreigen.

Wij weten hier nog te weinig over.

Wij hebben ons hierin nog te weinig verdiept.

Wat zijn eigenlijk de definities rondom cyberoperaties?

Hoe zien de ontwikkelingen in digitale oorlogvoering er precies uit?

Wat zijn de technische mogelijkheden?

Nu en over een paar jaar?

Het is de kunst ons te verplaatsen in de vuigste plannen, doelen en middelen van de tegenstander op dit vlak.

Pas als wij ons een voorstelling kunnen maken van wat de tegenstander voor schade kan aanrichten, kunnen wij die tegenstander van repliek dienen.

We hebben al wel een indruk.

We weten dat in het digitale domein de aanvaller sterk in het voordeel is.

Waar het nogal een uitdaging is om raketten of tanks te verbergen, kan een digitaal wapen relatief eenvoudig in het geheim ontwikkeld worden.

Daar komt nog bij dat de aanvaller zijn identiteit en locatie relatief eenvoudig verborgen kan houden.

We weten dat een vastberaden tegenstander in staat moet worden geacht elke verdediging te omzeilen. In veel gevallen zal dit snel worden ontdekt en blijft de schade beperkt.

Maar zekerheid dat alle aanvallen ontdekt en afgeslagen worden is er niet.

We weten ook dat het uitbreken van grootschalige cyberoorlogen niet meteen morgen zal gebeuren.

Want als middel om een politiek doel te bereiken heeft een pure cyberoorlog nogal wat beperkingen.

Zo is het moeilijk om op voorhand een gedegen beoordeling te maken van het effect van een aanval.

Het is lastig om een digitale aanval precies te richten en te beheersen.

Een aanval kan onvoorziene en ongewenste gevolgen hebben die het effect beperken.

Of juist veel meer schade aanrichten dan voorzien.

Ook de reactie van een tegenstander is moeilijk te voorspellen doordat er geen zekerheid is over de omvang en effectiviteit van zijn capaciteiten om terug te slaan.

Maar dát het platleggen van vitale verdedigingssystemen kan en gebeurt, toont aan dat we het digitale domein in de oorlogvoering zeker niet kunnen veronachtzamen.

De kerntaak van een krijgsmacht is handelend op te treden tegen een tegenstander.

Om die tegenstander het handelen onmogelijk te maken.

Kort gezegd: we moeten erop kunnen slaan.

Ook digitaal.

De krijgsmacht moet daarom in staat zijn digitale middelen in te zetten die het geïntegreerd optreden in alle dimensies versterken.

Zoals de Britse CDS het eerder al formuleerde: De krijgsmacht moet in cyber space kunnen verdedigen, vertragen, aanvallen en manoeuvreren.

We hebben twee dingen bij Defensie nu heel hard nodig.

- **Goede inlichtingen om de digitale vijand te kennen.**
- **En goede digitale wapensystemen. Defensief én offensief.**

In de nieuwe koers voor Defensie zoals ik die afgelopen vrijdag in een brief aan de Tweede Kamer heb geschetst, schep ik ruimte voor deze aanpak.
Ik investeer de komende kabinetsperiode 50 miljoen euro om aan de digitale frontlinie klaar te staan.

Wat gaan we bij Defensie doen?

Cyberspecialisten volgen eerst een opleiding tot militair.
Ik wil geen eenlingen die in achterafkamertjes op de kazerne, los van alles en iedereen, met cyber bezig zijn.
Het optreden van de krijgsmacht in het digitale domein moet een militaire specialiteit worden.
In 2016 moet de krijgsmacht beschikken over een nieuwe cyber eenheid.
Om kennis goed toegankelijk te maken binnen de krijgsmacht, richten we een Defensie Cyber Security Centrum op.
Er komt een technische cyber *test range* en een Opleidings- en Trainingscentrum.
Ook stellen we op de Nederlandse Defensie Academie een speciale leerstoel in en intensiveren we de samenwerking met universiteiten in binnen- en buitenland.

Specialisten op het gebied van cyber zijn schaars.
Om schaarse capaciteit beter te kunnen benutten, overwegen we de oprichting van een Cyber Reservisten Corps.
Zo kunnen we bij calamiteiten snel relevante kennis uit het bedrijfsleven in een groen pak hijsen en in actie komen.
U moet dat zien als digitaal zandzakken vullen bij een grote digitale overstroming.
In Estland bijvoorbeeld bestaat iets dergelijks al.

En we versterken het Defensie *Computer Emergency Response Team*, DefCERT, dat onze eigen netwerken en wapensystemen tegen aanvallen beschermt.

Wie het onderwerp cyberdreiging serieus neemt, moet serieus aandacht besteden aan het onderwerp inlichtingen, ik zei het zojuist al.
Een goede inlichtingenpositie in het digitale domein is essentieel.
Defensie moet actief netwerken kunnen binnendringen om spionage tegen te gaan en om te achterhalen waar een aanval vandaan komt.
Onze Militaire Inlichtingen en Veiligheids Dienst krijgt daarom fors meer cybercapaciteit.
Tevens komt er een nieuwe supercomputer waarmee we versleutelde berichten nog beter kunnen ontcijferen.

Binnen de Navo wordt gewerkt aan een brede cyber strategie. Wij sluiten daar bij aan.
Om onze kennispositie te versterken zal Defensie op korte termijn lid worden van het NAVO gelieerde *Cooperative Cyber Defence Center Of Excellence*.

Dames en heren,

Defensie doet dit alles niet op eigen houtje.
Wij werken intensief en structureel samen met andere partners.
Zowel met bedrijven als met mede-overheden.
Want Defensie heeft veel unieke capaciteiten en bevoegdheden.
Maar wij kunnen het niet alleen.

Al was het maar omdat 95 procent van de netwerken in Nederland in handen is van private partijen.

Alle partijen, ook Defensie, worden met dezelfde dreiging geconfronteerd.
Kwaadwillenden die onze netwerken willen lamleggen of informatie willen stelen, gebruiken steeds dezelfde techniek.
Maar… de motieven variëren.
Het kan gaan om criminaliteit, het stelen van geld bijvoorbeeld.
Het kan gaan om spionage.
Of om een aanval op ons grondgebied.

We moeten steeds per aanval bekijken wie bevoegd is om in actie te komen.
Dat vereist een platform waarin alle partijen elkaar treffen.
In zo'n platform kun je vooraf afspraken maken over het delen van informatie en hoe te reageren mocht het nodig zijn.
Nationale coördinatie is essentieel.
Daarom heeft Defensie meegeschreven aan de Nationale Cyber Security Strategie die onlangs door mijn collega Opstelten aan de Kamer is gestuurd.
Een van de belangrijkste acties die uit deze strategie volgt, is de oprichting van het Nationale Cyber Security Centrum door de Nationaal Coördinator Terrorisme Bestrijding.
Defensie werkt hieraan mee.
De MIVD en DefCERT nemen vanaf volgend jaar actief deel aan dit nationale cyber centrum.

Dames en heren,

Defensie zet de komende jaren sterk in op cyber.
Dat is pure noodzaak, wil de krijgsmacht zijn hoofdtaken kunnen blijven uitvoeren.
We ontkomen er niet aan, willen we in de toekomst ons eigen grondgebied en dat van onze bondgenoten kunnen beschermen.

Als krijgsmacht beschikken we in Nederland over unieke cyberkennis en uniek cybermaterieel.
Mocht dat nodig zijn, dan stellen wij die capaciteiten ook beschikbaar voor anderen.
Zoals wij dat ook op andere vlakken al doen.
Bijvoorbeeld bij de aanpak van onze binnenlandse veiligheid.
Dat kan de politie prima zelf af.
Als het om grote jongens gaat, komt justitie er aan te pas.
En bij echt grootschalige terreurdreiging, levert Defensie de Unit Interventie Mariniers.
Zo kunnen wij ook beschikbaar zijn in onze gezamenlijke strijd om Nederland digitaal veilig te houden.

Dames en heren,

Oorlogsvoering ontwikkelt zich voortdurend.
Van de conventionele tankbataljons in de Tweede Wereldoorlog naar asymmetrische oorlogsvoering met bermbommen in Afghanistan, naar het platleggen van vitale systemen als kerncentrales of luchtverdedigingssystemen.

De krijgsmacht zal zich steeds aan deze veranderende dreigingen moeten aanpassen.
Dat vergt voortdurende flexibiliteit en innovatiekracht.

Superieure technologie kan helpen om oorlogen te beslechten.
Wij moeten deze manier van oorlogvoering onderkennen, begrijpen, beheersen en kunnen inzetten.
Dat is mijn Cyber-agenda voor de komende jaren.

-0-0-0-