# Stilte voor de digitale storm

Binnenkort maakt het kabinet de plannen bekend voor de bezuinigingen op de krijgsmacht. Ongetwijfeld zal daarin worden beweerd dat de reducties weliswaar fors zijn, maar gezien de huidige veiligheidssituatie toch volledig verantwoord. Een hele generatie militairen is sinds 1990 vertrouwd geraakt met deze telkens terugkerende redenering. Zolang Nederland niet direct aangevallen wordt, is er immers ook moeilijk een speld tussen te krijgen. Natuurlijk is de kans dat ons grondgebied wordt aangevallen niet groot, achter de brede rug van Duitsland en onder de sterke paraplu van de VS. Ook het feit dat de expeditionaire missies van onze krijgsmacht steeds verder van huis worden uitgevoerd, versterkt bij veel Nederlanders het idee dat de veiligheid eigenlijk alleen maar toeneemt. Wie of wat kan Nederland nu nog militair bedreigen? Welke serieuze gevaren zijn er eigenlijk nog vandaag de dag?

Is het waar dat ons land zo veilig is, nu er geen manifeste bedreigingen zijn van ons grondgebied, luchtruim en kustwateren? Dergelijke geruststellende gedachten ontkennen helaas de revolutie in de oorlogvoering die momenteel gaande is. Dat is een vrij geruisloze revolutie, nauwelijks opgemerkt in de vaderlandse media, en ook deze vindt voorlopig ver buiten Nederland plaats. We hebben het over cyberwar, de oorlogvoering in de vijfde dimensie.

Langzamerhand worden de aanwijzingen steeds sterker dat nog geen jaar geleden de eerste echte cyberwar heeft plaatsgevonden. Officieel weten we nog van niets, maar waarschijnlijk hebben Israëlische en mogelijk ook Amerikaanse en andere experts rond de zomer van 2010 met succes een cyberattack uitgevoerd op het Iraanse nucleaire opwerkingsprogramma. Zich realiserende dat een reguliere oorlog en een verwoestende luchtaanval zijn uitgesloten, zijn ze op de digitale oorlogvoering uitgekomen. Naar verluidt is toen de zogeheten 'Stuxnetworm' ontwikkeld, die zich richt op de computerprogramma's die de centrifuges in de opwerkingsfabrieken bedienen. Terwijl de Iraanse technici ondertussen in de controleruimtes geruststellende mededelingen op hun schermen kregen, draaiden vele centrifuges zichzelf in de fabriek kapot. Doordat deze hightech installaties moeilijk te vervangen zijn, is het nucleaire wapenprogramma van Iran waarschijnlijk enkele jaren vertraagd. Het feit dat Stuxnet zich op meerdere plaatsen in en buiten dat land manifesteert is een belangrijke indicatie dat cyberspace is gebruikt om het te verspreiden. Nog onopgehelderd is de vraag hoe deze worm vervolgens in de betreffende computers is terechtgekomen, aangezien die waarschijnlijk niet direct op het internet zijn aangesloten.[1]

Op zich klinkt dit allemaal kinderlijk eenvoudig. Menigeen zal daarom denken dat een betere virusscanner Iran veel ellende had kunnen voorkomen. Dat zou echter een cruciale misvatting zijn. Als deze lezing van de gebeurtenissen klopt, is er sprake van een heuse cyberwar, één die met militaire precisie is voorbereid en uitgevoerd. De aanvallers moeten in detail op de hoogte zijn geweest van de betreffende centrifuges, de bijbehorende controlesystemen en hun software. Dat vergt de nodige kennis, research (lees: spionage) en ontwikkelcapaciteit. Het feit dat naar alle waarschijnlijkheid cyber-

2 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', *New York Times*, 15 januari 2011.

space is gebruikt om een heus 'wapen' van de ene naar de andere staat over te brengen, die daar tot ernstige fysieke gevolgen heeft geleid, maakt het tot de voortzetting van politiek met toevoeging van andere middelen. Oorlog dus.

Natuurlijk is cyberwar geen onbekend fenomeen. Het begrip werd al in 1993 gehanteerd en reeds in 1999 keurde de NAVO-Raad de 'MC-422 NATO Information Operations' goed. Ook in Nederland zien we een toenemende belangstelling voor de digitale veiligheid. Afgelopen november publiceerde het ministerie van Binnenlandse zaken het eerste 'Nationaal Trendrapport Cybercrime en Digitale Veiligheid', waarin ook specifiek aandacht was voor het vijfde domein van defensie.[2] Mede op aandringen van de Tweede Kamer zal minister Opstelten binnenkort een Nederlandse cyberveiligheidsstrategie bekend stellen, en naar verwachting zal minister Hillen daarop aansluiten en het cyberbeleid bij defensie versterken. Overigens blijft het niet bij schone woorden alleen. Ook in praktische zin zijn er veel ontwikkelingen. Het zou te ver voeren deze hier allemaal te noemen.

Als we dit alles overzien ontstaat ten eerste de vraag waarom er in het Nederlandse publieke debat zo weinig aandacht is voor de markante gebeurtenissen van vorig jaar zomer. Gerenommeerde dagbladen gaan niet veel verder dan het verkort weergeven van hetgeen internationale bladen al hebben geschreven. Eigen journalistiek onderzoek of opiniërende stukken zal men tevergeefs zoeken. Heeft deze beperkte interesse in cyberwar te maken met dat eerder genoemde gevoel van relatieve onkwetsbaarheid? In aansluiting daarop kan ten tweede de vraag worden gesteld of cyberwar nog wel in één adem moet worden genoemd met cybercrime, zoals we nu veelal in het officiële Nederlandse beleid zien. Alle nu bekende eerdere cyberaanvallen in het militaire domein waren meer storend of saboterend van aard, overeenkomstig de problemen in het civiele gebied. Stuxnet maakt echter duidelijk dat het digitale tijdperk ook een geheel eigen manier van oorlogvoering met zich meebrengt. Het idee dat vijandelijke staten, instellingen of groeperingen tijd, geld en energie steken in een heuse offensieve cyberwar, en daarmee een hele industrie fysiek kunnen uitschakelen zonder dat er een bom of granaat aan te pas komt, is echt van een andere orde. Net als toen het vuurwapen, de stoommachine, de dieselmotor, het vliegtuig en de atoombom werden ingevoerd, betekent dit een revolutie waarvan de volledige omvang nog niet duidelijk is.

Zoals gememoreerd bezuinigt Nederland al ruim twintig jaar op defensie. Telkens wordt de krijgsmacht een slag kleiner en spitst zich steeds verder toe op het uitvoeren van expeditionaire missies. En telkens krijgen we geruststellend te horen dat de veiligheidssituatie dat mogelijk maakt. Als er louter naar de klassieke militaire bedreigingen wordt gekeken, zit daar wel een kern van waarheid in. Maar Clausewitz zei al dat de oorlogvoering een soort kameleon is die zich telkens aanpast aan zijn veranderende omgeving. Het digitale tijdperk brengt het fenomeen cyberwar met zich mee. Sinds afgelopen zomer kan daar niet meer zo luchtig over worden gedaan. ■

1 Zie hoofdstuk vijf van het *Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010*, ministerie van Binnenlandse Zaken, 12 november 2010.