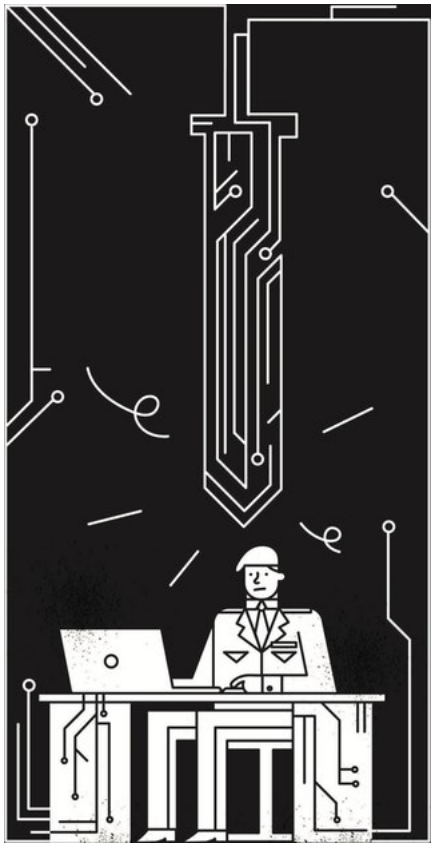
Wapengekletter in het geniep

cyberwapenwedloop | Waarin begeven de nieuwe Nederlandse cybermilitairen zich? De gevolgen van digitale oorlogsvoering zijn amper te overzien, blijkt uit de documentaire 'Zero Days', vanaf vandaag in de bioscoop.

KRISTEL VAN TEEFFELEN



illustratie Idris van Heffen

Het is een onvermijdelijke toekomst van oorlogsvoering. Eentje die bestaat naast land, water, lucht en ruimte. Waar we als Nederland wel in mee moeten gaan, omdat je er alleen kunt winnen als je anticipeert op de snelle veranderingen. Met die boodschap gaf minister Jeanine Hennis-Plasschaert van defensie in 2014 het officiële startschot voor het Defensie Cyber Commando. De nieuwe eenheid, bestaande uit tachtig cybermilitairen en burgers, richt zich volledig op het 'cyberdomein', en zal naast verdedigende taken, de militaire operaties van Nederland ook gaan ondersteunen door de vijand digitaal aan te vallen als dat nodig is, aldus de minister.

Sinds dat startschot in 2014 hebben de cybermilitairen vooral getraind in een speciaal daarvoor ontwikkeld oefennetwerk. Daar kunnen allerlei scenario's worden nagespeeld, en kunnen de door Nederland ontwikkelde digitale wapens worden getest. Het is nu alleen nog wachten tot het commando officieel operatief is, én echt in actie komt. Generaal Hans Folmer, commandant van de cybermilitairen, verwacht dat zijn mensen vanaf nu onderdeel zijn van elke buitenlandse missie van defensie, zei hij vorige week in deze krant.

Het is lastig voor te stellen in wat voor conflict de cybermilitairen dan terecht kunnen komen. Als er ergens een sluier van geheimzinnigheid omheen hangt dan zijn het de aanvals- en spionageacties van staten in de digitale wereld. Dat landen daar actief zijn - van de Verenigde Staten, tot Rusland, China, het Verenigd Koninkrijk en dus ook Nederland - is bekend. Wat ze er doen, is hoogst vertrouwelijk.

Dat de computerworm Stuxnet door een staat is gemaakt en ingezet als cyberwapen, daar is iedereen het over eens

Daar kwam ook de documentairemaker Alex Gibney achter. De Amerikaan, die zich voor eerdere films bezighield met thema's als scientology en Wikileaks, dook in de wereld van het even beroemde als beruchte computervirus Stuxnet. Beroemd vanwege de hoge kwaliteit, berucht vanwege de wereldwijde ophef die de computerworm veroorzaakte. Vanaf vandaag is de film die Gibney erover maakte, 'Zero Days', te zien in de Nederlandse bioscopen.

Op vrijwel alle vragen die over de oorsprong van Stuxnet gingen, ving Alex Gibney bot. Van de lange lijst mensen die hij voor zijn documentaire interviewde onthield iedereen zich van commentaar. Of zoals Michael Hayden, voormalig directeur van de geheime diensten CIA en NSA het omschrijft: "Ik weet het niet, en als ik het zou weten, zou ik het je niet vertellen."

Dat Stuxnet naar alle waarschijnlijkheid door een staat is gemaakt en ingezet als cyberwapen, daar is de beveiligingsbranche het wel over eens. Zo moet het ontwikkelen van de malware enorm veel tijd en geld hebben gekost, en vonden onderzoekers een einddatum in de code. Iets dat duidt op de input van juristen bij de opzet van de aanval.

Tikkende tijdbom

Om welke staat of staten het gaat, is ingewikkelder te bewijzen. Gibney kon daar alleen anonieme bronnen binnen de NSA en CIA over aan het woord laten. Die wijzen naar de Amerikanen en de Israëlische geheime diensten. Stuxnet was een gezamenlijk project gericht tegen het nucleaire programma van Iran. De malware wist centrifuges te manipuleren en op te blazen, waardoor het nucleaire programma wat vertraging opliep.

Opvallend is dat afgezien van de oorsprong - waar we het moeten doen met anonieme bronnen - er eigenlijk best veel over Stuxnet bekend is. Dat begon bij een computerbeveiligingsspecialist in Wit-Rusland, die de malware in 2010 opmerkte en alarm sloeg. Het virus bleek niet alleen bij het doel in Iran terecht te zijn gekomen. Het 'meest geavanceerde' computervirus tot dan toe dat door specialisten omschreven wordt als 'tikkende tijdbom' besmette wereldwijd veel meer systemen.

Zelfs in de VS werd er door Homeland Security - onbekend met het feit dat de computerworm waarschijnlijk van eigen makelij was - groot alarm geslagen. Dit virus was bedoeld én in staat om de kritieke infrastructuren, zoals elektriciteit- en waternet, te manipuleren. En daar zouden weleens doden bij kunnen vallen in de echte wereld, zo werd gevreesd.

Volgens Anouk Vos, mede-oprichter van technisch advieskantoor Revnext, laat het Stuxnet-verhaal vooral zien hoe moeilijk het is om de impact van een aanval met cyberwapens in te schatten. "Je stuurt malware de wereld in waarvan je de gevolgen niet kunt overzien. Het kan eenvoudig in verkeerde handen vallen. Afgevuurd, betekent afgevuurd." Vos begon haar carrière in de diplomatie

en kwam daar voor het eerst in aanraking met digitale aanvallen. Het deed haar besluiten om naar de cybersecuritybranche over te stappen.

Van Stuxnet verschenen later inderdaad verschillende mutaties. Een cyberwapen ontwikkeld door een staat, kan zo een 'doos van Pandora' worden, waarschuwt Albert Benschop, internetsocioloog aan de Universiteit van Amsterdam en auteur van het boek 'Cyberoorlog'. "En niet alleen cybercriminelen kunnen ervan leren. Ook je tegenstander steekt er veel van kennis op. Ik denk dat Stuxnet het wereldwijde niveau van malware omhoog heeft getild."

Plunderingen en chaos

Wat het virus ook duidelijk maakte, is dat een virtuele aanval met een computerworm, gevolgen kan hebben in de fysieke wereld. Benschop: "Beide werelden grijpen zo in elkaar, dat het met de inzet van cyberwapens bijzonder lastig is om geen burgers te treffen. Dat komt doordat de digitale infrastructuur die jij en ik gebruiken, grotendeels hetzelfde zijn als die van de militairen. De digitale aanvallen die vanwege een militair conflict worden uitgevoerd, kunnen daardoor diep ingrijpen op de informatie- en communicatiestructuren van een land. Wat als je het betaalverkeer van het land platlegt? Hoe doe je dan je boodschappen? En na hoeveel dagen beginnen de plunderingen en is er chaos?"

Juist daarom verbaast Anouk Vos zich over de geheimzinnigheid die om de inzet van cyberwapens heen hangt. Ook bij het Nederlandse Cyber Commando. Ze zeggen zich te houden aan het geldende oorlogsrecht - waardoor zij burgerslachtoffers moeten zien te voorkomen - maar ze vraagt zich af of dat wel zo één op één toepasbaar is op een conflict in de digitale wereld, waar burgers al snel de dupe zijn. Ook internationaal zijn er geen afspraken gemaakt. Vos: "Er zijn geen regels, er is geen doctrine. We práten er niet eens over."

Die kritiek komt ook aan bod in Gibneys documentaire. De norm in het cyberdomein is op dit moment: doe waar je mee weg kunt komen. Er zijn wel pogingen om richtlijnen op te stellen, maar dat blijft voorlopig nog vooral in de academische wereld hangen. Een internationaal akkoord, zoals er over oorlogsvoering op land, water, lucht en ruimte stuk voor stuk afspraken zijn gemaakt, lijkt ver weg.

Benschop ziet dat niet snel veranderen. Militairen geven niet graag hun strategie bloot. Bovendien is het buitengewoon moeilijk om te controleren wie welke cyberwapens heeft ontwikkeld. "We weten eigenlijk steeds minder van cyberwapens, ook omdat er zoveel partijen zijn die ze inzetten. Van staten, tot criminelen en activisten. Als ze ingezet worden, moet je ten eerste zien te achterhalen wat het was, en vervolgens wie het afvuurde. Ook bij Stuxnet werd in eerste instantie best geloofwaardig ontkend dat de Amerikanen de bron waren."

Ondertussen heeft de Navo wel al aangekondigd dat artikel 5 - oftewel: een gewapende aanval op één is een aanval op allen - ook van toepassing is in de digitale wereld. Het is een ontwikkeling die Vos zorgen baart. "Er is nog geen definitie gegeven aan wanneer een aanval reden geeft tot terugslaan. Er is niet duidelijk gemaakt of zoiets ook beantwoord kan worden in de fysieke wereld, of alleen met digitale wapens. Laat staan dat we weten wat de toelaatbare cyberwapens dan precies zijn."

Bovendien lijkt digitale oorlogsvoering, waar landen elkaar bestoken met aanvallen of spionage-acties, door het standpunt van de Navo een onvermijdelijke toekomst. Net zoals minister Hennis-Plasschaert bij de oprichting van het Defensie Cyber Commando ook sprak over 'anticiperen' op toekomstige oorlogsvoering.

Cybervrede

Vos ziet Nederland liever een andere weg bewandelen. Eentje die zij het streven naar cybervrede noemt. Een aanpak die Nederland wel heeft in het fysieke buitenlandbeleid - dat de nadruk legt op vrede en veiligheid en waarin Nederland altijd een belangrijke rol heeft gespeeld - maar in het cyberbeleid lijkt te worden vergeten, aldus Vos. "Daar lijkt alleen aanvallen en terughacken de optie."

Benschop noemt dat een mooi streven maar ook een utopie. "Het is hetzelfde als een mes gebruiken, terwijl je beschikt over een lange afstandsraket om je tegenstander op de knieën te krijgen. Een cyberwapen kun je inzetten vanachter je computer. Je hebt een paar knappe koppen nodig om het in elkaar te zetten. Dat maakt het ook nog eens een stap goedkoper dan de aanschaf van Joint Strike Fighters (de opvolger van de F-16, red.) of tanks. Het is nou eenmaal hoe de wereldverhoudingen op dit moment in elkaar zitten."

Maar juist daarom moeten we er alles aan doen om de ergste excessen te voorkomen, vindt Vos. "Cyberwapens zijn niet de oplossing voor alles. Iemand moet de eerste zijn die hierover het gesprek opent. Dat kan Nederland zijn. We kunnen nu nog een ander beleid kiezen, in plaats van meegaan in de wapenwedloop op het digitale slagveld. Ook daarmee doe je mee op het wereldtoneel."

De verwachting van beide experts: er zullen nog een hoop 'Stuxnetten' volgen. Misschien zelfs wel door Nederland gefabriceerd - al zullen we daar misschien nooit iets over te horen krijgen. Benschop: "Dat Stuxnet bekend werd, zou je vanuit militair opzicht een volledige mislukking kunnen noemen. Juist omdat we ervan afweten."

'We weten steeds minder van cyberwapens, ook omdat er zoveel partijen zijn die ze inzetten'