

Landmacht voert cyberwapen en elektronische oorlogvoering op, maar mag vanwege privacy niet realistisch oefenen

Posted on 20 september 2025 by Eric Vrijsen

Vijftien jaar geleden worstelde CDA-minister Hans Hillen van Defensie met een zware bezuinigingstaak. Hij riep een aantal generaals bij zich om de toekomst van de oorlog te bespreken. Kon het land goedkoper worden verdedigd, bij voorbeeld door gebruik te maken van het internet en de computersystemen van een potentiële vijand te verstoren? De minister vroeg de generaals over hoeveel hackers zij beschikten. Hij wilde graag eens met die jongelui van gedachten wisselen. De topmilitairen keken hem verbouwereerd aan: 'Hackers? Maar mijnheer de minister, dat is toch illegaal!'

Hillen verzekerde de generaals dat zij hackers in de gelederen hadden: 'Maar u weet het zelf niet.' Naderhand gaf hij zijn persoonlijk adjudant – een jonge officier – opdracht om een overlegje te organiseren met militaire cyberspecialisten. Kort

daarna zat een groep geüniformeerde wizzkids bij de minister aan tafel.

Het wapen van de toekomst

Onder zware druk van toenmalig VVD-premier Mark Rutte, schrapte Hillen de Leopardtanks. Wel bood hij de landmachtgeneraals perspectief op 'het wapen van de toekomst': cyber. Eerst moest de Adviesraad Internationale Vraagstukken echter rapport uitbrengen. Advies: uitsluitend defensieve cyberoperaties en alles strikt binnen de Nederlandse wet. Vervolgens werd een cyberstrategie uitgeschreven, die voorzag in defensieve én offensieve operaties. In 2014 werd het Defensie Cyber Commando opgericht om te hacken, te verstoren en te misleiden. Het werd onderdeel van de landmacht.

Je hoort er zelden iets over, want al het cyberwerk is heimelijk. Maar aangezien veel Trans-Atlantische datalijnen via de Nederlandse kusten aan land komen, moet de verdediging op orde zijn en moet je niet terugdeinzen voor offensieve inzet van je cyberwapen. De Oekraïneoorlog zet de hele zaak op scherp.

Behalve de cyberoperaties van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) van Defensie, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) van Binnenlandse Zaken en het Defensie Cyber Commando, bestaat er sinds kort ook een gespecialiseerd bataljon bij de Koninklijke Landmacht. Het doel van 101 CEMA-bataljon is om de militaire operaties van de vijand in de war te schoppen door 'Cyber en Electro-Magnetische Activiteiten'. CEMA kent een uitgesproken offensieve aanpak.

Op de legerplaats in Stroe was onlangs een openingsceremonie waar jonge militairen – hun gezichten verborgen onder bivakmutsen en sjaals – een inkijkje gaven in wat ze allemaal kunnen. Het Defensie Cyber Commando voert strategische hacks uit op de systemen van de vijand. Het 101 CEMA-bataljon doet hetzelfde, maar dan op tactisch niveau. De officieuze naam is 'hackersbataljon', maar dat dekt niet de hele lading. Cyber gaat over de data, de bits en bites. Electro-Magnetische oorlogvoering gaat over de golflengtes, frequenties, signaalverbindingen en over het elektromagnetisch veld. De strijd om die data is nauw verbonden met het hightech gevecht om de verbindingen.

Uit het boekje

Cyberanalist luitenant Jeroen staat net uit te leggen dat ook het onderscheid tussen strategische en tactische operaties tamelijk kunstmatig is, als een van zijn dienstmakkers plotseling opkijkt van zijn laptop en nuchter vaststelt: 'Ik ben binnen.' Toegegeven, het is een oefensituatie. De militairen mogen niet zeggen of ze daadwerkelijk de Russische systemen binnendringen. Maar deze exercitie is er een uit het boekje en die Russen lijken net mensen: 'Ik heb een paar voor de hand liggende wachtwoorden geprobeerd en met "I love you" zat ik erin. Toen bleek dat alle verdere wachtwoorden keurig te vinden waren onder een icoontje op het bureaublad. Ik heb meteen zoveel mogelijk bestanden gekopieerd.'

Hoe weten luit Jeroen en zijn cyberkameraad dat het geen digitale boobytrap was? Tja, dat weet je nooit.

Offensieve actie

De hackers van het CEMA-bataljon dringen binnen in de vijandelijke netwerken, speuren daar rond, tappen af. Zij gaan niet eigener beweging in het offensief. 'Wij geven advies aan de operationeel commandant. Die beslist,' zegt luitenant Jeroen. Hij verzekert dat zijn hackersgroep 'maatwerk levert'. Dat wil zeggen: de cyberdeskundigen en elektronische oorlogvoeringspecialisten penetreren niet alleen laptops en computers, maar ook drones, radarinstallaties, infraroodcamera's, videosystemen, akoestische sensoren, de hele santenkraam van het militaire *internet of things*.

Ze kunnen de vijand bespieden. Ze kunnen ook verbindingen verstoren (*jammen*), zodat de vijandelijke eenheden in paniek raken. Subtieler is *spoofen*: dan dringen ze stiekem systemen binnen om daar subtiele foutjes te introduceren, die 's vijands slagkracht aantasten. Nog iets geavanceerder is *meaconing*: ze vangen de vijandelijke satellietsignalen op en zetten die vervolgens door met een minieme vertraging. Slechts een ultrakort tijdsverschil volstaat om de precisie van de vijandelijke richtapparatuur en vuurleiding te doen haperen.

Stoorzenders zijn er in het leger al sinds jaar en dag. Van oudsher werden ze ingedeeld bij de Verbindingstroepen. Het idee is dat als je de eigen radioverbindingen op orde hebt, je ook in staat bent de signalen van de vijand in de

war te schoppen. En omgekeerd: als je traint op het verstoren van de vijandelijke communicatie, kun je de betrouwbaarheid van je eigen elektronische data beter beschermen.

De CEMA-eenheid staat overduidelijk nog in zijn kinderschoenen.

Om de oprichtingsceremonie in Stroe te verlevendigen, staan rond het exercitieterrein allerlei peilzenders en stoorzenders opgesteld. Het wekt de indruk van een allegaartje. Allerlei oude en nieuwe pantservoertuigen – een bijna antieke Duitse Fuchs, enkele twintig jaar oude Australische Bushmasters, maar ook een laatste versie van de Piranha van Zwitserse makelij, en de splinternieuwe Manticore-jeeps – staan te pronken met hun telescoopantennes.

Verlamd

Hoe kleiner het voertuig, hoe krachtiger, lijkt het wel. Op de Manticore-jeep staat een antenne voor het uitvoeren van een elektromagnetische aanval. Door een krachtige puls uit te zenden, vliegen alle schermen op zwart en raakt de tegenstander verlamd. 'Waarschijnlijk liggen wij er dan zelf ook uit,' zegt luitenant Jeroen. 'Maar wij weten dan tenminste waardoor dat komt.'

Om luistervinkje te kunnen spelen op een uitgestrekt slagveld in bij voorbeeld Litouwen, zou de CEMA-eenheid moeten beschikken over een veel grotere vloot voertuigen met zenders en receptoren. Daar wordt aan gewerkt, maar dit is alvast een begin en het hele idee van het cyberwapen is dat je met minimale inspanningen een maximaal effect kunt bereiken.

Privacywetgeving

Je moet het natuurlijk wel durven, kunnen en mogen. Achter hun bivakmutsen en sjaals hoor je de mannen van het CEMA-bataljon heel voorzichtig klagen over de geldende privacywetgeving in Nederland. Ze zouden felrealistische oefeningen willen doen, maar de regels en voorschriften leggen nogal wat beperkingen op. In hun stem klinkt gelatenheid door als zij vertellen dat ze alleen mogen oefenen in een digitale omgeving die nergens de grenzen van het virtuele kazerneterrein overschrijdt. Ze mogen alleen digitaal droogzwemmen, daar komt het op neer.

Nederland is het land waar legeroefeningen met observatiedrones moesten worden

gestaakt, omdat niet honderd procent viel uit te sluiten dat de camera's per abuis een passerende auto op een naburig landweggetje in beeld zouden brengen. Ja, de persoonlijke levenssfeer is heilig. Intussen fotograferen en filmen miljoenen Nederlandse burgers via hun deurbel en via de bij de MediaMarkt gekochte bewakingscamera's elke auto die door de straat rijdt en elke wandelaar die de voordeur voorbijloopt. Wie is hier nou gek?

De cybermethode

Cyberspecialist luitenant Jeroen zegt dat er strikte interne controle is op de naleving van privacyregels. Om toch te kunnen oefenen, worden er digitale netwerken aangelegd en daarop mogen ze hun vaardigheden testen. Ze mogen nu eenmaal niet zomaar hacken in een vrije omgeving. In sommige gevallen worden oefeningen gehouden op de uitgestrekte militaire terreinen in Duitsland. Daar hebben de hackers volop fysieke ruimte en dat draagt bij aan het realistische karakter van hun oefeningen.

Want uiteindelijk komt het daar natuurlijk op aan: met virtuele strijdmiddelen effecten bereiken in de fysieke omgeving. De commandant van 101 CEMA-bataljon luitenant-kolonel Peter Masseling heeft het in Stroe over 'bescherming en slagkracht'. Hij geeft het voorbeeld van een strategisch gelegen brug die je met artillerie of vanuit een straaljager kunt vernietigen, maar waarbij het veel slimmer kan zijn om met je cyberspecialisten de computerbesturing over te nemen. Dan haal je de brug op, zodat de vijand er niet meer overheen kan. Zodra jijzelf dat water moet oversteken, laat je dat brugdek op afstand weer naar beneden.

Kortom, de cybermethode is door geen zinnig mens te verwerpen. Het voorbeeld van overste Masseling wordt die middag door menigeen aangehaald.

Wie jong is en technisch onderlegd, kan bij deze eenheid snel carrière maken. Sergeant Tom begon acht jaar geleden bij de 'Verbindingstroepen' als soldaat, nu is hij analist-onderofficier en beschrijft hij de opmars van steeds krachtiger stoorzenders. De *jammers* zijn inmiddels verwikkeld in een wapenwedloop met zichzelf. Tom: 'Destijds volstond een zender van een paar honderd Megahertz. Nu gebruiken we een veelvoud daarvan.' Het bereik van een stoorzender wordt uitgedrukt in het aantal microgolven per seconde, waarbij 1 Gigahertz neerkomt op een miljard golven per seconde. De exacte getallen zijn operationeel vertrouwelijk. Het zou inmiddels gaan om veel meer dan 1 Gigahertz.

De voertuigen met de diverse elektronische systemen van het CEMA-bataljon dragen de namen van vissen. Kapitein Joep staat bij de Sawfish (Zaagvis). Het is een bermbombestendige Bushmaster, een pantservoertuig dat tijdens de Afghanistan-missie in allerijl werd aangeschaft om op een veiliger manier soldaten te vervoeren. De onderzijde was v-vormig, zodat de klap van een bermbom zich zijwaarts verplaatste en de inzittenden de explosie konden overleven. Weldra werden de voertuigen ook voorzien van stoorzenders. De Taliban en andere gewapende opstandelingen brachten hun bermbommen immers tot ontploffing met een signaal uit hun mobieltjes. Je hoefde de GSM-verbindingen maar te verstoren en die bommen ontploften niet meer.

‘Het zijn altijd de kleinkinderen’

Kijk eens wat voor antennes nu achter en bovenop de Zaagvis zijn gemonteerd. Vandaar ook die naam. Een Zaagvis is een dier dat met zijn spitse, zeer lange snuit door de zeebodem woelt om vervolgens zijn prooi te vangen. De Sawfish doet dat ook, maar dan door de lucht.

Naast de Sawfish staat de ‘Multirole Bushmaster’. Aan de linkerzijde van dit pantservoertuig bevinden zich de antennes om de vijand uit te peilen en te hacken. De antennes ter rechterzijde om te storen. Kapitein Joep wijst op een zwarte, kogelvormige monitor (circa een halve meter lang) die bedoeld is om vijandelijke drones te manipuleren. Daarnaast is een grote ‘hanenkam’ gemonteerd om radiosignalen te vervormen.

De kapitein gaat wijdbeens achter de Bushmaster staan om trots te poseren. De met antennes overladen pantserwagen is het rijdende bewijs dat de Koninklijke Landmacht de afgelopen jaren volop lering heeft getrokken uit de gebeurtenissen in Oekraïne. Zonder toenmalig minister Hillen van Defensie was dat misschien niet gelukt.

Terugblikkend op zijn gesprek met de generaals en zijn aanzet tot het offensieve cyberwapen, zegt Hillen: ‘Het zijn altijd de kleinkinderen die opa’s telefoon repareren en oma’s laptopje weer aan de praat krijgen.’

Wynia’s Week *brengt broodnodige, onafhankelijke berichtgeving: drie keer per week,* ***156 keer per jaar****, met artikelen en columns, video’s en podcasts. Onze donateurs maken dat mogelijk. Doet u mee? Hartelijk dank!*