Reservisten en *cyberoperations*

Schaarse expertise veiligstellen voor calamiteiten en militaire operaties

Het afgelopen jaar heeft Defensie de nodige stappen gezet op het gebied van *cyberoperations*. Cyber draait om technologie, maar is uiteindelijk mensenwerk en juist aan gekwalificeerde mensen is een tekort. In andere landen maken defensieorganisaties op verschillende manieren gebruik van cyberreservisten om het tekort aan te vullen en daar kunnen we van leren. Ook in Nederland kunnen reservisten in een deel van de groeiende behoefte aan specialisten voorzien, mits de propositie richting reservisten en vooral hun werkgevers aantrekkelijk genoeg is. Tevens zijn aanvullende afspraken met specifieke werkgevers nodig om de tijdige beschikbaarheid van goede mensen te garanderen.

*Mr. P. de Graaf en J.D. Harskamp MBA**

Kranten en digitale media zijn niet meer te raadplegen zonder iets over cyber te lezen: cybercrime, digitale spionage, *hacktivisme*. Het digitale domein heeft inmiddels ruime aandacht van media, bedrijfsleven en politiek, maar ook van Defensie. Ook in de *Militaire Spectator* zijn diverse artikelen over dit onderwerp verschenen. Het digitale dreigingsbeeld is, gezien zaken als Anonymous, Stuxnet, Duqu, KPN en DigiNotar, de afgelopen jaren aanzienlijk veranderd. Niet alleen neemt het aantal incidenten toe, maar ook zijn de aanvalsmethodes steeds geraffineerder.[1] In de militaire context is de uitdaging niet beperkt tot het beter beschermen van netwerken, systemen en informatie; de uitdaging waar Defensie voor staat is om te allen tijde de eigen vrijheid van handelen in het cyberdomein te waarborgen. Dit is – gegeven de interconnectiviteit van Defensie – van essentieel belang voor de inzetbaarheid, waar ook ter wereld.

Het afgelopen jaar heeft Defensie de nodige stappen gezet om in de toekomst het hoofd te kunnen blijven bieden aan de toenemende dreigingen en om beter gebruik te kunnen gaan maken van de kansen die het digitale domein biedt. Er is een visie op cyberoperations opgesteld en een bijbehorend intensiveringsplan.[2] Tot en met 2015 wordt op basis daarvan vijftig miljoen euro extra vrijgemaakt voor cyberoperations en in de jaren daarna ruim twintig miljoen per jaar. Om het programma te leiden is bij de Defensiestaf de Taskforce Cyber ingesteld.

Cyberoperations zijn onlosmakelijk verbonden met technologie. Maar hoe technologisch ook, cyber is uiteindelijk vooral mensenwerk, of het nu gaat om gebruikers, beslissers of technisch specialisten, kortweg de *hackers*. We richten ons in dit artikel juist op die specialisten, waaraan breed in de markt een tekort is ontstaan. Hierbij gaan we in op de mogelijkheden van een specifieke *pool* cyberreservisten als één

* Patrick de Graaf is adviseur op het gebied van cybersecurity, in het bijzonder strategie, organisatie en de *human factor*; Jurjen Harskamp is strategisch adviseur rondom de thema's defensie en cybersecurity.

1 GOVCERT.NL, *Cybersecuritybeeld Nederland*, december 2011.

2 Beleidsbrief van 8 april 2011, *Defensie na de kredietcrisis: een kleinere krijgsmacht in een onrustige wereld.*

van de maatregelen om dit tekort voor Defensie op te vangen. Tevens bekijken we hoe andere landen daarmee omgaan.

De zin van cyberreservisten

Cyberreservisten zijn civiele cyberspecialisten (technisch of op een aanpalend gebied), die Defensie op kan roepen in geval van cybercalamiteiten en voor militaire operaties. Goede kandidaten beschikken niet alleen over voldoende technische kennis, maar ook over de nodige creativiteit en kunde om deze technische kennis effectief in te zetten. Defensie heeft een toenemende behoefte aan cybersecurity-expertise binnen haar organisatie. Niet alleen bij calamiteiten, maar ook voor het mogelijk maken van de dagelijks werkzaamheden en om in geval van conflict over voldoende gekwalificeerd personeel met een militaire status te beschikken. Defensie staat echter niet alleen in de behoefte aan cyberexpertise, zoals blijkt uit de voorgenomen groei van het Nationaal Cyber Security Centrum, banken, IT-security bedrijven en digitale expertise als discipline bij de politie. De opschaling van cyberexpertise in deze organisaties leidt tot grotere schaarste in de arbeidsmarkt van cyberprofessionals. Het tekort aan cyberprofessionals lijkt ook structureel, gezien de lage aantallen studenten die jaarlijks op HBO- en WO-niveau met IT-specialisatie afstuderen. Deze aantallen zijn momenteel al onvoldoende om in de reguliere vraag vanuit IT-werkgevers te voorzien.[3] De minister en medewerkers van Defensie laten mede daarom weten de inzet van cyberreservisten te overwegen als oplossing om het onderkende tekort aan specialisten op te vangen.[4] Dit roept de vraag op of cyberreservisten het unieke geheime wapen vormen waarmee Defensie haar slag op de arbeidsmarkt kan slaan. De Adviesraad Internationale Vraagstukken is hier kritisch over: 'Mogelijk bestaat er in Nederland onvoldoende animo om zich als gekwalificeerd vrijwilliger te melden'.[5] Organisatiecultuur en arbeidsvoorwaarden zijn volgens de Adviesraad de belemmerende factoren. Is de kous daarmee af?

FOTO ANP, L VAN LIESHOUT

Met andere spelers, zoals het onlangs opgerichte Nationaal Cyber Security Centrum, vist Defensie in dezelfde vijver naar schaarse cyberexpertise

Nee, want het voordeel van cyberreservisten is te groot om het concept direct te verwerpen. Het maakt het aantrekken van mensen mogelijk die al (met succes) in het cybersecurity domein werkzaam zijn en als reservist bekend zijn met de defensieorganisatie. Zij kunnen snel en gericht aan de slag wanneer dat nodig is. Het is een manier om efficiënter om te gaan met schaarse expertise. Het DigiNotar-incident laat zien dat een plotselinge noodzaak tot opschaling en verschuiving van capaciteit in

3 Zie: www.ict-office.nl.

4 Minister van Defensie, *Van zwaard naar joystick. De rol van Defensie in de digitale frontlinie*, speech 13 april 2011 tijdens de conferentie Cyber Operations van het Koninklijk Instituut van Ingenieurs. Anoniem, *Defensie twijfelt over cybersoldaten*, op www.security.nl, 12 november 2010.

5 Adviesraad Internationale Vraagstukken en Commissie van Advies inzake Volkenrechtelijke Vraagstukken, *Digitale oorlogvoering*, december 2011.

de praktijk ook daadwerkelijk voorkomt.[6] Defensie heeft bij het afwikkelen van dit incident haar bijdrage geleverd door capaciteit uit het DefCERT team beschikbaar te stellen. Reservisten kunnen daarnaast – zoals de Adviesraad ook aangeeft – een rol spelen in opleiding, training en oefenen. Het is al met al duidelijk dat het concept cyberreservisten zowel in kwantitatieve als kwalitatieve zin (toegevoegde) waarde heeft en uitwerking verdient.

Cyberreservisten in andere landen

Verschillende landen schakelen al met succes civiele cyberspecialisten in om het landsbelang te dienen. Uiteraard is hier niet de reguliere inhuur bedoeld. Wat is hiervan te leren? Om hier antwoord op te geven beschrijven we kort de inzet van cyberreservisten in de Verenigde Staten, Groot-Brittannië, Estland en China. Waarvoor schakelen deze landen reservisten in, op welke schaal doen zij dit en op wie richten zij zich bij de werving?

Verenigde Staten: alles in het groot

De VS zet zwaar in op cyberspace als vijfde domein voor de krijgsmacht. De afgelopen twee decennia zijn militaire cyberorganisaties dan ook sterk gegroeid. Alle krijgsmachtdelen maken naast vast personeel en van de *National Guard* ook gebruik van cyberreservisten.[7] Het exacte aantal is niet openbaar, maar we schatten het op ongeveer tienduizend voor *U.S. Army*, *Air Force*, *Navy* en *Marines* tezamen.[8] De inzet is breed: defensieve taken, inlichtingen en offensief werk. De verschillende krijgsmachtonderdelen hebben ondanks de vele reservisten echter nog steeds verschillende tekorten, zowel kwalitatief (een scala aan specifieke functies), als kwantitatief (met name voor opschaling bij incidenten en operaties, de zogeheten *surges*).[9]

De samenwerking met de civiele sector voor – onder meer – een *exceptional cyber workforce* is één van de vijf speerpunten in de *Strategy for Operating in Cyberspace* van het Department of Defense.[10] Die samenwerking is mede gericht op het bevorderen van het heen en weer stromen van cyberprofessionals tussen de publieke en private sector. De VS richt zich op een brede doelgroep, mede gezien de brede vraag: van scholieren tot hooggekwalificeerde professionals op senior managementniveau in het (IT-security) bedrijfsleven. Op *LinkedIn* noemen Amerikaanse professionals zich vol trots cyberreservist. Om veelbelovende professionals aan zich te binden hebben de federale overheid, Defensie en de afzonderlijke krijgsmachtdelen diverse middelen ontwikkeld. Zo zijn er studiebeurzen voor relevante opleidingen, bijvoorbeeld het *Information Assurance Scholarship Program* (sinds 2001) en het *Federal Cyber Service-Scholarship for Service* (onder meer voor NSA en DISA) met daaraan gekoppeld de verplichting om een aantal jaar te dienen. Ook kent de VS diverse vormen van werk- en leertrajecten, wervings- en retentiebonussen en cybergames. Goed om te weten is dat reservisten in de VS ook kunnen rekenen op medische en tandheelkundige hulp en tegemoetkoming in huisvestingskosten.

De samenwerking met werkgevers is in de VS belangrijk om reservisten te werven, want ook daar moet de werkgever instemmen met de opkomst van werknemers als reservist. De samenwerking gaat echter verder dan *Employer Support* (het informeren van werkgevers). Zo heeft de U.S. Army een programma om voor specifieke profielen reservisten op te leiden en als werknemer te laten plaatsen bij civiele werkgevers.[11] Uiteraard in geschikte functies,

6 In september 2011 zei de Nederlandse overheid het vertrouwen in DigiNotar op nadat servers van het bedrijf waren gehackt en internetcertificaten onbetrouwbaar waren verklaard. Zie: www.rijksoverheid.nl.

7 Behalve de *United States Air Force*, *U.S. Army*, *U.S. Navy* en de *U.S. Marines*, kennen de *National Security Agency* (NSA), het *Defense Cyber Crime Center* (DC3), de *Defense Information Systems Agency* (DISA) en het *U.S. Cyber Command* cyberreservisten.

8 Deze schatting is gebaseerd op vergelijking van totale aantallen reservisten (exclusief National Guard) ten opzichte van de totale vulling van de Amerikaanse strijdkrachten, op basis van verschillende begrotingen van het Department of Defense (ongeveer 1:4). Deze verhouding hebben we toegepast op *information assurance* personeel (46.000 volgens het Department of Defense, *Cyber Operations Personnel Report* (Washington, D.C., April 2011). De uitkomst daarvan (12.000) hebben we naar beneden afgerond vanwege de schaarste aan cyberpersoneel.

9 U.S. Department of Defense, *Cyber Operations Personnel Report* (Washington, D.C., April 2011); U.S. Department of Defense, *DoD Fiscal 2012 Budget Proposal* (Washington, D.C., 2011). Zie voor een voorbeeld van vacatures www.afreserve.com.

10 U.S. Department of Defense, *Strategy for Operating in Cyberspace* (Washington, D.C., 2011).

11 United States Government Accountability Office, *Reserve Forces. Army Needs to Finalize an Implementation Plan and Funding Strategy for Sustaining an Operational Reserve Force* (Washington, D.C., 2009).

FOTO U.S. ARMY, M. GREESON

De Amerikaanse luchtmachtgeneraal Gregory Brundidge licht tijdens een conferentie over cybersecurity ook het belang van reservisten toe

zodat ze beschikbaar zijn én over actuele kennis beschikken. Dit programma is niet speciaal voor cyber ingericht. Tot slot doet het Department of Defense een proef met rotatie van personeel met enkele bedrijven, wel specifiek voor cyberpersoneel.[12]

Groot-Brittannië: groei verwacht

Ook in Groot-Brittannië zetten de krijgsmachtdelen reservisten in voor cyberoperations. Dit gebeurt uiteraard op een veel kleinere schaal dan in de VS. Volgens het Britse rapport *Future Reserves Review 2020* is er gezien de toegenomen bedreigingen en kansen echter een flinke uitbreiding nodig van cyberreservisten.[13]
De honderd reservisten van de *Specialist Group Royal Signals* (SGRS) zijn een goed voorbeeld van toepassing van het reservistenmodel op cyber. Deze reservisten zijn gescreende experts uit de civiele praktijk en zij vervullen onder meer IT-audits in Groot-Brittannië zelf en op buitenlandse missies. Ze dienen gemiddeld negentien dagen per jaar in *tours* van drie jaar. Gemiddeld zijn er een tot twee mobilisaties per persoon per jaar. Het is de bedoeling dat ook de SGRS groeit, naar tweehonderd man.[14]

Primaire doelgroep in Groot-Brittannië zijn de ervaren IT-professionals. De gereedstelling gebeurt volgens een constructie die sterk lijkt op ons Nederlandse reservistenmodel. Individuen kunnen zich vrijwillig aanmelden om te dienen als reservist voor Defensie. Hun werkgever moet hier ook mee instemmen. Interessant idee: de *2011 UK Cyber Security Strategy* bepleit legerreservisten in te schakelen bij de politie om schaarse vaardigheden efficiënt in te zetten. Gezien de groeiende behoefte van de Nederlandse politie aan digitale rechercheurs is zo'n samenwerkingsverband – of een variant daarvan – voor Nederland mogelijk ook relevant.[15]

12 U.S. Department of Defense, *Cyber Operations Personnel Report* (Washington, D.C., 2011).
13 The Independent Commission to Review the United Kingdom's Reserve Forces, *Future Reserves 2020* (Londen, 2011).
14 Lt Col Chris Barrington Brown RA, presentatie *Specialist Group Royal Signals (SGRS)*, 2011.
15 Zie onder meer de Nationale Cyber Security Strategie, 2011. Het team van het Programma Aanpak Cybercrime coördineert de intensivering bij de Nederlandse politie.

Estland: het beroemde vrijwilligersleger
Estland is een veelgenoemd voorbeeld voor cyberreservisten vanwege het vrijwilligers-cyberleger: de *Cyber Defence Unit of the Defence League*. Of op z'n Ests: *Küberkaitseliit*.[16]
De impact van de digitale aanvallen in 2007 op de Estse samenleving leidden daar tot de vorming van deze tak van het al bestaande vrijwilligersleger (*Kaitseliit*). De gereedstelling van deze geüniformeerde dienst lijkt bij nadere bestudering ook sterk op het Nederlandse reservistenmodel, zij het dat de Kaitseliit als apart legeronderdeel fungeert, enigszins vergelijkbaar met de Amerikaanse National Guard. Deze reservisten zijn dus niet ondergebracht bij een operationeel commando, zoals in Nederland. De Küberkaitseliit bestaat uit twee subunits van in totaal 94 mensen in Tallinn en Tartu. Deze mensen zijn over het algemeen patriottische individuen met IT-vaardigheden of andere specialisten op het gebied van cybersecurity, zoals juristen en economen. Deze professionals komen vooral uit de IT-afdelingen van Estse banken, hotels en overheden. De Küberkaitseliit heeft een puur defensief karakter en kan hooguit adviseren over offensieve acties. De belangrijkste activiteiten zijn kennisdeling, bouwen van een netwerk voor publiek-private samenwerking, training en *awareness* en online-cyberoefeningen.

Door afspraken te maken met werkgevers hebben andere landen al een *pool* van cyberreservisten op kunnen zetten

FOTO REUTERS, I. KALNINS

China: alles anders
Waar landen als de VS, Groot-Brittannië en Estland zich primair richten op individuen, kiest het Chinese Volksbevrijdingsleger voor meerdere wegen om de gewenste grote schaal te bereiken. Om een ruime pool van duizenden technische professionals aan zich te binden maakt het leger afspraken over hun beschikbaarheid met hun werkgevers. Dit zijn veelal high-tech bedrijven en instituten.[17] Deze groepen professionals heten in diverse publicaties ook wel cybermilities. Deze vullen de officiële cyber warfare unit van het leger (het Cyber Blue Team) aan,[18] alsmede de *Signals Intelligence and Cyber Reconnaissance* diensten.[19] De Chinese cybermilities kennen dan ook een brede *scope*: defensief, offensief en inlichtingen.

Het Volksbevrijdingsleger werft tevens op individueel niveau jonge hackers uit de Chinese (criminele) *cyberscene* en talentvolle studenten op universiteiten via hackingcompetities en *information warfare* onderzoek. Patriottische

16 G. Gelziss, Estonian voluntary cyber-soldiers integrated into national guard, *Deutsche Welle*, 5 april 2011; T. Gjelten, *Volunteer Cyber Army Emerges In Estonia*, zie: *www.npr.org.*; ministerie van Defensie Estland, *Government formed Cyber Defence Unit of the Defence League*, persbericht 20 januari 2011; C. Czosseck e.a., *Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security*, Cooperative Cyber Defence Centre of Excellence (Tallinn 2011).

17 J. Carr, *Inside Cyber Warfare. Mapping the Cyber Underworld* (Sebastopol, CA, O'Reilly Media, Inc., 2009) 171 e.v.; Bruce Schneier, *The Truth About Chinese Hackers*, 19 juni 2008 (www.schneier.com); Infosec Island Headlines, *China Beefs Up PLA's Cyber Militia*, 21 oktober 2011 (www.infosecisland.com); Kathrin Hille, 'Chinese Military Mobilises Cybermilitias' in : *Financial Times*, 12 oktober 2011.

18 'China admits cyber warfare unit', *Channel4 News*, 26 mei 2011.

19 Mark A. Stokes e.a., *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure* (Project 2049 Institute, 2011) 6.

Na de digitale aanvallen van 2007 kreeg Estland een leger van cybervrijwilligers en zette het land in op internationale samenwerking via het in Tallinn gevestigde Cooperative Cyber Defence Centre of Excellence van de NAVO

hackers zoeken en vinden ten slotte op individuele basis eer en glorie in activiteiten die de belangen van China dienen, zonder dat er rechtstreekse sturing door de staat lijkt te zijn. Denk hierbij aan politiek getinte aanvallen op Taiwanese websites.[20] Dergelijke puur vrijwillige initiatieven zijn in Nederland nog niet echt van de grond gekomen en dat lijkt ook slecht in onze landsaard te passen. Hier heeft de Adviesraad Internationale Vraagstukken een terecht punt.[21] Door de combinatie van de collectieve afspraken met werkgevers en de werving van individuele hackers heeft China inmiddels een aanzienlijke pool aan experts beschikbaar, vermoedelijk de grootste flexibele cyberschil in de wereld.

Wat leert ons dit?

De belangrijkste les die we uit andere landen kunnen trekken is dat het aanleggen van een flexibele schil aan cyberprofessionals in de vorm van cyberreservisten mogelijk en zinvol is. Het leidt voor de beschreven landen tot extra capaciteit en toegang tot kennis uit de civiele sector. Dit is goed nieuws, omdat de bestaande generieke reservistenconstructie bruikbaar zou zijn, met name die voor Reservisten met een Specifieke Deskundigheid. Dit maakt een snelle start mogelijk. Tevens zien we dat er in meerdere landen behoefte is aan extra flexibele capaciteit bovenop de aangetrokken reservisten. Gegeven de schaarste op de Nederlandse arbeidsmarkt is het aannemelijk dat er – op termijn – ook in Nederland aanvullende oplossingen nodig zijn.

Cyberprofessionals kunnen als reservist de nodige civiele kennis meebrengen naar Defensie

Zijn cyberreservisten in de Nederlandse context haalbaar?

Hoe lastig het ook is om aan goede mensen te komen, een 'rondje langs de velden' bij verschillende defensieonderdelen, civiele werkgevers en reservisten maakt duidelijk dat Defensie het met enige inspanning interessant genoeg kan maken voor cyberprofessionals om reservist te worden. Defensie heeft inhoudelijk interessant werk voor specialisten, waar onder omstandigheden dingen mogen die in de civiele sector altijd verboden zullen zijn of gewoonweg niet kunnen. Met zaken als oefenen in semi-live omgevingen, (buitenlandse) opleidingen, het ontmoeten van andere slimme mensen en *war gaming* kan Defensie mensen duurzaam aan zich binden. Geld is voor de echte hacker geen erg belangrijk onderwerp. Ze kennen echter ook wel hun waarde, afgaand op hoe ze op

20 Zie onder meer: Yao-chung Chang, 'Cyber Conflict Between Taiwan and China' in: *Strategic Insights*, Vol. 10, Issue 1 (Spring 2011).

21 REALCERT leek wat dit betreft veelbelovend als vrijwillige *incident response* organisatie, totdat het initiatief een dag na de start alweer stopte (zie: http://webwereld.nl).

FOTO AVDD, H. KEERIS

Als de krijgsmachtdelen reservisten inzetten voor een veelvoud aan taken, moet het ook mogelijk zijn een pool van cyberreservisten aan te leggen

internetfora oordelen over de arbeidsvoorwaarden van de overheid. Belangrijker dan geld is dat Defensie als werkomgeving vooruitgang laat zien in cyberoperations, specialisten op waarde weet te schatten en hen telkens nieuwe uitdagingen en ruimte om te experimenteren weet te bieden. Het leiderschap moet zich daarnaar plooien, om het meeste uit de cyberprofessionals te halen.[22] Cultuur, de focus op technische inhoud en de *drive* om steeds beter te worden zijn dus inderdaad belangrijke onderwerpen. Dit geldt overigens niet alleen voor de cyberreservisten; de Taskforce Cyber heeft hier nog een mooie uitdaging voor de boeg, maar heeft ook het tij mee.

Werkgevers, zeker die waar IT-security *core business* is, hebben een veel kleiner belang. Met hen is het lastiger tot een *win-win* overeenkomst te komen. Natuurlijk leren hun medewerkers van het werk bij Defensie en leren ze meer over Defensie als (toekomstige) klant, maar daar staat ook verlies aan productiecapaciteit tegenover. Dit wringt te meer wanneer reservisten ingezet zouden worden voor zaken waar Defensie anders de werkgever tegen commerciële condities voor zou inschakelen. Dergelijke bedrijven zijn beducht voor marktverstoring. De propositie naar werkgevers is erg belangrijk, omdat het reservistenschap niet alleen vrijwillig is voor de reservist, maar ook voor diens werkgever. Deze moet de reservist namelijk (onbetaald) verlof toekennen. De dialoog met werkgevers met een ruime populatie aan geschikte kandidaten (de 'grootleveranciers') over voldoende beschikbaarheid van professionals is daarom cruciaal. Het kan zelfs zijn dat een afzonderlijke afspraak nodig is over inhuur bij calamiteiten met duidelijke *service levels* over tijdigheid, kwaliteit enzovoort. Dit neemt niet weg dat een pool van cyberreservisten ook in de Nederlandse defensiecontext haalbaar lijkt.

Tot slot

Cyberreservisten bieden een oplossing voor Defensie om de eigen capaciteit te vergroten met een flexibele schil, mits de balans met reservisten en in het bijzonder de werkgevers kan worden gerealiseerd. De bestaande regelingen voor reservisten maken een snelle start mogelijk. Het is echter hoogstwaarschijnlijk geen volledige oplossing voor het capaciteitstekort, gezien de sterke concurrentie op de arbeidsmarkt, waarin zelfs overheidsorganisaties elkaar beconcurreren. De uitdaging ligt er niet alleen voor de reservisten, want in het algemeen zijn cyberprofessionals uit ander hout gesneden dan de doorsnee militair. Het overbruggen van cultuurverschillen is essentieel en zal van beide kanten moeten komen. ■

22 Een in dit verband lezenswaardig artikel is *Leadership of Cyber Warriors: Enduring Principles and New Directions*, van Gregory Conti and David Raymond in het *Small Wars Journal* van juli 2011. Overigens zullen cyberreservisten er waarschijnlijk in alle soorten en maten zijn, wat betekent dat enige differentiatie in benadering op zijn plaats is.