Cyber en militair vermogen

Het aantreden van de nieuwe minister en een nieuwe secretaris-generaal heeft de zachte krachten van Defensie vergroot. Met *@JeanineHennis* heeft Defensie de invloedrijkste twitterende minister in huis.[1] Zij scoort, met minder volgers (28.065) dan *@MinPres* (136.687) en *@LodewijkA* (34.842), vanwege betrouwbaarheid, engagement en omdat ze conversaties aangaat, hoger dan haar collega's. Let wel, de bron van dit bericht is een commercieel bedrijf dat webdiensten aanbiedt: het rangschikt onder meer 'invloed' en '*trending topics*' op sociale media: '*Is this real, or is it fantasy*'?[2]

Feit en fictie lopen overigens regelmatig door elkaar heen. *@Koningin_NL* is echt, maar hoogstwaarschijnlijk niet van ons staatshoofd, hoewel dat in theorie wel kan. Wie steekt zijn handen in het vuur voor zijn digitale relaties op *Facebook* en *LinkedIn*? Welke *social engineer* zit achter welke identiteiten, en vooral: met welk doel?

Met *@ErikAkerboom* krijgt Defensie een 'tweede' man die weliswaar slechts 1.068 volgers heeft, maar ook een uitgebreid netwerk bezit. Geldt ook voor een secretaris-generaal niet: kennis is macht, maar kennissen meer macht? Vanuit zijn vorige functies heeft de nieuwe SG relaties in binnenlandse veiligheid, crisisbeheersing, politie en inlichtingendiensten. Als Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) stond hij aan de wieg van de Nationale Cyber Security Strategie en het Nationale Cyber Security Centre. In zijn lezing op de Koninklijke Militaire Academie gaf Akerboom als NCTV zijn visie op de relatie tussen digitale veiligheid en defensie. Die bijdrage vindt u in dit nummer. Markant is het tweerichtingsverkeer: enerzijds de vertrouwde derde hoofdtaak, maar Akerboom wijst ook op 'de rol van de civiele autoriteiten in de ondersteuning van Defensie'. Wat dit precies omvat, zal moeten blijken. Vooralsnog kunnen we denken aan het daadwerkelijk invoeren van de 'cyberreservist', het poolen en uitwisselen van de schaarse ICT-kennis om bijvoorbeeld het digitale dreigingsbeeld voor meerdere sectoren te kunnen bepalen, het benutten van civiele relaties voor het genereren van draagvlak voor de krijgsmacht en haar operaties, of het daadwerkelijk toevoegen van tijdelijke civiele digitale capaciteiten aan militaire operaties en oefeningen.

Als NCTV stelde Akerboom dat 'Cyber Security [...] nog teveel een zaak van [ICT] techneuten [is]'.[3] Aannemende dat hij gelijk heeft en zijn observatie mede de krijgsmacht betreft, wat zijn dan de implicaties voor defensie? Allereerst dat digitale veiligheid meer is dan alleen ICT-hardware, software en protocollen of de mensen ('techneuten') die deze bedienen of ontwerpen. Digitale veiligheid gaat óók over menselijke interactie, over communicatie. Defensiepersoneel kan niet alleen het object van een digitale aanval zijn, maar ook een bron van een digitale infectie. De menselijke factor kan niet uit het oog verloren worden.
Ten tweede heeft Cyber Security evenzeer betrekking op de organisatie van het digitale domein en digitale veiligheid. Dit raakt niet alleen de organisatiestructuren, maar vooral de bedrijfsprocessen in vredestijd, commando-

1 Zie http://newsroom.edelmanpr.nl/jeanine-hennis-plasschaert-meest-invloedrijke-kabinetslid-op-twitter/. De volgers zijn berekend naar de stand van 02-12-2012.
2 Naar Queen.
3 Zie weekblad *Facilitair & Gebouwbeheer*, 15-11-2012, via: https://twitter.com/WeekbladFG.

voering tijdens inzet (in binnen of buitenland) en communicatie en samenwerking binnen en tussen organisaties die cyberspace veilig moeten houden en/of maken. Of dit nu defensieonderdelen zijn, civiele diensten, of publiek-private samenwerkingsverbanden maakt niet uit. Het gaat om een effectief (en efficiënt) antwoord op, en preventie van digitale dreigingen. Hierbij past de notie dat *security* meerdere betekenissen heeft: naast 'veiligheid' op microniveau ('safety') en macroniveau ('security'), betekent het ook 'zekerheid'. Verzekerd zijn, gegarandeerd zijn van communicatie(systemen) en van juiste, betrouwbare en tijdige informatie is van levensbelang. Dat vraagt niet alleen om ICT-oplossingen, maar ook om publieke en private *governance* van het digitale veiligheidsdomein.

Ten derde is cyber niet alleen een zaak van techneuten omdat iedereen zich in cyberspace beweegt en daarmee een speler, doelwit én potentiële strijder in het informatiedomein is. Wie mailt, post of googlet er niet? Met bedoelde of onbedoelde effecten. Een onbekende kan een potentiële 'strijdmacht' van duizenden volgers verzamelen. Voor populaire en invloedrijke figuren is dat nog eenvoudiger. Zelfs met een maagdelijk *tweet track record* verzamelde *@Pontifex* binnen één dag ruim 200.000 volgers, na vier dagen was dit aantal verdubbeld.[4] Technische kennis of functie is nauwelijks relevant. Internet telt 2,4 miljard gebruikers.[5] Ruim 1,2 miljard mensen 'zitten' op *Facebook*,[6] en volgens de *International Telecommunication Union* (ITU) bestonden er eind 2011 ruim 6 miljard mobiele connecties.

Ook voor onze krijgsmacht bieden deze digitale (mobiele) netwerken nieuwe mogelijkheden!

Cyber Security is dus een zaak ons allemaal. Het is daarom wijs om bij de ontwikkeling van nieuwe (of betere) cybercapaciteiten en de bescherming tegen dergelijke activiteiten van anderen niet alleen naar de technische ('harde') kant te kijken, maar ook naar de 'zachte' kant: naar mensen en processen en de kracht (en effecten) van informatie op mensen.

'Harde' en 'zachte' cybercapaciteiten bieden nieuwe mogelijkheden om ons militaire vermogen te versterken

Wie de Israëlische operatie tegen Gaza op *Twitter* volgde, zag hoe Hamas, de Palestijnse bevolking, de *Israel Defense Forces* (IDF), Israëlische burgers, NGO's (onder meer *Human Rights Watch*) en activisten het digitale domein als 'strijdperk' betraden. Geëngageerde activisten – of zijn het wellicht dekmantels voor anderen die zich als *Anonymous* voordoen – legden met 'harde' cyberacties overheidswebsites plat. Met beschuldigingen en stellingen hengelen de (strijdende) partijen om gehoor bij het publiek. Met informatie als wapen, vochten zij via cyber om de gunst van het publiek, om aandacht en erkenning, om draagvlak voor hun zaak.

Cyber is dus meer dan 'harde' techniek. Cyber heeft ook een 'zachte' component. Samen bieden 'harde' en 'zachte' cybercapaciteiten nieuwe mogelijkheden om ons militaire vermogen te versterken. ■

4 Het *Twitter*-account van Paus Benedictus XVI. Let wel: er zijn mogelijk ook volgers die geen 'vriend' van de Paus zijn.

5 http://www.internetworldstats.com/stats.htm, benaderd 5-12-2012.

6 http://www.statisticbrain.com/social-networking-statistics/, benaderd 5-12-2012.