# Cyber & marechaussee

De Defensie Cyber Strategie viert deze maand haar eerste verjaardag. In die strategie kondigde minister Hillen zijn cyber speerpunten aan op gebied van defensie, offensief optreden en inlichtingen verzamelen. Zo zal in 2014 het Defensie Cyber Commando worden opgericht. De trits defensief, offensief en inlichtingen dekt echter niet álle cyber inspanningen binnen defensie. Een vierde gebied vloeit namelijk voort uit de overkoepelende nationale Cyber Security Strategie: opsporing en vervolging van cyber criminaliteit en digitale strafbare feiten. Dit gebied is direct van toepassing op de Koninklijke Marechaussee als politiekorps.

Wie de media volgt, ziet dat cyber criminaliteit en (h)ac(k)tivisme alom is. Met martiale termen als 'aanvallen', 'aanvallers', 'cyber warfare' en 'cyberwapens' lijkt het overigens alsof er een militair conflict gaande is. Dat is misleidend! Het gros van de voorvallen betreft ordinaire – zij het soms spectaculaire – criminaliteit. Zoals de recente diefstal via digitaal gemanipuleerde creditcardrekeningen, waarbij in 24 uur met de hulp van handlangers, via 81.000 transacties 45 miljoen dollar werd buitgemaakt.[1] Hoe deze voorvallen ook geduid worden, ze tonen in ieder geval de kwetsbaarheid van onze maatschappij aan.
De *Distributed Denial of Services* (DDOS) 'aanvallen' op DigiD, ING en iDeal brachten die kwetsbaarheid merkbaar aan het licht. Klanten van iDeal – webwinkels en consumenten – klaagden meteen omdat zij het – gedurende een beperkte tijd – zonder deze digitale betalingsmogelijkheid moesten stellen. En fysieke winkels 'eisen' garanties voor de beschikbaarheid van pinbetalingen. Deze reacties staven dat onze samenleving – fysiek en mentaal – steeds afhankelijker wordt van het digitale domein. Dat moderne en snel groeiende samenlevingen digitaal kwetsbaar zijn, is een feit. Temeer indien overheden volledig digitaal willen werken. Ook Nederland heeft die ambitie: minister Plasterk wil in 2017 een honderd procent digitale overheid.[2] Digitaler dus, en onvermijdelijk ook kwetsbaarder, is een eenvoudige conclusie. Plasterk vertrouwt er mogelijk op dat Nederlands bekendste digitale misdaadbestrijders – het team *High Tech Crime* van de Landelijke Eenheid (voorheen KLPD) van de nationale politie[3] – zijn ambitie waar zal maken. Op de *National Cyber Security Conference 2013*, verwoordde Peter Zinn namens het team de ambitie om Nederland in 2017 het veiligste digitale land ter wereld maken.[4]

Volgens Zinn is dat nodig, want zoals in Nederland elke 37 seconden een fiets wordt gestolen, wordt in datzelfde interval een computer met *malware* geïnfecteerd. Voor die ambitie is overigens geld nodig! Tot nu toe had het team daaraan geen gebrek. Sinds zijn oprichting volgt het team de wet van Moore: iedere twee jaar een verdubbeling in computercapaciteit, in dit geval van het personeelsbestand.[5]
Deze digitale ontwikkelingen en ambities – op zowel militair als civiel gebied – beïnvloeden óók Nederlands militaire politiekorps, de Koninklijke Marechaussee. De vraag is wat dit voor 'het Wapen' zou moeten betekenen?

1 Zie de infographic: mashable.com/2013/05/25/45-million-stolen/.
2 Zie www.nu.nl/politiek/3483726/kabinet-wil-volledig-digitale-overheid-in-2017.html.
3 Zie twitter.com/PolitieTHTC.
4 Zie www.security.nl/artikel/44831/%27Nederland_veiligste_cyberland_ter_wereld_in_2017%27.html.
5 Zie criminaliteitswijzer.ning.com/profiles/blogs/klpd-verdubbelt-high-tech-crime-unit.

De Defensie Cyber Strategie noemt de KMar slechts eenmaal, namelijk in de context van het speerpunt 'Inlichtingen' als één van de opsporingsdiensten waarmee de MIVD zal samenwerken om de mogelijkheden tot toerekening (attributie) van cyber incidenten te verbeteren. Los van die korte vermelding wordt de marechaussee volledig geraakt door alle civiele maatregelen voor de aanpak van digitale criminaliteit. Het wetsvoorstel *Computercriminaliteit III* dat minister Opstelten op 2 mei 2013 naar de Tweede Kamer stuurde, is onverkort van toepassing op de KMar. De regering beoogt met dit voorstel de (verstoorde) balans tussen cyber criminaliteit en misdaadbestrijding te herstellen. Zo moet er een (her)nieuw(d) evenwicht tussen opsporingsbevoegdheden en technologie ontstaan.

Opsteltens wetsvoorstel, inclusief nieuwe digitale opsporingsbevoegdheden zoals het fameuze (terug)hacken, regardeert de marechaussee over de volle breedte van haar – civiele en militaire – taakstelling. Die taak is met de oprichting van de nationale politieorganisatie andermaal bevestigd en vastgelegd in artikel 4 van de Politiewet 2012. Maar ook zonder de nieuwe Politiewet, dus al ten tijde van de Defensie Cyber Strategie, deed de marechaussee reeds volop mee in het domein van cyber security. Een paar voorbeelden.
Eerst en vooral is de KMar belast met de 'politietaak ten behoeve van Nederlandse [...] strijdkrachten'. Met andere woorden: cyber criminaliteit door militairen gepleegd, wordt door de KMar opgespoord, een halt toegeroepen en vervolgd. Daarnaast is de KMar belast met de opsporing van cyber crime die tegen de krijgsmacht is gericht, bijvoorbeeld als het salarissysteem van Defensie door criminelen gehackt is. Ten slotte is de KMar verantwoor-delijk voor de politietaak op luchthavens zoals Schiphol. Diefstal via digitale logistieke systemen op Schiphol en het lamleggen van het vluchtleidingsysteem vallen binnen haar competentie. Ook 'handhaving van de openbare orde' op Schiphol biedt via bijvoorbeeld sociale media nieuwe kansen en bedreigingen.
Een belangrijke toevoeging met de komst van militaire digitale capaciteiten is de rol die de marechaussee speelt bij de beoordeling de rechtmatigheid van functionele activiteiten van de krijgsmacht. In dit geval dus cyber operaties. Net als bij functioneel fysiek geweld zal de KMar legitieme cyber activiteiten van de krijgsmacht moeten kunnen beoordelen. Dat geldt voor zowel defensieve acties in Nederland als offensieve cyber activiteiten tijdens operaties. En eventueel ook voor inlichtingenoperaties van CDS en MIVD.

Maar bovenal zal de KMar 'geraakt' worden door de ambities van de regering en de misdaadbestrijders: digitaler én veiliger. Deze ambities, nieuwe opsporingsbevoegdheden, nieuwe taken voor de krijgsmacht en de flux in cyber (h)ac(k)tivisme, criminaliteit en spionage, kunnen niet zonder gevolgen blijven. Hoe zal de marechaussee hier qua opleiding, organisatie, uitrusting, bemensing en optreden op anticiperen? Gaat ze zelfstandig aan de slag? Zal ze samenwerking zoeken met zusterdiensten en krijgsmachtdelen? De in 2011 uitgebrachte *Ontwikkelagenda Koninklijke Marechaussee* gaat hier vooralsnog niet op in. Hier ligt een mooie opdracht voor het jongste krijgsmachtdeel dat in 2014 haar tweehonderdjarige bestaan zal vieren: zonder vrees en zonder blaam, ook in het digitale tijdperk! ■