Column

Nederland heeft op het gebied van *cybersecurity* een goede internationale reputatie. Hackers van de AIVD/MIVD behoren tot de wereldtop, de hightech *crime unit* van de politie kraakt de ene criminele app na de andere en het Nationaal Cyber Security Centrum (NCSC) was lange tijd een voorbeeld voor veel landen.

Toch gaat het *cyber*landschap gebukt onder een enorme versnippering. Het Defensie Cyber Commando (DCC) is verantwoordelijk voor offensieve *cyber*, de AIVD/MIVD voor inlichtingen (BZK en Defensie), het NCSC (onder J&V) coördineert *cybersecurity* voor de vitale sector, en het Digital Trust Center voor het midden- en kleinbedrijf (EZK). Dan hebben we het nog niet over andere instanties belast met *cybersecurity & defence*. De samenwerking tussen al deze organisaties wordt bemoeilijkt door onduidelijke mandaten, doublures dan wel hiaten in capaciteiten en de gevoeligheid van de materie. Vergelijk dit met het VK, waar één loket (het NCSC) alle instanties bedient. Het valt direct onder de Britse SIGINT/*Cyber* inlichtingendienst die verantwoordelijk is voor zowel offensieve *cyber* als inlichtingen, en fungeert als *het cyber* expertisecentrum van de overheid. Het lijkt wel de Engels-Nederlandse zeeoorlogen van de 17e eeuw, waarbij de Staatse vloot maar liefst vijf admiraliteiten had – die eveneens met moeite samenwerkten. Ze moesten het opnemen tegen één gecentraliseerde Engelse organisatie. Het duurde nog ruim honderd jaar voordat Nederland één admiraliteit kreeg. Toen was de goede reputatie van de vloot al lang vergane glorie.

‘Is het nog opportuun om het DCC separaat te houden of ligt integratie in de MIVD voor de hand?’

Het DCC werd in 2014 opgericht met een missie die vaak aan de hand van een voorbeeld werd uitgelegd. In geval van een conflict zou het DCC bijvoorbeeld de vijandige luchtverdedigingssystemen hacken, zodat men het niet kinetisch hoefde uit te schakelen. Maar in de praktijk blijkt offensieve *cyber* gebouwd op inlichtingenoperaties. Hacken is de kunst om ongezien netwerken en systemen binnen te dringen en onopgemerkt te blijven. Als dit eenmaal lukt – en dat kan maanden duren – dan is de mogelijkheid tot sabotage automatisch inbegrepen. Hacken in vredestijd mag DCC echter niet. Alleen de MIVD mag dit op grond van de Wet op de Inlichtingen- en Veiligheidsdiensten. Ook beschikt het DCC niet over menselijke bronnen en inlichtingenpartners. Toen duidelijk werd dat DCC geen offensieve *cyber* kon uitvoeren, werd het concept van *Cyber Mission Teams* ontworpen. Samen met personeel van de MIVD zou DCC militaire missies in het buitenland ondersteunen. Na een valse start wordt deze samenwerking op betere leest geschoeid, maar intussen is de strategisch context veranderd. Het aantal missies in het buitenland neemt af en het belang van collectieve zelfverdediging neemt toe. Is het nog opportuun om het DCC separaat te houden of ligt integratie in de MIVD voor de hand?

In andere landen komen *Cyber Commands* eveneens moeilijk van de grond. In de VS heeft USCYBERCOM wel wapenfeiten op zijn naam staan, maar dit was mede mogelijk doordat het ingebed was in de National Security Agency. Onlangs werd besloten om deze (semi-)integratie te handhaven. Op het gebied van *cyber defense* worstelen landen ook met bestuursmodellen. Er is natuurlijk geen ideaal model; veel is afhankelijk van nationale context en cultuur. Maar het is wel opmerkelijk dat meerdere landen zowel de offensieve als defensieve *cyber*taak beleggen in hun inlichtingengemeenschap (zoals het VK, Canada, Australië en Denemarken). Zo wordt expertise gebundeld en kennisuitwisseling tussen aanvallers en verdedigers bevorderd.

Kortom, de nieuwe regering in Den Haag heeft straks een uitgelezen kans om het institutionele *cyber*landschap – zowel binnen als buiten Defensie – goed tegen het licht te houden. Als de versnipperde aanpak niet wordt doorbroken, dan kunnen de nieuwste dreigingen niet worden gekeerd en blijven operationele kansen liggen. Aangezien het *cyber*domein zich iets sneller ontwikkelt dan het 17eeeuwse maritieme domein, is enige besluitvaardigheid geboden.

Sergei Boeke is politiek adviseur bij het NAVO-hoofdkwartier JSEC in Duitsland. Hij schrijft op persoonlijke titel.