Cyberveiligheid: de NAVO en ons land

Didier Audenaert

Kolonel stafbrevethouder Didier Audenaert was van 2006 tot 2009 de Belgische *Faculty Adviser* aan het NAVO-Defensiecollege en is sinds 2009 de Defensieraadgever van de permanente vertegenwoordiger van België bij de NAVO (BELOTAN).

Il n'est nullement notre intention de décrire en un seul article la problématique complexe de la cyberdéfense (CD). L'OTAN forme une communauté de valeurs unique en son genre, attachée aux principes de la liberté individuelle, de la démocratie, des droits de l'homme et de l'état de droit. Nous connaissons tous la mission de défense collective de l'Alliance, ainsi que son principe de prise de décision par consensus et l'importance des consultations entre les alliés. Cet article se focalise surtout sur son rôle dans le domaine de la cyberdéfense. Nous tirons de l'approche collective les mesures qui s'imposent au niveau national.

Welke cyberbedreiging?

Open bronnen bevestigen dat vooral de Russische Federatie en de Chinese Volksrepubliek de grootste cyberbedreiging vormen voor de westerse landen, terwijl Iran en ook Noord-Korea in toenemende mate over offensieve cybercapaciteiten beschikken. Aartsmoeilijk blijft ook in de toekomst de attributie van een cyberaanval (m.a.w. de vragen beantwoorden "welke Staat of wie exact valt mij aan, van waar komt de aanval?"): toen in juni 2013 in Zuid-Korea websites van het presidentiële kabinet en van overheidsorganisaties verlamd werden, kon Seoel enkel maar Pyongyang verdenken. Bronnen bevestigen dat de computersystemen van de NAVO dagelijks geconfronteerd worden met acht tot tien gesofistikeerde aanvallen. In augustus werd ook bij onze Defensie een complex computervirus ontdekt, waarvoor Amerikaanse steun ingeroepen werd bij de analyse. In september kwamen onder andere Belgacom, FOD Buitenlandse

Zaken en het Kabinet Premier prominent in het cyberdaglicht te staan. Cyberbedreiging is een dagelijkse realiteit geworden.

Pakketten circuleren vrij en stellen relatief eenvoudig malware ter beschikking van individuen of organisaties met kwade bedoelingen. Deze pakketten vormen op zich niet altijd een grote bedreiging, maar vergroten in aanzienlijke mate het actieterrein en maken het daardoor voor een creatieve cyberaanvaller gemakkelijker om zich te verschuilen. Op dit vlak zien we cybercriminelen, hackers en (h)activisten aan het werk.

Cyberterrorisme heeft zich tot nu toe niet gemanifesteerd, maar het zou al te naïef zijn als we deze vorm van bedreiging voor de toekomst uitsluiten. Terroristische organisaties kunnen op termijn inderdaad kritische infrastructuur[1] viseren om terreur te bewerkstelligen. Net zoals de terroristische actie van 9/11 ongezien was, zo leeft de vrees dat terroristen de cyberruimte kunnen misbruiken om terreur te zaaien. Cybersabotage is alvast niet nieuw meer: de Stuxnet-worm berokkende schade aan de kritische infrastructuur van het Iraanse nucleaire programma. Op zijn beurt sloeg Iran in 2012 terug met een aanval op Aramco, de Saudische oliemaatschappij. Dichter bij ons: in februari 2013 gebruikte MiniDuke een "achterdeurtje" om onder andere in ons land overheidsinstellingen en instituten aan te vallen en in april van dit jaar moest ING Nederland online bankieren of winkelen zelfs een volle dag stilleggen wegens cyberaanvallen op het betalingsverkeer.

NAVO en cyberdefensie (CD): een nog jonge relatie met pit

In 1999, tijdens operatie *Allied Force*, werd de NAVO voor het eerst geconfronteerd met massale cyberaanvallen door pro-Servische hackers, die gedurende dagen erin slaagden om de verslagen over de oorlog in Kosovo op de website van de NAVO onbereikbaar te maken. Sindsdien is gestaag een lange weg afgelegd. Met hun goedkeuring van het Strategisch Concept (Lissabon, 2010) van de NAVO breiden de staatshoofden en regeringsleiders van de 28 NAVO-lidstaten het engagement van artikel 5 van het Verdrag van Washington uit naar de cyberruimte: de Alliantie zal elke vorm van bedreiging ontraden en zich verdedigen tegen de nieuwe veiligheidsbedreigingen als deze de fundamentele veiligheid van de individuele bondgenoten[2] of van de Alliantie zouden aantasten. Een cyberaanval kan dus in aanmerking komen voor de toepassing van artikel 5, maar een politieke afweging door de Noord-Atlantische Raad (NAR) zal steeds uitsluitsel moeten brengen: er is (terecht) geen automatisme ingesteld. De

staatshoofden en regeringsleiders erkennen dat cyberaanvallen enorme schade kunnen berokkenen en een drempel overschrijden waarbij ze de nationale en Euro-Atlantische welvaart, veiligheid en stabiliteit in gevaar brengen. Belangrijk is dat in hun Strategisch Concept de staatshoofden en regeringsleiders middelen willen ontwikkelen om cyberaanvallen te voorkomen en te detecteren, maar ook om zich ervan te herstellen. Ze zien hiertoe een rol voor het *NATO Defence Planning Process* (NDPP) dat de nationale CD-capaciteiten moet helpen verbeteren en coördineren.

NAVO verkiest vooreerst preventie boven reactie en wil daarom cyberincidenten kunnen weerstaan en de continuïteit van haar eigen communicatie- en informatiediensten verzekerd zien voor het volledige spectrum van de opdrachten van de Alliantie. De vereisten hiertoe worden vastgelegd in een serie richtlijnen, waaraan zowel NAVO-entiteiten als individuele lidstaten moeten voldoen als ze zich willen verbinden met de NAVO. Verder wil de NAVO elke vorm van duplicatie vermijden met lopende inspanningen van andere internationale organisaties of op het nationale niveau. De NAVO wil geenszins de concurrentie aangaan met bijvoorbeeld de Europese Unie, die actief samenwerkingsverbanden creëert, technische normen uitwerkt, instrumenten en organisatie verstrekt en, sinds 2006, vooral ook middelen aanreikt via de Commissie. Voorts beloven de bondgenoten dat ze informatie zullen uitwisselen in een geest van vertrouwen, wat als kritisch beschouwd wordt in het kader van CD-bewustzijn en van tijdige waarschuwing bij cyberincidenten. Topprioriteit voor NAVO is de gecentraliseerde cyberbescherming van de eigen netwerken (het hoofdkwartier in Evere, de geïntegreerde militaire structuur, operaties, agentschappen): de *NATO Computer Incident Response Capability* (NCIRC) staat in voor de gecentraliseerde cyberbescherming van de netwerken van de NAVO. Dit NCIRC werkt in Mons nauw samen met de diensten van SHAPE. De bondgenoten richten ook een *Cyber Defence Management Board* (CDMB) op, die autonoom kan handelen bij crisissen en die de NAVO-Raad informeert van zijn acties. Deze CDMB kan zich beroepen op de gemeenschap van *Civil Emergency Planning* met haar vooraf geselecteerde en getrainde nationale experts.

In het NDPP werden cyberdoelstellingen geformuleerd en opgenomen in de individuele nationale dossiers van de lidstaten, die zich bij monde van hun Defensieministers in juni geëngageerd hebben om die doelstellingen te realiseren tegen ten laatste 2019. Deze doelstellingen gaan onder andere over de instelling en de uitvoering van een nationaal cyberbeleid en cyberprocedures, en over een nationale *Computer Incident Response Capability*. Het NDPP verzekert de coherentie van wat de NAVO als organisatie en van wat de individuele lidstaten

doen. Het NDPP kan in een later stadium een nuttig instrument worden om de verschillende nationale capaciteiten te standaardiseren: zo kan op termijn gedacht worden aan de definiëring van wat een "cyber unit" kan zijn voor de verdediging tegen of het antwoord op een cyberaanval.

Waar wringt het schoentje bij de NAVO?

Ogenschijnlijk lijkt alles rozengeur en maneschijn binnen de NAVO. Reeds tijdens de besprekingen voorafgaandelijk aan de Top van Lissabon verschilden de bondgenoten grondig van mening over onder meer de benadering van cyber, en deze uiteenlopende visies werden achteraf nog meer geaccentueerd. De grootste breuklijnen situeren zich rond de relatie van de NAVO met partners, en over de vraag hoe de NAVO moet omgaan met een aanval op een lidstaat.

Eén bondgenoot blijft het politiek moeilijk hebben als de NAVO samenwerkt met derden, zogenaamd omdat dit indirect een invloed kan hebben op de capaciteit van de Alliantie om zelfstandig haar collectieve verdediging te kunnen uitvoeren. De gevoeligheden situeren zich echter vooral rond de Europese Unie en haar lidstaten. Deze gevoeligheden worden in de praktijk doorgaans handig diplomatiek omzeild door effectieve informele besprekingen tussen de staven van NAVO en van EU. De partnerlanden worden individueel geselecteerd, maar al te vaak vormt deze coöperatie nog steeds een spelbreker. Een andere gevoelige samenwerkingsvorm is deze met de industrie. NAVO erkent het belang van een dergelijk partnerschap voor uitwisseling van informatie, oefeningen, training van experts, enz. Alleen moeten de bondgenoten het over de parameters voor een dergelijke relatie met de industrie eens kunnen worden en hier verschillen doorgaans de voornaamste Europese bondgenoten om eng nationale economische redenen fundamenteel van visie.

Alle bondgenoten zijn het erover eens dat de hoofdverantwoordelijkheid van de NAVO de bescherming van de eigen netwerken moet zijn. De bescherming van de nationale kritische infrastructuur blijft dan weer strikt een nationale verantwoordelijkheid, wat tot gevolg heeft dat de individuele Naties voor hun nationale cyberveiligheid moeten investeren in eigen capaciteiten. Echt grondig verschillen de bondgenoten van mening over de steun die de Alliantie zou moeten geven aan bondgenoten die blootgesteld zijn aan een cyberaanval (*assistance to Allies*). Als onderdeel van NCIRC werden twee *Rapid Reaction Teams* opgericht die de bescherming van de NAVO-netwerken moeten verzekeren. Het is duidelijk dat deze twee teams slechts een beperkte (initiële?) capaciteit

betekenen en dus geen brandweerman kunnen zijn voor de hele Alliantie en haar 28 bondgenoten. Vooral Frankrijk en het Verenigd Koninkrijk voelen zich gesterkt in hun overtuiging dat op niveau van de NAVO geen bijkomende capaciteit nodig is, terwijl de meerderheid van de (kleinere) lidstaten wel steun en solidariteit verwachten van de NAVO en van de andere bondgenoten. Parijs en Londen beschikken zelf over structuren, organisatie, personeel, defensieve (en al dan niet bevestigde offensieve) middelen, knowhow, enz. om hun nationale cyberveiligheid te garanderen. Ze willen deze gevoelige investeringen in de eerste plaats voor hun eigen cyberveiligheid aanwenden, terwijl de kleinere Europese landen voor een gigantische uitdaging staan en doorgaans hiermee nog moeten starten. Parijs en Londen vinden dat andere (kleinere) bondgenoten individueel naar hen moeten komen voor bilaterale bijstand, terwijl bijvoorbeeld ons land doorgaans een multilaterale benadering verkiest. Duidelijk is dat de teneur binnen NAVO is dat elke lidstaat eerst grondig orde op zaken moet stellen in de nationale organisatie.

Het debat binnen NAVO draait dus rond de toepassingswijze van solidariteit en rond de keuze van nationale versus collectieve middelen.

Modaliteiten voor CD-bijstand, consultaties en coördinaties tussen de NAVO en de bondgenoten worden bepaald door *Memoranda of Understanding* (MoU), die tussen de CDMB en de nationale autoriteiten afgesloten worden. Ook onze Defensie heeft sinds 2011 zo'n MoU met de NAVO, waarin de NAVO belooft ons te zullen bijspringen in geval van cybernood. Uit de technische realiteit en uit de lopende harde discussies blijkt dat deze bijstand vandaag niet gegarandeerd is.

In de traditionele NAVO-oefeningen voor crisismanagement wordt ook het cyberdomein opgenomen in de scenario's. Dit heeft reeds tot nuttige lessen geleid voor de interne procedures. Zo zal in de crisismanagementoefening van 2014 een cyberincident plaatsvinden op een Belgisch stuk van de NAVO-pijpleiding. Met dergelijke oefeningen kunnen de nationale procedures getest worden.

Een omgeving van *trust and security* is nodig als bondgenoten en NAVO informatie over cyber willen uitwisselen. Op technisch vlak is er wel sprake van goede samenwerking of van enige transparantie, maar op het hogere politieke vlak bestaat ongetwijfeld nog veel ruimte voor verbetering.

Het is ook nuttig te melden dat de technische aspecten van cyber binnen NAVO (o.a. NCIRC, de *Rapid Reaction Teams*,…) uitgevoerd worden door het nieuwe

NATO Communications & Information Agency (NCI Agency) met hoofdzetel in Evere. Sinds zijn start in 2012 en voor de komende vijf jaar is dit Agentschap in volle hervorming; we kunnen ons niet volledig van de indruk ontdoen dat NCIRC niet de hoogste prioriteit geniet die het vereist. De invoering van NCIRC blijft gedurig aanzienlijke vertraging oplopen, vooral omwille van de technische complexiteit, maar moet tegen deze winter volledig operationeel geraken.

Tot slot melden we nog dat Estland zich als klein land consequent sterk profileert op het gebied van cyberveiligheid. Estland is in elk forum de actieve woordvoerder voor cyber: de pijnlijke ervaringen van 2007 liggen aan de basis van deze proactieve houding. In Tallinn bevindt zich het *Cooperative Cyber Defence Centre of Excellence*.

Hoe kan CD nationaal beter georganiseerd worden (vanuit een NAVO-perspectief)?

We beperken ons tot enkele kenmerken die nuttig kunnen zijn voor onze nationale organisatie en refereren vooral aan wat onze directe buren opbouwen.

We moeten volledigheidshalve melden dat in 2005 het Ministerieel Comité voor Inlichtingen en Veiligheid een overlegplatform *Belgian Network Information Security* (BelNIS) opgericht heeft, dat regelmatig de belangrijkste federale spelers rond de tafel brengt, en dat de *Federal Computer Crime Unit* van de politie het nationale en internationale invalspunt voor cybercriminaliteit is met een 24 urenpermanentie. Deze nationale structuur werkt vandaag over het algemeen suboptimaal.

In december 2012 keurde de ministerraad de nationale cyberstrategie goed, waarin onze regering de cyberdreiging erkent. De regering heeft echter spijtig genoeg geen middelen toegekend voor de uitvoering. Zo blijven waardevolle ideeën in de koelkast, zoals de oprichting van een Centrum voor Cyber Security in België (CCSB) onder het gezag van de eerste minister. Het CCSB, dat slechts een beperkt jaarlijks budget van 3 miljoen euro nodig heeft, zou in de eerste plaats zichtbaarheid kunnen geven aan ons cyberbeleid en het centrale coördinatieorgaan worden tussen verschillende overheidsdiensten die samen instaan voor de cyberveiligheid in België.

De meest gevorderde landen hebben een nationale cyberautoriteit aangeduid, die als “Mr. Cyber” zichtbaarheid geeft en een aanspreekpunt is, maar die ook

de verantwoordelijkheid draagt voor de nationale cyberveiligheid. De VS zijn duidelijk het meest gevorderd, zoals recent gebleken is. Frankrijk heeft een dienst voor de veiligheid van informatiesystemen, die rechtstreeks van de premier afhangt. Duitsland en het Verenigd Koninkrijk hebben voor hun cybercentralisatie aanzienlijke middelen geïnvesteerd: budget, hardware, software en personeel. De nationale cyberautoriteit bepaalt het nationale beleid en de nationale kritische afhankelijkheden: we denken hierbij aan regelgeving voor de administraties en voor de privésector, centralisatie van de veiligheid van de kritische netwerken, vorming, enz. De erkenning van de behoefte aan een nationale cyberautoriteit is zeker niet nieuw[3] meer, maar de concrete invulling van de positie laat al te lang op zich wachten. In ons land moet het nationale CERT.be de centrale coördinator zijn bij het behandelen van belangrijke nationale cyberaanvallen.

Bij onze buurlanden blijkt vandaag veeleer een gezonde concurrentie te bestaan tussen veiligheidsdiensten, die actief zijn in de cyberruimte, om middelen naar zich te trekken en hun verantwoordelijkheidsdomein uit te breiden. We stellen regelmatig vast dat in België een andere tendens zich aftekent: diensten willen al te dikwijls verantwoordelijkheid afschuiven omdat de noodzakelijke middelen niet toegekend worden voor de uitvoering van de taak.

Het Nederlandse ministerie van Veiligheid en Justitie heeft in 2011 een Nationale Cyber Security Strategie uitgebracht. Nederland heeft sinds 2012 een operationeel Nationaal Cyber Security Centrum. De Nederlandse Defensie werkt tegen 2016 aan een Defensie Cyber Expertise Centrum, dat over 200 medewerkers zal beschikken. Den Haag trekt 50 miljoen euro uit voor de oprichting van dit Centrum, dat coherent past in de Defensie Cyber Strategie, die richting geeft "aan de integrale aanpak voor de ontwikkeling van het militaire vermogen in het digitale domein. Zij is daardoor van wezenlijk belang voor de toekomstige effectiviteit en relevantie van onze krijgsmacht". Een derde actiedomein van onze noorderburen is het bevorderen van de samenwerking tussen cyberinlichtingendiensten, die hierdoor met hun 400 personeelsleden sneller en effectiever moeten kunnen optreden.

In een aantal landen wordt werk gemaakt van een moreel bindende gedragscode voor alle nationale organisaties. De meeste landen beschikken over een wettelijk kader voor de organisatie van hun cyberveiligheid. In Frankrijk wordt een wettelijk kader uitgewerkt met verplichtingen die gelden voor zowel de openbare als voor de privésector, zo worden organismen verplicht om cyberaanvallen te melden en om zich aan cyberaudits te onderwerpen.

De meest geavanceerde landen kennen een intense en eerder transparante samenwerking tussen de "IT-industrie", de nationale administratieve overheden en het bedrijfsleven. Een zorgvuldige afweging tussen cyberveiligheid en andere factoren, zoals de bescherming van de persoonlijke levenssfeer, dient ongetwijfeld gemaakt te worden. We moeten toegeven dat de vermelde "IT-industrie" in deze landen vaak een grondige nationale verankering heeft.

Een puur nationale benadering is in de globale cyberruimte noch efficiënt, noch effectief, zodat een land als het onze zijn cyberveiligheid best in een multilaterale context vastlegt. Zowel de EU als de NAVO maken op een aanvullende wijze werk van normen, criteria, enz. Vooral hier voelen we de behoefte aan duidelijke nationale sturing, vandaag manifesteert zich veeleer onduidelijkheid over onze nationale vertegenwoordiging binnen deze internationale fora.

Bij de buurlanden vervaagt de artificiële grens tussen cyberdefensieve en cyberoffensieve middelen. Louter over cyberdefensieve middelen beschikken biedt duidelijk een ontoereikende bescherming. De vraag waar de grens ligt, is inderdaad zeer relevant: ons land en zijn Defensie moeten hierop een passend nationaal antwoord formuleren.

EU en NAVO erkennen het belang van cyberoefeningen. Langs NAVO-zijde worden tijdens crisismanagementoefeningen ook nationale reacties getest op cyberincidenten op kritische infrastructuur (bv. energievoorziening, havens,…) om de gevolgen hiervan te beperken. De meeste landen zijn bereid om hieraan mee te doen en maken gretig gebruik van de NAVO-oefeningen om hun nationale procedures en organisatie te optimaliseren. België neemt dus in 2014 voor het eerst deel aan een NAVO-oefening met een cyberincidentscenario. Het is volgens ons nog onvoldoende duidelijk hoe ons land zijn crisiscentrum effectief zal inzetten om aan dergelijke EU- en NAVO-cyberoefeningen deel te nemen. Dit is deels te wijten aan het relatief jonge en virtuele karakter van het cyberdomein, terwijl de andere domeinen veel traditioneler, beter gekend en dus reëler zijn.

In de verschillende landen evolueert de rol van Defensie in CD, maar niet overal met dezelfde intensiteit. In de vermelde landen neemt Defensie gestaag een belangrijkere rol binnen de nationale organisatie. De Franse algemene bewapeningsdirectie telt vandaag voor CD nabij Rennes 1.200 mensen en voert tegen 2015 dit aantal op tot 1.400.

Conclusie

De focus van de NAVO ligt dus op de eigen cyberorganisatie. Vanuit een strikt NAVO-perspectief kunnen we daarom enkel de uitwerking van een effectieve nationale cyberveiligheid sterk bepleiten. Het is inderdaad op het niveau van de naties dat aan cyberveiligheid zal gewerkt moeten worden. Onder de NAVO-lidstaten zien we zich een (nieuwe) tweedeling aftekenen: een groep landen (de *haves*) die wel kunnen instaan voor hun effectieve nationale cyberveiligheid met de passende nationale middelen en een andere groep met beperkt of onvoldoend vermogen (de *have nots*). Gezien onze nationale afhankelijkheid van informatie en de kwetsbaarheid van onder meer onze economie moet ons land tot de eerste groep behoren. Slechts zo kunnen we een betrouwbare partner zijn die in aanmerking komt voor bilaterale of multilaterale samenwerking, die op zijn beurt onze nationale inspanningen kan versterken. België mag niet achterblijven ten opzichte van zijn buurlanden en moet een even sterke schakel in de ketting vormen. Ons land draagt bijkomend een verantwoordelijkheid door de aanwezigheid van de grootste hoofdkwartieren van EU en NAVO op ons grondgebied.

Een functionele cybercultuur wordt niet van vandaag op morgen in het leven geroepen. Zoiets vergt tijd voor ruime informatie, bewustwording, organisatie en vooral voor een breed gerichte vorming.

❐

Trefwoorden: Cyber Defence, NAVO, Organisatie

---

[1] In 2008 werd beslist dat voor ons land “kritische informatie-infrastructuur” bestaat uit telecommunicatie, energievoorziening, de financiële wereld, lucht- en treinverkeer. Dit werd bevestigd in de wet van 1 juli 2011. Onder de definitie valt vandaag dus niet vitale infrastructuur zoals onze economie, de basisvoorziening van water of voedsel,…

[2] Met de term “bondgenoten” verwijzen we in dit artikel naar de 28 lidstaten van de NAVO.

[3] Zie artikel *Cyber Defence* door luitenant-kolonel Miguel De Bruycker in het Belgisch Militair Tijdschrift Nr. 1, jaargang 2010.

Dit artikel werd in september 2013 afgesloten