Naar een Belgisch Cyber Command?

Filip GILLET
Luitenant-kolonel stafbrevethouder ir. Filip GILLET was van 2013 tot 2015 ondersectiechef Corporate CIS in MRC&I. Sinds oktober 2015 is hij chef van de directie Cyber bij ACOS IS.

Ces dernières années, nous constatons une augmentation systématique du nombre de cyberattaques et une communication plus ferme concernant les capacités en matière de cyberoffensives. Nos adversaires utilisent des maliciels (en anglais : malware) de plus en plus complexes et leurs techniques, tactiques et procédures se professionnalisent davantage. Nos systèmes sont perturbés au travers du cyberespace, sapant la confiance en l'information susceptible d'appuyer nos opérations. L'OTAN est à la recherche d'une solution et tente de s'armer face à cette évolution. Lors du dernier sommet de Varsovie, tous les chefs d'État et de gouvernement de l'Alliance ont unanimement soutenu un Cyber Defence Pledge (« Engagement en faveur de la cyberdéfense ») pour renforcer la résilience nationale. Les États membres garantissent ainsi que l'Alliance sera capable d'évoluer malgré la cybermenace et qu'ils planifieront eux-mêmes les investissements nécessaires pour se défendre dans le cyberespace. Pendant ce même sommet, ils ont aussi déclaré formellement le cyberespace comme un nouveau domaine opérationnel.

De ontwikkelingen op het gebied van het *Internet of Things* zullen individuen, systemen en dingen interconnecteren in een mate die tot voor enkele jaren geleden ondenkbaar was. Dagelijks worden vijf miljoen nieuwe systemen geconnecteerd met het Internet. Gartner[1] voorspelt dat dit in 2020 in totaal meer dan 20 miljard systemen zullen zijn. Het aantal vectoren dat vanaf dan aangewend kan worden om cyberacties te initiëren of om malware in onze netwerken en systemen te introduceren zal exponentieel toenemen. De technische uitdagingen om deze steeds

1 Gartner is een onderzoeks- en adviesbureau in de informatietechnologiesector.

groter wordende interconnectiviteit te beheersen en te beschermen zullen steeds ingewikkelder worden en dus nog meer expertise vereisen.
Die expertise is schaars, iedereen is vandaag op zoek naar dezelfde profielen. In België neemt de klassieke concurrentie op de arbeidsmarkt met de industrie nog toe door het grote aantal officiële instellingen dat België aantrekt met Brussel als hoofdstad van Europa. De opleiding en vorming van een voldoende grote pool van hooggekwalificeerde en competente cyberexperten moet een nationale prioriteit worden, met aansturing door de overheid en in nauwe samenwerking met de academische wereld en de industrie.
Vandaag is al heel wat malware verkrijgbaar op verborgen markplaatsen in het deep web en dark web. Gehackte exploits van inlichtingendiensten worden hier verhandeld door cybercriminelen. Minder technisch onderlegde individuen en organisaties komen hier in contact met groeperingen met een grotere technische kennis en kunnen zo toegang krijgen tot tools en technologieën om complexere cyberaanvallen uit te voeren. Momenteel is de dreiging van cyberterrorisme als eerder laag in te schatten, de vrije markt in cyberspace dreigt op middellange termijn hierin verandering te brengen.
Informatieoorlogen tussen naties, al dan niet gebruik makend van door naties gesponsorde groeperingen, worden meer en meer openlijk gevoerd. De retoriek in cyberspace neemt toe, wat leidt tot meer spanningen op diplomatiek vlak. De technologische ontwikkelingen in cyberspace verschaffen de naties een nieuwe reeks middelen om actief hun buitenlandse politiek te kunnen voeren zonder te moeten terugvallen op conventionele militaire acties. Cyberacties lijken op het eerste zicht makkelijker aanvaardbaar en proportioneler.

FUNDAMENTEN VAN MILITAIRE OPERATIES IN CYBERSPACE

Er is steeds sprake van een paradox in cyberspace. Geen enkele moderne krijgsmacht kan nog functioneren zonder genetwerkte wapensystemen en geïntegreerde logistiek en commando- en controleketens. Tegelijkertijd zorgt de makkelijke toegang tot de vele gesofisticeerde cybertools ervoor dat onze tegenstanders over de middelen beschikken om de integriteit en de beschikbaarheid van deze kritieke militaire systemen rechtstreeks of onrechtstreeks te compromitteren. De bescherming van militaire informatie en het garanderen van de betrouwbaarheid en de beschikbaarheid van netwerk- en wapensystemen vormen dan ook de hoofdopdracht van een militaire cybercapaciteit.
Een waterdichte cyberveiligheid bestaat niet. Het is meestal gewoon een combinatie van tijd en geld vooraleer een volhardende aanvaller een systeem kan binnendringen of een systeem kan ontregelen. Een

correcte cyberveiligheidsstrategie houdt, naast de onontbeerlijke verdedigingsmechanismen, dan ook rekening hiermee door de operationele impact van een intrusie zo klein mogelijk te houden en door erop voorbereid te zijn om militaire operaties te kunnen voeren in *degraded cyberspace conditions*.
De cyberdreiging komt mede tot stand door de diversiteit aan actoren. Het is van het grootste belang dat we de capaciteiten van alle actoren kunnen opvolgen en de impact van de dreiging kunnen inschatten op ons militair personeel, onze militaire systemen en onze operaties. Rusland, China, Noord-Korea en Iran zijn de naties waarvan de grootste strategische dreiging uitgaat. Vooral Rusland vertoont sinds kort een zeer hoge expertise en een veel agressievere houding. Een groot deel van de acties van deze landen vindt plaats via proxies[2], ze zijn het werk van groeperingen die door de naties gesponsord worden, wat attributie zeer moeilijk maakt.
Welke zijn nu de risico's? Bij gebrek aan een algemeen aanvaard lexicon kunnen we de offensieve capaciteiten in het cyberdomein voorlopig opdelen in *cyber exploitation operations* en *cyber offensive operations*. Tijdens *cyber exploitation operations* tracht de tegenstander onze systemen te infiltreren om *reconnaissance of surveillance* uit te voeren, spionageactiviteiten op te zetten, data te wijzigen, te compromitteren of te exfiltreren. *Cyber offensive operations* mikken eerder op sabotageacties, waarbij men de toegang tot onze systemen probeert te ontregelen of zelfs volledig te ontzeggen, of waarbij men de systemen tijdelijk of permanent onbruikbaar maakt.

HET ULTIEME WAPEN

Het cyberwapen zou wel eens het ultieme wapen bij uitstek kunnen worden. Het onderzoek en de ontwikkeling van offensieve cyberwapens ontsnappen volledig aan de nieuwsgierige blikken van de inlichtingendiensten. Grote, gemakkelijk op te sporen infrastructuren en installaties zijn niet nodig voor de ontwikkeling van deze capaciteiten.
Het cyberwapen is een asymmetrisch wapen. Alle klassieke grootmachten investeren in hoogtechnologische en continu geïnterconnecteerde wapensystemen. Een veel minder kapitaalkrachtige natie en zelfs niet-statelijke actoren kunnen vanuit cyberspace deze grootmachten monddood maken door de inzet van cybereffecten die slechts een fractie van de investeringen vergen dan deze voor conventionele wapensystemen. Klassieke operationele capaciteiten in het land-, lucht- en het maritieme domein riskeren irrelevant te worden door een technologische doorbraak in het cyberdomein.

2 Een proxy is een reële of virtuele entiteit in cyberspace die door een cyberactor gebruikt wordt om zijn werkelijke intenties of affiliatie te verbergen.

Het cyberwapen is multi-inzetbaar. Het is bruikbaar voor defensieve of offensieve operaties en voor spionage of sabotageacties. Cyberacties kunnen zowel kinetische als niet-kinetische effecten genereren, de effecten zijn vergelijkbaar met of kunnen zelfs groter zijn dan die van conventionele wapens. Het type effect kan variëren van beïnvloeding en ondermijning van het vertrouwen van de tegenstander in de eigen systemen tot de tijdelijke of permanente onbeschikbaarheid van de systemen. De cybercapaciteit is zowel tactisch en operationeel als strategisch inzetbaar tegen bijvoorbeeld de kritieke infrastructuur van een land.
Cybereffecten kunnen tot stand komen via proxies, zodat de verdenking in eerste instantie op iemand anders valt. De werkelijke actor achter een cybereffect is zeer moeilijk terug te vinden en komt bijna altijd neer op (soms sterke) vermoedens, vrijwel nooit concrete feiten. Het cyberwapen is dan ook bij uitstek inzetbaar in alle niveaus van een conflict, van vredestijd tot oorlog.
De effectieve inzet van een cyberwapen vergt geen enkele prepositionering. Vanuit eender welke geografische positie met internetconnectiviteit kan een cybereffect geïnitieerd worden naar eender welke andere wereldwijde locatie. Het cyberdomein is de facto een domein met strategische *reach*. De tegenstander krijgt geen waarschuwingstijd, het resultaat van een cybereffect is onmiddellijk. Een cyberaanval vindt plaats bij wijze van spreken aan de snelheid van het licht - men hoeft maar op Enter te drukken.

HOE ORGANISEREN WE ONS INTERNATIONAAL?

De NAVO bereidt zich voor op conflicten die zich zowel in cyberspace als op het klassieke slagveld zullen afspelen. Ze wenst even effectief te kunnen opereren in het complexe cyberdomein als in het domein van land-, lucht- en maritieme operaties. Op de laatste NAVO-top in Warschau hebben de lidstaten aanvaard dat cyberspace een nieuw operationeel domein wordt. Dit plaatst de cyberdimensie op hetzelfde niveau als de klassieke, conventionele operationele dimensies. De structuren van de organisatie, de processen en doctrines zullen aan deze nieuwe werkelijkheid aangepast moeten worden. Cybereffecten ter ondersteuning en voor de uitvoering van militaire operaties moeten deel uitmaken van het *targeting*- en het operationele planningsproces. Netwerken en wapensystemen zullen zodanig ontwikkeld en geïmplementeerd moeten worden dat ze nog inzetbaar zijn in *degraded cyberspace conditions*. Op termijn zal het cyberwapen een volwaardig alternatief vormen voor de klassieke kinetische wapensystemen.
Als gevolg van de erkenning als een nieuw operationeel domein bestudeert de Alliantie nu een *implementation roadmap*. Moet de NAVO een *cyber*

command-structuur opzetten? Hoe kunnen de offensieve capaciteiten van de lidstaten ingezet worden ten voordele van de organisatie? Wat met het inroepen van het principe van collectieve verdediging als een lidstaat het slachtoffer is van een cyberaanval?
Naast een correcte en coherente organisatiestructuur heeft het cyberdomein ook nood aan een legaal en procedureel kader voor het voeren van cyberacties. De *Tallinn Manual* van het *Cooperative Cyber Defence Centre Of Excellence* biedt een eerste, niet-juridisch bindend houvast voor nationale en internationale juridische adviseurs. Uitgangspunt van deze *Manual* is dat de bestaande internationale verdragen, rechtsregels en regelgeving ook van toepassing zijn op cyberspace. Deze visie wordt aangevochten door onder meer Rusland en China die liever een aparte specifieke wetgeving zien voor het cyberdomein. Hun uiteindelijke doelstelling is uiteraard incidenten in cyberspace niet onmiddellijk te laten erkennen als mogelijke agressie, wat hen dan weer de vrijheid geeft om hun favoriete spel van beïnvloeding en informatieoorlog te spelen zonder hiervoor met de vinger gewezen te worden. Een belangrijke discussie, zeker als men dit voor de NAVO extrapoleert naar het *framework of collective defence*.

BELGISCHE DEFENSIE EN CYBERSPACE

Bij de voorstelling van het nieuwe strategische plan verwijst de minister van Defensie in zijn analyse van de veiligheidsomgeving uitdrukkelijk naar de cyberdreiging. Vandaar dat de uitbouw van de militaire cybercapaciteit een van de speerpunten is in dit nieuwe plan. De doelstelling is tweeledig: een beter begrip en ook een betere bescherming tegen cyberdreigingen, maar ook een beter begrip van de opportuniteiten.

Het mandaat van de nieuwe militaire cybercapaciteit omvat inderdaad ook een offensieve subcapaciteit. We zullen dus ook zelf cybereffecten ontwikkelen ter ondersteuning of uitvoering van onze eigen militaire operaties. Op defensief vlak zal elke beheerder van een netwerk- of wapensysteem een eerste veiligheidslaag plaatsen rond zijn eindtoestellen en perimeters met commerciële middelen. De gecentraliseerde cyberexpertise legt een tweede en bijkomende laag van bescherming met een combinatie van specifieke en vaak zelf doorontwikkelde *toolsets* en heeft middelen ter beschikking om onmiddellijk en correct te kunnen reageren op een cyberincident. De inlichtingencapaciteit verschaft ons een coherent beeld van de cyberdreiging tegen onze militaire netwerken en wapensystemen en geeft indicaties die noodzakelijk zijn voor het onderzoek naar de attributie van een aanval. Diezelfde capaciteit wordt ook benut om de kwetsbaarheden bij onze tegenstanders in kaart te brengen.

De uitbouw van deze cybercapaciteit steunt niet zozeer op grote investeringen in materieel, maar noodzaakt wel de selectie en rekrutering van gemotiveerd en technisch competent personeel. Zowel binnen als buiten Defensie vinden geregeld rekruteringscampagnes plaats om de juiste experten aan te werven. Nieuwe rekruten worden onmiddellijk ingezet in één van de drie subcapaciteiten *cyberdefence*, *cyberintelligence* of *cyberoperations* en worden verder begeleid door een kader van permanente hoogtechnologische vorming en opleiding on the job. Inzake rekrutering moet Defensie haar specificiteit uiteraard uitspelen. Onze militaire cybercapaciteit is wettelijk gezien immers als enige ingedekt om bepaalde middelen te ontwikkelen en in te zetten terwijl bedrijven of burgers die niet mogen of kunnen gebruiken.

Welke zou nu de meeste geschikte organisatiestructuur zijn voor onze militaire cybercapaciteit? Noodzaakt een apart operationeel domein ook onmiddellijk een aparte structuur, hebben we nood aan een *cyber command* rechtstreeks onder bevel van de chef Defensie? Moeilijk om op deze vragen vandaag reeds een sluitend antwoord te formuleren. Het is wel zeer duidelijk dat de cybercapaciteit de komende jaren gecentraliseerd moet blijven. Deze capaciteit in opbouw vereist een zeer hoog expertiseniveau om correct te kunnen functioneren en door te groeien. Ze heeft eveneens nood aan specifieke processen en directe aansturing om te kunnen

anticiperen op de zeer snel evoluerende technologische uitdagingen, de continue wisselwerking tussen de verschillende subcapaciteiten en (inter)nationale partners. Een nichecapaciteit met grote uitdagingen voor de invulling van human en material resources moet dus minstens tot de *final operational capability*-fase gecentraliseerd blijven. Daarna kan men evalueren of de militaire cybercapaciteit op een andere manier gestructureerd moet worden. Maar op internationaal vlak merken we nu reeds dat vele partners ervoor kiezen om gecentraliseerd te blijven dan wel te evolueren naar een gecentraliseerde structuur (en dus naar een *cyber command*) indien ze op een andere manier opgericht zijn.

CONCLUSIE: ONZE DEFENSIE STAAT VOOR EEN ZEER GROTE UITDAGING

De aard van de cyberdreiging is recentelijk misschien niet gewijzigd, maar de snelle opkomst van het *Internet of Things* zal wel aanleiding geven tot een gloednieuwe reeks aan vectoren en kwetsbaarheden. Naties tonen verder ook veel minder schroom dan voordien en verkondigen nu publiekelijk dat ze offensieve cybercapaciteiten ontwikkelen en ook zullen inzetten indien nodig. De retoriek op diplomatisch vlak is veel agressiever geworden, het is duidelijk dat een volgend conflict deels in cyberspace zal uitgevochten worden.

Defensie moet zich aanpassen aan deze nieuwe realiteit om haar vrijheid van handelen te kunnen vrijwaren in dit nieuwe domein. De gedecentraliseerde netwerk- en wapensysteembeheerders moeten ondersteund worden om hun systemen optimaal te beschermen tegen cyberaanvallen. De *situational awareness* in cyberspace moet opgebouwd worden en geïntegreerd geraken in de *common operational picture*. Geavanceerde detectiesystemen moeten geïnstalleerd worden om malware of pogingen tot intrusie tijdig te kunnen detecteren. Er moet voldoende expertise opgebouwd worden en permanent beschikbaar zijn om adequaat te kunnen reageren op grote incidenten op het gebied van cyberveiligheid en op cyberaanvallen. En ten slotte moeten eigen cybereffecten gecreëerd, gevalideerd en geïntegreerd geraken in het operationele planningsproces en moeten *contingency procedures* geïmplementeerd worden opdat Defensie haar operaties kan blijven voeren, zelfs in *degraded* cyberomstandigheden.

Of dit alles zal lukken met een gespecialiseerde cybercapaciteit van slechts 200 experten in 2030 is nog maar de vraag. Zoals steeds, en zeker in deze budgettair moeilijke transitieperiode, zal veel afhangen van de prioriteit die toegekend wordt aan de implementatie van deze nieuwe, onontbeerlijke capaciteit. ◅

Trefwoorden: cyber, internet, asymmetrisch