De Belgische cyberdefensie: welke mogelijkheden voor een Europese samenwerking?

Jeroen VAN EYCK

Majoor stafbrevethouder Jeroen VAN EYCK, ir., is sinds juli 2018 werkzaam bij de divisie Integrated Capability Management van het stafdepartement Strategie. Tijdens zijn hogere stafopleiding schreef hij een onderzoeksartikel[1] over de domeinen waarin de Europese samenwerkingsmechanismen de opbouw van de Belgische cyberdefensiecapaciteit kunnen versterken.

Le domaine « cyber » est essentiel pour l'Union européenne (UE) et les États membres. Non seulement pour protéger le marché commun, mais également pour permettre à l'UE d'acquérir plus d'autonomie stratégique. En reconnaissant le « cyber » comme cinquième domaine, à côté des domaines terrestre, aérien, maritime et spatial, l'UE a souligné son importance. D'où la nécessité pour la Belgique, comme pour les autres nations, d'augmenter sa capacité de défense dans ce domaine. Parallèlement, l'UE met à la disposition des États membres et de l'industrie des outils, tels que la coopération structurée permanente (CSP) et le Fonds européen de la défense (FED), qui visent à promouvoir la coopération européenne. La question centrale de cet article porte sur la manière d'identifier les domaines dans lesquels ces outils européens peuvent renforcer les structures « cyber » de la Défense.

Cyberveiligheid is zowel binnen de Europese Unie (EU) als voor de individuele lidstaten cruciaal om de eigen samenleving en economie te beschermen. Dagelijks zijn er berichten over pogingen om via cyber invloed op onze democratieën uit te oefenen en over de economische schade die cybercriminaliteit berokkent. Wil de EU haar (digitaal) eengemaakte markt verder versterken, zal ze moeten investeren in cyberbeveiliging. Daarnaast streeft de EU naar een grotere strategische autonomie die haar, ook militair, minder afhankelijk moet maken van de rest van de wereld.

---

[1] Van Eyck, J. (2018). De Belgische cyberdefensie en EU-samenwerking, verdiepingsprestatie voorgelegd tot het behalen van het diploma van master na master in de politieke en militaire wetenschappen, Defensiecollege, Brussel.

Het uitroepen door de NAVO en de EU van cyber als vijfde domein, naast de domeinen land, lucht, zee en ruimte, onderstreept daarbij het belang dat cyber heeft als een van de militaire tools.

Zowel militair als civiel wint cyber dus aan belang, waarbij beide werelden elkaar overlappen, wat onder andere zal leiden tot de ontwikkeling van tweeledig inzetbare capaciteiten (in het Engels: "*dual-use capabilities*").

Zowel de EU als de NAVO beschouwen de ontwikkeling van cybercapaciteiten als een nationale aangelegenheid. Ook België bouwt daarom een eigen cybercapaciteit uit met de directie Cyber binnen het stafdepartement Inlichtingen en Veiligheid (ACOS IS). Internationale samenwerking is daarbij een must, aangezien het cyberdomein niet stopt bij de landsgrenzen. Verregaande samenwerking blijkt vooralsnog moeilijk gelet op de nationale belangen die soms op het spel staan. De cyberstrategie voor Defensie uit 2014 wil toch rekening houden met de internationale opportuniteiten die zich kunnen aanbieden. Het EU-Defensiepakket is zo'n gelegenheid.

DE EUROPESE UNIE EN CYBER

De top van de staatshoofden en regeringsleiders van de EU in 2016 in Bratislava besliste om een nieuwe impuls te geven aan de Europese samenwerking inzake externe veiligheid en defensie. Dit resulteerde in het EU-Defensiepakket dat drie domeinen omvat. Een eerste luik omvat de implementatie van de integrale EU-strategie voor het buitenlands en veiligheidsbeleid van de Europese Unie (hierna afgekort als "EUGS", acroniem van "EU *Global Strategy*"). Hiermee moet de EU in staat zijn om te reageren op externe conflicten en crisissen, haar partners ondersteunen en haar burgers beschermen. Een tweede luik omvat het ontwikkelen van het Europees defensieactieplan (EDAP), wat geleid heeft tot de oprichting van het Europees Defensiefonds (EDF) door de Europese Commissie. Een derde luik is de verdieping van de samenwerking tussen de EU en de NAVO met het oog op complementariteit en het vermijden van overlappende capaciteiten. De mechanismen die in die drie domeinen vervat zijn, bieden mogelijkheden voor de ontwikkeling van nationale cybercapaciteiten.

Binnen de EUGS zijn cyberveiligheid en -defensie een prioriteit en zowel de hernieuwde rol van het Europees Defensieagentschap (EDA) als de permanente gestructureerde samenwerking, beter gekend onder de Engelse benaming *Permanent Structured Cooperation* (kortweg PESCO), bieden mogelijkheden voor initiatieven in het cyberdomein. Het EDA speelt daarbij een centrale rol, waarbij cyberdefensie een van

de vier topprioriteiten binnen het Agentschap is. In overeenstemming met het vermogensontwikkelingsplan, beter bekend onder de Engelse term "*Capability Development Plan*", ligt de focus op het ondersteunen van de lidstaten om cyberdefensiecapaciteiten op te bouwen en de beschikbaarheid van de nodige technologie te bevorderen. Verschillende projecten lopen momenteel, met wisselend succes. PESCO is dan weer een vorm van defensiesamenwerking. Ze zag het licht dankzij het Verdrag van Lissabon, maar bleef zonder gevolg tot de komst van de EUGS. Door PESCO kunnen lidstaten die willen samenwerken rond een concreet thema dit ook doen, waarbij er bindende afspraken worden gemaakt tussen de lidstaten. Een initiële lijst van zeventien initiatieven werd opgesteld, waaronder twee cyberprojecten. Een eerste project heeft als doel informatie over cyberincidenten te delen tussen de lidstaten via een IT-platform: het *Cyber Threats and Incident Response Information Sharing Platform* ("platform voor het delen van informatie over cyberdreigingen en respons op incidenten"). Griekenland leidt dit project. Een tweede project wil response teams oprichten die niet alleen andere lidstaten, maar ook EU-instituten en GVDB-operaties kunnen ondersteunen met *deployable cyber toolkits*: het project C*yber Rapid Response Teams and Mutual Assistance in Cyber Security* ("snelle-reactieteams bij cyberincidenten en wederzijdse bijstand op het gebied van cyberbeveiliging"). Dit project staat onder leiding van Litouwen. De eerste response teams zouden in 2019 beschikbaar moeten zijn. België stapte niet mee in dit tweede project door twijfels over de haalbaarheid en de tijdslijn. Voor het eerste project is Griekenland nog volop bezig met het juist definiëren van het bereik. Eind 2018 werden in het kader van PESCO nieuwe initiatieven voorgesteld, maar geen enkel project was cyber gerelateerd.

Het EDAP heeft als doel de Europese defensie-industrie te versterken. Kmo's worden ondersteund en bestaande onderzoeksprogramma's zoals *Horizon Europe* worden opengesteld voor het ontwikkelen van tweeledig inzetbare capaciteiten, voor zover het civiele karakter duidelijk aanwezig is. Het paradepaardje van het EDAP is echter het EDF. Dit fonds ter ondersteuning van gezamenlijk onderzoek en ontwikkeling van defensiemateriaal en technologieën vindt haar wettelijke basis in het artikel 173 van het Verdrag van Lissabon, waardoor de Commissie de industriesector kan ondersteunen. Het moet leiden tot meer samenwerking en kostenreductie bij de productie van state-of-the-arttechnologie en uitrusting, alsook een stimulans zijn voor meer innovatie en onderzoek binnen de Europese defensie-industrie. Op 7 juni 2017 werd het EDF formeel opgericht. Momenteel wordt het geleidelijk aan uitgerold en dit in een onderzoeks- en capaciteitsdeel. Een capaciteitsdeel kwam expliciet erbij, want men heeft vastgesteld dat veel nuttige R&D-projecten nooit doorgroeien tot volwaardige capaciteiten. Het EDF moet de nodige

financiële ondersteuning geven om dit wel te doen. Onderstaande figuur geeft een overzicht van de financiële middelen die worden vrijgemaakt.

EUROPEAN DEFENCE FUND	2017-2020	Post 2020
RESEARCH Fully and directly funded from EU budget	€90 million total	€500 million* / year
DEVELOPMENT Member States budget at least 80%	€2 billion total	€4 billion* / year
Co-financing from EU budget up to 20%	€500 million total	€1 billion* / year
* Budget expectations per year		€5.5 billion* / year

Figuur 1. EDF: Overzicht financiële middelen[2].

De samenwerking tussen de EU en de NAVO kreeg in 2003 vorm met de Berlijn Plus-regeling. De veranderde internationale situatie in 2014 creëerde het politieke momentum om de samenwerking te verdiepen. In juli 2016, tijdens de top van Warschau, werd dit geconcretiseerd in zeven domeinen, waaronder het cyberdomein. Daarbij zal gestreefd worden naar een zo hoog mogelijke complementariteit en een vlotte gegevensuitwisseling tussen beide organisaties. Verder zullen de EU en de NAVO trachten om zo veel mogelijk op elkaar af te stemmen, bijvoorbeeld op het gebied van de vorming.

SAMENWERKEN OF NIET?

De verschillende door de EU ontwikkelde tools zijn positief voor de Europese defensie, maar het gebruik ervan vereist samenwerking tussen lidstaten en industrieën. Toch willen landen, wanneer het aankomt op veiligheid en defensie, maximaal de controle houden over hun eigen middelen en over het beslissingsproces binnen internationale organisaties.

[2] Europese Dienst voor Extern Optreden, "Defending Europe: European Defence Fund – factsheet", 5 maart 2018, geraadpleegd op 10 maart 2018, https://eeas.europa.eu/headquarters/headquarters-Homepage/35203/defending-europe-european-defence-fund-factsheet_en

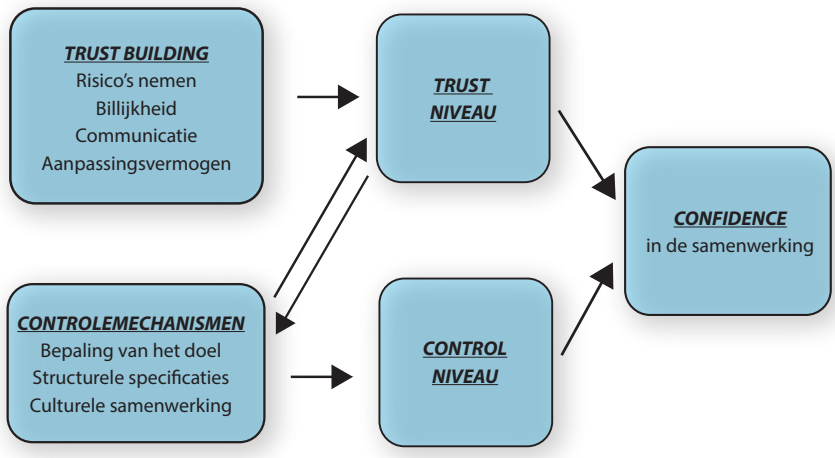
Deze neiging zal nog meer toenemen wanneer het over kritische nationale infrastructuur gaat, zoals bij cyber, om bij een mogelijk conflict niet het onderspit te delven.

Enerzijds zijn er een aantal obstakels voor verdere samenwerking. Zo is bij een cyberoorlog het offensief in het voordeel. De kosten voor de ontwikkeling en het gebruik van offensieve cybertools worden immers lager geschat dan deze voor cyberbeveiliging en –defensie, waarvoor een compleet arsenaal aan complexe software en hardware nodig is. Die complexiteit is voor de aanvaller van minder belang. De verdediger heeft ook het nadeel dat alle netwerken, die verschillende beheerders kunnen hebben, beveiligd moeten worden en dat zwakheden inherent zijn aan de software/hardware. Aangezien die kwetsbaarheden van voorbijgaande aard zijn, nodigen ze uit tot preventieve aanvallen. Tot slot is het aanwijzen van de dader vaak onmogelijk, waardoor de aanvaller buiten schot kan blijven, aangezien het moeilijk is om terug te slaan. Naast het voordeel dat een offensief met zich meebrengt, is het ook moeilijk om te achterhalen of een land al dan niet offensieve cyberintenties heeft: investeringen in cyberdefensie kunnen relatief eenvoudig aangewend worden voor offensieve doeleinden. Wanneer een land zijn cyberdefensie opbouwt, maar een ander land dit percipieert als de eventueel heimelijke voorbereiding van een cyberaanval, kan het zelf meer gaan investeren in zijn cyberdefensie. Dit veiligheidsdilemma kan leiden tot een cyberwapenwedloop. Volgens de neorealistische denker Jervis[3] maakt bovenstaande combinatie van factoren de situatie extra gevaarlijk en samenwerking moeilijker.

Anderzijds is samenwerking noodzakelijk. Het cyberdomein is een globaal publiek goed en is dus niet-uitsluitend en niet-rivaliserend. Er is met andere woorden geen manier om te beletten dat het niet gebruikt wordt. Indien het toch gebruikt wordt, blijft het nog steeds beschikbaar voor anderen. Dit is een tweesnijdend zwaard. Het voordeel is dat het cyberdomein continu voor iedereen beschikbaar is en door investeringen in cyberveiligheid draagt een land ook bij aan meer globale cyberveiligheid. Aangezien het echter een publiek goed is, is het risico groot dat veel landen zich als *freerider* gaan gedragen doordat er nu eenmaal veel landen deelnemen. Dit zorgt ervoor dat andere landen bijkomende investeringen moeten doen om dit risico op te vangen. Bij samenwerking moet er dus een mechanisme van toepassing zijn dat dergelijk gedrag kan identificeren en eventueel bestraffen. Verder zorgt het grensoverschrijdende karakter van de cyberruimte ervoor dat er toch een stimulans is om over te gaan naar een of andere vorm van

[3] Robert Jervis (1978), "Cooperation Under the Security Dilemma", World Politics 30, no. 2, blz. 211

samenwerking. Voor organisaties zoals de EU en de NAVO is het van belang dat alle lidstaten eenzelfde beveiligingsniveau hebben, zo niet kan een zwakke schakel de rest van de Unie of Alliantie bedreigen. Een gebrek aan samenwerking heeft bovendien nadelen bij de aanpak van cyberaanvallen. Kleinere landen (in het cyberdomein) hebben immers niet de mogelijkheid om bij een cyberaanval de (vermoedelijke) agressor officieel te beschuldigingen en moeten bijgevolg ofwel samenwerken met die agressor dan wel om steun vragen aan een bondgenoot.



Figuur 2. Trust en control in strategische allianties[4].

Samenwerking zal alleen mogelijk zijn wanneer er voldoende vertrouwen is tussen de partners. Figuur 2 toont dat vertrouwen of *confidence* gebaseerd is op twee belangrijke elementen die met elkaar verbonden zijn: *trust* en *control*. *Trust* kunnen we definiëren als het vertrouwen in het gedrag van de ander zonder verder onderzoek of bewijs. Er is met andere woorden een zekere mate van controle over de belangen van de andere, waarbij men erop vertrouwt dat deze dit niet zal misbruiken.

[4] T.K. Das en Bing-Sheng Teng, (1998). "Between Trust and Control: Developing Confidence in Partner Cooperation Alliances", Academy of Management Review 23, blz. 497

Control is de macht om gebeurtenissen of gedrag te beïnvloeden of te sturen. *Control* zal dus bereikt worden door een aantal mechanismen in te voeren die uiteindelijk leiden tot een samenwerking die voorspelbaarder wordt.

Samenwerking kan ontstaan wanneer er weinig trust is, maar indien er genoeg controlemechanismen zijn, kan er toch voldoende *confidence* zijn om een samenwerkingsverband aan te gaan. Andersom, wanneer er veel *trust* is tussen de partners, is er weinig *control* nodig. De vraag is hoe staten, en België in het bijzonder, bij hun samenwerking trust kunnen creëren en een niveau van *control* kunnen bereiken dat effectieve samenwerking mogelijk maakt.

WAY AHEAD VOOR DE BELGISCHE CYBERDEFENSIECAPACITEIT

Voor de opbouw van de Belgische cyberdefensiecapaciteit is het enerzijds noodzakelijk dat de mogelijke internationale partners het nodige vertrouwen hebben in de directie Cyber van het ACOS IS. Ten eerste is het daarbij van belang te erkennen dat een samenwerking altijd risico's zal inhouden. Ten tweede moet onze bijdrage billijk zijn. Europese regelgeving, zoals de Europese richtlijn over netwerk- en informatieveiligheid (NIS-richtlijn), die ervoor moet zorgen dat de verschillende lidstaten een gelijkaardig niveau van cyberbeveiliging hebben, moeten bijvoorbeeld daarom onverwijld worden omgezet in nationale wetgeving en geïmplementeerd worden. Communicatie is een derde aspect dat van belang is. Onze intenties moeten duidelijk zijn voor onze mogelijke partners: hebben we enkel defensieve ambities of ook offensieve? Communicatie betekent ook dat er voldoende informatie gedeeld wordt en dat de personen die de samenwerking opzetten en uitvoeren lang genoeg aangesteld blijven zodat er een vertrouwensrelatie kan ontstaan. Ten vierde is het nodig dat samenwerkingsakkoorden voldoende flexibel zijn. Een zeker aanpassingsvermogen van de verschillende partners draagt bij tot een betere verstandhouding.

Anderzijds helpen controlemechanismen om een mogelijk tekort aan trust weg te werken. Ten eerste dient het doel van de overeenkomst oordeelkundig bepaald te worden: bilaterale akkoorden maken het mogelijk om veel preciezere akkoorden te sluiten dan multilaterale, waar het maximaal haalbare misschien beperkt is, maar waar deze voldoende is om een initieel niveau van vertrouwen te creëren. Een tweede controle-element zijn de specificaties in de akkoorden. Zowel de NIS-richtlijn als de PESCO-bepalingen hebben een groot aantal specificaties waaraan moet voldaan worden om te vermijden dat landen zich als freerider gedragen.

Ten derde kan elkaars cultuur begrijpen bijdragen tot het sluiten van akkoorden. Gemeenschappelijke oefeningen en uitwisselingen dragen hier zeker toe bij.

De directie Cyber dient te streven naar een voortzetting van het huidige beleid. Er wordt reeds ingezet op internationale oefeningen, vormingen en trainingen, en dit zowel in het kader van de EU als de NAVO. De reeds bestaande informatie-uitwisseling en de verschillende R&D-projecten, waarbij de directie betrokken is bij het EDA, dienen voortgezet te worden. Wanneer het aankomt op de bescherming van onze nationale belangen lijkt diepgaande samenwerking nog een brug te ver. De Europese verplichtingen zoals de NIS-richtlijn zijn echter een minimum minimorum en kunnen aangevuld worden met formele of informele bilaterale samenwerkingen. Dankzij de huidige Europese tools die ontwikkeld worden, kan de directie Cyber volop Europese steun genieten in het kader van operaties en missies. De verschillende landen die deelnemen aan een operatie of missie hebben immers dezelfde doelstellingen. Dit betekent dat goed gedefinieerde PESCO-initiatieven de directie Cyber kunnen helpen, en dat ze in dit domein ook initiatief kan nemen wanneer ze daarvoor over voldoende mankracht beschikt en zo ook de industrie mee kan laten profiteren van het EDF. Programma's zoals Horizon Europa bieden dan weer de mogelijkheid om dual-use technologie te ontwikkelen met de Europese steun.

De defensieontwikkelingen in Europa bieden kansen voor de ontwikkeling van nationale capaciteiten. Cyber krijgt daarbij een hoge prioriteit. Het is dan ook de komende jaren dat de directie Cyber van die mogelijkheden zal moeten gebruik maken.

Trefwoorden: EU, cyber, samenwerking