Koninklijk Hoger Instituut voor Defensie

VEILIGHEID & STRATEGIE
SÉCURITÉ & STRATÉGIE

Nr 119
November 2014

C4ISR: een transitie naast de technologie?

Kapitein-commandant van het vliegwezen Bart Smedts
Vorser bij het Studiecentrum voor Veiligheid en Defensie

DEFENSIE

.be

Een elektronische versie van dit document is beschikbaar en kan gedownload worden van onze website www.khid.be.

De in dit document geuite standpunten vallen uitsluitend onder de verantwoordelijkheid van de auteur en geven niet noodzakelijkerwijs het officiële standpunt van het Koninklijk Hoger Instituut voor Defensie, het Ministerie van Landsverdediging of van de Belgische regering weer.

Vragen, commentaren of opmerkingen met betrekking tot dit document kunnen gestuurd worden naar volgend adres:
Directeur van het Studiecentrum voor Veiligheid en Defensie
Koninklijk Hoger Instituut voor Defensie
Renaissancelaan, 30
1000 Brussel
Of elektronisch naar : irsd-cesd-scvd@mil.be

ISSN: 0770-9005

C4ISR: een transitie naast de technologie?

Kapitein-commandant van het vliegwezen Bart Smedts
Vorser bij het Studiecentrum voor Veiligheid en Defensie

Koninklijk Hoger Instituut voor Defensie
Studiecentrum voor Veiligheid en Strategie

Renaissancelaan 30
1000 Brussel

Executive Summary

Communication architecture planning and technical documents nowadays all refer to C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) or one of its derivatives. The aforementioned acronym bears as many definitions as there are perceptions of it: sometimes common elements exist between them. In this study we try to find out if there is some common ground in C4ISR matters and what could be the cause for misunderstandings and wrong perceptions. For example, is it possible today to conduct any military operation without any C4ISR resources? And more importantly, is it possible today to run military C4ISR-operations without interfering in any way with civilian networks or civilian infrastructure? The interconnected structure of the C4ISR architecture on the one hand and the vast array of coupled sensors and platforms on the other hand make it less than likely: C4ISR-genesis arose from military needs but the extension of the operational fields had as a net result a bigger colaterral impact in the functioning of civil society. As a consequence C4ISR-transition transcends technological adaptation and needs a dedicated dynamic organizational chart. A dynamic and supportive C4ISR-cyber architecture is even needed in the background. The examination of the genesis of the communication architecture will provide us explanation on these perceived differences. States implementing the transition from "joint" to "joint C4ISR" architectures are driven by the latest security challenges: subject to almost instantaneous metamorphosis, these new security issues have operational consequences.

In part one of this study, we highlight the military origin of the C4ISR-acronym, its evolution and the supporting cyber-dimension. We examine how the sketched evolution has influenced operational needs and vice versa. From this description, we try to establish whether the transition under study could be seen as an endpoint or rather as a transit point towards further integration beyond what has been achieved until now. We try to find out whether we are witnessing pure technical and instant (r)evolution or a dynamic phenomenon: the success stories and failures of leading nations and coalitions, at home and abroad, could provide a guideline for optimal management of a revolution in kind.

After this state of affairs and lessons to be drawn, we look in how far the military genesis of the C4ISR architecture has matured beyond its sole military purpose. Again, leading countries show us in what context a civial C4ISR and supportive cyberdefence has been integrated in the homeland security context. Our findings show that the pure military origin has been outstripped due to the anchorage of the networks and sensors in civil society. We try to evaluate this push into the Europan institutions in section two. We examine the means by which one tries to cope with rapidly changing circumstances and determine whether national resources or supranational commitment is to provide for the management of this spearhead capacity.

In the final section we explore the national military capacity and try to evaluate the existence of a civilian equivalent. We attempt to focus on the lessons from national and coalition approaches in order to distil recommendations: we work out whether an isolated department approach can still hold today. The growth to a full fletched national homeland security comparable to supranational organisations or leading nations has not been reached due to a lack of assets and common organization. Investment has to be maintained in order to obtain a technical required national level matching international interlocutors.

The views expressed are only those of the author and do not necessarily reflect the views of Belgian Defence or the Royal Higher Institute for Defence.

Inhoudstafel

Executive summary i
Inhoudstafel iii
Lijst van afkortingen 1
Inleiding 3

DEEL 1: C4ISR: EEN MILITAIRE START 5
1.1. INLEIDING 6
1.2. DEFINITIES EN STRUCTUUR 7
1.3. LEIDENDE LANDEN 12
1.3.1. DE VERENIGDE STATEN 12
1.3.2. CHINA 16
1.4. FUTURE MISSION NETWORK:
militaire implicaties van het concept 22
1.5. CYBEROPERATIES EN NNEC 36
1.6. DE NAVO-BIJDRAGE 50
1.7. DEELBESLUIT 61

DEEL 2: DE EXTRA-MILITAIRE DIMENSIE 63
2.1. INLEIDING 64
2.2. DE ROL VAN DE LEIDENDE LANDEN 65
2.3. DE ROL VAN DE EUROPESE UNIE 71
2.4. VEREISTEN VOOR NIEUWE OPERATIETONELEN:
concepten en netwerk 84
2.5. CYBERVERDEDIGING IN DE EUROPESE UNIE 88
2.6. MILITAIRE C4ISR IN EEN CIVIELE ORGANISATIE OF
DEPARTEMENTELE TRANSITIE IN DE EUROPESE UNIE 94
2.7. DEELBESLUIT 98

DEEL 3: C4ISR IN BELGIË EN AANBEVELINGEN **101**
3.1. C4ISR: BELGIË 102
3.2. AANBEVELINGEN 110
3.3. DEELBESLUIT 114

ALGEMEEN BESLUIT **117**

BIJLAGEN **121**
BIJLAGE 1: PERCEPTIE VAN DE CYBERDREIGING 122
BIJLAGE 2**:** NATO COMMON OPERATING PICTURE 124
BIJLAGE 3: ORGANISATIE US DEPARTEMENT HOMELAND SECURITY 125
BIJLAGE 4**:** ORGANISATIE EU DIRECTORAAT-GENERAAL HOME 126

BIBLIOGRAFIE **127**

Lijst van afkortingen

AAF	Ambient Assisted Fighting
ACCS	Air Command-and-Control System
ACO	Allied Command Operations
ACO	Airspace Coordination Order
ADIV	Algemene Dienst Inlichtingen en Veiligheid van de Krijgsmacht
AGS	Alliance Ground Surveillance
AMDC	Air and Missile Defence Committee
AMN	Afghanistan Mission Network
AOD	Air Order Directive
APT-D	Advanced Persistent Threat Detection
ASDE	Air Situation Data Exchange
ATC	Air Traffic Control
ATO	Air Task Order
BICES	Battlefield Information Collection and Exploitation Systems
BiSC	Bilateraal Strategisch Commando
BLOS	Beyond Line of Sight
C3I	Commando en Controle Communicaties en Intelligence
C3I2	Command, Control, Communications and Intelligence / Information
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAOC	Combined Air Operations Centre
CDMA	Cyber Defence Management Authority
CDMB	Cyber Defence Management Board
CIRC	Computer Incident Response Capability
CIS	Communicatie en informatiediensten
COTS	Commercial-Off-The-Shelf
CPCC	Civil Planning and Conduct Capability
DARPA	Defense Advanced Research Projects Agency
DEC-CII	Directorate for Equipment Capability-Command, Control and Information Infrastructure
DOTLMPFI	Doctrine, organisatie, training, leiderschap, materieel, personeel, voorzieningen en interoperabiliteit
ECAP	European Capabilities Action Plan
EDA	Europees Defensieagentschap
EEAS	European Union External Action Service
EU	Europese Unie
EUMS	European Union Military Staff
FM2RN	Future Military Radio Node

FMN	Future Mission Network
GIG	Global Information Grid
IA	Information Assurance
ICT	Informatie-en communicatietechnologie
IHL	International Humanitarian Law
IP	Internet Protocol
ISRTA-WTM	Intelligence, Surveillance, Reconnaissance, Target Acquisition and Weapon-to-Target Matching in Complex Environments
JISR	Joint Intelligence, Surveillance and Reconnaissance
KEI	Kritieke Energie-Infrastructuur
LOAC	Law of Armed Conflict
MAJIIC	Multi-Intelligence All-Source Joint Intelligence Surveillance and Reconnaissance Interoperability Coalition
MOB	Main Operating Base
MoU	Memorandum of Understanding
MOTS	Military-Off-The-Shelf
MUSIS	Multinational Space-based Imaging System for Surveillance
NATO AWACS	NATO Airborne Early Warning and Control System
NATO C&I Agency	NATO Communication and Information Agency
NAVO	Noord-Atlantische Verdragsorganisatie
NCO	Network-Centric Operations
NCW	Network-Centric Warfare
NDPP	NATO Defence Planning Process
NEC	Network Enabled Capability
NNEC	NATO Network Enabled Capability
NORDEFCO	Nordic Defence Cooperation
PLA	People's Liberation Army
PLC	Programmable Logic Controller
RAP	Recognized Air Picture
R&D	Research and Development
SA	Situation Awareness
SACT	Supreme Allied Commander Transformation
SCADA	Supervisory Control and Data Systems
SEW	Shared Early Warning
SitCen	Situation Centre
SOA	Service-Oriented Architecture
TA	Target Acquisition
TCP/IP	Transmission Control Protocol/Internet Protocol
TDL	Tactische Datalinks
VK	Verenigd Koninkrijk
VS	Verenigde Staten
WSN	Wireless Sensor Networks

Inleiding

Vandaag vindt men weinig planning en technische beschrijvingen omtrent communicatiearchitectuur zonder verwijzing naar C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) of een van zijn afgeleide vormen. Van de integratie die dit acroniem voorstelt was tot enkele jaren terug nog veel minder sprake weze het onder de vorm geïntegreerde structuren, netwerken van netwerken of hun beveiliging. Het is voornamelijk in militaire middens en ten gevolge van de mutatie van het conflictspectrum vanaf het einde van de Koude Oorlog dat het besef is gerezen van een nog complexere omgeving. De integratie van een zo ruim mogelijk informatiespectrum moet toelaten om voor en tijdens een conflict inzicht te verschaffen over betrokken partijen, hoe men burgers van strijders kan onderscheiden welke troepenformaties deelnemen aan vijandelijkheden en wat hun bewapening is. Dat overzicht bewaren is essentieel voor de leiding van het gevecht maar ook voor het schatten van wat de eigen mogelijkheden zijn en de opties van de tegenpartij. Een dergelijk overzicht betitelt men vaak met de Engelse benaming "Situation Awareness". Tijdens de Koude Oorlog was dit de topprioriteit voor de snelste en eerste fasen van de oorlogvoering waarbij hoofdzakelijk het luchtoverwicht werd nagestreefd. Vandaag hebben we structuren zien veranderen: de lucht-, zee- en landmacht opereren niet meer alleen maar samen en op een gecoördineerde wijze (*joint*) en vaak in internationaal verband (multilateraal). Dit stelt eisen voor interoperabiliteit, het vastleggen van verantwoordelijkheidszones en gemeenschappelijke procedures. Maar bovenal vereist dit een gemeenschappelijk en uniek overzicht.

De trans-Atlantische band heeft ervoor gezorgd dat internationale samenwerking al ruimere tijd "bekend terrein" was. Het bestaan van gemeenschappelijke procedures mag dan al vanzelfsprekend lijken voor de identificatie van vriend en vijand, maar ze zijn veel minder vanzelfsprekend wanneer verschillende wapens opereren in hetzelfde gebied. Bovendien zijn sinds de Koude Oorlog een vierde (de ruimte) en een vijfde (cyber) dimensie het al complexe beeld gaan vervoegen. Het gebruik van traditioneel niet-militaire omgeving voor militaire doeleinden genereert nieuwe gevoeligheden: de bescherming van kritieke energie-infrastructuur zijn daarvan een voorbeeld. We merken dat het ontstaan van het overzichtsbeeld gekoppeld is aan de evolutie van de samenstelling van onze krijgsmachten en het belang ervan in

nieuwe dimensie verruimende domeinen. Het is dan ook niet verwonderlijk dat een uiteenlopende documentatie bestaat over de integratie van de systemen met als doel inzicht te verschaffen in de totstandkoming van een netwerk dat *situation awareness* (SA) garandeert: de meeste documenten behandelen slechts één bepaald aspect van de problematiek (bv. cyberbeveiliging). Wat we in deze studie beogen is te vertrekken van een basisdefinitie voor ons onderwerp: wat houdt de term C4ISR in en wat bedoelen de meeste auteurs wanneer ze over deze term schrijven? We proberen in een eerste deel een beeld te schetsen van wat de implicaties zijn van een dergelijke definitie (of het gebrek ervan). We trachten vanuit militaire toepassingen, te schetsen of er een evolutie waar te nemen valt in de benadering van ons onderwerp en hoe die tendens zich in de leidende landen in dit domein enerzijds en een militaire structuur bij uitstek als de NAVO anderzijds concretiseren.

De integratie van C4ISR is echter niet beperkt gebleven tot het militaire domein: in hun voortrekkersrol van militaire C4ISR, hebben leidende landen de transitie ingezet naar een luik "homeland security" doorgezet. In een tweede gedeelte wordt een overzicht gegeven van die "homeland security"-stuwing naar een extra-militair luik en hoe ver we in de EU als "policy begeleidende structuur" staan met betrekking tot die C4ISR-integratie.

In een laatste deel trachten we de positie van België in dit landschap te bepalen: we geven een overzicht van de eigen militaire en civiele capaciteit en trachten een idee te schetsen van de richting die we in ons land kunnen geven voor een geïntegreerd C4ISR structuur die kadert binnen het multilateraal kader waarbinnen we ons bevinden. We trachten ook te achterhalen of dit technische domein al dan niet kan geholpen worden door een louter technische aanpak en of we daarvoor kunnen uitgaan van onze eigen middelen alleen dan wel moeten rekenen op de welwillende hulp van anderen, en welke dat dan ook mogen zijn (publieke of private actoren).Bovendien trachten we de lessen te trekken van ontwaarde tendensen en trendbreuken uit voormelde structuren en trachten we aanbevelingen te genereren die zowel de nationale als de internationale positionering van ons land binnen het kader van het debat ten goede komen.

Een woord van dank gaat uit naar mensen die door hun informatie bijgedragen hebben tot de realisatie van dit werk: majoor van het vliegwezen stafbrevethoudster Ann D'Hondt en luitenant-kolonels stafbrevethouder Jan Abts en Sam Raeves.

Deel 1

C4ISR: een militaire start

1.1. Inleiding

Enkele jaren terug werd veel minder dan vandaag gesproken over geïntegreerde structuren, netwerken van netwerken of hun beveiliging. Het is voornamelijk in militaire middens dat het besef is gegroeid van een noodzaak aan efficiënte netwerken en communicatie voor commando en controle. Daarnaast kan commando en controle vandaag niet meer efficiënt werken zonder de integratie van inlichtingen, observatie en verkenningen. Dit vereist uiteraard de beschikking van de daartoe noodzakelijke sensoren en de efficiënte samensmelting van de informatie die deze sensoren genereren.

We onderzoeken in dit gedeelte de genese van de militaire netwerken: werden zijn *ab nihilo* samengesteld of volstrekte hun expansie zich eerder naar aanleiding van een concrete vraag? Vertrekkende van een aantal definities, zullen we zien dat de operaties in Afghanistan een belangrijke toedracht hebben gehad tot het inzicht van de netwerkbehoeften van de toekomst. Hieruit merkt men vrij snel dat cyber, en dus ook cyberverdediging, een centrale dimensie innemen in wat we vandaag netwerk centrische operaties noemen: de afhankelijkheid van informatie- en communicatietechnologie (ICT) voor de constructie van een C4ISR-architectuur behelst niet enkel meer een fysische beveiliging, eigen aan wapenplatformen bijvoorbeeld, maar ook de beveiliging van de informatie en de informatiedragers. We gaan na wat dit voor implicaties heeft voor de uitvoering van netwerk centrische operaties.

Wat dat impliceert voor een militaire organisatie als de NAVO, die eigen infrastructuur beveiligt, maar tegelijk afhankelijk is van de inspanningen van de bondgenoten, is voor ons zeer belangrijk. Leidende grootmachten hebben die beperking immers niet: hun C4ISR-evolutie geeft daarom mogelijk indicaties van optimalisatie van keuzes, zowel in het kader van het bondgenootschap als op nationaal vlak.

1.2. Definities en structuur

C4ISR staat in de vakliteratuur omschreven als *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance* (JAPCC, 2007; B-1): hoewel de definitie niet in het officiële NAVO-glossarium opgenomen is (AAP-06(2012)(2)), vinden we in andere documenten een waaier van benaderende verklaringen van het acroniem, vertrekkende van Commando en Controle (C2) over C3I (met toevoeging van *Communications en Intelligence*) tot enkele andere exotische varianten die in meer of mindere mate overeenkomen met de definitie zoals ze hoger werd aangegeven. Het verschil in de acroniemen is mogelijk toe te schrijven aan een evolutief proces in het creëren van een architecturaal netwerk. De evolutie van het acroniem en de betekenis die men dan eraan koppelt stemt vaak overeen met de technologische vooruitgang die de betrokken periode bestrijkt. Zo bijvoorbeeld wordt C4ISR in de VS doctrine (en alle samenstellende delen daarvan) beschouwd als een netwerk dat taakgericht wordt georganiseerd en gestuurd met als doel een opdracht te kunnen uitvoeren met een netwerkcentrale visie (*Network-Centric Operations*). De verschillende informatiebronnen die hiervoor vereist zijn, zijn niet noodzakelijk dezelfde voor iedere opdracht: nochtans moet de verbinding van sensoren en wapensystemen gerealiseerd kunnen worden volgens een herbruikbare technologie en met vastgelegde en beproefde procedures. Het afleveren van de juiste informatie aan de juiste besluitvormingsketen moet dus passen in een structuur die flexibel genoeg is om aangepast te kunnen worden naargelang de vereisten of de prioriteiten van het ogenblik. Men spreekt daarom van een dienstgerichte architectuur (*Service- Oriented Architecture* - SOA). Aangepaste software, hardware (sensoren en transmissiecapaciteit) en voornoemde procedures behoren dus tot de vereisten voor het bekomen van efficiënte commando- en controlesystemen. Het gebruik van een koppeling tussen hardware en software die vaak gebaseerd is op het Internet Protocol (IP) geeft ook aan militaire communicatienetwerken een output die sterk gelijkt op de Internetweergaven. Naar de structuur die erachter schuilgaat wordt vaak verwezen met de term “globaal informatienetwerk” (*Global Information Grid*-GIG).

Voorlopig kan men, <u>in een poging tot definitie</u>, stellen dat C4ISR de actuele weergave materialiseert van de integratie van systemen in een netwerk dat diensten verschaft met het oog op het verbeteren van het overzicht en het

inzicht in het besluitvormingsproces met als einddoel adequate commando en controle.

De benadering die in de vakliteratuur wordt gehanteerd, erkent de problematiek van het achterwege blijven van een officiële omschrijving voor het acroniem en hanteert daarom de volgende omschrijving:

> *The provision of information and intelligence to commanders that enables decision superiority necessary to execute the Commander's Intent, along with the appropriate level of situational awareness, to the point of achieving the desired effect.*

Hetzelfde document meent aandacht te moeten geven aan het feit dat de praktische implicaties van C4ISR slechts kunnen begrepen worden na het onontbeerlijke onderzoek van processen die beïnvloed worden door elementen van het C4ISR-acroniem (en omgekeerd ook processen die het resultaat van C4ISR-onderdelen beïnvloeden): zowel de informatie en de inlichtingen als de commando- en controleketen zijn daarom essentieel in het verwerven van *situation awareness*, waardoor tijdens een gewapend treffen doelaanduiding mogelijk moet worden met een minimum aan collaterale schade voor derde partijen of schadelijke gevolgen voor eigen troepen. Het bestaan van nieuwe domeinen die militair geëxploiteerd kunnen worden, zal deze definitie uiteraard verruimen, in het bijzonder voor het onderdeel dat proportionaliteit van het gebruikte geweld (beperken van collaterale schade) en discriminatievermogen bestrijkt in overeenstemming met het recht der gewapende conflicten. Men kan C4ISR begrijpen als een instrument ten dienste van het commando teneinde het besluitvormingsproces te vereenvoudigen: inlichtingen (Intelligence), maar ook permanente of occasionele observatie (Surveillance and Reconnaissance) leveren data van menselijke of technische sensoren die door computer en communicatietechnologie worden overgebracht naar de commandostructuur, waardoor het voormelde besluitvormingsproces wordt mogelijk gemaakt.

Een aantal essentiële onderdelen zijn de noodzakelijke voorwaarde voor C4ISR. In de eerste plaats zijn dat een beveiligde communicatietechnologie en computers. Gezien de noodzaak van verschillende sensoren en informatiebronnen is het onvermijdelijk dat ook de communicatietechnologie een waaier van systemen betrekt en integreert tot één netwerk dat in sommige gevallen ook nog eens bestendig moet zijn tegen toevallige of moedwillige verstoringen (*jamming*) en de informatie ongewijzigd aan de gebruiker moet kunnen afleveren zonder dat de informatie gelezen wordt door onbevoegden (gecrypteerd). Tabel 1 geeft een overzicht van de verschillende verbindingen die bijvoorbeeld bij de marine daarvoor noodzakelijk zijn.

Tabel 1: C4ISR en communicatiesystemen bij de marine (National Academies Press, 2006; p. 152).

Line of sight	Beyond line of sight	Satellietcommunicatie
CEC DDS	CEC DDS	Narrow band (UHF, UFO, MUOS)
Link-16	Link-16	Wideband (EHF, AEHF, SAT)
Link-11	JTRS WNW	Protected (DSCS, WGS, GBS, TSAT)
Link-22	Data link	Commercial
Link-4A		
Data link		
UHF, VHF, HF		

Legende:

CEC DDS, Cooperative Engagement Capability Data Distribution System; JTRS WNW, Joint Tactical Radio System Wideband Network Waveform; VHF, very high frequency; HF, high frequency; UHF LOS, ultrahigh frequency line of sight; UFO, Ultra High Frequency Follow-On (Navy satellite program); MUOS, Mobile User Objective System; EHF, extremely high frequency; AEHF, advanced extremely high frequency; TSAT, Transformation Satellite; DSCS, Defense Satellite Communications System; WGS, Wideband Gapfiller System; GBS, Global Broadcasting System.

Een studie met betrekking tot bestaande en in de toekomst vereiste architectuur bij de marine (National Academies Press. 2006) kwam tot vaststellingen die eigen zijn voor marine toepassingen maar daarnaast ook een aantal geselecteerde bevindingen die gemeenschappelijk zijn voor het volledige C4ISR-spectrum, ongeacht het domein waarin het opereert (land, lucht, zee, ruimte of cyber). Een eerste van de rij geeft aan dat het intense gevecht significant aan efficiëntie kan winnen door gebruik van een genetwerkte structuur die C4ISR integreert in de intensiefste operationele fases van de gevechtsleiding (bevinding 1). Bovendien zou het netwerk er goed bij varen om het aantal geïntegreerde sensoren uit te breiden om de “surveillance”-capaciteit op te voeren (bevindingen 2 en 3). Verder moet een commando- en controleketen kunnen opereren met C2 van andere departementen: nationale joint moet overstegen kunnen worden om in coalitieverband te kunnen streven naar een C4ISR-interoperabiliteit (bevinding 5). Interoperabiliteit zal door de volatiliteit van het dreigingspatroon moeten garant staan voor flexibele architectuur (bevinding 6).

Het bestaan van een netwerk vereist communicatie die op een veilige en efficiënte wijze tot stand komt. Vandaag kan dat niet meer zonder

geautomatiseerde systemen die informatie (zoals identificatie, positie eventueel aangevuld met bewapening) met betrekking tot vriend en vijand delen met coalitiepartners. De volledige (mogelijk tijdelijke) architectuur die hierdoor tot stand komt behelst bestaande deelnemende componenten maar ook hoe ze zich tot elkaar verhouden (hiërarchie), operationele procedures en de evolutie ervan in de tijd. Zoals vermeld zal een volatiel dreigingsspectrum eerder zorgen voor een dynamische architectuur: vaste structuren worden in die omstandigheden mogelijk sneller vervangen om plaats te maken voor aanpassingen *ad hoc*. De vragen die zich in dat kader altijd opnieuw zullen stellen zijn kenmerkend voor een dynamische architectuur die zich aanpast aan de vereisten van het ogenblik. Zo zal men iedere keer opnieuw moeten evalueren met welke partners of geallieerden het netwerk moet kunnen worden gedeeld en welke veiligheidsmachtigingen daaraan moeten gekoppeld worden? Welke instanties/ of departementen van iedere partner moeten geïntegreerd worden in het netwerk? Welk spectrum van opdrachten zal toelaten een dergelijk netwerk uit te bouwen binnen de limieten van de poging tot definitie die we hoger hebben vastgelegd: zal het mogelijk zijn een bruikbaar en operationeel netwerk tot stand te brengen voor het hoogste geweldspectrum van conflict of beperkt men zich tot crisisbeheer of rampenbeheer? Het antwoord op deze vragen is eveneens een dynamisch gegeven zolang de concepten aangepast worden.

Een vastgelegd doel in een netwerk dat moet instaan voor de bevordering van operationele C^2 is het verbinden van de hoofdkwartieren. Na tien jaar Future Mission Network (FMN) als verlengde van het netwerk dat in Afghanistan (Afghanistan Mission Network – AMN) uitgebouwd werd, heeft men een operationeel netwerk dat op veilige communicatie is gestoeld (exclusief WiFi) voor bureautica maar nog niet voor tactische informatie (Future ISR, 2012). Het eigenaarsrecht van tactische informatie, en dus ook de toegang voor deelnemers in de operatie, werden bijvoorbeeld duidelijk vastgelegd tijdens operatie *Active Endeavour* en de daaropvolgende operatie *Unified Protector* (Libië). De lessen uit tien jaar operaties in Afghanistan hebben ongetwijfeld bijgedragen tot een begin van doelgerichte deling van tactische informatie. Een van die lessen houdt ook verband met de fasen van het conflict: de voorbereidende fasen van een conflict zullen voornamelijk hardware oplossingen vereisen (bijvoorbeeld de optimale selectie en integratie van sensoren voor die specifieke opdracht alsook de verzameling van gegevens).

Een essentieel element in de C4ISR-architectuur is de betrouwbaarheid: hiervoor is men genoodzaakt een zekere graad van redundantie in het systeem te verwerken. Deze zal zorgen voor herstelvermogen in geval van uitval van individuele componenten (sensoren of transmissieknooppunten). We zien dat de nood aan redundantie, eigen aan de veerkracht van een militair netwerk, niet

noodzakelijk compatibel is met de vereisten van een commercieel product: de maximalisatie van winst gaat lijnrecht in tegen iedere vorm van redundantie, een bron van winstverlies in een kader van aanvaard risicospectrum. In een militair kader zijn die risico's niet aanvaardbaar en tot een minimum te herleiden, wil men de betrouwbaarheid van de architectuur garanderen. De vraag die men zich nu moet stellen is hoe ver men gaat in dat streven naar redundantie: elk element van de architectuur kan immers gedekt worden door een back-upsysteem, maar is dat wel efficiënt? Met andere woorden, men moet zich de vraag stellen welke de noodzakelijke elementen zijn in deze context die de operationaliteit garanderen zonder een excessieve kostprijs of logheid van het systeem te genereren. Het antwoord op deze vraag kan uiteraard niet gevonden worden door praktische uitvoering, maar moet gemodelleerd worden: een eerste poging hiertoe werd gedaan in 1997 door Lakey en Neufelder. Ze hebben een methode voorgesteld om de betrouwbaarheid van een systeem na te gaan dat samengesteld is uit hardware en software, zoals dat voor C4ISR-systemen het geval is. Het model is toegespitst op softwareconfiguratie met het oog op de optimalisatie van de algemene betrouwbaarheid van het systeem: heden ten dage is het echter vanzelfsprekend dat een louter softwarematige optimalisatie niet meer volstaat. Moderne systemen zijn in verschillende knooppunten van hun architectuur samengesteld door COTS-hardware waar niet noodzakelijk een volledig softwarematig inzicht of zelfs toegang te verkrijgen is. Om die reden werd het bestaande model bijgesteld. Een voorbeeld is het model van Vasilescu, die het geheel benadert als een complex systeem waarin zowel software als hardware de elementen zijn die de algemene betrouwbaarheid van het systeem zal bepalen.

Het cyberdomein neemt in dit opzicht een bijzondere plaats in tegenover de overige domeinen: het is het enig synthetische domein in de rij, wat als gevolg heeft dat bestaande doctrines van fysische domeinen (land, lucht zee en ruimte) niet zo maar kunnen getransponeerd worden naar het cyberdomein. In het bijzonder het element betrouwbaarheid vergt een zeer bijzondere bijdrage aan dit domein. Als pijler in een genetwerkte architectuur heeft men bijgevolg vragen die voortvloeien uit de specificiteit van het cyberdomein. Welke zijn de actoren die erin opereren, met welke visie, strategie of programma's? En hoe kan de betrouwbaarheid van het hele systeem verbeteren rekening houdend met de specificiteit van dit domein? Met deze vragen leidt men het belang in van *cybersecurity* in de ondersteuning van C4ISR.

We zullen in het volgende hoofdstuk nagaan in welke mate bestaande concepten een antwoord kunnen bieden aan voormelde vragen.

1.3. De leidende landen

1.6.1 De Verenigde Staten

Vanaf het prille begin van het concept netwerk centrische operaties (Network-Centric Operations - NCO) heeft men in het land het belang onderstreept van een gewijzigd gebruiksconcept van het militaire apparaat. Alleen dan is geconnecteerde oorlogvoering (Network Centric Warfare – NCW) mogelijk. De transitie van Dai Qingmin, zoals hiervoor uiteengezet, zou de VS in de tweede fase positioneren. Zowel de *jointness*, de militaire integratie en interdisciplinaire aanpak, als de politieke fundamenten geven dit land een voorspong op al de anderen met betrekking tot projecteerbaarheid van macht. De eerste nationale strategie terzake werd opgesteld in 2003 en herzien in 2011.

Enkele begrippen werden hierdoor belangrijker (Money and Alberts, 2000; p. 90):

- Het gebruik van geografisch verspreide eenheden of wapensystemen: eerder waren communicaties, projectiecapaciteit en manoeuvreerbaarheid beperkende factoren. Hierdoor waren troepen genoodzaakt om geografisch tot dichtbij hun doelwit te manoeuvreren. Vandaag laat de connectie en de uitwisseling van informatie toe om informatie eerder dan troepen of capaciteit te laten bewegen. De concentratie van troepen kan worden vervangen door de concentratie van geografisch verspreide wapensystemen en eenheden tot een geconcentreerd effect.

- Eenheden worden ingegeven met een hoger niveau van kennis: hierdoor hebben ze een groter besef van de gevechtssituatie en de deelnemende actoren dan voordien het geval was. Hierdoor kunnen ze beter autonoom opereren voor een gemeenschappelijk te bereiken effect.

- Eenheden vormen een collectief netwerk door het gemeenschappelijk gebruik en de exploitatie van de beschikbare informatie.

De vaak voorkomende misvatting bestaat erin dat men de nadruk legt op communicatie- en informatienetwerken, terwijl de hoofdbekommernis zich zou moeten situeren op vlak van informatie-uitwisseling, de aard en de informatie-

interoperabiliteit van de eenheden en de procedures om die uitwisseling te formaliseren. Bovendien wordt met deze benadering een veel grotere beslissingsmacht gegeven aan kleinere actoren die op een "gedecentraliseerde" wijze tot een gemeenschappelijk resultaat komen. De voorstelling van een netwerk dat dit mogelijk maakt is op elk ogenblik slechts een momentopname van de realiteit: men moet beseffen dat de voorstelling ervan grafisch niet weer te geven is door één figuur of diagram. In de plaats van een statisch geheel moet men oog hebben voor de dynamiek van een dergelijke structuur. Niet enkel verbindingen zijn belangrijk, maar veeleer welke er zijn, welke informatie erlangs transiteert en hoe men die exploiteert. Een voorbeeld maakt dit concept duidelijker: eenheden van luchtverdediging hadden een verantwoordelijkheidszone waarbinnen, naargelang de gangbare alarmstadia, toegewezen sensoren werden gebruikt voor informatievergaring en wapensystemen konden worden aangewend. In het netwerk centrische concept zou men eerder in een bepaalde zone de aanwezigheid van meerdere actoren kunnen hebben die elk naar eigen inschatting het gebruik van wapens of sensoren optimaliseren om het gemeenschappelijke doel te bereiken. Dit stemt niet noodzakelijk overeen met de afscherming of zuivering van de hele zone die toegewezen werd. Het gedecentraliseerde aspect komt tot uiting in het feit dat iedere actor bijdraagt tot het vervolledigen van de beeldvorming, besluitvorming en uitvoering ervan.

Dit concept biedt een aantal voordelen met betrekking tot de snelheid van de commandoketen, de samenwerkingsverbanden, de engagementen *Beyond Line of Sight* (BLOS) en de reactiesnelheid. De verbetering van deze elementen is onderhevig aan het bestaan van een aangepaste doctrine: de neutralisatie van de juiste doelen op het juiste ogenblik wordt belangrijker dan de vernietiging van een zo groot mogelijk aantal doelen. Hierdoor worden de kwaliteit van de informatie over de doelen en de uitwisseling ervan, als ook de doctrine een beperkende factor: de beslissing om die te wijzigen ter verdeling van verantwoordlijkheden en exploitatie van informatie zal niet alleen de efficiëntie, maar ook de kostprijs van een operatie drukken. Het drukken van de kosten is uiteraard van belang in het huidige financiële en budgettaire klimaat: kostendrukking met verruiming van efficiëntie kan in de toekomst enkel met toepassing van het NCO-concept. Dit impliceert mogelijk een verkorting van de termijn tussen de planningsfase en de uitvoering ervan (of zelfs tot de fusie van beiden).

Operationele gevolgen van dit concept worden mee door de visie op de opdrachten van de toekomst bepaald: eerder vermelde voordelen van de netwerk centrische benadering worden gedeeld door de visie op middellange termijn (Shelton, Henry H., 2000) in een *joint* omgeving. Hierbij doelt Shelton met *joint* omgeving op de integratie van competenties van individuele

krijgsmachtonderdelen, maar evenzeer op de intellectuele, operationele, doctrinaire en technische integratie die ervoor moet zorgen dat die krijgsmacht flexibel inzetbaar is. De krijgsmacht dient immers in staat te zijn om een heel gamma aan operaties te realiseren, verspreid in tijd en ruimte in een organisatie die niet noodzakelijk dezelfde commando- en controleketen behelst (coalitie, interdepartementaal, supranationaal): hiervoor moet men sneller, preciezer en accurater kunnen opereren, een element waartoe netwerkcentriciteit en *jointness* kunnen bijdragen. De mate waarin die integratie zal bereikt worden is beïnvloed door twee factoren, met name de overheersing van de informatie enerzijds en de intellectuele en technische innovatie anderzijds. Deze laatste draagt ook bij tot de snelheid waarmee het strategische landschap zal wijzigen en kan ook een effect hebben op de mate waarmee asymmetrische aanvallen kunnen worden gegenereerd. Maar dominantie kan alleen bereikt worden in die omstandigheden indien de beschikking over en de exploitatie (verwerking en verspreiding) van de informatie beheerst worden. Dominantie van de informatie kan echter geen doel zijn op zich: het moet vertaald worden naar kennis en besluitvorming. Hiervoor zijn eveneens (zoals voor *jointness*) aanpassingen vereist in de organisatie, doctrine, opleiding en training, commando en controle. Hieruit kunnen we besluiten dat *jointness* ook geen doel op zich mag zijn maar slechts een etappe betekent in de transformatie van de krijgsmacht naar een structuur die in staat zal zijn om aan de uitdagingen van de toekomst het hoofd te kunnen bieden: hierbij moet voldoende flexibiliteit gegarandeerd worden om de onzekerheden of onvoorzienbare speelmarges op te vangen. Factoren die mee zullen bepalen in welke mate de *jointness* bereikt zal worden zijn:

- Mensen die opgeleid zijn volgens de standaarden die vereist worden voor het realiseren van snelle en geografisch verspreide opdrachten.

- Interoperabiliteit (het vermogen van systemen of eenheden om diensten te verlenen of te ontvangen van andere systemen of eenheden en efficiënter samen te kunnen werken); internationale en interdepartementale opdrachten.

- Operationele concepten zoals dominant maneuver (het vermogen van geïntegreerde troepen om snel het voordeel van de positie te behalen teneinde krachten te kunnen bundelen of hetzelfde effect te bekomen met geografisch verspreide krachten), accuraatheid (het vermogen om doelen te lokaliseren, te observeren, te onderscheiden, te volgen en de gewenste effecten te bereiken), aangepaste logistiek (het vermogen om de strijdkracht op het juiste ogenblik kwantitatief en kwalitatief uit te rusten met het juiste personeel en materieel.

- Informatiebeheersing en in het bijzonder niet-traditionele vijanden in niet-traditionele conflicten of crisissen (bijvoorbeeld humanitaire opdrachten en hun gevolgen) zullen het uitgelezen terrein zijn voor asymmetrische resultaten.

- Commando en controle die gebaseerd zijn op de correcte exploitatie van die informatie en de daaruit voortvloeiende besluitvorming.

Vooral dit laatste element zal het begrip *jointness* tastbaar maken in die zin dat een geconcentreerde uitwerking van het functioneren van eenheden die verspreid zijn in tijd en ruimte zichtbaar wordt. Dit element impliceert dat menselijke tussenkomst gebeurt door hen die vertrouwd zijn met nieuwe technologie en domeinen en de voordelen alsook de beperkingen ervan kennen: in de Verenigde Staten is men zich bewust van het belang van het gebruik van overeengekomen terminologie, doctrine, organisatie, opleiding en training voor de operaties van de toekomst. De netwerk centrische operaties nemen daarin een centrale rol en overschrijden het zuiver technische aspect ervan: het groot aantal betrokken actoren impliceert een interdepartementale en multinationale betrokkenheid.

Uiteraard reikt de uitvoering van dit concept verder dan de uitsluitend militaire sfeer. Het nationaal interdepartementale element impliceert de samenwerking met civiele en zelfs private partners: cyberveiligheid wordt in dat kader nagestreefd ten opzicht van een dreiging die uitgaat van hackers en criminele organisaties. Het belang en de rol van de nationale actoren werden hiervoor al vastgelegd in 2003 (White House National Strategy to Secure Cyberspace). Het multinationale element wordt dan weer belicht in het kader van de bescherming van vitale belangen waartegenover de dreiging uitgaat van terroristische organisaties en natiestaten of coalities ervan. De geïntegreerde aanpak bracht de VS zo tot het uitschrijven van een nationale veiligheidsstrategie in 2002 (herzien in 2010), voorbeeld dat later door vele andere landen werd gevolgd (China - 2004, Groot-Brittannië - 2010, Nederland -nog te publiceren). Het cyberaspect wordt terecht beschouwd als een klein onderdeel van een groter geheel in de genese va n de nationale veiligheid. Vandaag wordt er echter veel aandacht geschonken aan de interconnectie van dreigingen en hun cascade-effecten. In dat opzicht kan een cyberincident ook aanleiding geven tot ingrijpendere incidenten in domeinen als economie of industrie. Nochtans vergt deze problematiek, gezien het potentieel van groot economisch verlies, eveneens een internationale aanpak. Geen enkel land is vandaag in staat om zijn eigen veiligheid te garanderen: niet fysisch en ook niet virtueel. Daarom kan men zich ook vragen stellen met betrekking tot de efficiënte werking van de bescherming van kritieke infrastructuur als de organisatie ervan aan de grenzen eindigt: in de VS maakt men immers een

onderscheid tussen de internationale of de nationale aanpak. Voor de nationale aanpak is het departement Homeland Security bevoegd. Onder dit departement worden alle andere actoren gecoördineerd die op nationaal vlak relevant zijn. Aangezien het virtuele platform gedragen wordt door een groot aantal private partners (die het merendeel van de infrastructuur bezitten), zijn specifieke akkoorden vereist om al die departementen ook met de private partners te linken (National Cyber Security Partnership).

Voor Defensieaangelegenheden zijn evengoed overeenkomsten met private partners verankerd (Robinson et al, 2013; p. 31). De specifieke verhouding die Defensie daar tot stand heeft gebracht is een vergelijking waard met enerzijds de organisatie van de EU en anderzijds van de NAVO. We bespreken hieronder deze supranationale organisaties, meer bepaald met betrekking tot het onderscheid tussen civiele en militaire activiteit, maar ook met betrekking tot het onderscheid tussen een nationale en een supranationale organisatie.

We hebben in wat voorafging al aangehaald hoe dit tegelijk zwakheden aan het licht kan brengen die niet noodzakelijk gekend waren bij de ontwikkeling van het C4ISR-netwerk of zijn toepassingen. Tegelijk heeft het land ingezien dat het de bestaande dreiging (zeker voor de bescherming van kritieke infrastructuur) niet alleen kon beheersen: daarom hebben de VS de nadruk gelegd op de medewerking van internationale platformen. Binnen de VN is er vooralsnog geen echte samenwerking zoals die wordt ontwikkeld binnen de NAVO en de EU. We zullen echter merken dat de aanpak van deze twee platformen fundamenteel verschillen.

1.6.2 China

Hoewel China een sterk gecentraliseerd besluitvormingsorgaan heeft, en de noodzaak en de sterkte van een ontwikkeld en geïntegreerd informatienetwerk heeft ingezien, hebben operationele verbeteringen nog een lange weg te gaan. De publieke opinie gaat ervan uit dat China een sterke cybercapaciteit heeft en in bezettingsgraad of uitrusting kan dit kloppen: de toedracht hiervan wordt mee geleverd door verslagen die in de media verschijnen. Zo kan de koppeling van de cyberactiviteit met het bestaan van een militaire eenheid (zie hiervoor het Mandiant rapport met betrekking tot eenheid 61398) van de People's Liberation Army (PLA) de indruk wekken dat een partijpolitieke strategie haar praktische uitvoering vindt. De operationele aanwending van een dergelijke capaciteit heeft echter niets te maken met absolute cijfers noch met het bestaan van een dergelijke eenheid: het eerder aangehaalde probleem van attributie zorgt vandaag mee voor onzekerheid betreffende de uitvoerbaarheid of de wil om de theoretische "strategie" om te

zetten in operationele uitvoerbaarheid en uitvoering. Het is niet omdat men transitie naar een gedigitaliseerde en netwerk centrische structuur nastreeft, dat dit ook op korte termijn mogelijk is. Vooral in China wordt die transitie naar operationele capaciteit vooral ervaren als een puur technologisch vraagstuk. In de werkelijkheid is er aan een even belangrijk organisatorisch aspect aan verbonden en we zullen verder zien dat dit ook voor andere landen of supranationale organisaties het struikelblok vormt om tot een operationeel concept te evolueren. De technologische invulling wordt in het Chinese voorbeeld gerealiseerd door platformen en sensoren, niet noodzakelijk door het realiseren van een netwerk van sensoren of de gemeenschappelijke exploitatie van informatie die uit die sensoren en/of platformen voortspruit. Het aantal (wapen-) platformen gaat grotendeels gepaard met kinetische operaties die in verzuilde organisatiestructuren worden uitgevoerd. Een genetwerkte krijgsmacht is echter in staat om de inspanning door aantallen te beperken en te compenseren met een snelle commandoketen. Hiervoor is integratie en *jointness* vereist en dit is net een aspect waarin de Chinese verzuilde krijgsmacht nog niet voldoende vooruitgang heeft geboekt. Het is pas sinds 2004 en het operationele gebruik van observatie- en verkenningstechnologie in de derde dimensie dat China oog kreeg voor het belang van geautomatiseerde en gestandaardiseerde commando- en informatiesystemen (Pollpeter, 2010; p. 198). Het bestaan van onafhankelijke systemen per militaire regio met niet noodzakelijk compatibele technologie wijst op het gebrek aan integratie op niveau van het beleid in China. Ten minste tot 2003 was het commando nog gericht op de coördinatie van middelen in de plaats van echte integratie in een geïntegreerde structuur die verder reikt dan een samenwerking op stafniveau. Interne rivaliteit kan hierdoor nog een ernstige hinderpaal vormen in de verdere stappen die dit land moet zetten naar een genetwerkte structuur. Technologische ontwikkeling van C4ISR-systemen zonder geïntegreerde structuur mist immers architecturale basis en uitvoerbaarheid van doctrine. De noodzakelijke vereisten in de toekomst bestaan voor de PLA uit vier aspecten:

- De correcte identificatie van operationele vereisten voor informatisatie van de krijgsmacht waaronder men verstaat de informatisatie, automatisatie en vernetwerking: gangbare gebruiken om de technologische vooruitgang te kopiëren en in individuele aantallen te overtroeven zonder netwerking heeft hierin geen meerwaarde en dat heeft China begrepen. Dit verklaart ook de inspanning die door dat land sinds 2004 geleverd worden om informatietechnologie ten dienste te stellen van operaties, de militarisatie van de ruimte voor een andere potentiële tegenstrever en de verdediging van maritieme belangen vanaf een perimeter die verder gelegen is dan de eigen kustlijn;

- Technologische ontwikkeling in dienst van combinatie van middelen: hierdoor wil men een netwerk tot stand brengen dat moet toelaten diensten te synchroniseren en te coördineren, om sterktes uit te baten en zwaktes te compenseren in alle domeinen en in alle omstandigheden;

- Het gebruik van civiele informatietechnologie en toepassingen daarvan voor militaire doeleinden; de ontwikkeling van het defensieapparaat is in China ondergeschikt aan de economische ontwikkeling en bijgevolg de ondersteuning van groeimaatregelen. Het onderscheid met westerse landen is dat operationele wapensystemen en commandoketens steunen op overheidsontwikkeling en niet onderhevig zijn aan de soms ondoorgrondbaarheid van COTS-technologie;

- Het vooruitstuwen van ICT-ontwikkeling en innovatie: dit kan gemakkelijker uitgevoerd worden door in een eerste fase ICT-technologie te kopiëren, wat niet het geval is voor andere toepassingen van militaire technologie. De inhaalbeweging die moet uitgevoerd worden door dit land kan versneld worden door te vermijden dat integratie departementaal benaderd wordt en in tegenstelling een overkoepelende aanpak van commando en controle te garanderen.

Drie fasen zijn volgens Dai Qingmin te onderscheiden in de transitie naar een netwerk ondersteunde architectuur (Dai Qingmin, 2001; p. 78): in een eerste fase ontwikkelen individuele diensten of eenheden informatiesystemen en integreren hun platformen in dit geïnformatiseerde systeem. Dit is de fase waar volgens de auteur China zich in 2010 bevond. In een volgende fase worden verschillende bestaande informatiesystemen geïntegreerd en worden structurele aanpassingen uitgevoerd aan de organisatie betreffende opleiding, training en onderzoek. In deze fase plaatst de auteur de capaciteiten van de VS. De derde en laatste fase materialiseert de vervolmaking van de genetwerkte structuur waarin krijgsmachten in staat zijn om op basis van geïnformatiseerde gegevensuitwisseling de operationele opdracht tot een goed einde te brengen. Deze gegevens zijn mogelijk ontsproten uit grond-, lucht-, ruimte-, zeegebaseerde sensoren, het elektromagnetische spectrum of het netwerk zelf. Het probleem van deze benadering in fasen is voor elke nieuwe actor het gebrek van overkoepelende insteek waardoor de integratie van niet-gestandaardiseerde systemen veel moelijker wordt. De achterstand van China had merkelijk beter ingelopen kunnen worden door a priori een concrete overkoepelende strategie aan te wenden voor de ontwikkeling van een geïntegreerd netwerk. Vandaag is dat niet het geval en hinkt China nog altijd achterop ten opzichte van de VS. De transitiefasen van voormelde fase plaatst de PLA respectievelijk in 2010, 2020 en 2050. De integratie over de grenzen

van militaire regio's en stafdomeinen zullen in dit tijdsschema essentiële onderdelen zijn zonder dewelke het einddoel nooit kan bereikt worden. Anderzijds opent die gefaseerde transitie ook de deur voor nieuwe gevoeligheden: de aanpak naar een meer geïntegreerde informatisatie en netwerking zal zwakheden doen opduiken die een achterop hinkend land altijd bij zijn tegenstrever heeft kunnen uitbaten. Zelf in de spits lopen van de vooruitgang houdt het risico in dat men niet altijd op de hoogte zal zijn van de nieuwe zwakheden die opduiken door of in het transitieproces.

Een concreet voorbeeld van dat dilemma dat samenwerking vereist en tegelijk nieuwe zwakheden blootlegt wordt geïllustreerd door integratie van lucht- en ruimtemacht. Het samengesmolten *aerospace* domein zou het land toelaten om de middelen beter op elkaar af te stemmen: hierdoor kunnen strategische en theaterobjectieven steeds bereikt worden. Zonder die samensmelting van het luchtdomein zouden doelstellingen wellicht niet kunnen bereikt worden bij gebrek aan een veel groter aantal middelen in ieder deelgebied (lucht of ruimte). Het nadeel is dat procedures, doctrines, opleiding en training op elkaar moeten afgestemd worden. Pas dan kan men oog hebben voor eventuele nieuwe zwakheden: een proces van jaren voor het samensmelten van een verzuilde en opdrachtgerichte krijgsmacht in vergelijking met een van bij aanvang geïntegreerde aanpak. Deze samensmelting is nochtans maar een eerste stap in de integratie van de volledige PLA. De mate waarin voormelde samensmelting geslaagd zal zijn, zal afhangen van het bereik en de complexiteit van het observatie-, commando- en controlenetwerk: in eerste instantie zal dat gemeten kunnen worden aan de manier waarop de luchtmacht en de tweede pijler van de artillerie (raketten en ruimtetuigen) met elkaar zullen kunnen samenwerken in het realiseren van hun vuurkrachtopdracht: die vuurkracht moet op zichzelf in staat zijn om strategisch en zelfs politieke doelstellingen te bereiken. Luchtaanvallen en raketopdrachten moeten daarom ondersteund worden door inlichtingen en moeten traditioneel grootschalige opdrachten van grondtroepen kunnen ondersteunen (Stokes, 2012; p. 40). Oorlogvoering wordt daarom ook gevoerd in disciplines als inlichtingen, elektronische (lees ook cybernetische) en psychologische operaties teneinde de C4ISR-keten van de tegenstrever te onderbreken. Dat is ook het hoofddoel van netwerkgericht oorlogvoering: een belangrijk verschil met andere militaire middelen is dat dit domein niet echt volledig in handen is van militairen alleen. Een tweede essentieel verschil is dat de grotere sofisticatie van China net ook gevoeligheden zal creëren die het voor het ogenblik bij tegenstrevers tracht te kunnen exploiteren.

Vooralsnog beschouwt China dit middel als de betere weg om op een legitieme en actuele manier zijn eigen politieke drijfveren kracht bij te zetten. In het bijzonder wordt de bijzondere plaats in de verf gezet die Taiwan

inneemt. Het is belangrijk te onderstrepen dat een politieke visie hier de grondslag legt voor alle strategische implicaties en operationele aspecten en niet andersom: in operationele vertaling betekent dit dat China de bekwaamheid wenst tot het verstoren en verlammen van C4I-systemen van Taiwan of andere partijen die het land trachten te steunen tegen China. Strategisch gezien bevordert men in de eerste plaats de verdediging van eigen netwerken (SSI, 2009; pp.259). Vervolgens worden netwerkoperaties beschouwd als een verrassingselement dat vóór een conflict kan worden gebruikt: in een open strijd verliest het gebruik ervan aan onvoorspelbaarheid. Daarom zal het ook ondersteund worden door andere middelen zoals elektronische oorlogvoering. Hiermee tracht men de acquisitie van informatie te verstoren of tegen te gaan. Mocht dat toch niet lukken, zullen computernetwerkoperaties zo veel mogelijk verhinderen dat de vergaarde informatie wordt geëxploiteerd. Het gebruik van het cybernetische domein voor het behalen van militaire objectieven laat op die manier toe om de informatieoorlog te winnen vooraleer een conventioneel of ander type aanval moet worden verwacht of uitgevoerd. De tegenstrever wordt beschouwd al zijnde afhankelijk van informatie voor dagelijks werking: *in casu* is dat het geval voor Taiwan en de Verenigde Staten. In het bijzonder vormt het cyberdomein in dit geval de toegang tot vitale (informatie-)infrastructuur van Taiwan en het C4I-netwerk van de VS: dit land moet verhinderd worden om troepen of geweld te projecteren ter ondersteuning van Taiwan. China evalueerde dat beide landen afhankelijk zijn van elkaars netwerk dat ondersteund wordt door private firma's en rekent op de zwakheden van die niet-militaire infrastructuur om logistieke ondersteuning voor Taiwan te dwarsbomen. Deze ingreep is vooral bedoeld om een preventief effect te genereren en te vermijden dat welke partij dan ook een fysische versterking zou kunnen leveren aan het eiland. Blijkbaar schat China niet in staat te kunnen zijn om ook operationele eenheden op het terrein enkel met cybernetische middelen te kunnen hinderen of tegen te houden (SSI, 2009; p. 271). Talrijke voordelen worden volgens auteurs aan deze strategie verbonden: operationaliteit kan op korte termijn bereikt worden, fysische aanwezigheid is niet vereist, de cybernetische aanval heeft de mogelijkheid om de geografische toegang te ontzeggen, het buit afhankelijkheid van de VS ten opzichte van informatiesystemen uit en ten slotte biedt het een afschrikkingseffect voor VS-interventie. Bovendien is hierdoor een belangrijke greep verzekerd op een informatieknooppunt waar de handel in de hele wereld van afhangt.

China ziet in dat een wapensysteem zonder ondersteuning van een uitgebreid C4ISR-netwerk een zeer beperkte bijdrage kan leveren bij de beslechting van een dispuut. Het mag hieruit blijken dat China in het streven naar de uitbouw van een dergelijk netwerk en het operationaliseren van computernetwerkoperaties mee aan de basis zal liggen van de genese van eigen kwetsbaarheden: de zwakte die het land wenst uit te buiten bij zijn tegenstrever

zal ook zijn eigen zwakheid worden. China is in transitie tussen twee ontwikkelingsfasen van het netwerk. Of het dat nu wil of niet, de verdere uitbouw ervan zal ervoor zorgen dat de eigenschappen van het eigen netwerk ook door die tegenstrever kunnen uitgebuit worden.

1.4. Future Mission Network: militaire implicaties van het concept

De grondvesten van de toekomstige netwerksamenstelling en architectuur zijn de lessen getrokken uit voorafgaande opdrachten. De opdrachten in Afghanistan en Libië zijn daarom zeer belangrijk voor de taken in de toekomst. Hoewel de capaciteiten nog steeds gegenereerd worden door lidstaten en bondgenoten, wordt binnen de NAVO veel belang gehecht aan het vermijden van duplicatie. De netwerkarchitectuur van de toekomst wijst daarom voor zijn implementatie op het belang van doctrine, maar ook van organisatie, training, leiderschap, materieel, personeel, voorzieningen en interoperabiliteit (DOTLMPFI). De sinds Afghanistan al ontwikkelde elementen van die keten moeten in aanmerking genomen worden wil men synergie en interoperabiliteit nastreven. Dat is ook het voordeel dat de NAVO als platform heeft ten opzichte van de EU: ze kan zich beroepen op een basis van conceptuele en praktische ervaring die de EU ontbreekt. Figuur 9 illustreert de moeilijkheden en de modulariteit waarmee rekening moet worden gehouden voor de netwerksamenstelling in de toekomst. De voorstelling in vier kleuren illustreert de alternatieve of complementaire mogelijkheden van de samenstellende delen van het netwerk:

- donkerblauwe kernelementen (optie A) zijn leden die een eigen infrastructuur hebben die multilateraal gecertifieerd is: zij vormen de ruggengraat van het gehele netwerk en zullen diensten genereren die ook een bijdrage leveren voor meer perifere leden (lichtblauw) die zich kunnen voegen bij het netwerk;

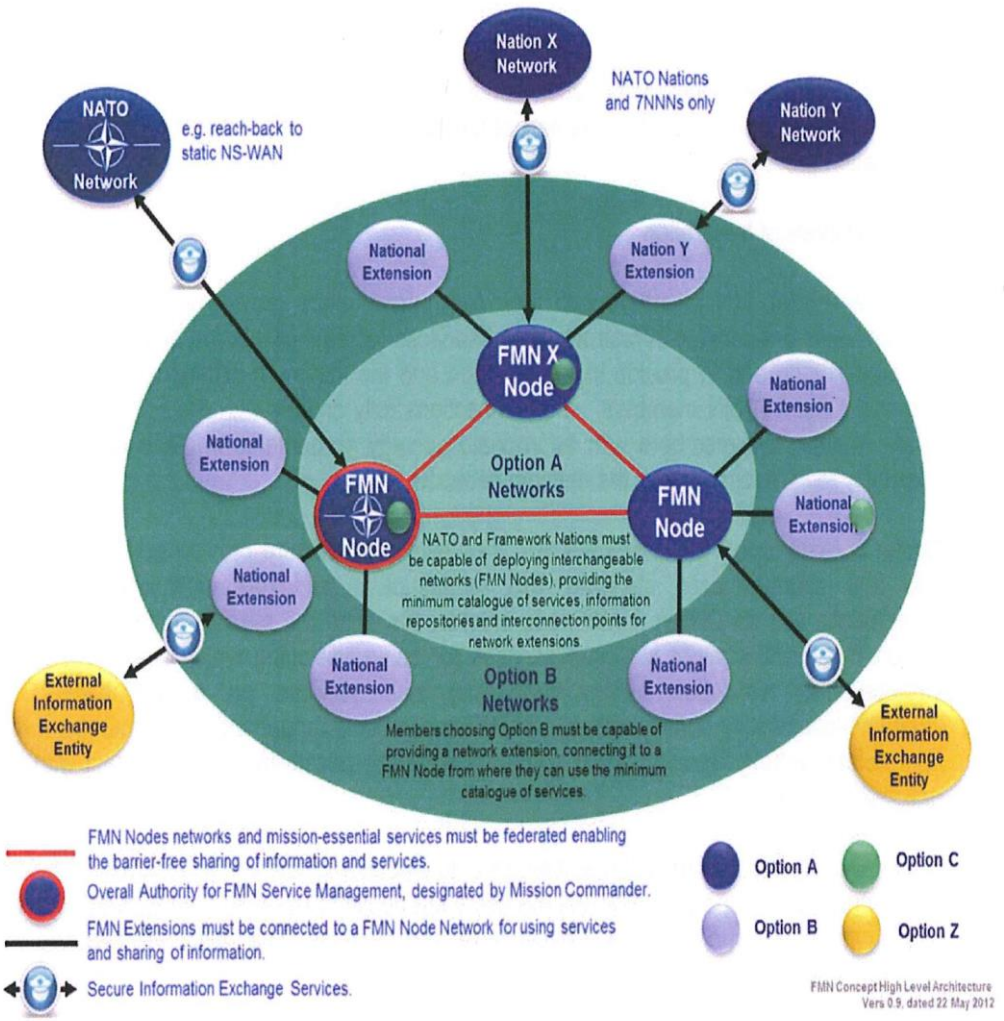
- lichtblauwe elementen (optie B) zijn die samenstellende elementen van het perifere netwerk. Zij breiden de absolute volumes van het netwerk uit en genieten overeenkomsten met de kern voor het gebruik van diensten die door de exploitatie van het netwerk mogelijk worden: het netwerk wordt gedragen door nationale bijdragen die op hun beurt diensten kunnen genieten die een nationale meerwaarde kunnen opleveren (bijvoorbeeld noodcommunicatie of beeldvorming met betrekking tot de evolutie van een natuurramp);

- een derde optie (groen) is een gastland van de twee eerdere opties: elementen van optie A en/of B worden gehuisvest door een derde die zowel de infrastructuur als de ondersteunende diensten levert. Ook in operaties is het daarom essentieel in te zien dat de sterkte van het gehele netwerk voor een deel zal berusten op bestaande en informatie- en andere infrastructuur. De overeenkomsten van optie A en B met deze partners zullen berusten op bilaterale akkoorden;

- occasionele partners van het netwerk kunnen op een beveiligde manier aansluiten bij het geheel. De modaliteiten voor gegevensuitwisseling worden voor ieder geval afzonderlijk bepaald alsook de informatie die ermee wordt uitgewisseld. Deze occasionele connecties vormen geen structureel deel uit van het uitgebouwde netwerk, maar kunnen zich in ieder van de operaties van de toekomst voordoen zoals ze in het verleden ook telkens voorkwamen.

De diensten die zich praktisch inschrijven in een dergelijke netwerkarchitectuur zijn onder meer logistiek, communicatie en informatiediensten (CIS), inlichtingen en verwerking van gegevens, commando en controle diensten, netwerkcommunicatie, dienstenbeheer en controle, informatieveiligheid, intrusiedetectie en basisdiensten zoals opslagcapaciteit, weergavecapaciteit enz.

Figuur 1: mogelijke FMN structuur (NATO, 2012).

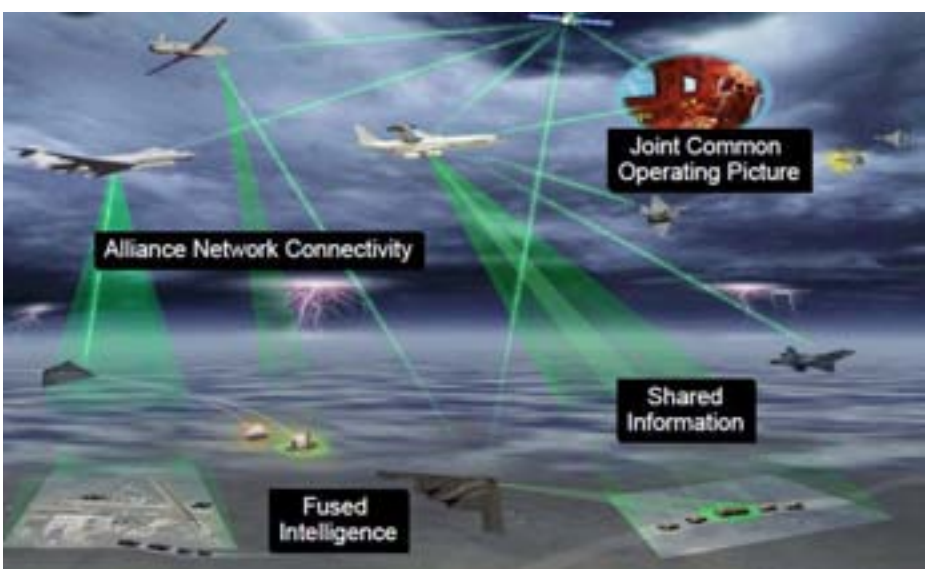


Voornoemde diensten moeten over het volledige geweldsspectrum de beschikbare eenheden toelaten om in de fysische en virtuele domeinen te opereren als een vereende *joint* kracht. Het belang van die *jointness* werd al eerder in dit werk aangehaald: dit zal helpen de doelstellingen van de operaties te behalen door het realiseren van een naadloze communicatie tussen eenheden en personen, een eenduidig zicht over het strijdtoneel, de tijdige voorziening van een netwerk, het tijdig afleveren van juiste en accurate opdrachtgegevens, het herkennen van operationele tekorten en ze verhelpen, het uitbaten van geoefende besluitvormingscycli. Maar tegelijkertijd heeft ieder domein op zich

een transitiefase door te maken wil het in staat zijn om op een geïntegreerde manier te kunnen interageren in operaties. Zo was heel specifiek voor het domein lucht al in 2007 in een stappenplan voorzien dat de weg moest afzetten naar de C4ISR-transitie. In de wetenschap dat de snelheid van denken en besluitvorming de beperkende factor is voor de besluitvorming in het gevecht voor de beheersing van het luchtruim, zo ook is de mens de beperkende factor voor de wendbaarheid van zijn bemande wapenplatformen. De overgang naar meer computergestuurde en minder bemande platformen vergde in het bijzonder voor de "luchtmachten" een nieuwe benadering, een nieuwe manier van denken over het voeren van het luchtgevecht en in de aanloop daartoe de gevolgen voor de samenwerking van inlichtingenvergaring en communicatie- en informatiesystemen (CIS). De samenstelling van de C4ISR capaciteiten, zelfs binnen de NAVO, is een samensmelting van nieuwe maar ook van oude systemen die werden samengevoegd door de operationele noden van het ogenblik. In dat opzicht was het vertrekpunt van de NAVO niet veel verschillend van dat van de EU en had de EU gebruik kunnen maken van die ervaring. Feit is dat de NAVO architectuur ondertussen, mede door de ervaring van operationele inzet een hele transitie heeft ondergaan, wat ontbreekt bij de EU. Maar zelfs bij de NAVO is er dus nog dat besef dat het groeiende systeem een operationeel compromis is van disparate systemen die samengevoegd zijn om het beoogde effect te bereiken.

Het beoogde einddoel van C4ISR, het ideaalbeeld als het ware voor het domein *air* wordt het best weergegeven door figuur 10.

Figuur 2: objectieven van C4ISR domein "air" (JAPCC, 2007; p. 8).



Destijds begon het al te dagen dat er geen allesomvattende of zelfs overkoepelende strategie bestond om het C4ISR-einddoel te bereiken, dat er een ontkoppeling bestond tussen besluitvorming en de ontplooiing van strijdkrachten, dat het overzicht op strategisch en operationeel niveau ontoereikend was, dat het informatiebeheer tekortschoot en ten slotte dat er een tekort was in terugkoppeling van getrokken lessen uit operaties in het genereren van nieuwe capaciteiten. Een illustratie daarvan bestond uit een breed spectrum aan sensoren en verwerkingssystemen binnen de NAVO, aangevuld met zuiver nationale systemen. In het totaal had West-Europa 143 radarbeelden te integreren met meerdere verschillende dataverwerkingssystemen: in dat opzicht kon men zelfs het gemeenschappelijke domein "air" niet als "geïntegreerd" beschouwen. De uitbreiding van het luchtbeeld werd al minder statisch door de integratie van het NATO Airborne Early Warning and Control System (NATO AWACS). Ook was er een cultuur van uniformiteit in de procedures, die zich vertaalde in zeer concrete instrumenten waardoor de luchtverdediging zich perfect kan integreren in een C4ISR-concept. Het nastreven van een gemeenschappelijk doel gebaseerd op een uniforme interpretatie van de gevechtssituatie werd bijvoorbeeld gematerialiseerd door de Air Order Directive (AOD) terwijl de interpretatie van het luchtbeeld afgebakend is door elementen als het Air Task Order (ATO) en het Airspace Coordination Order (ACO). Op zich zijn elementen als deze aanvulbaar met informatie uit de andere domeinen waardoor het luchtbeeld alle *battle space* informatie draagt. Dit leidt tot een geheel dat door alle domeinen tegelijk exploiteerbaar is. Dit zal tevens toelaten om de doelaanduiding (Target Acquisition - TA) ondubbelzinnig uit te voeren waardoor men van een C4ISR naar een C4ISTAR-architectuur evolueert en de vernietiging van eigen troepen ("blue on blue") beperkt wordt. De inspanningen om dat doel te bewerkstelligen werden verdeeld over NC3 Agency enerzijds en ACT anderzijds. Een van de belangrijkste opdrachten voor de NAVO is tegemoet te komen aan de noden van vandaag en tegelijk de destijds geïdentificeerde tekorten te compenseren. De gestaag gegroeide integratie in het domein "air" is niet voltooid gebleken maar de inspanning in dit domein naar C4ISR transitie kan als referentie dienen voor het onderzoek van andere domeinen naar de identificatie van nog bestaande tekorten zoals:

- Staan bestaande interoperabiliteitsstandaarden garant voor een geïntegreerd gebruik van middelen die het volledige spectrum van opdrachten kunnen dekken?

- Zijn de beschikbare middelen kwalitatief en kwantitatief afdoend (sensoren, effectoren, personeel)?

- Wordt de *joint* samenwerking optimaal benut zodat de coördineerde samenwerking een meerwaarde biedt en bestaat daarnaast ook een gecoördineerd samenwerkingsverband op interorganisationeel en interdepartementaal vlak?

- Bestaat er operationeel een echte gemeenschappelijke basis voor exploitatie van alle bruikbare informatie en in welke mate is het bestaan van meerdere geïsoleerde databanken een bron van vergissing of verwarring?

- In welke mate laat het bestaande netwerk toe om de uitwisseling van die informatie op een veilige manier mogelijk te maken?

Herinneren we er nog aan dat de NAVO in Europa het enige platform van betekenis is waar men die inspanning daadwerkelijk levert. Wat in NAVO-termen geïdentificeerde operationele tekortkomingen zijn, is op EU-niveau niet eens een vooropgestelde capaciteit.

Hoewel men naargelang de partner en om redenen die, zoals eerder uitgelegd, verband houden met de graad van maturiteit, eigen invullingen geeft aan de definitie van C4ISR, is men in de NAVO geëvolueerd tot een gemeenschappelijk begrip van het concept dat nog aan evolutie onderhevig zal zijn. De tendens die men kan verwachten in die evolutie wordt gekenmerkt door de volgende krachtlijnen:

- beslissingssuperioriteit kan enkel bekomen worden bij een gewijzigd gemoedsinstelling die zich in de praktijk zal weerspiegelen in een toename van de hoeveelheid gedeelde informatie: een benadering van deling van gegevens op basis van *need to know* zal evolueren naar een standpunt van *need to share*;

- de aanpassing van de procedures en de infrastructuur aan die nieuwe benadering met inachtname van de toegenomen expeditionaire eigenschappen van nieuwe opdrachten die op korte termijn tot stand moeten kunnen komen;

- een inzicht in een dreigingsbeeld dat rekening houdt met een sterker asymmetrisch karakter, wat impliceert dat het discriminerende vermogen van eigen strijdkrachten moet versterkt worden: het belang van de voormelde evolutie naar een C4ISTAR-architectuur wordt hierdoor onderbouwd;

- het samenvloeien van de afdeling inlichtingen met de C4SR-architectuur (waaronder de commando- en controleketen) welke vandaag nog te vaak de perceptie van concurrerende dienstverlening hebben: deze benadering onderstreept het belang van de menselijke factor van C4ISTAR terwijl vandaag de dag nog te veel de nadruk wordt gelegd op de zuiver technische benadering van het probleem;

- een engagementsduur die langer kan uitlopen dan vroeger waardoor de fasen van conflict tot reconstructie in elkaar overlopen en troepen ook hun informatie zullen moeten delen met andere actoren (humanitaire hulpverlening, ngo's,…).

Terwijl de eerste drie vereisten vooral de nadruk leggen op technische of procedurele aspecten, valt op dat de laatste ook het niet-technische in de verf zetten. We moeten eveneens onderstrepen dat een vrijheid van handelen vaak te maken heeft met kansvensters en dus een aspect tijd behelzen. In dat kader komt men ook hier tot het besluit dat een snelle besluitvorming en een snelle aanpasbaarheid vereist zijn, wat ook impliceert dat een lange latentie voor aankoopprocedures en een daaruit voortvloeiende verlenging van gebruik van hetzelfde materieel niet de beste garanties daartoe bieden.

Men kan zich in het verlengde daarvan afvragen wat de militaire implicaties zijn van die krachtlijnen. We hebben al eerder enkel concrete gevolgen van de theoretische aspecten aangekaart. Een interdepartementaal overkoepelende organisatie van het netwerk heeft ook gevolgen voor de krijgsmachten. Hier willen we een niet-exhaustieve blik werpen op de specifieke militaire implicaties van de krachtlijnen zoals eerder besproken. Vooreerst zal de strategie in een netwerkstructuur niet dezelfde zijn als voorheen: de concentratie van een groot aantal troepen is niet meer nodig en wordt vervangen door een concentratie van het effect door een breder en meer gediversifieerd pallet actoren. Zowel de planning als de uitvoering van een dergelijk systeem zullen sterk afwijken van wat eerder gebeurde: het aantal actoren dat vereist is voor het behaalde effect mag dan wel dalen in absolute waarden, het aantal soorten verschillende actoren die erbij betrokken zijn zal toenemen en dat is niet mogelijk zonder een duidelijke afbakening van verantwoordelijkheden en een aanpassing van de opleiding en de training. Deze benadering betekent ook dat de uitvoeringsfase sneller na de planning uitgevoerd kan worden. Hiervoor is een garantie nodig voor de beschikbaarheid van informatie die op dat ogenblik relevant is. Met informatie wordt zowel verwezen naar de gegevens van sensoren (zowel technische als menselijke middelen) als de verwerking ervan tot inlichtingen. De nood aan informatie zal bovendien leiden tot de noodzaak om permanent aangepast en beschikbaar gemaakt te worden voor de relevante gebruiker. Zowel de toegang tot

informatie als de verwerking ervan maar ook de verspreidingskanalen moeten hiervoor beveiligd worden. Deze beveiliging behelst zowel de zekerheid dat gevoelige informatie enkel door de bevoegde actoren kan worden geraadpleegd als ook het feit dat de beschikbaar gemaakte informatie niet moedwillig werd gewijzigd. Deze noodzaak maakt het zeer moeilijk om nog uitsluitend nationaal op te treden: de afhankelijkheid van externe bronnen of actoren maakt afspraken en ondersteunende infrastructuur wat dat betreft cruciaal voor het welslagen van de opdrachten zoals die in de toekomst mogen worden verwacht (DCDC, 2010; pp.36-37):

> "We should expect that operations will be increasingly interdependent. It will therefore be necessary to seek closer joint integration. Future operations are likely to be conducted in increasingly complex terrain. We must adjust capabilities for operations in the urban and littoral environment, where the people live; operations will be about influencing people. We must structure and train to provide persistent security effect, to operate closely with partners including indigenous forces and, where necessary, to enable the delivery of civil effect.… Future operations will be conducted in a competitive and complex information environment so we must develop the tool sets to fight and win the battle for influence – regionally, domestically and globally – and also in space and the cyber domains. Future operations will require the support of, and closer integration with, the other instruments of national power; the development of this 'super-joint approach' will be critical to success."

In een eerdere studie hebben we al aangegeven welke gevolgen die opdrachten zouden hebben voor de samenstelling van krijgsmachten en hebben we enerzijds het essentiële karakter van *jointness* onderstreept en anderzijds de nood aan een multi departementale aanpak van conflicten (Smedts, 2013; p. 75):

> "De inherente volatiliteit laat ons niet toe om een gedetailleerde omschrijving te geven van het capacitaire profiel in de toekomst. Veeleer zullen een aantal principes mee bepalen hoe het defensielandschap er mogelijk kan uitzien. We geven er hier enkele mee. Kwantiteit in de slagorde zal geen garantie meer bieden voor het behalen van een overwinning: eerder zullen kwaliteit, aanpassingsvermogen, publieke steun (perceptie van de bevolking), politieke steun (overeenkomend met de politieke agenda) en juridische steun (actie gestoeld op principes van het internationaal recht) sleutelbegrippen zijn bij het beheer van een conflict in de toekomst: *jointness* is een noodzakelijke maar geen voldoende voorwaarde voor succes. Pluridisciplinaire vaardigheden en een multi-departementale aanpak, die uitmondt in civiele-militaire

samenwerking en zelf partnerschappen met private bedrijven zijn daarom sleutelbegrippen in het beheer van een conflict. Aanpassingsvermogen zal ook bepalend zijn in het beheer van risico's en voor het genereren van veerkracht."

In het verlengde daarvan besloot de Noord-Atlantische Raad Tijdens de Top van Chicago (2012) om de data van *Alliance Ground Surveillance* (AGS-MOB Sigonella wordt AGS operationeel verwacht vanaf 2017), *NATO Airborne Early Warning and Control* (NAEW&C-MOB Geilenkirchen) en nationale bijdragen te integreren in een coherent geheel. Hierdoor worden verbanden gemaakt met nationale programma's in een multinationale context. Ook de integratie van projecten als *Multi-Intelligence All-Source Joint Intelligence Surveillance and Reconnaissance Interoperability Coalition* (MAJIIC) en *Battlefield Information Collection and Exploitation Systems* (BICES) worden concrete testmogelijkheden om de ervaring van de JISR-integratie tijdens de laatste operationele opdrachten (Aghanistan, Libië) te laten renderen in toekomstige operaties: hoewel de benaming het niet laat vermoeden, laat het MAJIIC-programma (sinds 2011 in zijn voorgezette versie MAJIIC2) toe om gelijk welke type sensor te integreren en niet enkel de al bestaande sensoren uit het domein "air". Zo is het ook mogelijk om ruimtesensoren, zee platformen, grondradars en zowel bemande als onbemande sensoren in het netwerk te integreren. Het BICES-systeem laat toe om, specifiek voor inlichtingen, een uitwisseling mogelijk te maken via het speciaal daarvoor ontworpen computernetwerk. Dit netwerk maakt een veilige uitwisseling van inlichtingen mogelijk tussen inlichtingendiensten van de bondgenoten maar ook met partnerlanden en de EUMS. Twee opmerkingen dringen zich hier op. Vooreerst stellen we vast dat er met dit systeem, dus ook voor de EU, een basis is om zich toe te leggen op de interoperabiliteit van haar toekomstige JISR-capaciteit die potentieel verder kan reiken dan enkele concrete maar disparate projecten die eerder werden aangehaald. Ten tweede is men genoodzaakt vast te stellen dat de voormelde projecten nog steeds een verzuiling van inlichtingen materialiseren ten opzichte van andere (sensor-)informatie. De vooropgestelde *jointness* kan slechts tot stand komen met een integratie van die beide aspecten op straffe van het behoud van een gescheiden architectuur tussen de C4SR-zuil enerzijds en anderzijds de I-zuil.

Het is duidelijk dat de C4ISR-interactie slechts die sterkte heeft als de zwakste van alle geïntegreerde domeinen. Anderzijds is het ook zo dat nieuwe domeinen als cyber zullen moeten beveiligd worden wil men kunnen beschikken over een exploiteerbaar platform.

De tenuitvoerbrenging of ontwikkelingslijn van een C4ISR-concept zal moeten voldoen aan enkele principes die kaderen binnen de algemene transitie

naar interoperabiliteit die overkoepelend is voor alle aankopen en procedures van de Alliantie. Vooreerst is een netwerk zoals C4ISR-integratie vereist niet denkbaar zonder aanpassing van doctrine. De ervaringen uit Afghanistan zullen daarom belangrijk zijn: de praktische ontwikkelingen voor de realisatie van de opdrachten en de integratie van de verschillende domeinen hiertoe geven voor de toekomst aan wat werkbaar is en wat niet. De lessen uit Afghanistan zijn niet louter politiek maar hebben ook operationele gevolgen. De vastgelegde doctrine zal zich onmiddellijk weerspiegelen in de organisatie: zowel de transitie naar *jointness* als de nieuwe genetwerkte structuur zullen een soepele invulling vereisen van wat het organogram voorstelt. De nationale trainingsconcepten zullen bijgevolg ook moeten kaderen binnen de nieuwe benadering die de Alliantie onderschrijft: multilateralisme en interoperabiliteit worden daarom de hoekstenen van het merendeel van de opdrachten in de toekomst. Het materieel, los van de gemeenschappelijke eigenschappen die gedragen worden door die interoperabiliteit zal zo veel mogelijk moeten worden hergebruikt: het gebruik, van bestaande capaciteit moet zich daarom integreren binnen het kader van de nieuwe opdrachten. Het kan daarom belangrijk zijn om legaatinvesteringen te herevalueren met betrekking tot hun relevantie: de aanwending van het juiste materieel voor de juiste opdracht op het gewenste tijdstip vormt een van de uitdagingen in de toekomst. De transitie naar *jointness* is geen eindpunt en moet slechts een baken zijn naar een genetwerkte structuur: dit zal enkel mogelijk zijn indien de leiders (zowel politieke als militaire) van alle partners overtuigd zijn van het grens- en departement overschrijdende karakter van de toekomstige opdrachten. Deze gedachte kan zich enkele vertalen in opdrachten indien ook het personeel daarvan overtuigd is, in die zin wordt opgeleid en op een flexibele manier kan omgaan met de aanpassingen aan een nieuwe omgevingen en manier van werken.

Het mag duidelijk zijn dat we in de toekomst meer dan vroeger zullen inspelen op het aanbod van de private sector. Daaruit besluiten dat het de agenda is van de private sector die zal bepalen hoe het technologische beleid er moet uitzien is een brug te ver: commerciële bedrijven hebben immers hun commerciële doeleinden te vervullen terwijl de overheid in de eerste plaats moet ervoor zorgen haar strategische objectieven en prioriteiten te definiëren enerzijds en anderzijds vast te leggen hoe (lees op welke manier en met welke middelen) ze die wil bereiken.

De belanghebbers, zowel op beleids- als gebruikersniveau maar ook op verkopersniveau zijn niet altijd eensgezind in de koers die bewandeld dient te worden. Vanuit commercieel oogpunt zijn het uiteraard de commerciële belangen die primeren: een technologisch beleid dat door producten wordt aangestuurd kan daarom geen overkoepelende strategie opleveren die ook de

belangen van een alliantie zal nastreven. Daarmee wordt het belang van de technologische insteek niet onderschat: de input van onderzoek en industrie zijn belangrijk om een geactualiseerd zicht te hebben van wat reilt en zeilt in dit snel veranderende domein. Een strategie moet echter daarboven uittorenen en de algemene richting verankeren, de prioriteiten stellen waarvoor men instaat en wat men wil veiligstellen: een strategie gaat nog een stap verder dan een concept en legt de verantwoordelijkheden en bevoegdheden vast van elk van de betrokken actoren en kan tegelijk een gemeenschappelijk verzoenend standpunt innemen ten opzichte van soms tegenstrijdige belangen (cfr. commercieel versus staatsbelang).

Om die belangen te behartigen en de inspanningen te stroomlijnen, heeft men een aantal aandachtspunten willen onderlijnen die kunnen bijdragen tot een coherente uitbouw van een C4ISR-architectuur (JAPCC, 2007; pp. 27 e.v.):

-verspreide belangen: verschillende verantwoordelijken gaan verschillende agenda's opvolgen en dit zal niet noodzakelijk bijdragen tot een coherent geheel. C4ISR is een ruim project met een impact in verschillende domeinen. Toch moet de verantwoordelijkheid binnen één coördinerend orgaan gecentraliseerd worden;

-interoperabiliteit: omwille van het ruime bereik van de architectuur, zijn er *de facto* afhankelijkheden tussen diensten. Een inzicht in mogelijke afhankelijkheden en belangen voor het delen van informatie zal daarom bijdragen tot een meer geïntegreerd beeld. Het inzicht in afhankelijkheden kan ook bijdragen aan de motivatie om te streven naar interoperabiliteit;

-nieuwe leden: de vernetwerking van onze samenleving heeft ook de procedures binnen krijgsmachten er niet eenvoudiger op gemaakt. De meeste van de landen hebben die echter zien groeien en evolueren terwijl ze lid waren van de Alliantie en hebben daarom een geschiedenis in de constructie en het onderhoud van een gemeenschappelijk dreigingsbeeld. Nieuwe leden missen die voorgeschiedenis en zijn geconfronteerd met een technische en procedurele revolutie die verbonden is aan hun toetreding tot de Alliantie. In het bijzonder de transitie tijdens de implementatie van wat men van het oorspronkelijke ACCS-programma nog wil overhouden zal bijzondere aandacht vergen van en voor nieuwe leden. Het belang om nieuwe leden te integreren zonder daarom vertraging op te lopen met de verdere integratie van systemen is belangrijk;

-ondersteuning: de korte reactietijd en het snel evoluerende dreigingslandschap vragen ook een snelle reactiesnelheid van planning en ondersteuning van operaties;

-leidraad: de eerder gedane vaststelling van het gebrek van een overkoepelend beleidsdocument met betrekking tot C4ISR moet worden rechtgetrokken. Zowel de verantwoordelijkheden als de transversale samenwerking dienen in die leidraad te worden onderstreept;

-opleiding en training: de gedeelde verantwoordelijkheid van zowel de NAVO als organisatie als de bondgenoten individueel zou ervoor kunnen zorgen dat in het domein dat ons aanbelangt overlappingen tot stand komen. De uitgebreide waaier aan opdrachten die in het kader van de NAVO aan actoren wordt toevertrouwd maakt er de uitvoering ervan niet eenvoudiger op. De afbakening en verdeling van verantwoordelijkheden met betrekking tot opleiding en training kan meer doorgedreven samenwerking bevorderen en tegelijk minder individuele inspanning vragen van de bondgenoten;

-*joint* omgeving: C4ISR-integratie kan een meerwaarde bieden op elk uitvoeringsniveau van de opdrachten. Tot vandaag is men in Europa echter nog te veel ingesteld op de optimale integratie van componenten en machten in een *joint* structuur. De exploitatie van C4ISR zou veel meerwaarde kunnen bieden aan die *joint* structuur die geen eindpunt mag zijn in de transitie en evolutie van een moderne krijgsmacht;

-middelen: het gebruik van nieuwe middelen of de upgrades daarvan (zoals NATO Airborne Early Warning and Control - AEW&C) vraagt om voortdurende aanpassing van concepten en procedures;

-beheer van systemen: het bestaan van het luchtverdedigingsbeeld heeft een canvas gecreëerd voor de transitie naar Air C4ISR. De nieuwe systemen die naast het JTIDS-netwerk werden ontwikkeld moeten echter aansluiten bij de behoeften en de structuren die al werden uitgewerkt. In de rij van die nieuwe systemen tellen we de eerder vermelde AWACS-upgrades maar ook bijvoorbeeld ACCS, AGS, BiSC-AIS, BICES of geselecteerde elementen van deze respectievelijke systemen. De diensten die door deze verschillende systemen kunnen geleverd worden zullen bijdragen tot de verdere ontwikkeling van C4ISR vanuit het geïntegreerde luchtbeeld. Het huidige probleem is de veelheid aan gegevens, door die systemen gegenereerd, te beheren en te integreren in een uitbaatbaar geheel: NATO C4ISR in wording. Elk van die projecten is echter geïsoleerd en het beheer combineren en sturen vormt een

afzonderlijke uitdaging: de moeilijkheid is een overzicht te bewaren en een overkoepelend beleid tot stand te brengen. Het voordeel waarop de NAVO kan rekenen ten opzichte van de EU, waar ook een veelheid aan geïsoleerde projecten tot stand komt, bestaat erin dat ze kunnen gehecht worden aan een bestaande en dragende structuur. De synchronisatie van de programma's en de afstemming van de *deliverables* is een vereiste wil men tot een coherent en bruikbaar geheel komen. Om het met de woorden van ACT te zeggen:

"We must build on our existing capabilities. Transformation is not an end in itself but must be driven by what is required to succeed in today's and tomorrow's engagements. ACT ensures that NATO and nations, when faced with the inevitable defence and security challenges of a complex tomorrow, have the right capabilities, procedures, processes and training needed to meet their obligations and to work effectively with others" (Generaal Stéphane Abrial, Supreme Allied Commander Transformation-SACT).

Naast het ACCS-programma is ook een parallelle systeemontwikkeling tot stand gekomen die vooral bedoeld was ter ondersteuning van ISAF-operaties. De geïntegreerde Command and Control Software voor Air Operations (ICC) is een geïntegreerd Command, Control, Communications and Intelligence / Information (C3I2) platform dat informatie management en ondersteuning toelaat ten voordele van de besluitvorming van de NAVO-luchtexploitatieactiviteiten vanaf vredestijd tot oorlogstijd. Het systeem werd ontwikkeld door het NCI Agentschap en werd onderhouden in een samenwerkingsverband met het NPC (applicatie software ontwikkeling, COTS software onderhoud, hardware en software kwaliteitscontrole). ICC biedt functionele ondersteuning voor de meest kritische commando- en controlefuncties in het domein Air ten voordele van de Component Commander en CAOC (Combined Air Operations Centre) niveaus. De ondersteunde functionaliteiten omvatten planning en tasking, generatie van Air Operations order, Airspace Control Orders, gezamenlijke doelaanduiding, genereren van Air Tasking Orders (dus zowel offensieve als defensieve opdrachten). Het ICC-platform levert een regionale erkend luchtbeeld (RAP) aan het NAVO-hoofdkwartier en ondersteunt de verspreiding van snelle waarschuwing (Shared Early Warning - SEW). Beide systemen zijn niet bedoeld om naast elkaar te blijven bestaan: ICC heeft op kortere termijn toegelaten om een leerproces op gang te brengen die de netwerking ten goede komt. Waar nodig is een interface mogelijk tussen ACCS en ICC en de operationele leerjaren van ICC dragen bij aan de verdere maturatie van ACCS en zal dit systeem zeker niet vervangen.

-praktische implicaties: aan de realisatie van de doelstellingen zijn een aantal praktische gevolgen verbonden. De netwerkcapaciteit van de NAVO dient verder uitgebouwd te worden met als doel zowel de informatievergaring en de exploitatie van gegevens (ISR) te verbinden met het luik commando en controle (C2). Dit kan alleen indien het Bilateraal Strategisch Commando (Bi-SC), ACO en ACT het overzicht bewaren om bestaande communicatiesystemen te integreren: het geheel zal de vormgeving materialiseren van NNEC. Verder zullen de tactische datalinks voor een beperkte tijd nog in gebruik zijn naast het bestaan van een IP-gebaseerde communicatie. Ook zijn de verdere updates van het E-3A-systeem nodig om de netwerkcompatibiliteit te garanderen: oorspronkelijk werden alle opdrachten uitgevoerd door dit platform aan de hand van TDL's. Door de overgang naar IP-gebaseerde technologie is men ook voor dit platform gedwongen om een migratie naar nieuwe communicatiemiddelen uit te voeren.

1.5. Cyberoperaties en NNEC

De in een vorig hoofdstuk aangenomen definitie van C4ISR leidt onvermijdelijk tot een afhankelijkheid van informatie- en communicatietechnologie (ICT) voor de constructie van een architectuur: zowel de fysische beveiliging als de beveiliging van de informatie staat centraal in C4ISR-systemen. De aandacht in de VS met betrekking tot deze problematiek is al langer aan de orde van de dag. Op het einde van de vorige eeuw werd al nagegaan welke de praktische gevolgen konden zijn van gerichte aanvallen op civiele en militaire communicatiesystemen en stroomvoorziening op de werking van Defensie (Eligible Receiver 1997; Solar Sunrise 1998). Voornamelijk gericht op het testen van de informatieveiligheid werd nagegaan in welke mate de systemen van Defensie konden worden gepenetreerd, data gestolen of gewijzigd of zelfs besmet kon worden door schadelijke software. Nog tien jaar duurde het vooraleer het ook voor de publieke opinie duidelijk werd dat een virtueel platform aanleiding kon zijn tot fysische schade. De Stuxnet-worm was hiertoe de aanleiding: na analyse bleek dat het doel van Stuxnet de wijziging was van industriële controlesystemen (Supervisory Control and Data Systems - SCADA) door de programmeercode te wijzigen, terwijl de toezichthouders van het systeem geen argwaan kregen. Naar de vorm zou alles normaal verlopen, terwijl de sensoren zouden moeten aangegeven hebben dat er abnormale parametergegevens vastgesteld werden (bijvoorbeeld in de frequentie van centrifuges). De specificiteit van deze aanval bleek door het gerichte karakter: de code werd geschreven om zich specifiek op Siemens' *operating system* te werpen en controleerbaar te maken door externe operatoren (Symantec, 2011; p.3). Dit is merkwaardig daar de controle van het netwerk niet gebeurde via een connectie met een extern netwerk. Men spreekt in dit geval over een *air gap,* met andere woorden de gesaboteerde code moet via een externe drager in het systeem geladen worden. Men gaat ervan uit dat in dit geval een geïnfecteerde USB-drager en/of een draagbare computer gebruikt werden. Eenmaal geïnfecteerd kon de artificiële code zich via het interne netwerk verspreiden. De malware werd pas tijdens de zomer 2010 ontdekt terwijl het aangenomen is dat dit al minstens een jaar actief was en drie selectieve aanvalsgolven omvatte. Uiteindelijk bleek dat naast aanrijkingsfaciliteiten voor uranium ook persoonlijke computers in een Iraanse kernreactor (Bushehr) besmet werden. Oorspronkelijk dacht men dat deze reactor het hoofddoel was, maar de Stuxnet-codes maken die hypothese

onwaarschijnlijk: het einddoel van Stuxnet was de infectie van specifieke programmeerbare controlesystemen (Programmable Logic Controller - PLC) die de rotatiefrequentie van centrifuges bepalen. Vandaar ook de mogelijkheid om de aanrijking van uranium te verstoren en de centrifuges fysisch schade toe te brengen via het virtuele platform. De besmetting in Iran omvatte bijna 60% van alle door deze *malware* veroorzaakte infecties: ondanks de zeer gerichte aanval bleek collaterale besmetting dus onvermijdelijk. Wat door *Farwell en Rohozinski* bestempeld werd als een 'fire-and-forget'-*malware*, blijkt in de praktijk ook gevaren in te houden voor ander gebruikers die niet noodzakelijk op de hoogte zijn van een gerichte aanval. Vooreerst maakt dit mogelijk dat militaire offensieve cybertoepassingen burgers gaan treffen zonder de noodzakelijke discriminatie- en proportionaliteitsvereisten te kunnen aanwenden die de wet op de gewapende conflicten voorschrijft voor het rechtmatig gebruik van geweld. Bovendien laat dit de mogelijkheid bestaan dat een cyberwapen na aanwending ook eigen capaciteiten zal besmetten, naar analogie met een biologische besmetting. Dit kan gespreid in de tijd voorkomen, waardoor permanente waakzaamheid vereist is na het gebruik van een dergelijke methode. In het geval van ons voorbeeld blijkt dit ook gebeurd. Een gedeelte van de code werd na het incident teruggevonden in gewijzigde vorm. Wat op het eerste gezicht deed vermoeden dat nog een eerdere versie van de Stuxnet-code op het netwerk actief was (Duqu), bleek later een herschreven versie met als doel informatie te bekomen over industriële systemen. Het had als voornaamste taak data te stelen uit servers en die op regelmatige basis door te sturen naar niet nader geïdentificeerde actoren.

De vaststelling van deze aanvallen "op maat" van respectievelijk het Iraanse uraniumaanreikingsprogramma en economisch-industriële data, was een aandachtspunt voor technici maar ook voor politieke leiders: voor het eerst was het duidelijk dat bestaande netwerkconnecties niet voldoende beveiligd waren, zelfs indien ze op lokale netwerken opereerden. Met dit inzicht werd duidelijk dat het merendeel van wat men vandaag aanziet als kritieke infrastructuur (zie verder) een gemakkelijk doelwit zou kunnen worden voor kwaadwillige actoren (staten of niet-staatsactoren). De afhankelijkheid van private partners, die het merendeel van de netwerken beheren, maakt de beveiliging vandaag nog bijzonder moeilijk regelbaar. De economische beperkingen hebben bovendien geleid tot een toename van commerciële producten in toepassingen voor defensie, wat aanleiding gaf tot nieuwe gevoeligheden: commerciële systemen (hard- of software) zijn niet altijd afgestemd op een optimale beveiliging. Daarenboven toont het voorbeeld van de Duqu-code aan dat industriële gegevens gestolen kunnen worden van systemen die later door een krijgsmacht zouden aangekocht kunnen worden. Ook de aansluiting van bestaande sensoren op het informatienetwerk biedt nieuwe uitdagingen voor de beveiliging en de exploiteerbaarheid van de

sensorgegevens: de vraag stelt zich meer bepaald hoe te kunnen garanderen dat de gegevens van bestaande sensoren niet worden gelezen door partijen die geen bestemmeling zijn van de data, dat de doorstroming van de gegevens niet wordt verhinderd of nog dat de gegevens niet worden gewijzigd). Vast staat dat voormelde incidenten nieuwe inzichten hebben gegenereerd in de prioritering van de cyberdreiging. Bijlage 1 geeft een overzicht van een dergelijke prioritering alsook de omschrijving van die dreiging en de (nationale) autoriteit die de leiding heeft bij het nemen van maatregelen (Rand, 2013; pp. 9 e.v.). De in bijlage omschreven dreiging toont aan dat er nog een duidelijk verschil bestaat in de perceptie: zo is er in Scandinavische landen vooral een dreigingsinschatting die gepaard gaat met financieel verlies, terwijl in Angelsaksische landen (VK, VS, Canada) meer nadruk gelegd wordt op hackers, criminele netwerken en terroristen. Slavische landen (bijvoorbeeld Rusland) leggen dan weer de nadruk op het onderscheid tussen interne (criminaliteit en corruptie) en externe dreiging (staten, terrorisme, buitenlandse competitie). In de agentschappen die gemandateerd werden om de respons te genereren valt de grote verscheidenheid aan uitvoerende organen op binnen de organisatie van de Europese Unie (EU), terwijl dat nationaal, maar ook bij de NAVO een eerder gecentraliseerde uitvoering blijkt te zijn. Ook hierdoor stelt men in de praktijk een verschil in perceptie van de dreiging vast. Of de dispariteit binnen de EU te wijten is aan een gebrek aan dreigingsidentificatie dan wel aan coördinatie van de inspanningen is niet duidelijk.

Dat enkel de EU een dergelijke dispariteit vertoont, is niet te verklaren door het gebrek aan definities of procedures. Alle actoren werken wat dat betreft met dezelfde werktuigen. Alleen zorgt het wegblijven van een gemeenschappelijke omschrijving van deze dreiging en overeengekomen actiepunten tot grote verschillen in aanpak. Het zorgt bovendien voor een wildgroei aan definities en termen die al naargelang de perceptie van de betrokken actoren een andere betekenis krijgen: in het beste geval zullen we zien dat de aangenomen definities worden weergegeven in het nationale standpunt (beleidsdocumenten zoals *policy* of *strategy*). Deze onenigheid is trouwens niet eigen aan het cyberdomein: of men nu spreekt over oorlog, terrorisme, criminaliteit, spionage of *hacking*, in vele domeinen is men het oneens over de afbakening van de term. Dit maakt ook de organisatie van de bestrijding ervan moeilijk omdat nationale en meer nog internationale verantwoordelijkheden niet kunnen vastgepind worden. Als de bepaling van definities belangrijk is voor het bepalen van verantwoordelijkheden, stelt men tevens vast dat operationele capaciteit geen beperkende factor is. In vele gevallen zijn operationele actoren het eens over de elementen die in een goede cyberstrategie in aanmerking moeten worden genomen (Future ISR, 2012; Folmer): het verhogen van de kennis en de expertise, intensieve interdepartementale samenwerking, het integreren van inlichtingenvergaring in

cybercapaciteit, de ontwikkeling van militaire capaciteit en de afbakening van haar verantwoordelijkheden. Over de tendensen betreffende cybertoepassingen is men het grotendeels eens: het is een reeks vaststellingen die als gevolg hebben dat cyber nog jaren herhaaldelijk in de agenda's van de wetgevende, uitvoerende en rechterlijke macht zal blijven opduiken. Vooreerst blijkt de asymmetrische factor belangrijk te zijn: kleine actoren of niet-staatsactoren hebben weinig nood aan investeringen om hinder te laten ondervinden bij anderen. Hierdoor krijgen ook kleinere landen een forum en wordt het hun mogelijk gemaakt om een vorm van *soft power* te genereren. Vervolgens blijken offensieve technieken, door de beperkte attributie mogelijkheden, relatief meer slaagkans te hebben dan defensieve opstellingen: men is immers niet in staat om het volledige netwerk af te schermen. Om die reden blijft dit domein ook voor de grootmachten een uitdaging. Ten slotte merkt men dat private actoren een niet onbelangrijke rol spelen: hoewel de beslissingsbevoegdheid en de regulering bij de overheid gevestigd zijn, is het overgrote deel van de infrastructuur in privaat bezit. Zoals later zal blijken is deze problematiek gelijkaardig aan deze van de energie-infrastructuur. Door het grensoverschrijdende karakter is men ergens geneigd om zich tot de overheid te richten als belangrijkste spreekbuis voor de internationale regelgeving, maar tegelijk weet men dat de eigenaars van het netwerk niet bereikt worden.

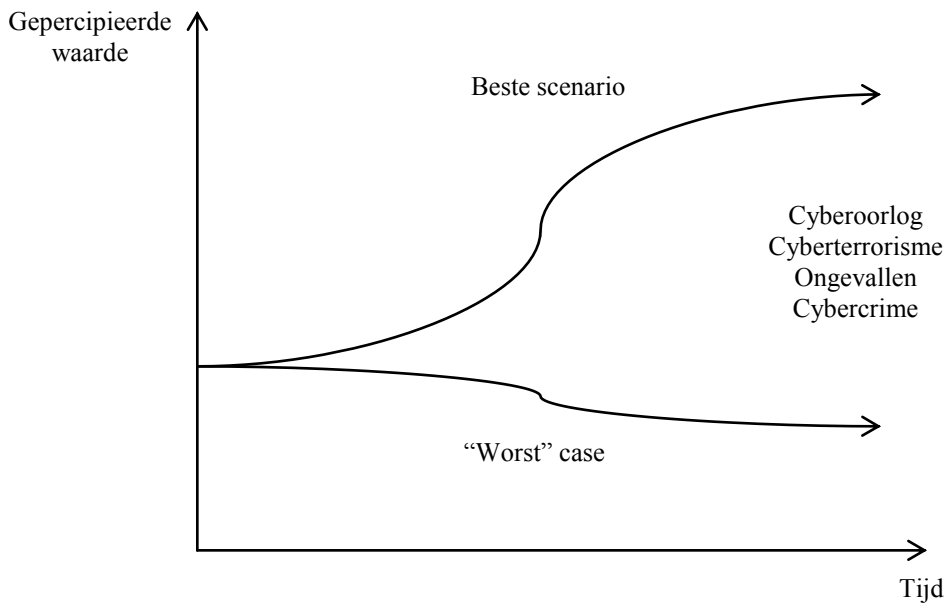
In welke zin voornoemde tendensen een dreiging vormen is afhankelijk van de "militarisatie" van de toepassingen, met andere woorden of de tendensen gebruikt kunnen worden met militaire doeleinden: hoewel men in de literatuur niet over een eensgezind standpunt kan beschikken, is men het wel eens over het feit dat een aanval met als doel een tegenstander fysische schade te berokkenen of fysisch te hinderen, niet uitsluitend door middel van het cyberdomein kan bereikt worden. In dat opzicht is het bestaan van dit domein niet veel verschillend van de andere (zee, land lucht, ruimte): men zal eerder een combinatie van middelen moeten inzetten om een grootschalig effect te bekomen. Het gevolg daarvan is wel dat militaire toepassingen oog zullen moeten hebben voor de eigenheid van de architectuur van het virtuele platform. Afhankelijk van de omvang en de aard van de ingezette middelen kan men immers een grotere perimeter beveiligen. Meer middelen mobiliseren in het virtuele domein heeft niet noodzakelijk als gevolg dat men het virtuele netwerk beter kan beveiligen. In een eerste benadering kan men hieruit besluiten dat men een verdedigbaar netwerk moet creëren in de plaats van een veilig netwerk. Ieder virtueel platform zal immers een of andere intrinsieke zwakheid vertonen die met tijd en middelen kan omzeild worden. De behaalde veiligheid zal daarom een gelaagdheid moeten vertonen: in de plaats van de fysische perimeter stelt men een beveiliging in de diepte voor. Hoe belangrijker de gegevens en het netwerk, hoe moeilijker het moet zijn om de beveiliging ervan te omzeilen. Een moduleerbare en flexibele structuur, afhankelijk van de noden

van het ogenblik, schijnt op het eerste gezicht beter geschikt dan een statische structuur. De samenwerking tussen civiele en militaire actoren, tussen publieke en private partners lijkt daarom de beste keuze. Op overheidsniveau zal een interdepartementale aanpak waarschijnlijk tot de beste resultaten leiden. De operationele militarisatie van het cyberdomein zal *jointness* afdwingen. In deze architectuur is het immers niet mogelijk een perimeter af te bakenen en te beveiligen zoals dat fysisch wel het geval is. Hoewel a priori een zeker vergelijk mogelijk is tussen het synthetische domein en de fysische domeinen, zijn we genoodzaakt om ook de verschillen in te zien. Er is een duidelijk verschil met bestaande doctrines van andere domeinen: hooguit laten ze toe om een eerste benadering van de noden te omschrijven. We zullen in het deelbesluit op deze bemerking terugkomen en uit de bestudeerde aspecten nagaan of verdere elementen van onderzoek inderdaad kunnen leiden tot een dergelijke conclusie. Internationale fora met betrekking tot deze discipline leggen in afwachting van een dergelijk antwoord op nationaal vlak de nadruk op een vrijblijvende gedragscode in cyberspace, zonder verplichtingen noch internationale verdragen. Eerder wordt de nadruk gelegd op het uitwisselen van beste praktijken om economische groei te stimuleren, mensenrechten na te leven en toch te kunnen voorzien in cyberveiligheid, vergaring van inlichtingen en bestrijding van cybercriminaliteit. In dat opzicht wordt de cyberdimensie aanzien als een kritieke economische facilitator. In dat opzicht heeft het beperken van veiligheid of het wegblijven van operationele doctrines een impact op de economische welvaart van een land en mogelijk zelfs van de wereldeconomie.

De perceptievraagstukken met betrekking tot wat cyberveiligheid zou moeten voorstellen is belangrijk: teren op het vertrouwen in de goede werking en het verantwoordelijke gebruik van het virtuele platform is niet meer mogelijk gezien de zwakheden die aan het licht gekomen zijn sinds de ingebruikname van het oorspronkelijke netwerk en de dimensies die het nu heeft bereikt (Isaac Ben-Israel in SDA 2012). Bovendien hebben heel wat landen een offensieve activiteit ontwikkeld, al was het maar om zich “met alle beschikbare middelen” te kunnen verdedigen wanneer ze aangevallen worden. De perceptie van een al maar ingewikkelder systeem met connectie van een exploderend aantal perifere sensoren of controlesystemen zal een nieuwe visie vergen voor de organisatie van de veiligheid: hoe kunnen industriële gegevens en data beveiligd worden indien ze fysisch niet meer opgeslagen worden op de plaats van exploitatie? Wie is juridisch gezien eigenaar van die gegevens en wie is verantwoordelijk voor hun beveiliging: deze vragen zijn opgedoken bij het ontstaan van nieuwe mogelijkheden in stockage en werkgeheugen (*cloud computing*) en wijzigen eveneens de perceptie van de cyberveiligheid. De gepercipieerde veiligheid is het gevolg van wat zich op het virtuele platform afspeelt (met inbegrip van internet omschreven als wereldwijd

informatiesysteem dat bronnen van informatie met elkaar verbindt en informatie laat uitwisselen door gebruik van bepaalde vastgestelde protocollen (waaronder IP) of hun logische uitbreidingen - eigen vertaling van Kahn, 2013; p. 208).

Figuur 3: extrema die de perceptie van cyberveiligheid bepalen (Schwartz, 2011; p. 227).



Het aantal incidenten en hun impact zullen de waarde bepalen die de samenleving aan het virtuele platform wil geven in de toekomst. Uitgaande van een projectie van de penetratiegraad van het informatienetwerk zou men geneigd zijn te denken dat die waarde enkel kan toenemen. In dat geval bevindt men zich volgens Schwartz in één extremum, het ideale scenario waarin de toegang tot internet gedemocratiseerd is (en driemaal zoveel connecties kan tellen dan de wereldbevolking). De activiteiten worden in dat geval meer beveiligd tegen criminele activiteit en niet-staatsactoren die opereren als *proxy*. De offensieve cybercapaciteiten van staatsactoren ervaren een zekere ontrading door de verstrengeling van verantwoordelijkheden en wederkerende effecten. De toegenomen zichtbaarheid en identificatievereisten bij gebruik zorgen voor een toename van het verantwoordelijkheidsbesef. Aan de andere zijde vindt men het worstcasescenario waarin de gepercipieerde waarde voor de samenleving afneemt. De aanleiding daarvan zijn voortdurende aanvallen en conflicten, het gebrek aan organisatie van de beveiliging of visie. Een aantal tendensen zijn volgens Schwartz onontbeerlijk om de richting van de eindbestemming te kunnen ontwaren:

- de snelheid van de technologische evolutie;

- de aanpasbaarheid van de huidige internetarchitectuur voor beveiligingsvereisten;

- de toename van (sociale) controle en de afname van internationale spanningen;

- de toename van het vertrouwen in de instellingen en het beleid.

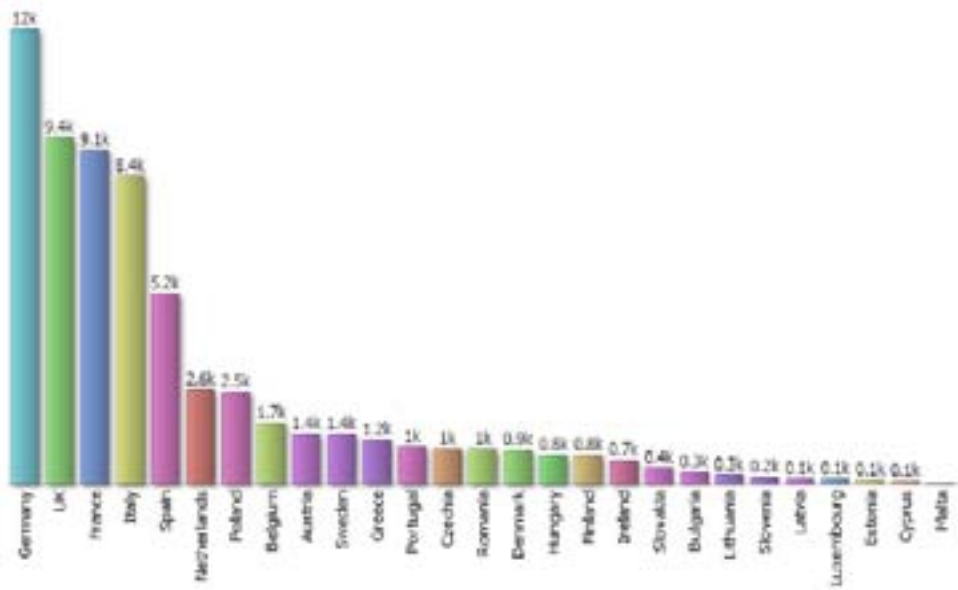
De werkelijke toekomst van wat de maatschappij denkt te kunnen winnen bij de uitbating van het virtuele platform ligt waarschijnlijk ergens in het midden: incidenten en criminaliteit (misschien zelfs sommige fasen in oorlogvoering) zullen niet uitblijven, maar de mogelijkheid om in de goede richting te evolueren blijft bestaan, zonder daarom aan de utopie te grenzen.

Even belangrijk is de perceptie dat samenwerking geen bedreiging vormt voor de eigen soevereiniteit. De algemeen aanvaarde definitie van deze term rust op een tekst die dateert van 1928, periode waarin nog geen sprake was van cyberspace: de definitie legt de nadruk op de territoriale onafhankelijkheid en de rechten en plichten te vervullen met exclusieve rechten (Island of Palmas, 2 R.I.A.A. 829, 838 (Perm.Ct.Arb. 1928)). Een aspect dat eigen is aan de cyberdimensie en de territoriale dimensie overstijgt omvat juist grensoverschrijdende afspraken over de organisatie van een veiliger cyberlandschap en mogelijk sancties voor wie zich daar niet aan houdt. In het minst restrictieve geval zullen in het leven geroepen vertrouwenwekkende maatregelen zorgen voor een internationale samenwerkingsbasis. Die geven andere instanties een soort inzagerecht of verificatierecht, met andere woorden men kan niet op een volledig verdoken wijze handelen volgens eigen normen zonder dat het gedetecteerd kan worden door andere partijen. Hierdoor verliest men een zekere maat van zelfbeschikking of alleszins vrijheid van handelen. Het beginsel van territorialiteit mag hier al dan niet vernoemd worden, maar in het post-Westfaalse staatsconcept waarin het belang van geografische grenzen vervaagt, is net die vrijheid van handelen in het beschikbare opportuniteitsvenster een laatste “strohalm” van soevereiniteit die overblijft. Dit beperken zou economisch en/of politiek nadeel kunnen opleveren. In de gegeven economische omstandigheden is dit evenredig met zichzelf te benadelen in een arena van concurrenten die elk hun eigen belang najagen.

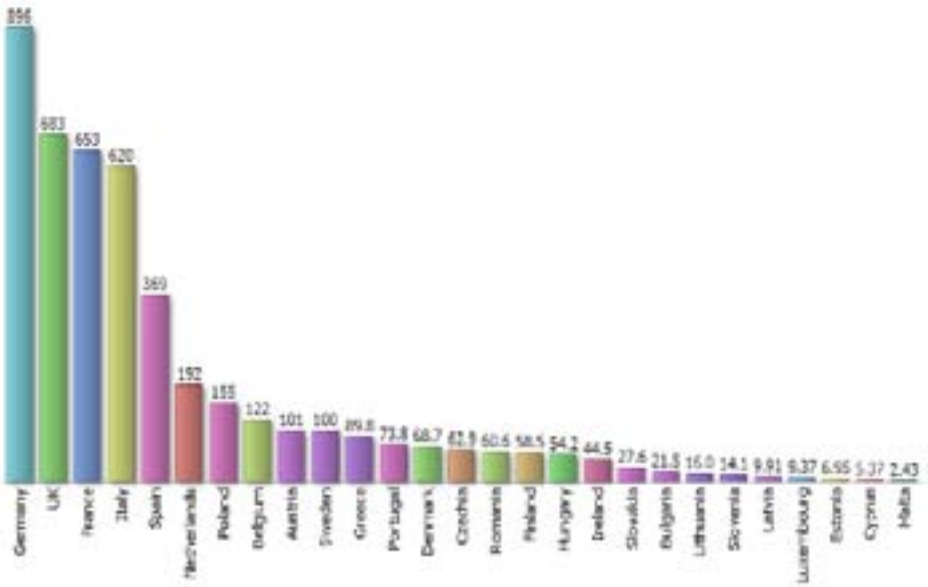
Tegenover de soms vage omschrijvingen van de dreiging (of de perceptie ervan zoals hiervoor besproken) wordt de nood aan beveiliging tegen cyberdreiging concreter dan vroeger: de ontkoppeling van het internet van het controlenetwerk van een kerncentrale in Zuid-Korea wijst op een nieuwe trend in de beveiliging van kritieke infrastructuur: de goedkopere benadering die erin

bestaat om alle mogelijke toepassingen te koppelen aan een bestaande netwerkstructuur, ook al werd die niet specifiek daarvoor ontwikkeld, heeft niet meer de voorkeur. Commerciële beleidskeuzes beginnen meer rekening te houden met de gevolgen van veiligheidsrisico's van het gebruik van een bestaand cyberplatform. Het is daarom belangrijk een beeld te hebben van het financieel gewicht van veiligheid en meer bepaald de bijdrage van ICT. Deze bijdrage wordt geïllustreerd aan de hand van figuren twee en drie:

Figuur 4: EU-lidstaten en hun investeringen in veiligheid in miljoen euro (Innovasec, 2013).



Figuur 5: EU-lidstaten en hun investeringen in ICT in miljoen euro (Innovasec, 2013).



Enerzijds laten deze cijfers een gemiddelde bijdrage van ICT in veiligheidsinvestering in de EU-lidstaten van 14 procent zien. Anderzijds zien we dat de grote lidstaten een grotere inspanning kunnen leveren voor de totale investeringen, maar het blijft een nationale aangelegenheid die niet gecoördineerd is op Europees niveau.

In vergelijking merken we dat de NAVO-investeringen met betrekking tot *cyberdefence* en C4ISR-capaciteit veel gerichter zijn. Hoewel de voorziening van deze capaciteit eveneens door bondgenoten wordt gerealiseerd, hebben we een gerichte krachtinspanning vastgesteld in specialiteiten als *Afghan Mission Network, Missile Defence, Cyber defence, Air C², BiSC AIS, Joint Intelligence Surveillance and Reconnaissance*. Deze kritieke capaciteit geeft ook een operationele plaats aan het virtuele platform. De uitvoering en het toezicht van alle ICT-aanwendingen vallen onder de auspiciën van het NATO Communication and Information Agency (NATO C&I Agency): voor de periode tot 2014 biedt dit de mogelijkheid tot investeringen a rato van 2,1 miljard euro (Vandenberghe, 2012; NATO C&I Agency, 2012). De afname van de investeringen van de Verenigde Staten op gebied van C4ISR (-17% voor het jaar 2014) hebben niets te maken met een vermindering van de inspanningen in het domein, maar alles met de vermindering van de fysische aanwezigheid en de inspanningen in Irak en Afghanistan.

Zowel de dreiging als de politieke en militaire operationele organisatie wijzen in de richting van een toegenomen belang voor cyberaangelegenheden. Het is echter weerom niet vanzelfsprekend wat men met de term

cyberveiligheid onder deze noemer dekt: verschillende definities en/of omschrijvingen worden namelijk gehanteerd. Volgens het technologiebedrijf THALES behelst cyberveiligheid het geheel van gecoördineerde acties die als doel hebben cyberaanvallen te verhinderen, te analyseren en adequaat erop te reageren. De hoofddoelstelling moet zijn de gebruiker permanent te beschermen en tijdig te wapenen met adequate maatregelen om het hoofd te bieden aan de risico's die verbonden zijn aan de informatiesystemen (Thales, 2010; p. 4 – eigen vertaling). Een verwante term die vaak gebruikt wordt is informatiezekerheid (Information Assurance – IA) en doelt op maatregelen die gericht zijn op de bescherming en de verdediging van informatiesystemen door hun beschikbaarheid, integriteitauthenticatie en geheimhouding te garanderen. Deze maatregelen voorzien in de veerkracht van informatiesystemen door bescherming, detectie en reactie mogelijk te maken (CNSS, 2010; p. 38 eigen vertaling). Het Tallinn-handboek biedt een handige leidraad voor definities: terwijl elke bron een eigenhandige definitie hanteert, is het handboek opgesteld op basis van het gewoonterecht en vertrekkende van een consensus over geldende regels. Bovendien baseert het zich op definities die gebruikt zijn in bestaande doctrines van de VS, Canada, Denemarken en het Verenigd Koninkrijk. De opstellers, een groep van experten, telden in hun rangen waarnemers van de NAVO (ACT), het Internationaal Comité van het Rode Kruis (ICRC) en US Cyber Command. Definities en omschrijvingen die besproken en geïllustreerd worden aan de hand van bestaande en geëxtrapoleerde jurisprudentie handelen over:

- staten en cyberspace (soevereiniteit, jurisdictie, controle en staatsverantwoordelijkheid);

- het gebruik van geweld (verbod op het gebruik van geweld, zelfverdediging, acties van internationale gouvernementele organisaties);

- de wet van gewapend geweld toegepast op het cyberdomein (de wet der gewapende conflicten, aanvallen, aanvallen op personen, aanvallen op objecten, middelen en methodes van oorlogvoering, leiding van aanvallen, voorzorgsmaatregelen, verraad, onbehoorlijk gebruik en spionage, blokkades en afgebakende zones);

- specifieke personen, objecten en activiteiten (medisch en religieus personeel of transport, personeel of uitrusting van de Verenigde Naties, gevangenen, kinderen, journalisten, installaties die bijzondere krachten bedwingen, objecten die onontbeerlijk zijn voor de overleving van burgers, cultureel erfgoed, de natuur,

diplomatieke archieven en communicatie, collectieve bestraffing, humanitaire hulp);

- bezetting;

- neutraliteit.

In het geheel zijn de besproken onderwerpen niet nieuw maar ze worden belicht vanuit een nieuwe invalshoek en een benadering die de wet der gewapende conflicten specifiek voor het virtuele platform illustreert. Zo kan het voormelde Stuxnet-voorbeeld getoetst worden aan deze interpretatie om in te schatten of we in dit specifieke geval al dan niet met het gebruik van geweld te maken hebben, met andere woorden of we hier te maken hebben met een aanval. Enkele opmerkingen gaan hieraan vooraf: Stuxnet werd ontworpen op basis van gedetailleerde kennis met betrekking tot de technische werking van getroffen systemen; authentificatiegegevens moesten omzeild kunnen worden; Stuxnet werd ontworpen met een zelfvernietigingsmechanisme, met andere woorden een systeem om collaterale schade te beperken. Schmitt omschreef hiertoe een parametrering van wat volgens hem de voorwaarden waren om een aanval te catalogiseren als gebruik van geweld volgens de voorzieningen van artikel 2 (4) van het Handvest van de Verenigde Naties (Foltz, 2012; p. 44):

- Ernst *(Severity)*: cyberoperaties die de fysische integriteit bedreigen zijn sterk vergelijkbaar met een gewapende aanval. Factoren die in deze vergelijking relevant zijn omvatten het bereik, de duur en de intensiteit.

- Onmiddellijkheid *(Immediacy)*: gevolgen die snel tot uiting komen zonder de mogelijkheid om bedwongen te kunnen worden of een vreedzame oplossing te vinden worden sneller beschouwd als gebruik van geweld.

- Directheid *(Directness)*: hoe directer het verband tussen een cyberincident en de gevolgen ervan, hoe meer staten geneigd zullen zijn het te beschouwen als een gewelddadige aanval.

- Invasiviteit *(Invasiveness)*: hoe meer een operatie afbreuk doet aan de fysische integriteit van een staat, hoe waarschijnlijker dat beschouwd wordt als geweldsdaad.

- Meetbaarheid *(Measurability)*: staten beschouwen een cyberoperatie als geweldsdaad indien een gevolg identificeerbaar en objectief kwantificeerbaar is.

- Veronderstelde wettelijkheid *(Presumptive legitimacy)*: in de veronderstelling dat handelingen gewettigd zijn buiten het cyberdomein, dan blijven die gewettigd binnen dat domein (bijvoorbeeld spionage, psychologische operaties en propaganda).

- Verantwoordelijkheid *(Responsibility)*: hoe groter het verband van een staat met een welbepaalde cyberoperatie, hoe waarschijnlijker dat het bestempeld wordt onder de noemer gebruik van geweld.

Voor wat de toetsing van het incident betreft, hellen elementen als ernst (*severity*), directheid (*directness*), invasiviteit (*invasiveness*), meetbaarheid van de schade (*measurability*) zeker in de richting van een vaststelling van het gebruik van geweld. Bovendien is er in dit geval geen sprake van legitimiteit gezien enig mandaat van de Verenigde Naties ontbrak en het algemeen aanvaarde principe geldt dat men geen kerninstallaties van een andere staat bestookt. De elementen die de evaluatie dan weer naar de andere kant van de balans doen overhellen zijn de latentie van de effecten en de attributieproblematiek. Hiervoor zijn de aanvankelijke opmerkingen belangrijk: beide elementen kunnen een antwoord vinden in de voorbereiding van de actie: een nauwkeurige voorbereidingsfase (met intensieve exploitatie van inlichtingen) schijnt aan Stuxnet voorafgegaan te zijn. In totaliteit genomen lijkt deze evaluatie te duiden op het gebruik van geweld. Een belangrijke bemerking hierbij vormt het attributieprobleem. Hoewel de vormgeving en de voorbereiding aanwijzingen geven van een statelijke inmenging, is men vandaag nog niet bij machte om de verantwoordelijke achter deze aanval aan te wijzen. Ook de houding van het slachtoffer, met name Iran, is hiervoor belangrijk: het wegblijven van officiële erkenning het slachtoffer geweest te zijn van een aanval of enige verwijzing naar een mogelijke oorsprong, zorgt voor een juridisch vacuüm in de voorgestelde analyse. De benadering die in de definities van het Tallinn-handboek gegeven worden, sluiten dichter aan bij de wet op de gewapende conflicten: dat de evaluatie of er al dan niet sprake kan zijn van het gebruik van geweld is meer gericht naar de inschatting van de gevolgen van het incident. Zo omschrijft men in het handboek een cyberaanval als een offensieve of defensieve operatie waarvan men redelijkerwijs kan aannemen dat personen gekwetst of gedood worden of schade of vernieling wordt toegebracht aan objecten (Tallinn manual, 2013 – p. 92 – eigen vertaling). Met de aandacht voor de gevolgen van zowel de offensieve als defensieve operaties wordt ook onrechtstreekse schade door uitval van SCADA-systemen ondergebracht bij de interpretatie van een aanval.

In de beschrijving van de juridische implicaties van het ontstaan en de uitbating van het cyberdomein moet men beseffen dat de overgrote meerderheid van de informatiedragers en informatie-infrastructuur in privaat

bezit is. Het bestaande netwerk, zowel de structuur ervan als de instrumenten om cyberwapens te genereren, behoren tot het private domein. Dit is een bijkomende moeilijkheid in de regulering door de overheid of het afdwingen van een regelgeving die voldoet aan het internationaal recht (International Humanitarian Law - IHL, Law of Armed Conflict - LOAC). Civiele actoren worden immers gedreven door economische motieven en hebben niet noodzakelijk dezelfde maatstaven als de overheid op het internationale toneel. Het Tallinn-handboek over cyberoorlogvoering wil daarom een leidraad zijn door de transpositie van het gewoonterecht naar dit nieuwe domein. Zoals we zullen zien laat het handboek meer ruimte voor conventionele antwoorden op cyberaanvallen die preventief uitgevoerd worden, maar met de bedoeling zich te verdedigen tegen een imminente cyberaanval.

Alle elementen die in aanmerking komen in het recht van de gewapende conflicten zijn ook in dit domein van toepassing: het discriminatieprincipe (regel 31); het verbod tot aanval van burgerbevolking (regel 32); de dreiging met een aanval (regel 36); het verbod om onnodig lijden te veroorzaken (regel 42) of over te gaan tot represaillemaatregelen (regel 46) en ten slotte de noodzaak tot proportionaliteit in de zelfverdediging (regel 51). Onmiddellijk vallen een aantal elementen op die voorlopig nog een probleem vormen in hun praktische toepassingen. Het eerste is het discriminatieprincipe: vandaag is het niet uit te sluiten dat een aanval aanleiding zou geven tot collaterale schade. Precisiemunitie maakt dat in sommige conventionele aanvallen quasi onmogelijk. Voorlopig is dit in het cyberdomein nog uitgesloten, waardoor regels 31, 32 en 42 al overtreden kunnen worden. De proportionaliteit in de zelfverdediging (regel 51) wordt hierdoor ook moeilijk af te bakenen. Hierdoor zal geen staat officieel toegeven betrokken te zijn bij een cyberaanval: de attributie is niet vast te leggen in tegenstelling tot wat men wel zou kunnen voor een kinetische aanval. De regels 36 en 46 vinden dus weinig of geen toepassingsveld.

Ten slotte is de afdwingbaarheid van dit gewoonterecht problematisch. Geen enkele instantie is vandaag bevoegd om de naleving van deze regels internationaal na te gaan of ten gevolge van een overtreding sancties op te leggen. Vooral natiestaten zullen liever in een grijze zone opereren dan zich te laten beperken in hun eigen mogelijkheden (bijvoorbeeld tegen niet-staatsactoren). Het enige orgaan dat hierdoor voorlopig in aanmerking komt voor het opleggen van sancties is de VN-Veiligheidsraad.

Welke gevolgen dit heeft voor het nationale beleid met betrekking tot cyber operaties en NEC moet men toelichten met specifieke nationale invalshoeken die in het meeste van de gevallen de basis zullen vormen voor de militaire implicaties daarvan. We lichten in wat volgt dit standpunt toe aan de

hand van wat in een militaire commandostructuur als de NAVO werd gerealiseerd in transitie naar een genetwerkte structuur en de plaats die het cyberdomein hierin neemt.

1.6. De NAVO-bijdrage

De NAVO is het schoolvoorbeeld van een militaire C4ISR-architectuur die voortspruit uit de gedreven vooruitgang en metamorfose van de grootste van zijn bondgenoten: de alliantie hanteert met betrekking tot de C4ISR architectuur is er een van gestage vooruitgang en voortdurende constructie. De structuur en de organisatie van alle C4ISR elementen zijn onderhevig aan een dynamisch proces waarbij concrete oplossingen passen in een groter geheel en daardoor coherentie van aanpak vergen. Dit heeft gevolgen voor het resultaat (de concrete oplossingen en capaciteiten) maar ook voor het conceptuele en het langetermijndenken. In 2011 formuleerde het toenmalige NC3 Agency het nog als volgt (NC3A, 2011; p. 5):

> "In general, development of enterprise C4ISR capabilities results from the identification of a need for such capabilities through the NATO Defence Planning Process (NDPP) or as a result of a capability gap analysis for current operations. In a complex, dynamic and loosely coupled environment like the NATO C4ISR Entreprise, centralized long-term planning approaches have limitations. Therefore all architectural and acquisition activities should apply an evolutionary approach where in parallel to the on-going planning activities projects are realizing field able systems that deliver required functionalities. In order to succeed, projects shall work incrementally starting small and targeted, expanding over time."

Eerder dan een bottom-up benadering moet men voor oog hebben dat het gehele planningsproces en dan in het bijzonder op lange termijn zoals ze vandaag bestaat, beperkingen kan hebben voor de uitbouw van een coherente C4ISR-architectuur. Eerder hebben we al aangegeven dat de diffuse dreigingen van vandaag een grotere benadering *ad hoc* vereisen. Oplossingen op korte termijn rijmen inderdaad niet altijd met acquisitieprogramma's die over decennia gespreid zijn. Het mogelijke gevolg is een verkorting van de plannings- en de uitvoeringsfase die rekening houdt met de interoperabiliteitsvereisten. Deze vereisten hebben betrekking op twee toepassingen, te weten enerzijds de communicatiesystemen en anderzijds de informatiesystemen. Vandaag de dag weet men aan welke eisen een interoperabel communicatiesysteem moet voldoen: zonder dat is geen operatie mogelijk. Maar moeilijker wordt het indien ook criteria de praktische implicaties voor informatie-uitwisseling gaan bepalen. Deze vaststelling heeft

na de NAVO-top van Praag geleid tot een besef dat dergelijke criteria deel moeten uitmaken van een concept dat door alle partners wordt gedragen.

De VS en het VK hadden in hun transitie naar C4ISR-capaciteit al in de uitwerkingsfase van operationele concepten de sterk op elkaar gelijkende US Network-Centric Warfare (NCW) en UK Network Enabled Capability (NEC). Het in de VS gestarte concept om informatiesuperioriteit te verwerven werd voor het eerst beschreven door Money en Alberts aan de vooravond van de 21ste eeuw (Alberts et al.; Money et al.): het oorspronkelijke einddoel muteerde al gauw van informatiesuperioriteit naar kennissuperioriteit en vervolgens naar besluitvormingssuperioriteit. Het netwerk centrische concept zou toelaten om op een kostenefficiënte manier de ontwikkeling van nieuwe wapensystemen toe te laten en nationale interoperabiliteit te garanderen. Van het Amerikaanse NCW-concept werd om budgettaire redenen door het VK onmiddellijk afgeweken. De bedoeling van NEC was een netwerk uit te bouwen dat zou toelaten om (NATO RTO, 2004; p.7-6):

- de bestaande informatie- en planningsnetwerken nationaal af te stemmen;

- door integratie de militaire taken beter af te stemmen op de noden van het ogenblik;

- door langetermijnconcepten een visie uit te bouwen voor de toekomst;

- te leren uit de ervaring van een transformatieproces en plannen maken voor 2015;

- de optimale technologische oplossingen aan te wenden die voorhanden zijn.

De uitvoerbaarheidsstudie van een gelijkaardig concept voor de NAVO heeft geleid tot het uitwerken van NATO Network Enabled Capability (NNEC). De componenten die de steunberen van de NNEC moesten worden zijn (NATO RTO, 2004; p.2-1):

- onderliggende netwerken en systemen;

- de te delen informatie;

- de procedures om dat “delen” in de praktijk toe te passen;

- doctrines en politieke visie die de verantwoordelijkheid van de deelnemers definieert.

De eerste praktische uitvoering van het NNEC-concept werd in Afghanistan gerealiseerd (Afghan Mission Network – AMN). De lessen die uit die toepassing werden getrokken, worden gebruikt voor het conceptualiseren van de architectuur van opdrachten in de toekomst: met architectuur doelen we in het vervolg van ons betoog op de specificatie van deelnemende actoren, hun verantwoordelijkheden en onderlinge verhoudingen, alsook de procedures, principes of richtlijnen die die verhoudingen formaliseren. Dit geheel identificeren en omschrijven is net wat beoogd wordt met Future Mission Network (FMN). FMN blijkt meer een langetermijnvisie over een gecombineerde civiele en militaire architectuur met voor het militaire aspect inachtname van de lessen die uit Afghanistan en Libië werden getrokken. De ontwikkeling van doctrines en richtlijnen was een eerste bijdrage aan het NNEC-concept. Dat de praktische realisatie van een dergelijk concept ook afhangt van de innovatie op technologisch vlak staat buiten kijf, maar de dienstencentrische benadering en de interoperabiliteit van alle besluitvormings- en uitvoeringsniveaus ter mobilisatie van effectoren en collectoren zullen steeds de basis blijven van het overkoepelende concept. Dat betekent dat een deel van de architectuur niet statisch maar intrinsiek dynamisch is: ze is onderhevig aan de wijzigingen die gegenereerd worden door opduikende technologie of nieuwe toepassingen ervan.

Een voorbeeld daarvan wordt gegeven door het platform dat binnen de NAVO het luchtbeeld en de raketafweer zou aansturen: Air Command-and-Control System (ACCS). Initieel bedoeld om de waaier van nationale systemen te integreren, zou het toelaten om NATO luchtcommando en -controle op een gemeenschappelijk leest te schoeien en tegelijk ontplooibare systemen te genereren. De software ervan werd getest en gevalideerd in vier landen, te weten België, Duitsland, Frankrijk en Italië: de volledige implementatie van het systeem had tegen 2019 voltooid kunnen zijn. Dat systeem voorziet in interoperabiliteit tussen 165 verschillende interfaces (zowel civiele als militaire) met dynamische specificaties: die veranderingen in configuratie zijn te wijten aan bijvoorbeeld updates van het besturingssysteem voor communicatiemanagement of radargegevens en moeten tegelijk toelaten om de bestaande systemen (sensoren bijvoorbeeld) te blijven gebruiken. Hergebruik en aankoop van militaire of civiele commerciële producten (Military or Commercial-Off-The-Shelf MOTS/COTS) heeft het tot 2001 mogelijk gemaakt om dat lapwerk samen te smelten tot een coherent en operationeel geheel. De invoering van Java-programmeercode zou het mogelijk moeten maken om het netwerkplatform onafhankelijk te beheren: de invoering van een virtueel platform met Java laat immers toe dat voor elk geconnecteerd object een

virtuele machine bestaat die websoortige applicaties kan exploiteren. Vandaar dat men ook spreekt van objectgeoriënteerd programmeertaal of syntaxis. Drie ACCS-toepassingen illustreren waarom dit een voorloper kan zijn in de queeste naar interoperabiliteit namelijk:

- gemeenschappelijke dienstverlening beschikbaar voor alle aangesloten gebruikers (tijdsreferenties, alarmering, prioritering, beveiliging);

- *real time* toepassingen zoals radarinformatie of raketafweer;

- een kader voor niet-tijdsafhankelijke verwerking van gegevens (bijvoorbeeld informatiebeheer of verspreiding van geografische gegevens).

ACCS voorziet geen communicatiemogelijkheid op zich maar maakt gebruik van Transmission Control Protocol/Internet Protocol (TCP/IP) waardoor tactische datalinks (Link 1, Link 11, Link 16, …) en gegevensuitwisseling worden ondersteund, met een toegang tot een nationaal netwerk dat TCP/IP ondersteunt. De ontwikkeling van nieuwe systemen voor collecte en disseminatie van inlichtingen (AGS, BiSC-AIS, BICES, …) voldoet aan de interoperabiliteitsvereisten en zou het mogelijk maken om zowel de oude als de laatst ontwikkelde systemen te behouden in de architectuur. De budgettaire beperkingen hebben van bij de aanvang de ontwikkeling van dit systeem afgeremd. Nadien is een *downsized*-versie uitgewerkt (ACCS Light) voor pc's met Windows of Linux Operating System (OS) die vooral voor mission planning kunnen gebruikt worden: het gebruik en de exploitatie van *real time* toepassingen is te belastend voor de huidige generatie pc's. Veiligheidsredenen laten het daarom niet toe om gebruikt te worden voor luchtverdediging of zelfs Air Traffic Control (ATC). Het is duidelijk dat slechts de initiële versie van ACCS in staat zou zijn om te voldoen aan de operationele en interoperabele vereisten als springplank voor een NATO NEC.

Om dat te vermijden werd ook het bestaande luchtverdedigingsnetwerk van het NAVO-luchtruim uitgebreid met partnerlanden. Wat binnen NAVO-kringen nagestreefd wordt is een erkend luchtbeeld (Recognized Air Picture - RAP) waarbij gefilterde en niet-geclassificeerde informatie wordt uitgewisseld met aangrenzende landen: het is een werkinstrument dat tot stand komt door de uitbreiding van een operationele capaciteit. Het operationele programma dat deze nieuwe infrastructuur wil realiseren is het NATO Air Situation Data Exchange –programma (ASDE). Dit programma werd door de Noord-Atlantische Raad goedgekeurd in 2001 met als doel zowel de NAVO-bondgenoten als partnerlanden bij te staan in het beheer van nationale soevereiniteit van het luchtruim, grensoverschrijdingsincidenten, strijd tegen

het terrorisme en reactie tegen het gebruik van burgervliegtuigen als wapen. 18 naties hebben tot nu toe hun deelname aan het programma aangevraagd. Het doel is luchtbeeldgegevens uit te wisselen door tactische datalinks (TDL) vanuit partnerlanden naar NAVO-bondgenoten en omgekeerd. De uitwisseling van gegevens gebeurt op basis van Link 1- protocols. In dit geval worden niet-gecrypteerde en niet-geclassificeerde plot-informatie[1] uitgewisseld via commerciële communicatielijnen die aan deze taak worden gewijd. Het belang van wat eerder werd besproken over cyberbeveiliging van commerciële lijnen wordt hiermee onderstreept en dit komt ook tot uiting in de operationele procedures voor het gebruik van deze informatie: indien de kwaliteit van de gegevensuitwisseling langer dan 8 uren in beslag neemt, dient het hoofdkwartier van het geallieerde commando "air" hiervan op de hoogte gebracht te worden. Indien het probleem aanhoudt en langer dan 24 uren duurt, moet zelfs het hoofdkwartier van *Allied Command Operations* (ACO), het militair hoofdkwartier van het bondgenootschap op de hoogte worden gebracht. De connecties met partnerlanden werd voor het eerste operationeel in 2006 en sindsdien werd ook zijn nut bewezen voor andere dan de voormelde doelen, zoals voor de organisatie van een politieke topbijeenkomst of grootschalige culturele evenementen. Het onderhoud van een geactualiseerd dynamisch luchtbeeld dat voortdurend aangepast dient te worden is het moeilijkst te realiseren aan de grenzen van het bondgenootschap. Het is daarom essentieel om een uitwisseling van informatie mogelijk te maken (3D-positie, richting, …) vooraleer de fysische grenzen worden bereikt. Het principe van uitwisseling van gegevens bestaat erin om de informatie te declassificeren vooraleer ze uitgewisseld wordt. In 2013 was het vorderingsstadium van de uitwisselingen als volgt:

- operationele verbindingen met Oostenrijk (via Duitsland), Georgië (via Turkije) en Oekraïne (via Hongarije en Turkije);

- verbindingen te valideren met Finland (via Litouwen) en Zweden (via Noorwegen);

- in aanvaardingsprocedure: Finland (via Noorwegen), FYROM (via Griekenland), Oostenrijk (via Hongarije), Bosnië-Herzegovina (via Kroatië), Montenegro (via Kroatië), Moldavië (via Roemenië).

[1] Met plot-informatie doelt men op de ruwe positie-informatie zoals die kan worden gegenereerd door een radar. Bijkomende gegevens zoals IFF-codes, houding, bewapening of identificatie van het platform horen niet daarbij. Deze gegevens brengt men onder bij de trackgegevens waarvan de kwaliteit het erkend luchtbeeld zal vormen.

Teneinde de overlap van informatie mogelijk te maken, wordt in verschillende werkingsmodi voorzien die men kan vergelijken met alarmstadia:

- vredestijd: geografische zone uitgebreid met 100 nautische mijlen (NM) aan weerskanten van de betrokken landsgrenzen;

- oefening: geografische zone uitgebreid met 200 NM aan weerskanten van de betrokken landsgrenzen;

- crisis: geografische zone uitgebreid met 300 NM aan weerskanten van de betrokken landsgrenzen;

- artikel 5 operatie: geografische zone uitgebreid met 400 NM aan weerskanten van de betrokken landsgrenzen.

Naast de operationele aspecten geldt dit programma ook als vertrouwenwekkende maatregel: vooreerst wordt de nodige openheid gecreëerd en tegelijk krijgen partners ook beter inzicht in de vereisten die worden gesteld aan operationele partners van het NAVO-bondgenootschap. Naast de technische interoperabiliteitsvereisten laat dit programma de noodzaak blijken van een procedurele interoperabiliteit. Tevens laat het toe om de veiligheid van de burgerluchtvaart te verbeteren en om de conflicten tussen commerciële en militaire vluchten sneller en adequater op te lossen. Aan een aantal operationele vereisten moet worden voldaan om in het netwerk te worden opgenomen, met name de capaciteit bezitten om bij te dragen aan de verbetering van het collectieve luchtbeeld, een commando- en controlecapaciteit bezitten en ten slotte een communicatiecapaciteit hebben die toelaat om de gegevens met de NAVO-partner(s) uit te wisselen. Het orgaan binnen de NAVO dat verantwoordelijk zal zijn om nieuwe kandidaturen voor te stellen aan de Noord-Atlantische Raad is de Air and Missile Defence Committee (AMDC): door de structuur van luchtverdediging en raketafweer samen te smelten geeft men het belang aan om operationeel commando en controle ervan te willen integreren. Dit garandeert tegelijk het gebruik van gestandaardiseerde procedures en erkent *a priori* het belang van het bestaande Air Defence-netwerk in de aanwending van een recentere applicatie als Missile Defence.

Het is een dergelijk voorbeeld met concrete resultaten dat de basis kan zijn voor de verdere uitwerking van een volledige C4ISR-architectuur: het is dus wel degelijk met een overkoepelende visie dat men het project moet beginnen wil men een gecoördineerde inspanning leveren die tot tastbare resultaten kan leiden. Concrete projecten moeten die genese echter zichtbaar maken en moeten ook als basis dienen voor de verdere uitbouw en de mogelijke exploitatie van het netwerk. In wat voorafging is die werkwijze

aanwezig in de NAVO-benadering terwijl de EU-methodologie nog moet geschreven worden. In de praktijk kan dat betekenen dat EU-geleide opdrachten gebruik maken van de NAVO-architectuur. Losse EDA-projecten zonder geïntegreerd eindresultaat of demonstrator brengen immers geen enkele meerwaarde aan de gemeenschappelijk capacitaire ontwikkeling. Defensie is een van de laatste bastions waarvan de landen (en hun respectieve defensie-industrie) de perceptie koesteren dat engagementen nationaal bepaald worden. Deze soevereiniteitsperceptie wordt echter overschaduwd door de mogelijkheid van deelname: enkel een multilateraal en geïntegreerd platform laat dit in de toekomst nog toe. De terughoudendheid van de lidstaten om de planning en programmering van capacitaire clusters uit handen te geven moet overwonnen worden door realistische doelstellingen die ook voor de bevolking een gepercipieerde meerwaarde creëren.

Volledig analoog aan de evolutie van de C4ISR architectuur is cyberverdediging in de organisatie onderhevig aan verandering. Organisatorisch werd het verantwoordelijk agentschap, het NATO C3 Agency herschapen tot het NCI Agency (NATO Communications and Information Agency). De verantwoordelijkheden ervan zijn ook uitgebreid tot enerzijds de connectie van eenheden en naties in een operationeel netwerk door middel van *interoperabele* communicaties en diensten en anderzijds *cyberdefence*. Het gevolg van deze uitbreiding is dat nu ook de raketafweer tot het takenpakket behoort en dan in het bijzonder voor het fuseren van sensordata die het gemeenschappelijk besluitvormingsproces kunnen verbeteren.

Vooreerst brengt het NAVO netwerk en de operationele exploitatie ervan − NATO Network-Enabled Capability (NNEC) − een aantal gefedereerde capaciteiten onder één centrale controle. De efficiëntie van een dergelijke omgeving is sterk afhankelijk van de mate van interoperabiliteit, wat eerder al als opmerking bij de bespreking van staten tot uiting kwam. De organisatie van informatievergaring en exploitatie door civiele en militaire organen binnen de organisatie wordt gegeven door de NATO Information Management Policy (C-M(2007)0118, NATO Information Management Policy). De concrete uitvoering behelst een aantal principes die ervoor moeten zorgen dat die informatie tussen diensten kan uitgewisseld worden binnen Consultation, Command and Control-architectuur (onder de bevoegdheid van NATO C3 Agency) en NAVO C4ISR-architectuur. De concrete uitwerkingsprincipes (de praktische realisatie) zijn gebaseerd op de grondvesten van beleidsrichtlijnen en omvatten (NC3A, 2011; pp. 3-10):

- Informatie-uitwisseling: zowel de informatie als de informatiedrager moeten in staat zijn tegemoet te komen aan de vereisten van snelle beschikbaarheid, waar ook ter wereld voor om het even welke partner

die erom zou vragen. Standaardisatie van de vorm is dus essentieel voor de verwerking ervan.

- Bezit van informatie: het gevaar voor de grote beschikbaarheid is de mogelijke fysische duplicatie van informatie waardoor er onzekerheid bestaat op de geldigheid en accuraatheid van de updates ervan. Daarom moet een verantwoordelijke beheerder en uitgevend organisme aangeduid worden.

- Verzekering van informatie: uit wat voorafging kan men afleiden dat de juiste en snelle informatieverdeling meer dan ooit de sleutel zal zijn tot elke NAVO-operatie in de toekomst. De verantwoordelijkheid om informatie beschikbaar te stellen impliceert bovendien dat die ongewijzigd door verschillende veiligheidsniveaus kan migreren om in de juiste vorm bij de juiste gebruiker toe te komen. Het is net dit proces dat het eerste en belangrijkste doelwit zal zijn van mogelijke tegenstrevers: nieuwe dreigingen in dit domein moeten daarom op permanente basis geschat worden om tijdig tegenmaatregelen te kunnen nemen.

- Hergebruik: een uniform platform van hardware en een uniforme software moeten vermeden worden. Eerder zal men streven naar het gebruik van meerdere heterogene systemen die de internetprincipes als ruggengraat hebben. De ontwikkeling van systemen wordt daardoor nooit zo specifiek als dat ze voor slechts één enkele opdracht kan worden uitgevoerd. Verder laat het toe dat een legaat van systemen steeds operationeel kan blijven gezien de nieuwste systemen steeds compatibel moeten zijn met de oudere.

- Architectuurplanning: door de snelle evolutie van de noden en de soms specifieke vereisten voor operaties, geïdentificeerd als een capaciteitstekort, kan langetermijnplanning zoals ze nu wordt geconcipieerd een te beperkte benadering zijn voor een efficiënte uitwerking van een C4ISR-infrastructuur. Eerder zal men zich moeten richten op concrete projecten die passen in een coherent geheel en uitbreiding kunnen nemen. Hiermee onderschrijft men de bottom-up aanpak.

- Een gebruiker centrische benadering doelt op de diensten die kunnen geleverd worden aan de gebruiker: in dit geval zijn dat de diensten die vereist zijn voor het goede verloop van operaties die zullen uitgevoerd worden in de toekomst. De zuiver technische benadering aan de tegemoetkoming van punctuele noden doet soms tekort aan operationele vereisten of noden die moeten kaderen in zeer specifieke operationele omstandigheden. Een geïsoleerde technische benadering van een dergelijk probleem doet in sommige gevallen tekort aan dit aspect en zal in de toekomst meer in rekening moeten gebracht worden. Operationele vereisten kunnen ook vaker en sneller veranderen (wat mogelijk een sneller en flexibeler samenwerkingsverband met private partners zal vergen).

- Standaarden voor datamodellering en -uitwisseling moeten ervoor zorgen dat zowel de gebruiker als de toepassingen gecollecteerde gegevens kunnen exploiteren, vandaag maar ook morgen. Technische standaarden mogen zich niet beperken tot eigenschappen van specifieke commerciële producten of firma's.

- Communicatie en infrastructuur van het netwerk zullen bepalen hoe snel data kunnen uitgewisseld worden. Men moet echter rekening houden met onderbrekingen van de informatiestroom. De niet-permanente beschikbaarheid van het netwerk maar beschikbaarheidsvensters moeten desgevallend toelaten om autonoom te opereren. Het feit dat communicatie wordt losgekoppeld van infrastructuur toont dat het virtuele (hoewel gedragen door een fysisch element) niet verengd mag worden tot de fysische infrastructuur die eraan gekoppeld is.

- Verificatie en validatie zijn niet alleen bedoeld om vergelijkingen uit te voeren tussen systemen op dossier maar zeker ook om in operationele omstandigheden de capaciteit voor de verwerking van grote informatiestromen en de exploitatie ervan te testen. De bestaande standaarden garanderen nog steeds geen interoperabiliteit, zeker voor wat betreft het verschil tussen civiele en militaire systemen: naast de standaardisatie zal men bijgevolg ook de betrouwbaarheid van systemen moeten nagaan.

*Cyberdefence v*ervolgens, wordt in NAVO-verband nog steeds aangezien als een van de belangrijkste opdrachten van de Alliantie sinds het vastleggen van het vernieuwde strategische concept zoals voorgesteld in Lissabon in 2010. Nochtans staat de alliantie enkel garant voor de bescherming van eigen materieel en zijn het de bondgenoten zelf die nationaal moeten voorzien in de

bescherming van het eigen netwerk. In essentie wordt de dreiging supranationaal ervaren en moet de verdediging op een gelijkaardig niveau georganiseerd worden. Hiervoor heeft de Alliantie zich uitgerust met een structuur die zowel de beleidssturing (*Cyber Defence Management Authority - CDMA*) als de concrete behandeling van incidenten tot doel heeft (*Computer Incident Response Capability - CIRC*). De exhaustieve bespreking van de betrokken organen of actoren valt buiten het bestek van deze studie en kan ook teruggevonden worden in een eerder verschenen studie in deze reeks en van dezelfde auteur (Veiligheid en Strategie Nr 105: Bescherming van nationale kritische infrastructuur tegen een dreiging van asymmetrische proliferatie, 2010). Terwijl de aandacht van de beleidsverantwoordelijken vijf jaren geleden in dit domein nog andere prioriteiten kreeg, vergaderden in 2013 de ministers van Defensie van de bondgenoten om de samenwerking in dit domein vast te leggen door Memoranda of Understanding (MoU). In die enkele jaren werd de mankracht van de VS in dit domein vervijfvoudigd en binnen de Alliantie worden nu ook doelstellingen bepaald voor de 28 bondgenoten (Pressreview Defensie, 2013). Het actieplan dat de herziene politiek moet materialiseren wordt vandaag nog stapsgewijs in werking gesteld: hierbij worden overheden betrokken, maar ook de private sector, academische instellingen en zelfs landen die niet lid zijn van de Alliantie (zoals Oekraïne of Israël) maar die hiervoor in een partnerschap willen samenwerken. Ondanks deze gemeenschappelijke basis blijft ieder land zelf verantwoordelijk voor de organisatie van zijn cyberveiligheid. Daartoe werken alle bondgenoten elk een eigen strategie uit. Voor België is dat niet anders: de ministerraad kon in december 2012 de eerste minister belasten met de uitvoering van zijn eigen strategie. De nationale input laat echter mogelijkheden tot divergentie in de aanpak waardoor de slagkracht van de Alliantie zou kunnen gefnuikt worden. Bovendien kan de Alliantie slechts advies verlenen voor de sturing tijdens een incident, maar in geen enkel opzicht dient dit advies nageleefd te worden door private actoren die de meerderheid van de infrastructuur en de informatie-infrastructuur bezitten. Als militaire alliantie bij uitstek is de organisatie al helemaal niet bevoegd voor al wat onder de civiele noemer van de activiteiten van de lidstaten valt, laat staan over de activiteiten van private partners. Nochtans is de dreiging niet afgenomen en vandaag ziet men ook in dat dreigingen van morgen meerdere disciplines bestrijken. De bevoegdheid van het coördinerend orgaan (*Cyber Defence Management Board - CDMB*) welke het interveniërende orgaan aanstuurt in geval van incidenten is niet veranderd. Het is aan dit orgaan dat door getroffen bondgenoten assistentie kan worden gevraagd.

Rationalisatie enerzijds en het besef dat meer en meer disciplines verbanden hebben en gemeenschappelijke sturing vereisen anderzijds hebben als gevolg dat NAVO-agentschappen zijn samengesmolten. Het is de toegenomen aandacht voor cyberverdediging en aanverwante disciplines die

mee ervoor heeft voor gezorgd dat de NAVO in juli 2012 een nieuw agentschap in het leven heeft geroepen met meer bevoegdheid: de ondersteuning van de Alliantie inzake communicatie- en informatie-infrastructuur heeft geleid tot organisatorische samensmelting van communicatie- en informatiesystemen met *cyber* en *missile defence*. De gecentraliseerde C4ISR-capaciteit wordt hiermee door één enkel agentschap ondersteund, namelijk het NATO Communications and Information (NCI) Agency dat de ontwikkeling van het concept (de operationele vereisten, de maintenance) voor zijn rekening neemt. Deze organisatie laat voor de toekomst de systematisering toe van *ad hoc* coalitieaanpak. Tevens draagt het bij tot een uitgebreidere benadering dan enkel de interoperabiliteit van communicatie: de gestandaardiseerde behandeling van de informatieverwerking zal vereisen dat een architectuur wordt uitgewerkt die voldoet aan de vereisten van de operaties van de toekomst waar en wanneer die ook zullen plaatsvinden. Niet alleen de samenstelling van die architectuur is belangrijk maar ook de exploitatie ervan. De transformatie van een operationeel netwerk *ad hoc* naar een dergelijke architectuur is werk van jaren en het eindpunt is waarschijnlijk niet eens bekend. De evolutie van de technologie laat nieuwe mogelijkheden toe die zowel voor de omschrijving van risico's als de beschrijving van de middelen om die te bestrijden in alternatieve scenario's voorziet. Een exacte omschrijving van die architectuur is om die reden niet mogelijk. In deel 1.5 zullen we echter een poging ondernemen om de richting aan te wijzen van de ontwikkelingen en gevolgen die dat kader ons aanbiedt.

In tegenstelling tot China is in de NAVO al een geïntegreerde commandostructuur operationeel. De *C4ISR-jointness* echter is nog niet tastbaar: wel wordt een 'customized oplossing' gevonden om informatie voor te stellen die eigen is aan iedere component van een joint omgeving (zie bijlage 2 voor een illustratie van NATO Common Operating Picture-NCOP) . De opeenvolgende verlagingen van de investeringsdrempels gaan in dit domein op korte termijn zorgen dat China in de organisatorische transitie fasen snel de NAVO zal hebben ingehaald. De verschuiving van de aandacht van de VS naar het oosten en de vermindering van de investeringen bij de bondgenoten kan zorgen voor een vertraging in evolutie naar *joint-ISR* capaciteit. De nationale strategieën vervullen dus een essentiële rol voor het bereiken van de vooropgestelde doelstellingen op hoger niveau. Het ritme van de technologische evolutie is echter zo groot dat het de snelheid overstijgt van de operationele aankoopplanning. Niet alleen de doelstellingen van de bondgenoten moeten dus op nationaal vlak beter aansluiten met de operationele realiteiten die ondersteuning van het groter geheel toelaten: ook de procedures voor technologische ontwikkeling en aanwerving moeten op die leest geschoeid zijn.

1.7. Deelbesluit

De operationele militaire vereisten hebben de genese van een C4ISR-architectuur in de hand gewerkt. De operaties in Afghanistan zijn daar een voorbeeld van: ze zijn bepalend geweest voor het identificeren van tekorten ten voordele van de vereisten van toekomstige operationele netwerken. De afhankelijkheid van de C4ISR-architectuur ten opzichte van informatie- en communicatietechnologie (ICT) maakt van de beveiliging van informatie en de informatiedragers een noodzakelijke voorwaarde voor het welslagen van netwerk centrische operaties.

Een vanuit conceptie militaire organisatie als de NAVO die eigen infrastructuur beveiligt, maar tegelijk afhankelijk is van de inspanningen van de bondgenoten, illustreert hoe die architectuur evolueert: het is geenszins een statische capaciteit maar intrinsiek dynamisch: ze is onderhevig aan de wijzigingen die gegenereerd worden door technologische innovatie. Als voorbeeld hebben we het platform omschreven dat binnen de NAVO het luchtbeeld en de raketafweer zou aansturen: Air Command-and-Control System (ACCS). Initieel bedoeld om de waaier van nationale systemen te integreren, zou het toelaten om NATO lucht commando en -controle op een gemeenschappelijk leest te schoeien en tegelijk ontplooibare systemen te genereren. De ontwikkeling van nieuwe systemen voor collecte en disseminatie van inlichtingen (AGS, BiSC-AIS, BICES, …) voldoet aan de interoperabiliteitsvereisten en zou het mogelijk maken om zowel de oude als de laatst ontwikkelde systemen te behouden in de architectuur.

Landen als China en de Verenigde Staten hebben niet de beperking die een multinationale organisatie heeft, zoals de integratie van verschillende nationale systemen. Doch ook daar ziet men de organisatorische consequenties van een aangepaste architectuur in: beiden tonen ons dat die in haar evolutie geen eindpunt heeft bereikt. In wat volgt zullen we merken dat stuwing van militaire C4ISR integratie zich heeft voortgezet in wat we vandaag kennen als homeland security. *Jointness* is daarom slechts een etappe in de C4ISR-evolutie. De *C4ISR-jointness* echter is nog niet tastbaar in multinationaal verband: opeenvolgende verlagingen van de investeringsdrempels gaan in dit domein op korte termijn zorgen dat China in de organisatorische transitie fasen snel de NAVO zal hebben ingehaald.

Hoewel *a priori* een zeker vergelijk mogelijk is tussen het synthetische domein en de fysische domeinen, zijn we genoodzaakt om ook de verschillen in te zien. Dit heeft gevolgen voor het nationale beleid met betrekking tot cyberoperaties en netwerk centrische operaties: specifiek nationale interpretaties zullen andere achtergronden en uitkomsten hebben met betrekking tot de uitoefening van *jointness*. Maar het uitstippelen van een beleid in een intrinsiek dynamisch systeem is niet vanzelfsprekend. Voormelde evolutie is daarom vaak gestoeld op de uitvoering van concrete projecten die passen in een coherent geheel: de bottom-up aanpak. Een gebruiker centrische benadering evenals een zuiver technische benadering aan de tegemoetkoming van punctuele noden kunnen echter tekort schieten aan operationele vereisten die moeten kaderen in een multilateraal verband. Operationele vereisten kunnen ook vaak wijzigen waardoor snellere en flexibelere samenwerkingsverbanden mogelijk zijn.

Desgevallend is sturing vereist zonder dewelke fragmentatie van de architectuur dreigt. Die sturing vereist een langetermijnvisie: een dergelijk visie is noodzakelijk om drie redenen: vooreerst ondersteunt het de operationele vereisten van de C4ISR-architectuur (en zijn cybernetische ondersteuning). Vervolgens laat ze toe om verantwoordelijkheden van alle actoren (zelfs extra-departementaal) af te lijnen. Ten slotte laat een dergelijke visie ook toe dat een eventueel vacuüm in het supranationale niveau wordt opgevangen.

Deel 2

De extra-militaire dimensie

2.1. Inleiding

We hebben in het vorige deel gezien hoe C4ISR een transitiebegrip is een hoe het van land tot land kan verschillen door de opvattingen, de prioriteiten en strategie. We hebben ook gezien hoe de NAVO de transitiestructuur in werking wenst te krijgen en in dat opzicht een overkoepelend concept heeft uitgewerkt dat gebaseerd is op de ervaringen van uit opdrachten getrokken lessen.

In wat volgt zullen we merken dat de transitie in de leidende landen niet beperkt is gebleven tot een integratie op militair vlak: de aanzet van de beweging had initieel een militaire opzet. Sinds 2001 is gebleken dat eerst in de VS en vervolgens ook in China de militaire opzet is geëvolueerd naar een interdepartementale benadering van veiligheid die we vandaag kennen als "homeland security". Die overgang is ook te merken bij de EU: vertrekkende vanuit nationale militaire ervaringen (en enkele concrete projecten die in militair kader worden gelanceerd), willen we nagaan welke de plannen zijn van de Europese Unie met betrekking tot interdepartementale integratie, cyberverdediging en C4ISR. We zullen merken dat de relevantie van fysische grenzen ook hier meer en meer zal vervagen. We gaan de verschillende bijdragen na van in de materie leidende lidstaten en zullen trachten de vergelijking te maken met wat we bij de NAVO hebben kunnen vaststellen.

2.2. De rol van de leidende landen in de extra-militaire dimensie

1.6.1 De Verenigde Staten

Het is naar aanleiding van de aanslagen van 11 september 2001, dat men in de VS tot de vaststelling kwam dat de samenwerking van diensten en vooral de informatie-uitwisseling (vooral het gebrek daaraan) de impact van die aanslagen hebben vergroot: het psychologische gevolg van de vaststelling dat de sterks beveiligde natie onderhevig was aan de meest spectaculaire aanslagen sinds mensenheugenis. Nog tijdens het verloop van de aanslagen werd beroep gedaan op het militaire apparaat om erger te voorkomen. In de onmiddellijke nasleep werden alle overheidsdiensten in de VS onderworpen aan een herschikking van structuren en middelen. De aanpassing ervan paste niet alleen in het kader van terrorismebestrijding maar ook in de reactiviteit in geval van natuurrampen. De organisatietabel van het departement Homeland Security wordt bij wijze van inlichting meegegeven in bijlage drie.

De opdrachten die dat departement wil realiseren kaderen binnen het doel om een het land te vrijwaren tegen terrorisme (en andere dreigingen) door grenzen te bewaken, immigratiewetgeving uit te voeren, het cyberlandschap te beveiligen en veerkracht te bewerkstelligen in geval van rampen (http://www.dhs.gov/): praktisch wil men vooral een coördinerend orgaan gerealiseerd zien tussen de publieke en private sector voor het geval zich een terroristische aanslag, een natuurramp of een andere grote noodtoestand voordoet. Maar de taken beperken zich niet tot coördinatie van samenwerking. Wat betreft de immigratie bijvoorbeeld heeft het ook als verantwoordelijkheid om de wetgeving omtrent het onderwerp te faciliteren en de naleving ervan af te dwingen. In hetzelfde kader wordt informatie-uitwisseling vergemakkelijkt om binnen het wettelijk kader te informeren over werkgelegenheid zonder de veiligheid van de grenzen in gevaar te brengen. Die veiligheid wordt verder verzekerd door technologie, mankracht en infrastructuur. Maar naast de bescherming van fysische grenzen wordt ook het virtuele domein bewaakt.

Het cyberlandschap is het enige domein dat in de opdrachten wordt vermeld: naast de bewaking van de fysische grenzen wil het hiermee onderstrepen dat het virtuele domein een noodzakelijk element is voor de

realisatie van een robuuste C4ISR capaciteit. Hiertoe tracht het departement de coördinatie te bewerkstelligen tussen overheidsdiensten en de industrie alsook tussen lokale en federale overheden. Daartoe wil het de dreiging analyseren en de nodige alerten verspreiden.

De instrumenten die in het kader van die nationale veiligheid worden aangewend spruiten voort uit taken die even uitgebreid zijn als wetgeving, politionele opdrachten, inlichtingen en ook militaire opdrachten. Zoals weergegeven door de organisatorische tabel, dient zowel de informatie als de uitvoering door deze actoren optimaal gecoördineerd te worden. Binnen die Homeland Security opdracht, hebben eenheden specifieke budgeten en taken toegewezen gekregen. Maar ook in de VS ontsnappen deze budgeten en de reorganisatie van krijgsmachten in een post-Afghanistan conflict scenario niet aan de beperking van budgettaire austeriteit. Sinds 1991 werd zo naar schatting 30% van de middelen van de luchtmacht in die opdrachten beperkt en werden de middelen en het personeel aan deze nieuwe situatie aangepast. Naast numerieke inkrimping zijn modernisering en de operationalisering van nieuwe capaciteiten ook een permanente zorg van de competentiecentra in het domein C4ISR (C4ISR CoE) die van Homeland-opdrachten een prioriteit maken: deze competentiecenta werken aan de ondersteuning van de landmacht en de joint force tegen horizon 2020 (DiMichele, 2013).

De bevelvoerder van de elektronische communicaties binnen de krijgsmacht heeft daartoe vier prioriteiten uitgewerkt. Een eerste prioriteit is het beheer van de levenscyclus van C4ISR systemen binnen het kader van een partneriaat tussen de overheid en de private sector. Een tweede prioriteit is de aanpassing van de opleiding: de operator te velde zal in staat moeten zijn om zijn uitrusting zelf te installeren, in werking te stellen en te onderhouden met de nodige software-updates. De derde prioriteit is het samenstellen van een strategie voor het bekomen en behouden van de noodzakelijke mankracht om dergelijke systemen in stand te houden en te exploiteren. In een post-conflict scenario en in een interdepartementale omgeving zoals Homeland Secutiy impliceert dit dat operatoren vooral de selectie van de informatie kunnen optimaliseren en dat hun training daartoe wordt afgestemd. Bovendien moet de generatie van informatie uit eigen systemen eveneens niet leiden tot een te groet flux van onbruikbare informatie: zowel in input als in output moeten eenheden hierop worden voorbereid. Dit impliceert ook ondersteuning waar vereist o.m. het onderhouden van logistieke steunpunten in regionale centra verspreid over de hele wereld (in Europa, Korea) maar ook in het thuisland (Washington, Texas). Ten slotte is de laatste maar niet minst belangrijke prioriteit gericht op het consolideren van het beheer van middelen voor commando en controle (dit omvat zowel personeel als ICT). De aankopen binnen het Homeland Security-concept werden in de loop der jaren permanent

afgetoetst op hun efficiëntie, maar de laatste jaren werd ook de factor betaalbaarheid meer en meer in rekening gebracht: de kosten van de overheid moeten immers worden gereduceerd en in het C4ISR- domein mag dat niet ten koste gaan van cyberveiligheid, positionering, navigatie en timing: deze prioritaire elementen worden naar voren geschoven door de directeur onderzoek en ontwikkeling van het directoraat inlichtingen en informatie-oorlogvoering. Praktisch wil men vanaf nu volledige systemen aan bevelhebbers kunnen worden afgeleverd in de plaats van eigen lokale systemen in te pluggen in een overkoepelend netwerk.

De vaststelling dat C4ISR ondersteuning ook in dit kader voornamelijk gesteund is op de operationele cybercapaciteiten heeft van het virtuele domein een kritisch element gemaakt voor het behoud van de capaciteit. Potentiele vijanden hebben bovendien meer en meer de mogelijkheden om via het cybernetische domein te interfereren met de C4ISR capaciteit. Daarom wil men binnen de USAF de redundantie inbouwen dat een militair cybernetwerk nodig heeft om de continuïteit van de operaties en de besluitvorming te kunnen garanderen zelfs na een eventuele aanval. De criticaliteit van het cyberdomein wordt steeds opnieuw onderstreept en meer nog binnen het kader van een interdepartementale samenwerking zoals die in Homeland Security wordt vooropgesteld: zowel militaire als civiele capaciteiten (hardware, software en infrastructuur) worden hiervoor ingezet van het Department of Defence, de Overheid of zelfs internationale organisaties. Het netwerk dat aldus tot stand komt omvat land, zee, lucht en ruimteassets maar evenzeer PCs, servers en mainframes. De uitwisseling van vitale C4ISR data van en naar beslissingscentra is daarvoor noodzakelijk en gebeurt soms via een beveiligd protocol (Secret Internet Protocol Router Network-SIPRNET), hoewel niet permanent. De meest gangbare uitwisseling gebeurt nog steeds via het Non-secure Internet Protocol Router Network (NIPRNET). En dit blijft alleen mogelijk voor zover dat zowel de civiele als de militaire energievoorziening die transfers van gegevens kan blijven ondersteunen. In het onderzoek naar de kritieke elementen van een dergelijk netwerk komt men bijgevolg tot de vaststelling dat niet enkel (al dan niet menselijke) sensoren (front-end C4ISR) maar vooral de exploitatie van hun gegevens van belang zijn (back-end C4ISR). De combinatie van beiden, en meer nog in een interdepartementaal kader, kan enkel tot stand komen door de beschikbaarheid van het virtuele domein en de energie-infrastructuur die deze moeten ondersteunen: deze twee elementen zijn vanuit Amerikaans oogpunt een kritieke zwakte van ieder C4ISR capaciteit. Dat standpunt wordt bovendien ook gedeeld door de andere landen die de trend bepalen in het domein C4ISR (China en Rusland). Niet enkel commando, controle en communicaties, maar ook de logistiek en de administratie die de beschikbaarheid en de operatie van sensoren moeten mogelijk maken, zijn daarvan afhankelijk.

Tot deze vaststelling gekomen, weet men in de VS dat het materieel niet mogelijk is om het geheel van netwerken en de ondersteuning ervan te voorzien van een ondoordringbare bescherming tegen aanval: de kost ervan loop immers veel te hoog op ten opzichte van assymetrische destructie of aanval via een ondersteunend (cybernetisch of energie) netwerk.

Voor de VS, is het cybernetische domein cruciaal voor de exploitatie van informatie in het kader van Homeland Security: de opdrachten die deze moeten ondersteunen verschillen enkel door de context waarbinnen ze moeten kunnen worden ingezet. Deze behelzen zowel de informatievergaring door middel van sensoren, kinetische aanval, operaties in het virtuele domein, elektronische oorlogvoering en antisatelliet operaties, kritieke energie-infrastructuur enz.

1.6.2 China

Ook China onderschrijft het idee dat C4ISR al lang uit de enge visie is gegroeid dat zich zou beperken tot een militaire rol. Niet enkel de gebruikte technologieën en de complexiteit van de netwerken, maar ook de globale verspreiding van knooppunten van transmissielijnen, sensoren en servers maken het vandaag onmogelijk om C4ISR te beperken tot een militaire rol. En het land beperkt zich daar ook niet toe: het ontwikkelt een uitgebreid glasvezelnetwerk ter ondersteuning van civiele infrastructuur. Eerder dan de transmissie van gegevens draadloos te laten ondersteunen, wil het hiermee een veerkracht kunnen ontwikkelen vanaf de ontwikkeling van het netwerk dat compatibel wil zijn met de sensoren die bestaan en of nog in ontwikkeling zijn. In alle toepassingen zorgt China voor een duale toepassing van zijn capaciteit. Zo zijn ook de satellieten van het civiele programma niet enkel tot civiele toepassingen beperkt: zelfs de aangekochte GEO-satellieten worden gebruikt om de beschikbare bandbreedte aan te vullen in noodgevallen. Uiteraard heeft het ook specifiek militaire transmissie uitgerust met een aan NAVO equivalente Link-16 en Link-22 (Kopp, 2014).

Ter ondersteuning van de natie in noodgevallen wordt die capaciteit bijvoorbeeld ingezet ter exploitatie van beeldvorming na aardbevingen. Uiteraard kan dit ook een zuiver militaire exploitatie genieten, waardoor ook de classificatie dubbel gebruik komt.

De investeringen in 2011 bedroegen 305 miljard USD voor de globale Homeland Security and publieke veiligheid. Voor het eerst zal China de VS in 2014 van de eerste plaats stoten: de tendens wijst immers op een schatting van om en bij de 55 miljard USD voor China alleen (Homeland security and market research, 2014). Dat maakt de investering van homeland security, naar

eigen zeggen groter dan zijn defensie investeringen. Voor een deel gaat ook de VS daar in mee aangezien het de export van militair materieel naar China wel heeft aan banden gelegd, maar niet het materieel van Homeland Security waardoor de Amerikaanse overheid een grotere exporteur wordt naar het land dan het Department of Defense.

Het project Homeland Security wordt niet enkel meer gemotiveerd door militaire of civiele doelstellingen voor ondersteuning, maar wordt het een prestigeproject van de overheid die er evengoed economische wenst mee te moduleren: tegelijk tracht het hiermee de sociale spanningen, maar ook de inheemse etnische terreur zowel in de motivatie als in de reactieve overheidsmaatregelen een halt toe te roepen. De investeringen die daartoe moeten bijdragen worden verdeeld over verschillende toepassingen van Homeland Security te weten:

Tabel 2: Homeland Security Market van China (Homeland Security Research, 2014).

Domein Homeland Security	Verdeelsleutel budget (% in 2011)
Bescherming kritieke infrastructuur	41
Vliegtuigveiligheid	12
Maritieme veiligheid	4
Beveiliging van massatransport	4
Beveiliging van landsgrenzen	3
Eerste hulpverlening	10
Beveiliging van steden	21
Veiligheid van evenementen	5
Andere	1

Het is nog vermeldenswaard dat de term Homeland Security uit de VS niet zomaar in de Chinese context kan worden getransponeerd zonder aanpassingen van de begrippen: Homeland Security heeft voor China ook een connotatie van verdediging tegen separatistische krachten van Taiwan. In dat opzicht zijn militaire investeringen anders te beschouwen in een kader van Homeland Security dan in de VS. Bovendien is een ander onderscheid te vinden de organisatie van Homeland Security: het land beschikt immers niet over een eigen departement. Ten slotte is er ok geen juridische onderbouwing van de taken van elke actor in het domein. Voor elk specifiek noodgeval wordt wel een relevant wettekst gevonden (bijvoorbeeld de wetgeving over bescherming tijdens aardbevingen, bescherming tijdens overstromingen of brandhaarden). De interdepartementale samenwerking is echter niet bij wet beschreven noch is er een strategische visie, plan of wetgeving die

noodtoestanden behandelt. De overeenkomsten worden *ad hoc* genomen op het ogenblik zich een noodtoestand voordoet.

Ten opzichte van de VS heeft het land nog een weg te gaan. Om een vergelijkbare paraatheid aan de dag te kunnen leggen heeft het land nood aan:

-het interdisciplinair departement Homeland Security moet worden opgericht;
-de wettekst die de bevoegdheden van dat departement omschrijft (zoals daar zijn terrorisme, cyberdefence, noodplanning tijdens natuurlijke of door de mens gegenereerde rampen) evenals alle relevante actoren kadert, moet nog worden opgesteld;
-de administratie voor de coördinatie van de actoren die samenwerken in dat departemement is onbestaande.

Daarentegen is het land wel bewust van de eigen mogelijkheden van de eigen offensieve cyber-capaciteit: het maakt van het land een actor die bewust is van het potentieel dat een vijandige actor in werking kan zetten. Daarom stelt het ook alles in het werk om a priori een veerkrachtig netwerk uit te bouwen van bij aanvang en terwijl het netwerk zich ontwikkelt, in tegenstelling tot wat men in het Westen gewoon is. In wat volgt gaan we na hoe de Europese Unie zich engageert in het C4ISR-domein en of de EU zich door het Amerikaanse voorbeeld al dan niet heeft laten inspireren om zijn homeland security te organiseren.

2.3. De rol van de Europese Unie

2.3.1 C4ISR in de EU

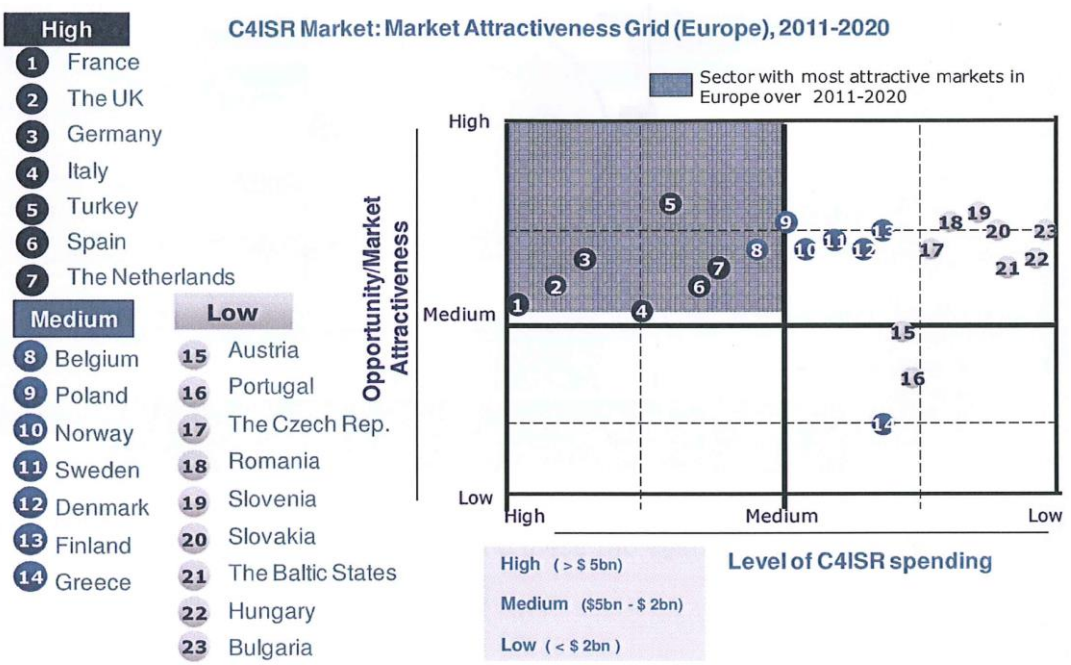
De EU is een civiele organisatie bij conceptie en in opzet met een beleid oriënterend doel. Vooreerst betekent dit dat er een fundamenteel verschil bestaat ten opzichte van de NAVO met betrekking tot de C4ISR-materie. Indien men al geruime tijd ook een gemeenschappelijk veiligheids- en defensieluik wil creëren, is men genoodzaakt vast te stellen dat de uitvoering ervan nog ver te zoeken zijn. In het bijzonder is er geen vergelijk met de *jointness* waarvan eerder sprake en is men op dit niveau nog bezig met de realisatie van interoperabiliteit. 1999 was het jaar waarin het Verdrag van Amsterdam in werking trad: dit had de start moeten inluiden van een gemeenschappelijk defensie- en veiligheidsbeleid. In 2004 omschreven Adams et al. de situatie als volgt (Adams et al., 2004; p. 83):

> "Although the EU may evolve into an important future context for coordinating European policy, requirements, and acquisition in the C4ISR arena, its military planning work is far too preliminary to provide a context for resolving interoperability problems of today. In addition the United States plays no part in the internal military and security policy structure of the EU, making a separate context for dealing with the transatlantic relationship necessary."

Tien jaar later is de EU wat dat betreft nog niet veel verder in zijn stappen naar volwaardige interoperabiliteit, laat staan *jointness*, zoals eerder uiteengezet een noodzakelijke stap in de transitie naar operationele C4ISR. Waar de VS de netwerkcentriciteit hoog in het vaandel draagt en de NAVO haar capaciteiten toetst aan het vermogen om netwerkgerichte operaties te kunnen uitvoeren, is de EU in vergelijking nog niet ver geraakt. Het woordgebruik terzake werpt een niet oninteressant licht op de doelstellingen van eenieder. In de Angelsaksische literatuur vindt men voor de VS de term *Network-centric warfare* (NCW) het vaakst terug: dit wijst op een geoperationaliseerde capaciteit die centraal staat, zelfs in de meest intense fasen van een conflict. Het NAVO-kader verwijst eerder naar *Network Enabled Capabilities (NEC),* wat wijst op een vermogen om op een interoperabele manier trans-Atlantisch te kunnen opereren. Met betrekking tot

de EU bestaat er geen consistent systematisch woordgebruik, hetgeen de onduidelijkheid van de finaliteit en van de samenwerking onderstreept: de jongste voorstellen van het Europees Defensieagentschap (EDA) duiden op de verbeteringen die in deze nog aangebracht moeten worden: *Towards improved C4I functional performance and interoperability* is de gedragen titel van het programma 2013 dat als referentie moet dienen. Van de oorspronkelijke capaciteiten (European Capabilities Action Plan - ECAP) die tien jaar geleden deel uitmaakten van het plan om de Europese defensiecapaciteit aan te zwengelen, waren drie projecten gericht op die beoogde verbetering in het besproken domein, met name hoofdkwartieren, onbemande vliegtuigen en een ruimteprogramma. De verantwoordelijkheid van de projecten werd respectievelijk gedragen door het Verenigd Koninkrijk voor het eerste en Frankrijk voor de twee overige. Ook op middellange termijn zien we dat deze landen waarschijnlijk de belangrijkste inspanning zullen genereren voor de mobilisatie van hun respectieve defensie-industrie. Frost en Sullivan extrapoleren de attractiviteit van deze markt zoals aangegeven in figuur 4.

Figuur 6: attractiviteit en investeringsniveau C4ISR voor EU-lidstaten (Frost & Sullivan, 2012; p. 4).



De inspanningen die onder de EDA-koepel de functionaliteit en interoperabiliteit moeten verbeteren omvatten vijf projecten in een gemeenschappelijk clusterprogramma onder de hoofding *Intelligence, Surveillance, Reconnaissance, Target Acquisition and Weapon-to-Target*

Matching in Complex Environments (ISRTA-WTM), vandaag gekend onder de benaming JANUS (Joint Advanced Networking in Urban Scenarios): het project is een combinatie van overheid gestuurde (Cat A) en bottom-up gestuurde (Cat B) projecten in vijf deelgebieden (EDA (a), 2013; annex 2):

- Wireless Sensor Networks (WSN) integreert verschillende sensoren voor observatie in grote steden en voorziet in de mogelijkheid om ook robotica te connecteren en machines met elkaar te laten communiceren en interageren. In het verlengde hiervan is men het eens over de exhaustieve interpretatie van de context van een dergelijke communicatie.

- Future Military Radio Node (FM2RN) zou oplossingen moeten bieden voor *ad-hoc* netwerken in het UHF/VHF-bereik.

- Civil communications technologies: de militaire toepassing van civiele technologie kan tegelijk de performantie, de informatiestroom en de veerkracht in tactische applicaties verhogen.

- Semantic grid: een integratie en automatisatie van de beslissings- en commandoketen veronderstelt dat er een aangenomen begrip bestaat van de context waarin termen gebruikt en geïnterpreteerd worden. In een netwerk waarin vooral diensten worden aangeboden en waar zowel sensoren als wapensystemen op ieder moment kunnen worden aangesloten of weggehaald naargelang de noden van de opdracht, moet uitgegaan worden van een gemeenschappelijke basis en interpretatie van opdrachten en procedures, ook wanneer de menselijke factor minder belangrijk wordt.

- Ambient Assisted Fighting (AAF): is een toekomstgericht concept waarin zowel bemande als onbemande operaties in complexe (stedelijke) gebieden kunnen plaatsvinden. Dit project zou moeten toelaten om te compenseren voor het asymmetrische voordeel.

Zowel private bedrijven als academische instellingen en overheden zijn betrokken in deze cluster. De verscheidenheid aan toepassingen draagt het intrinsieke gevaar mee van fragmentatie in de plaats van bij te dragen aan een uitgewerkte en dragende structuur voor de C4ISR-architectuur. Een snelle technologische innovatiecyclus maakt bovendien de sturing overheidshalve noodzakelijk wil men het gemeenschappelijke doel niet voorbijschieten. De betrokkenheid van nationale defensie-industrie in een context van economische crisis houdt bovendien het gevaar in dat economische motieven worden verkozen boven de politieke-strategische multilaterale belangen (in deelbesluit over EU).

Voor het sturen van de besluitvorming zijn inlichtingen noodzakelijk, onder meer afkomstig van informatie ontsproten uit beeldverwerking. Hiervoor heeft de EU een satellietcentrum operationeel in Torrejon de Ardoz. Klanten van hun producten vind men onder meer bij de EDEO (Europese Dienst voor Extern Optreden), CPCC (Civil Planning and Conduct Capability), EUMS (European Union Military Staff) en SitCen (Situation Centre). Om de inlichtingen te genereren heeft het centrum echter civiele of militaire satellietbeelden nodig die het vandaag nog moet kopen van niet-Europese landen of nationale of multinationale programma's (zoals HELIOS-2). Op korte termijn zijn lopende militaire programma's die als input dienen voor dit agentschap op het einde van hun levensduur. Een valabele opvolger zou het programma Multinational Space-based Imaging System for Surveillance (MUSIS) kunnen zijn, ontworpen door Frankrijk, Italië en Duitsland. De realisatie van dit programma zou een zekere onafhankelijkheid kunnen genereren ten opzichte van niet-Europese bronnen met betrekking tot het bekomen van betrouwbare inlichtingen op langere termijn (horizon 2030). We stellen echter vast dat voor de EU alle elementen die zouden kunnen bijdragen tot de uitbouw van een C4ISR-netwerk en de beveiliging ervan niet gecoördineerd zijn of slechts beperkte capaciteiten hebben.

In de transitie naar een netwerk ondersteunde architectuur kan men de EU daarom hooguit in de eerste fase plaatsen: interoperabiliteit in defensieaangelegenheden is een dagelijkse zorg voor het Europees Defensieagentschap (EDA) en meer bepaald de vooruitgang met betrekking tot het domein C4ISR: het zijn de vaststellingen van de tekorten in operationele omstandigheden (al dan niet in multilateraal verband) die ervoor hebben gezorgd dat dit onderwerp überhaupt aandacht heeft gekregen. Een tweede parameter die in die richting heeft gewerkt is de verandering van de houding van de VS: *strategic shift* naar het Verre Oosten zal Europa dwingen om te investeren wil het in de toekomst een politieke rol van betekenis blijven spelen die zich kan beroepen op een militaire capaciteit. De discussie met betrekking tot de noodzaak van vooruitgang in dit domein is immers niet eens

aan de orde: of men de gemeenschappelijke troepenmacht kwalitatief dan wel kwantitatief heeft omschreven of niet, en of die dan wel zeer mobiel zou moeten zijn of net eerder traag inzetbaar zou kunnen zijn, C4ISR is een onvermijdelijke capaciteit waarop iedere krijgsmacht (of onderdeel ervan) zich zal moeten kunnen beroepen indien het in multilateraal verband wil opereren.

Een onscheidbaar onderdeel van die architectuur wordt samengesteld door het cyberdomein en zijn beveiliging. Ook op dit vlak heeft de EU nog inhaalwerk ten opzichte van een operationeel platform als de NAVO. Ondanks het feit dat een cyberstrategie werd uitgewerkt, zijn de bevoegdheden voor de uitvoering, de controle op de naleving ervan en de respons verspreid over drie actoren in de organisatie, te weten:

- de commissaris voor de digitale agenda (DG CNCT)

- de commissaris voor interne aangelegenheden (DG HOME)

- de hoge vertegenwoordiger van de externe dienst (EDEO)

De strategie die voorgesteld werd op 7 februari 2013 is getiteld *An Open, Safe and Secure Cyberspace* en heeft vijf krachtlijnen, namelijk het versterken van de veerkracht in het cyberdomein, het verminderen van de impact door cybercriminaliteit, het beleid betreffende *cyber defence* in het kader van het gemeenschappelijk veiligheids- en defensiebeleid, de ontwikkeling van industriële en technologische oplossingen voor de verbetering van cyberveiligheid en ten slotte een coherent beleid in dit domein dat de waarden van de EU weerspiegelt. Elk van deze krachtlijnen vereist een deel uitvoeringsverantwoordelijkheid van elke van de voornoemde actoren, waardoor coördinatie essentieel wordt op straffe van onwerkbaarheid of verlamming. Op beleidsniveau is niet één enkele entiteit bevoegd voor de coördinatie van de responscapaciteit zoals dat het geval is bij de NAVO. Waar de verantwoordelijkheden duidelijk afgebakend en de activiteiten van elke van de betrokken actoren gecoördineerd worden, hoeven er nog niet meteen vragen te rijzen met betrekking tot de haalbaarheid van de gestelde doelstellingen van de strategie. De problemen rijzen wanneer men tot de vaststelling komt dat de verantwoordelijkheid van actoren overlappen: cybercrime is de bevoegdheid van DG HOME, terwijl de cybercrime buiten het territorium door EDEO zou moeten behandeld worden. Rekening houdend met het grensoverschrijdende karakter van de problematiek kan men zich vragen stellen bij de verdeling van de bevoegdheden. En zo gaat het ook met capacitaire ontwikkeling voor gebruik binnen of buiten de EU-grenzen.

Mogelijk is dit het gevolg van de structuur binnen een oorspronkelijk civiele organisatie als de EU.

Maar meer nog dan voor de civiele toepassingen is de militaire operationaliteit afhankelijk van de goede en ook snelle werking van de opgestelde architectuur. Net dit aspect vertoont nog ruimte voor verbetering volgens een EDA studie waarvan de resultaten in mei 2013 werden voorgesteld (EDA (b), 2013). In het bijzonder de uitrusting blijkt in het capacitaire domein volgens de studie tekort te schieten. De lidstaten blijken sterktes te kunnen genereren in domeinen als leiderschap, personeel en interoperabiliteit. Doctrine, organisatie en training daarentegen blijken in een vroeg stadium van maturiteit te verkeren wat te wijten zou kunnen zijn aan de complexiteit enerzijds en de vereiste inspanning op langere termijn anderzijds. Vooruitgang wordt echter niet in de hand gewerkt door opgesplitste mandaten en niet- opgelijnde strategieën van individuele lidstaten. Interoperabiliteit in dit domein wordt gerapporteerd als een van de domeinen waarin sterktes worden getoond door lidstaten en tegelijk beveelt men de lidstaten aan om werk te maken van interoperabiliteitsaspecten van *cyberdefence*. Om die op te vangen duidt het agentschap drie prioritaire projecten *ad hoc* aan:

- Cyber Ranges: doelt op het gemeenschappelijk gebruik van trainings- en testfaciliteiten.

- Deployable cyber situational awareness-kit: doelt op het realiseren van een gemeenschappelijk *cyberdefence*-planning- en managementplatform.

- Advanced Persistent Threat Detection (APT-D): doelt op snelle waarschuwing en het matigen van dreigingen.

Het bestaan van projecten *ad hoc* in het specifieke cyberdomein doet het vermoeden rijzen, zoals in het geval van de NEC-transitie, dat defensie-industrie in concrete gevallen projecten aanstuurt zonder dat er ook op beleidsniveau een aansturing mogelijk is die de rationale uitbouw van de uiteindelijke C4ISR-architectuur zou moeten mogelijk maken, althans binnen het EU-platform. Prioriteiten enerzijds en een agenda anderzijds moeten gecoördineerd worden met lidstaten maar eveneens met andere platformen zoals daar zijn de NAVO en de VN. Zonder die coördinatie zal men vroeg of laat geconfronteerd worden met redundanties die in strijd zijn met het nagestreefde rationele gebruik van middelen en zodoende economisch en sociaal voordeel ontlopen boven op de operationele ontoereikendheid.

We hebben eerder aangehaald dat een strategische visie is vereist op nationaal vlak. De invulling van een dergelijke visie is noodzakelijk om drie redenen: vooreerst legt een dergelijke visie de plaats van C4ISR en cyber in onze samenleving vast, alsook de relatie van deze domeinen ten opzichte van andere architecturen die onze samenleving draaiende houden (een schematisch aspect van deze relaties wordt in het volgende hoofdstuk over kritieke energie-infrastructuur behandeld). Vervolgens laat ze toe om de mandaten van nationale actoren te verankeren en af te lijnen. Ten slotte laat een dergelijke visie ook toe dat een eventueel vacuüm in het supranationale niveau wordt opgevangen. Wachten op een supranationale visie (en die dan vertalen naar nationaal niveau) gaat in C4ISR-ondersteuning en cyberpolitiek leiden tot onoverkomelijke tekorten. We weten ondertussen dat de nationale standpunten ook belangrijk zijn om private actoren te integreren in een overkoepelende visie: deze actoren bezitten in het C4ISR-en cybertweeluik een groot deel van de exploitatiemogelijkheid, wat coördinatie vereist boven op de bepaling van verantwoordlijkheden. Tot op vandaag blijkt een dergelijke visie, die zich kan materialiseren in een nationale veiligheidspolitiek, niet voorhanden in België. Het enige nationale veiligheidsplan dat bestaat is er een dat het politiebeleid van de geïntegreerde politie toelicht en de opdrachten van de federale politie vastlegt. Sinds december 2012 heeft ons land ook een cyberstrategie. De doelstellingen die deze nastreeft zijn drievoudig (Kanselarij van de Eerste Minister, 2012; p.1):

- streven naar een veilige en betrouwbare cyberspace met respect voor de fundamentele rechten en waarden van de moderne samenleving;

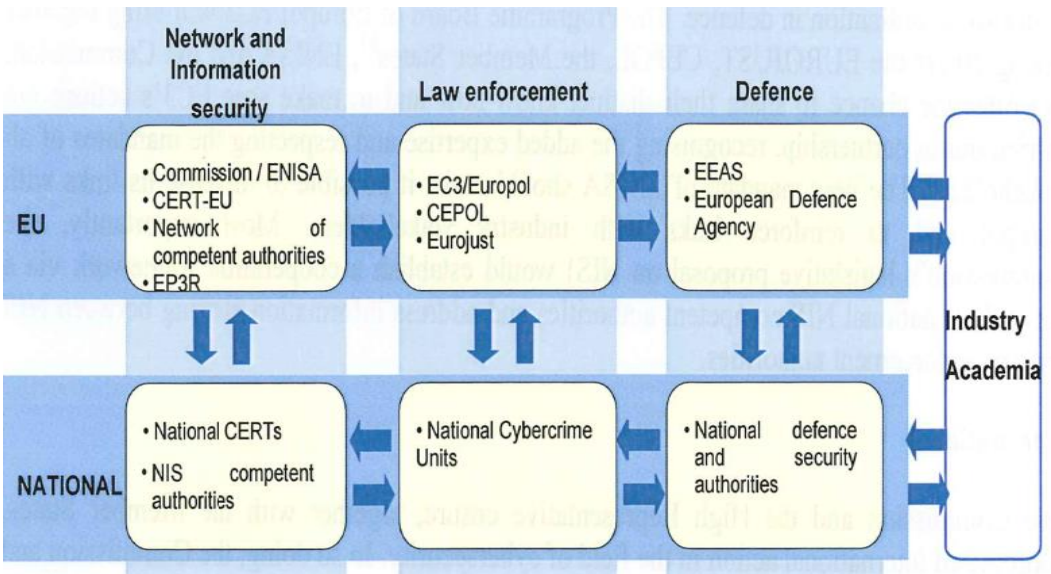
- streven naar een optimale beveiliging en bescherming van de kritieke infrastructuren en overheidssystemen tegen de cyberdreiging;

- ontwikkelen van eigen cybersecuritycapaciteiten voor een onafhankelijk veiligheidsbeleid en een gepaste reactie op veiligheidsincidenten.

Cyberveiligheid isoleren komt erop neer dat men geen algemeen zicht heeft op de dreigingen en zwakheden. De combinatie van het cyberelement met inlichtingen, observatie en verkenning (ISR) draagt bij aan het scheppen van een overkoepelend beeld van dreigingen, risico's en opportuniteiten ter ondersteuning van besluitvorming. Cybersecurity is daarom een begrip dat past in een groter geheel. Niet het minst voor de operationele werking van C4ISR en in die hoedanigheid is het van het grootste belang dat cyberveiligheid wordt nagestreefd. Anderzijds is er ook een versterkende of verzwakkende terugkoppeling tussen C4ISR en cyberveiligheid. Een *a priori* gecoördineerde aanpak van C4ISR binnen de actoren van de EU laat toe om

een efficiënte vorm van cyberveiligheid te realiseren. De uitwerking van een cyberstrategie zonder inachtname van een overkoepelende visie voor de C4ISR-architectuur zou de operationele resultaten ervan in het gedrang kunnen brengen of de toekomstige Europese capaciteit beknotten.

Figuur 7: interdepartementale en supranationale actoren in de EU-strategie (EEAS, 2013; p. 17).



Vele landen kaderen daarom hun cyberstrategie in een groter geheel: de visie van nationale veiligheid. In ons land is dat op het ogenblik van de redactie van dit werk nog niet het geval. Nochtans, zoals de cyberveiligheid geen exclusief civiele aangelegenheid is, is ook C4ISR geen exclusief militaire applicatie. De C4ISR-transitie overkoepelt daarom het EU-schema en beperkt zich niet tot de defensietak. Alleen die benadering garandeert een interoperabel en operationeel geheel dat kosten batenefficiënt is.

We hebben eerder aangegeven dat de transitie naar C4ISR de connectie van nieuwe sensoren en het gebruik van nieuwe toepassingen impliceert: dit kan ook nieuwe gevoeligheden aan het licht brengen die het cyberaspect overstijgen en de gehele architectuur betrekken in het veiligheidsaspect. Meer en meer zal men daarom met een term als veiligheid moeten duiden op het onderscheid dat men in de Angelsaksische betekenis maakt tussen de termen “safety” enerzijds en “security” anderzijds. Wat wij verstaan onder de noemer veiligheid zal een aspect behelzen van gebruikersveiligheid enerzijds (de mogelijkheid van het gebruik en de zekerheid van de beschikbaarheid van middelen en diensten) en een aspect van veiligheid van het netwerk anderzijds, zijn sensoren en zijn architectuur die zowel data als hardware moet

kunnen vrijwaren (tegen aanvallen en/of beschadiging en/of diefstal), zelfs indien ze niet worden gebruikt. De integratie van departement, nationale en supranationale actoren in die transitie vereist daarom een strategie die militaire operaties mogelijk maakt, maar ook de niet-militaire toepassingen vereenvoudigen. Een voorbeeld hiervan is de coördinatie van noodhulp bij rampen zowel *in situ* als het beheer van die hulp op het beleidsniveau. De toedracht van C4ISR bij de realisatie van die hulp is voorlopig slechts heel beperkt en is tot hiertoe een civiele toepassing gebleken van militaire middelen in een civiele omgeving. De veelheid aan actoren en respectieve mandaten alsook hun standpunten maken van het *network of things* een constructie die de militaire aspecten van het netwerk overstijgt. Alhoewel in dit specifieke geval ook militaire sensoren kunnen worden gebruikt om de impact van een ramp in te schatten, is de civiele sector evenzeer betrokken door de coördinatie van transport per trein, over de weg of in de lucht, energievereisten en medische hulpverlening. Het gebruik van het *global information grid* zal ook toelaten om een ogenblikkelijke stand van zaken te kennen in die coördinatieoefening. De *situation awareness* wordt hiermee gegarandeerd. Bovendien wordt de transitie van onmiddellijke noodhulp naar de organisatie van de reconstructie eenvoudiger. Uiteraard vergt dit niet alleen een technische connectie van sensoren en middelen, maar ook een "politieke connectie" (verder vermeld als Connectie), met andere woorden een gemeenschappelijk standpunt dat raakpunten vindt en toelaat om de beschikbare middelen in een gemeenschappelijke visie aan te wenden. Zonder deze Connectie zal het onmogelijk zijn, ondanks het bestaan van een geïntegreerd netwerk, om enige meerwaarde uit de nieuwe architectuur te winnen. Misschien wordt dit wel het kritieke element voor de realisatie van een dergelijk netwerk. De eigenheid ervan is de snelle beschikbaarheid en de mogelijkheid tot snelle besluitvorming aan de hand van juiste informatie: indien niet de beschikbaarheid van informatie de snelheidsbepalende stap wordt maar eerder divergerende politieke standpunten in dat proces, dan zal geen enkel netwerk (bestaand of toekomstig) de snelheid en de efficiëntie van de besluitvorming kunnen beïnvloeden. Reden waarom een minimale "politieke connectie" moet bestaan waarmee we doelen op de mogelijkheid tot het bereiken van overeenkomsten in een tijdsbestek dat niet de snelheidsbepalende stap zal worden. De voorbeelden die we, zowel uit nationale als supranationale fora hebben kunnen ervaren, maken voor dit aspect duidelijk dat niet alle fora kwalitatief gelijkwaardige dragers kunnen zijn van de C4ISR-architectuur: hooguit kunnen ze klant ervan worden eenmaal deze architectuur operationeel. Nochtans kan deze slechts een optimale werking garanderen bij de integratie van alle besluit- en uitvoeringsniveaus. In die hoedanigheid is men ertoe geneigd te besluiten dat die voornoemde Connectie een noodzakelijke voorwaarde zal zijn voor de optimale werking ervan.

We komen tot de conclusie dat een nationale cyberstrategie slechts een gedeelte is van de oplossing: een noodzakelijke maar geen voldoende voorwaarde. Naar Nederlands voorbeeld moet deze passen in een groter geheel dat alle nationale veiligheidsaspecten betrekt. Enkel deze benadering laat toe om supranationaal te integreren en te komen tot voormelde Connectie. We hebben de grootste spelers in het cyberdomein overlopen, hoe ze zich ten opzichte van elkaar positioneren en hoe ver ze zijn in de transitie naar C4ISR. We zijn tot de vaststelling gekomen dat het cyberdomein slechts een onderdeel is van de C4ISR-koepel, met als logische gevolg dat een cyberstrategie moet passen in een ruimere benadering van het begrip veiligheid: enkel op die manier kan de genese van een netwerkarchitectuur geoptimaliseerd worden. Een noodzakelijke voorwaarde voor de werking ervan is de realisatie van een Connectie. We gaan in het volgende hoofdstuk na in welke mate die Connectie alleen regulerend kan zijn en in welke mate die kan beïnvloed worden door externe factoren.

2.3.2 EU's eerste stappen in Homeland Security

De benadering in de EU is anders dan die in de VS of China: de taken die de EU zich vandaag toebedeelt onder het directoraat-generaal home beslaan volgende thema's:

-immigratie
-asiel
-het beheer van de Schengen-zone en visa
-interne veiligheid
-georganiseerde misdaad en mensenhandel
-grootschalige rampen en terrorisme
-politiesamenwerking
-internationale veiligheid (thematische prioriteiten: asiel, migratie en veiligheid; geografische prioriteiten: kandidaten voor toetreding, onmiddellijke nabijheid van de EU en strategische partners)

De bestrijding van terrorisme wordt in tegenstelling tot in de VS in de eerste plaats behandeld als de strijd tegen een criminele organisatie die samenwerking vereist van inlichtingendiensten, justitie en politiediensten maar niet meteen militaire middelen. Bovendien is de inzet van militaire middelen in velen landen van de EU slechts voorzien in het kader van steun bij rampen die de civiele capaciteiten van een land zodanig zouden ontwrichten dat enkel nog de bijkomende inzet van militaire middelen zou kunnen helpen. Het zijn dus voornamelijk politiediensten en civiele structuren die in de EU instaan voor de preventie, reactie en herstel bij terroristische aanslagen of rampen van natuurlijk of veroorzaakte oorsprong. Merk op dat in sommige landen, zoals het Verenigd Koninkrijk, Duitsland en België, middelen nog verspreid zijn over het federale en het lokale niveau: in dat

kader wordt een bijzondere aandacht geschonken aan kritieke infrastructuur, volksgezondheid, en hulpverlening bij rampen maar in geval van gedelegeerde bevoegdheden is een nationale coördinatie voorzien wanneer de in te zetten middelen de capaciteit van het lokale bestuur overtroeven. Het enige domein waarin het Amerikaanse departement Homeland security en de EU rechtstreeks samenwerken op supranationaal vlak is voor het ogenblik beperkt tot cyberveiligheid: in een gemeenschappelijke verklaring (Joint Declaration between the Department of Homeland Security and the European Commission) wordt een open en toegankelijk Internet nagestreefd waarin een gemeenschappelijke inzet de cyberveiligheid ten goede zou moeten komen. Hiertoe wordt vooral de samenwerking van de overheid met private partners, politiediensten en industrie aangemoedigd (EU Commission, 2012):

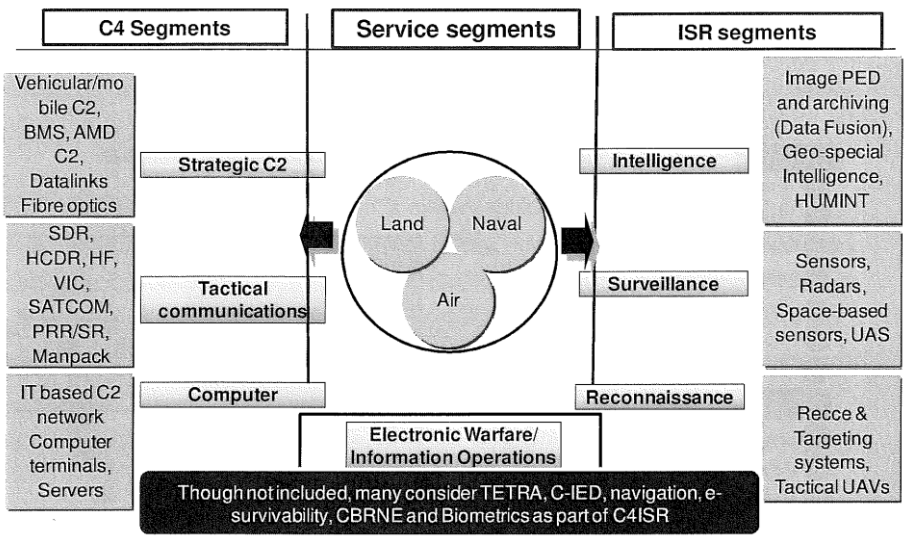
"The U.S. and the EU intend to continue to work to raise cyber security awareness, promote public-private partnerships, and improve our ability to collaborate on cyber security issues of mutual concern. Through such work we hope to reduce risk for our societies and improve our ability to mitigate harm and prosecute perpetrators of heinous crimes such as child exploitation."

De taken die DG HOME wil uitvoeren zijn vooral sturend/coördinerend. Het blijven de lidstaten die beslissen over de te nemen maatregelen en middelen die het hiervoor wil aanwenden. De disciplines waar het directoraat zich wil op toespitsen zijn de beveiliging van de externe grenzen (Frontex), de strijd tegen het terrorisme en criminele organisaties (Europol, cepol), asiel en migratie (EASO), cyberveiligheid (eu-LISA). Al bij al is het geheel nog niet proactief gecoördineerd: het komt erop neer dat reacties volgen op dramatische incidenten. Om dit te verhelpen werd het voormalig pilaren-systeem geïntegreerde en zag het departement homeland het licht. Echter het bestaan van een dienst voor extern optreden en het daaruit voortvloeiende scheidingslijn tussen interne en externe veiligheid laten niet altijd de coördinatie toe die een strijd tegen terrorisme zou vereisen, bijvoorbeeld in het domein van de informatievergaring en verwerking. Bovendien blijven de inzetbare middelen in voormelde domeinen nationaal: het is niet vanzelfsprekend om aan het supranationale niveau middelen toe te reiken die de laatste barrières van soevereiniteitsperceptie weg te halen.

Of het nu gaat over de interne veiligheid of projecteerbare capaciteit, de EU is meer dan ooit toegewezen op het delen van middelen en het collectief aankopen ervan. De economische en financiële crisis van 2008 hebben de financiële beperkingen van de lidstaten, en van het collectief immers nog meer in de verf gezet. De principes van "pooling en sharing" worden daarom in de EU ook toegepast. Maar de EU blijft nog steeds naar de NAVO kijken voor het ontwikkelen van strategische communicatiemiddelen en raket

afweersystemen. Beide projecten hebben hun plaats in homeland security en maken deel uit van het grotere C4ISR geheel dat uiteraard ontsproten blijft uit het militaire milieu. Het geheel van middelen, ook van militaire niche, is van dien aard dat een dubbel gebruik tegelijk een garantie is voor operationele beschikbaarheid en tegelijk de best beschikbare mogelijkheden van interoperabiliteit toelaat. Figuur 6 geeft weer welke segmenten een aanboorbare markt vormen voor de realisatie van een geïntegreerd C4ISR netwerk binnen de EU (homeland operaties).

Figuur 8: bruikbare marktelementen in de EU ontsproten uit militaire toepassingen (Frost en Sullivan, 2012; p.3).



C4ISR laat toe om de inzetmogelijkheden van militaire platformen of civiele capaciteit te optimaliseren optimaliseert en tegelijk verschillende departementen beter te connecteren. Dit kan op dezelfde manier worden gerealiseerd als de connectie die tussen de verschillende machten binnen de krijgsmacht uitgegroeid is tot een joint architectuur. Meer nog dan dat, kan binnen het Europese kader, en dankzij C4ISR, een netwerking tot stand komen tussen verschillende lidstaten in een operationele context, bijvoorbeeld tijdens crisisbeheer na een ramp.

In het bijzonder zijn snelle waarschuwingsnetwerken en centra de uitgelezen plaats om de informatie van de C4ISR architectuur te integreren binnen het kader van de taken die homeland security wil realiseren. Enkele voorbeelden omvatten: MIC (Civil Protection Monitoring and Information Centre: een waarschuwingssysteem om wederzijdse hulp sneller op gang te brengen

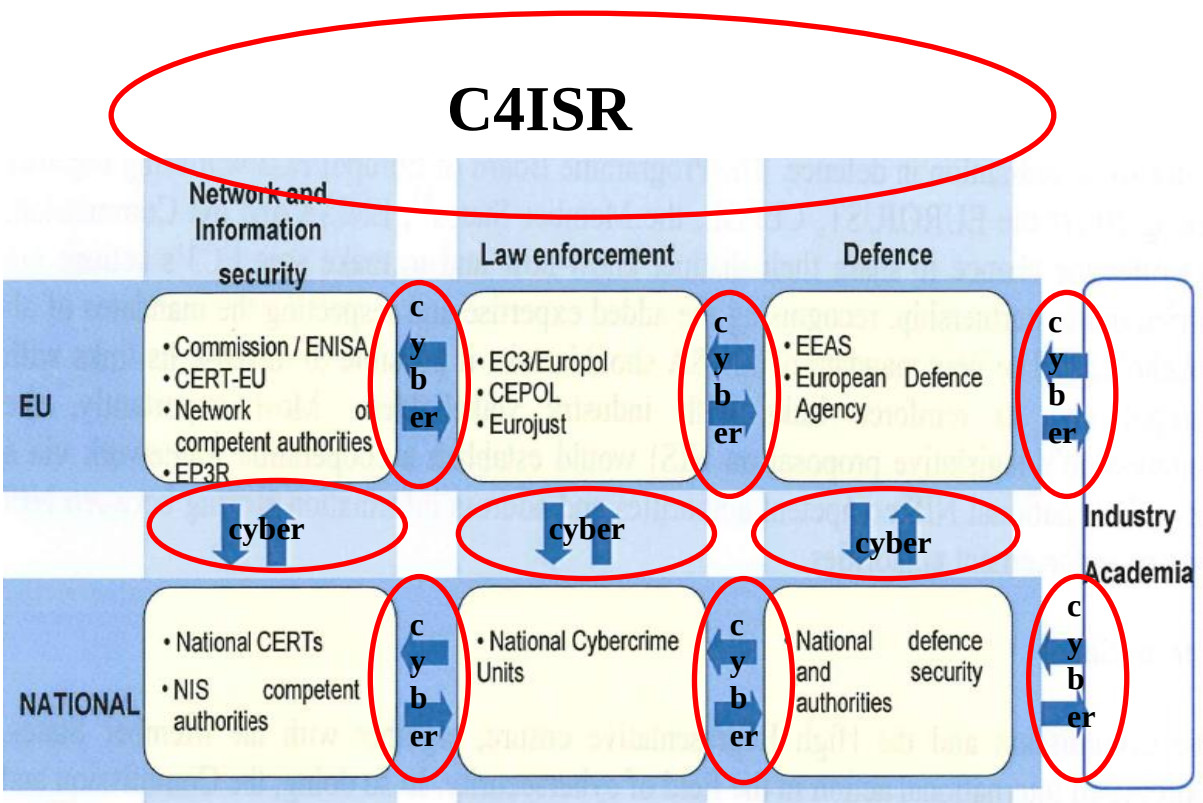
tussen lidstaten in geval van ernstige noodgevallen); ECURIE (European Community Urgent Radiological Information Exchange: informatienetwerk bij radiologische noodgevallen; BICHAT (program for cooperation on preparedness and response to Biological and Chemical Attacks: waarschuwingssysteem voor biologische en chemische dreiging en aanval aangevuld met het mondiaal medisch waarschuwingsnetwerk MedISys); RAPEX (Rapid Exchange of Information of alarmerinssysteem voor consumptiegoederen die niet voedsel gebonden zijn); RASFF (Rapid Alert System for Food and Feed databank voor voedselgebonden gezondheidsrisico's); EWRS (Early Warning and Response System voor besmettelijke ziekten); EUROPHYT (phytosanitaire databank); SHIFT (databank voor veterinaire gezondheidscontrole met het oog op import); ADNS (Animal Disease Notification System); ARGUS (General Rapid Alert System: intern netwerk voor verspreiding van informatie binnen de directies en diensten van de Commissie bij het voorkomen van een crisis). Men kan zich echter de vraag stellen omtrent het operationeel beheer van een dergelijk groot aantal waarschuwingsnetwerken die vaak door specifieke hardware worden ondersteund: in iedere discipline heeft men de neiging om voor een geëigend transmissiekanaal voor informatieverwerking te kiezen. Op het gebied van de integratie van de informatie en de gebruikte hardware voor de verspreiding van de berichten is er echter mogelijkheid tot vereenvoudiging. De efficiëntie die een C4ISR-netwerk nastreeft veronderstelt het gebruik van een beperkt aantal systemen die de informatie kunnen integreren en laten doorstromen naar de gebruiker.

We stellen vast dat tegelijk een groot aantal beschikbare systemen en het actoren in de EU waarschuwingsketen moeten worden geïntegreerd. Het front-end C4ISR binnen de EU is bijgevolg tamelijk goed voorzien. De back-end moet echter nog worden uitgewerkt en ge-exploiteert op een niveau dat de directoraten-generaals overschrijdt: het is bijvoorbeeld vermeldenswaard dat grote en complexe crisissen zoals natuurlijke rampen worden behandeld door een ander directoraat dan DG Home. Het netwerk van civiele bescherming valt immers onder de bevoegdheid van DG ECHO (humanitaire hulpverlening) en het operationele centrum ervan is het eerder vernoemde MIC. We komen tot de vaststelling dat zowel de grote dispariteit aan verschillende systemen als de verscheidenheid aan actoren zou gebaat zijn met een grotere C4ISR-integratie: zowel de coherentie van de besluitvorming als de optimalisatie van operationele inzet van als maar schaarser wordende middelen wordt hierdoor mogelijk.

2.4. Vereisten voor nieuwe operatietonelen: concepten en netwerk

We kwamen tot de vaststelling dat zowel de integratie van bestaande systemen als het grote aantal actoren dat een EU homeland security betrekt een integratie van de *front-end* C4SR als van de *back-end* C4ISR vereisen. We gaan na welke de praktische gevolgen zijn voor de implementatie ervan. We verwijzen hiervoor opnieuw naar figuur vijf die alle EU-actoren herneemt, hun positionering en wisselwerking maar passen die grafiek aan met de plaats die C4ISR en *cyberdefence* in dat schema innemen.

Figuur 9: C4ISR en *cyberdefence*.



Figuur 8 illustreert hoe C4ISR in het voorbeeld van de EU de huidige verzuilde en overlappende verantwoordelijkheden overkoepelt. Dit specifieke voorbeeld werd uitgekozen omdat we hiermee kunnen illustreren dat we niet

louter over militaire toepassingen spreken: de bestaande structuren en departementen, zowel op nationaal als op internationaal vlak, werden in het leven geroepen om verankerde taken uit te voeren maar zijn in die hoedanigheid niet meer aangepast aan een veranderend dreigingsbeeld noch aan een snel wijzigend takenpakket. In een genetwerkte structuur zijn effectoren en collectoren (zoals wapensystemen en sensoren) verbonden en betrokken in de informatievergaring en -uitwisseling. Deze kan op haar beurt beschikbaar worden gemaakt voor eender welke klant in het netwerk. Zowel het nationale als het supranationale niveau bieden in deze voorstelling de mogelijkheid om te fungeren als klant (troepen, hoofdkwartieren en beslissingsorganen, hulpdiensten, …) of als voeder/effector van het netwerk (sensor/wapensysteem). De structuur van het netwerk laat toe om zowel de besluitvorming als de sensoren en effectoren met elkaar te verbinden. Hiertoe worden de technische mogelijkheden uitgebreid van zowel civiele als militaire informatie en communicatietechnologie. Het cyberdomein is in dat opzicht niet anders dan één van de beschikbare middelen om de communicatie tussen die oude departementale begrenzing tot stand te brengen: dit domein verhoogt de connectiviteit en maakt samen met de overige architecturale elementen (zoals procedures en doctrines) zuilen overschrijdende communicatie in die configuratie mogelijk. Hieruit blijkt dat de eerder aangehaalde C4ISR architectuur meer behelst dan defensiegerichte toepassingen.

Deze structuur laat toe om vandaag een systeem uit te denken dat de opportuniteit biedt om ook bruikbaar te zijn in de uitdagingen van de toekomst: het is niet met één welbepaald (civiel of militair) doel dat het werd uitgewerkt en het is aanpasbaar aan de noden van het ogenblik, vooropgesteld dat de interoperabiliteit tussen klanten en effectoren wordt nageleefd. Methodes en oplossingen voor civiele of militaire interoperabiliteit zijn wat dat betreft zeer gelijkaardig en het resultaat is ook voor de twee gemeenschappen in aanvullende toepassingen bruikbaar: openbare orde en veiligheid, rampenplanning, veiligheid van ondernemingen en optimaliseren van de besluitvorming in reële of gesimuleerde omstandigheden zijn daarvan slechts enkele voorbeelden. Interpretatiestandaarden, definities en methodes moeten daarom wel overeengekomen zijn met alle klanten en effectoren van alle niveaus die in het netwerk operationeel zijn, ongeacht de functie die ze erin uitoefenen. Deze benadering laat ook toe om zowel nieuwe systemen als oude in te bedden in het geheel: het zorgt ervoor dat niet elke nieuwe opdracht een eigen duur beveiligd communicatiesysteem zou vereisen, los van het feit dat men die opdracht zou kaderen binnen militaire of politiediensten of andere civiele overheids- of private taken. Ook kan men erin slagen om de exploitatie van informatie te optimaliseren: in periodes van besparingen laat dit ook toe om af te stappen van platform centrische oplossingen voor een probleem. De belangrijkste doelstelling zal zijn de operationele resultaten te verbeteren.

Zonder exhaustief te willen zijn, kan men voordelen van deze architectuur waarnemen door de verbetering van:

- communicatie: hoewel in een communicatiesysteem is voorzien met grote capaciteit kan ook de optimalisatie van lagere capacitaire elementen bewerkstelligd worden. Door het gebruik van bestaande zo wel civiele als militaire netwerken kan niet enkel de densiteit maar ook de redundantie (alternatieve routes) gerealiseerd worden;

- *situation awareness*: de integratie van een groot aantal sensoren maakt het beeld dat men kan gebruiken voor de besluitvorming vollediger en minder vatbaar voor verkeerde interpretatie. Maar ook andere elementen dragen daartoe bij. Zo geeft de integratie van inlichtingen en andere dan sensorinformatie (media, meteo, seismische gegevens, databanken) een belangrijke meerwaarde aan complementaire sensordata (radar, spectra).

- informatie operaties: een groot aantal sensoren en bronnen integreren levert een completer beeld. De toegenomen communicatiemiddelen staan bovendien toe om deze gegevens sneller uit te wisselen en desgevallend tot bij de exploitant te brengen, terwijl de mogelijkheden van eventuele tegenstrevers of andere partijen worden onderbroken of vertraagd;

- commando en controle worden aangepast aan de kwaliteit van de gecollecteerde informatie. Bovendien wordt de besluitvorming sneller in concrete gevolgen omgezet ondanks het feit of commando-elementen al dan niet geografisch zijn verspreid of niet. De verkorting van de planning-uitvoeringcyclus kan, zoals hoger vermeld, leiden tot de mogelijkheid om die cyclus fysisch en organisatorisch te verkorten;

- ondersteuning: door conceptie wordt iedere opdracht het resultaat van de best voor de hand liggende combinatie van het drieluik informatie-commando en controle-effector.

Voor de capaciteiten in de toekomst heeft dit theoretisch volgende implicaties:

- uitbreiding van de rol van traditionele militaire effectoren, gericht op het veroveren van een territorium, door geautomatiseerde opdrachttransmissie enerzijds en sensoren die het geïntegreerde netwerk verruimen anderzijds. Tegelijk laat dit toe om de identificatie van alle partijen in de betrokken zone uit te voeren. Hiermee kan het

nagestreefde effect behaald worden met inachtname van het discriminatiebeginsel dat wil dat niet-strijdende partijen niet aangevallen mogen worden. Tegelijk biedt het de mogelijkheid om collaterale schade te beperken;

- hetgeen men zou kunnen omschrijven als "spectruminteroperabiliteit" betekent dat men zowel voor het hoge geweldspectrum als voor ondersteunende opdrachten gebruik kan maken van beschikbare capaciteit. Het ontwikkelen van nieuwe effectoren die enkel voor één type opdracht kunnen ingezet worden zijn vandaag nauwelijks economisch haalbaar en hebben bovendien weinig rendement. Het feit om ook tactische interoperabiliteit te moeten vertonen, impliceert dat niet enkel kan geopereerd worden met gelijkaardige effectoren, maar ook in verschillende coalitieverbanden en organisaties;

- "omgevingsinteroperabiliteit" betekent dat de effectoren of sensoren zich aan wisselende (fysische en/of geografische omstandigheden) kunnen aanpassen. Zowel buiten als in de stad maar ook in alle weersomstandigheden en inzetbaar tegen geregelde troepen of niet-staatsactoren.

Houden we rekening met het feit dat de transitie naar C4ISR een stapsgewijze overgang is die een capacitaire toename en integratie toelaat in de tijd: een nieuw concept zonder praktische gevolgen (zoals de encapsulering van bestaande systemen of gebruiksstandaarden) heeft daarom weinig zin en kan leiden tot overlapping met reeds bestaande capaciteiten in andere fora. Evenzeer is het omgekeerde het geval: de uitwerking van concrete projecten die niet passen in het grotere kader of die niet op zijn minst een operationele exploiteerbaarheid garanderen die compatibel is met bestaande procedures, werkt tegen de evolutie naar de realisatie van een groter netwerk. Het formuleren van operationele capaciteiten die te behalen zijn tegen een vooropgesteld termijn zonder de eindstaat van de volledige architectuur vast te leggen, helpen echter sneller die integratie te concretiseren. Het loont dan ook de moeite om na te gaan welk forum of netwerk al het verst gevorderd is in die transitie en in welke mate van daaruit voort kan gewerkt worden. Een verkapte vorm van sponsoring van eigen defensie-industrie zonder meerwaarde voor de gemeenschappelijke ondersteuning van de transitie kan enkel maar tijdelijk voordeel bieden aan lokale en nationale industrie, maar biedt geen structurele oplossingen, noch in het bereiken van het operationele einddoel (geïntegreerde C4ISR), noch in een garantie van enige geldelijke return op langere termijn.

2.5. Cyberverdediging in de Europese Unie

In 2010 hebben we in een studie over de bescherming van kritieke infrastructuur en informatie-infrastructuur gewezen op het belang van het uitwerken van een visie. Dienaangaande bestaat een behoefte om de actoren te betrekken waarvan men op het eerste gezicht niet zou verwachten dat ze met het veiligheidsvraagstuk gerelateerd kunnen worden (Smedts, 2010). De vaststelling dat er daarom zowel een strategie als aangepaste structuren en werkmethodes nodig waren, heeft verschillende landen tot inspanningen gedreven in die richting.

In Europa is de organisatie van het cyberplatform pas opgestart na de incidenten van Estland in 2007. De nationale strafwetgeving werd daarom in vele landen aangepast aan het nieuwe domein, waardoor de facto samenwerking vereist wordt tussen veiligheidsdiensten (politie, inlichtingen), de krijgsmacht en private partners. Met de toegenomen beveiliging tegen cybercriminaliteit groeide ook het besef van de eigen gevoeligheid voor externe (statelijke of niet-statelijke) aanvallen op kritieke infrastructuur via het netwerk of de collecte van gevoelige informatie waardoor economische activiteit schade wordt toegebracht. Het inzicht van het belang van de beveiliging van dit domein voor de commerciële exploitatie heeft ervoor gezorgd dat investeringen in dit kader niet onderhevig zijn geweest aan de drastische besparingen die andere departementen te beurt zijn gevallen. We geven een niet-exhaustief overzicht van de meest markante aanpassingen in de afgelopen drie jaren.

In Duitsland is de bevoegdheid voor cyberveiligheid verdeeld over verschillende lokale en federale niveaus van de staatsstructuur en is ook in dit geval duidelijk te onderscheiden van de militaire cyberverdedigingstak. Als gevolg van het ontwerp van de cyberstrategie werd onder de bevoegdheid van het ministerie van Binnenlandse Zaken in april 2011 het Nationales Cyber-Abwehrzentrum in Bonn in het leven geroepen dat zowel mensen van de krijgsmacht, de politie, de inlichtingendiensten, civiele veiligheid en beveiligingsdiensten bij elkaar brengt. Daarnaast werd ook de Nationale Cyber-Sicherheitsrat gecreëerd die de bondskanselier, de gefedereerde entiteiten en de ministeries met elkaar onderling en met de private partners in contact brengt rond hetzelfde thema. Het centrum van Bonn dient het nodige advies en aanbevelingen te geven aan de Raad om het beleid te kunnen bepalen. Los van deze initiatieven die vooral op cyberverdediging zijn gericht

is in het militaire luik ook sinds 2012 een offensieve capaciteit voorhanden met hoofdzetel in Reinbach. De grondwet van Duitsland verbiedt echter de inzet van de krijgsmacht in offensieve operaties tenzij het parlement daartoe uitdrukkelijk de toestemming verleent. Het aanwenden van offensieve computernetwerkoperaties ontsnapt niet aan deze wettelijke beperking. Deze capaciteit is duidelijk te onderscheiden van de cyberverdediging binnen de krijgsmacht waarvan de verantwoordelijkheid bij andere eenheden gevestigd is.

In het Verenigd Koninkrijk zoals in de VS is veiligheid een topprioriteit en cyberveiligheid maakt daarvan integraal deel uit. De *Cyber Security Strategy* vermeldt dat de audit van 2010 als aanbeveling in een investeringsprogramma van vier jaren voorzag (National Cyber Security Programme - NCSP) met een totaal bedrag van 650 miljoen GBP om de beveiliging van dit nog steeds groeiende domein verder uit te bouwen (Cabinet Office, 2011; p. 25). Deze materiële middelen moeten toelaten om de engagementen na te komen die binnen het kader van de NAVO-top van Lissabon in 2010 prioriteit hebben gekregen. Ook in 2015 zullen die investeringen voortgezet worden. Deze investeringen komen boven op de gelden die toebedeeld werden aan departementen die actoren zijn in cyberverdediging maar uit hoofde van hun dagelijkse taken al investeringsgelden ontvangen van hun respectieve departementen. Bovendien werd het belang van kritieke infrastructuur en de rol van geautomatiseerde beheerssystemen door het virtuele netwerk ingezien: het bezit en het beheer ervan is voor het grootste deel in privaat bezit. Vijf sectoren die daarom vanaf het begin aan de basis hebben gelegen van intensieve samenwerking zijn defensie, financiën, telecommunicatie, de farmaceutische industrie en energie. Indien men meer aandacht krijgt voor het beveiligen van de door de netwerking gecreëerde gevoeligheden, is men tegelijk tot de vaststelling gekomen dat diefstal van gegevens enorme directe economische verliezen genereert. Waar beveiliging erop gericht is om vooral schade te beperken en indirect ook economisch gevolgen kan hebben (bijvoorbeeld door het wegvallen van stroomvoorziening voor industrie of de ontoegankelijkheid voor transport van afgewerkte producten), zijn cyberaanvallen op de industrie vooral gericht op het stelen van intellectueel patrimonium, wat rechtstreeks aanleiding kan geven tot economische schade. De frequentie van dergelijke aanvallen neemt toe (tot 70 gesofisticeerde aanvallen per maand) en de oorsprong ervan is vaak te herleiden tot andere staten volgens het hoofd van het *government's intelligence-gathering operation* (GCHQ), Iain Loban. Dat het GCHQ in Cheltenham zich ook toespitst op de aanvallen van niet-militaire doelwitten mag op het eerste gezicht vreemd lijken. Het feit dat aanvallen niet uitsluitend op militaire doelwitten worden uitgevoerd noch noodzakelijkerwijs met militaire middelen is één van de lessen die na de aanslagen van 11

september 2001 getrokken zijn geworden. Om die reden wil het Verenigd Koninkrijk de forensische capaciteit op het virtuele platform verder uitwerken om naast de mogelijkheid een cyberaanval te ontwaren ook de oorsprong ervan ondubbelzinnig en met kracht van bewijslast te kunnen vastleggen. Daarom vallen cyberaanvallen in het VK onder de bevoegdheid van een militaire afdeling van de inlichtingendiensten. Ondanks het feit dat aanvallen niet louter als militair te bestempelen zijn, is een *Joint Cyber Unit* in het leven geroepen waarmee men "joint" eerder moet begrijpen als "interdepartementaal" in partnerschap met het ministerie van Defensie. De slaagkans van de strategie zal te meten zijn aan de wil van private partners om mee te werken in dat platform: de natuurlijke terughoudendheid van private partners om informatie te delen die tegelijk betrekking heeft op de veiligheid en tegelijk op de informatie die vaak winstbepalend is, de *core business* van ieder commercieel bedrijf, zal overwonnen moeten worden wil men slagen om op langere termijn een cyberveilige omgeving uit te kunnen baten.

De samenwerkingsakkoorden tussen de Scandinavische landen worden vaak door de Benelux als voorbeeld gebruikt. Ze hebben binnen het kader dat ons aanbelangt een gemeenschappelijk samenwerkingsplatform ontwikkeld voor concrete projecten in defensiesamenwerking: op 5 april 2011 werd de basis gelegd van de *Nordic Declaration on Solidarity* dat opgevolgd zou worden met concrete projecten, waaronder cyberveiligheid als uitloper van de politieke wil om samenwerking in dit domein tot een goed einde te brengen. Noorwegen, Denemarken, Zweden, Finland en IJsland hebben daarom in het kader van de *Nordic Defence Cooperation* (NORDEFCO) een samenwerkingsplatform op touw gezet met als doel tegen 2015 over een operationeel netwerk van nationale cyberdefence centra (CDC) te kunnen beschikken. De samenwerking in deze regio is belangrijk voor de rest van de wereld, omdat deze landen de grootste penetratiegraad van het virtuele platform toelaten en het bestuur en de administratie grotendeels via elektronische weg wordt uitgevoerd. Ze erkennen dan ook hun afhankelijkheid van de goede werking van het netwerk voor de economische welvaart van de deelnemende landen en hun bevolking en tegelijk zien ze in dat de activiteit in het virtuele domein niet gedomineerd wordt door staten, maar eerder door individuen en bedrijven, dit in tegenstelling met de meeste landen die nog steeds een anachronistische soevereiniteitsinvulling willen verbinden aan dit nieuwe domein. Deze defensiesamenwerking wil de nationale centra op een geïntegreerde manier. Dit omvat een gemeenschappelijke strategie, gemeenschappelijke opleiding en training als toepassing van overeengekomen en uniforme procedures en technische compatibiliteit die gestoeld is op een gemeenschappelijk wettelijk fundament omtrent cyberverdediging. Deze integrale samenwerking zou moeten uitmonden in een *Nordic Cyber Defence Centre* die niet enkel de verdediging,

maar ook de snelle waarschuwing zou moeten coördineren. Deze multilaterale constructie is uiteraard het sluitstuk van wat er op nationaal vlak kan gerealiseerd worden en dat als fundering dienst moet kunnen doen. In Noorwegen is de nationale organisatie een gedeelde verantwoordelijkheid met een eenheid voor cyberverdediging onder het beheer van het ministerie van defensie (*Cyberforsvaret* opgericht in 2012) die de capaciteiten samenbrengt van verschillende diensten zoals de inlichtingendiensten van de krijgsmacht, de nationale veiligheid (*National Security Authority*) en de politiediensten (*Norwegian Police Security Service*). Eveneens in 2012 richtte Denemarken zijn cyberverdedigingscentrum van de krijgsmacht op als gevolg van de evaluatie van de potentiële dreiging met het virtuele platform als vector. Zo gaat de nood aan connectiviteit voor economische groei gepaard met een toename van de kwetsbaarheid volgens directeur Thomas Ahrenkiel van de Deense inlichtingendienst (*Forsvarets Efterretningstjeneste/DDIS*). Finland beoogt met zijn vierjarige strategie een operationele infrastructuur in plaats te hebben tegen 2016. Op nationaal vlak wil men de interdepartementale samenwerking bevorderen alsook de coördinatie met de wetenschappelijke en de zakelijke wereld: een succesvolle verdediging is intrinsiek verbonden met het succes dat Finse bedrijven kennen (*Secretariat of the Security Committee*, 2013; p. 25) en in wat volgt zullen we merken dat ook andere nationale benaderingen in die richting gaan. Als internationale partnerschap voorziet Finland in de eerste plaats de NAVO, de EU en de samenwerking binnen NORDEFCO. Ook in Zweden ten slotte zijn cyberverdediging en inlichtingendiensten sterk met elkaar verweven: informatievergaring is een essentiële capaciteit die de samenwerking vergt van militaire signaalverwerkingseenheden met militaire inlichtingendiensten en nationale politie-inlichtingendiensten.

Frankrijk is begonnen met de afbakening van de domeinen cyber en C4ISR aan de hand van een witboek defensie in 2008. Het werd al gauw duidelijk dat de dreiging in dit domein aan snelle mutatie en evolutie onderhevig is: zowel het groeiende belang van informatiesystemen in ons dagelijkse leven als de technologische evolutie vergen aangepaste beschermingsmaatregelen. Een belangrijke dreiging is de grootschalige aanval op nationale systemen. Belangrijk om te benadrukken: Frankrijk is een van de weinige landen dat zijn verdediging kadert binnen een soevereiniteitsperimeter die wordt bepaald door de vitale sectoren. De door Frankrijk gedefinieerde vitale sectoren zijn dezelfde als diegene bepaald in het ontwerp van Europese Richtlijn voor de bescherming van kritieke infrastructuur, te weten (Livre Blanc, 2013; p.105): “Activités civiles de l’État – Activités judiciaires – Activités militaires de l’État – Alimentation – Communications électroniques, audiovisuel et information – Énergie – Espace et recherche – Finances – Gestion de l’eau – Industrie – Santé – Transports”.

De bescherming van informatiesystemen heeft als doel de soevereiniteit (de vrijheid van handelen) veilig te stellen door middel van de economie en de werkgelegenheid. De capaciteiten die daarvoor moeten gemobiliseerd worden, kunnen zowel defensief als offensief zijn en moeten autonoom ingezet kunnen worden: een essentieel onderdeel daarvan zijn detectiemiddelen en de uitrusting (hardware) die het virtuele netwerk zullen dragen. Wetenschappelijke en technologische performantie worden in dat opzicht elementen die kunnen bijdragen tot de bescherming van de nationale soevereiniteit. Met het inzicht van wat eerder werd uiteengezet, is het merkwaardig dat Frankrijk in het algemeen maar vooral met betrekking tot het cyberdomein blijft vasthouden aan het soevereiniteitsprincipe om zijn strategie te bepalen. De strategische objectieven die in het cyberdomein worden gedefinieerd zijn: een wereldmacht te zijn inzake cyberverdediging (behoren tot de belangrijkste actoren die de cyberverdediging kunnen ontwerpen), de beslissingsonafhankelijkheid te garanderen door de bescherming van de soevereiniteitsinformatie (de competentie bewaren om beveiligde informatie te genereren en uit te baten), bescherming van de cyberveiligheid van vitale en kritieke nationale infrastructuur en de veiligheid in cyberspace te garanderen (ANSSI, februari 2011; pp. 7-8). Naar eigen verklaring is het behoud van een prestatiegerichte nationale en Europese industrie in dit domein een essentiële doelstelling. Deze doelstelling in verband brengen met een domein dat in eigen strategische inzichten een soevereiniteitselement behoudt is verrassend. Het centrale element dat vandaag vaak aan de basis ligt van een moeizame vooruitgang in de Europese integratie, al dan niet met betrekking tot defensie, is precies de discussie en de perceptie omtrent soevereiniteit. We hebben reeds vermeld dat actuele dreigingen (en in het bijzonder voor het virtuele platform) niet meer door soevereine statelijke actoren alleen het hoofd kunnen geboden worden. De bespreking van de verschillende vormen van soevereiniteit (zie hoger) heeft ons bovendien geleerd dat de enige vorm van soevereiniteit waarvan vandaag moest afgestapt worden wil men de transitie naar multilaterale integratie kunnen realiseren, precies de Westfaalse sturing is die fysische grenzen als referentie gebruikt voor het bepalen van doelstellingen. De belangen van nationale industrie die overeenkomstig dat principe winst tracht te maximaliseren zijn net omwille van die doelstelling niet altijd verzoenbaar met de belangen van de overheid die niet de winst maar de efficiëntie van staatswerking boven het commercieel belang stelt. Internationale afspraken, engagementen en samenwerking zijn daarom essentieel vandaag. Frankrijk erkent het belang van private partners en onderstreept daarin de nood om normen te bepalen waaraan moet worden voldaan om de vitale belangen van de natie te vrijwaren. “Ce dispositif précisera les droits et les devoirs des acteurs publics et privés, notamment en matière d’audits, de cartographie de leurs systèmes d’information, de notification des incidents et de capacité pour

l'agence nationale de la sécurité des systèmes d'information (ANSSI), et, le cas échéant, d'autres services de l'État, d'intervenir en cas de crise grave." (Livre Blanc, 2013; p.105). Het belang van andere partners wordt buiten de commerciële context ook in hetzelfde document erkend: "Toute politique ambitieuse de cyberdéfense passe par le développement de relations étroites entre partenaires internationaux de confiance. Les relations seront approfondies avec nos partenaires privilégiés, au premier rang desquels se placent le Royaume-Uni et l'Allemagne. Au niveau européen, la France soutient la mise en place d'une politique européenne de renforcement de la protection contre le risque cyber des infrastructures vitales et des réseaux de communications électroniques." De vooropgestelde strategische doelstellingen worden bereikt door de hoofdkrachtinspanning te bundelen tot het anticiperen en analyseren van de omgeving teneinde de juiste beleidskeuze te maken, aanvallen detecteren en tegenhouden en slachtoffers ervan bijstaan, de wetenschappelijke industriële en technische en menselijke mogelijkheden uitbaten om de autonomie te vrijwaren, de informatiesystemen van de staat beschermen voor een betere nationale veerkracht, wetteksten aanpassen aan de technologische realiteit, internationaal samenwerken om betere bescherming te bekomen van nationale informatiesystemen, de bevolking informeren over de belangen die moeten verdedigd worden. Ook in de concrete uitwerking van zijn cyberstrategie beperkt Frankrijk zich dus tot internationale samenwerking omdat dit de mogelijkheid kan geven de nationale systemen te versterken en niet noodzakelijk omdat de internationale samenwerking mogelijk zou kunnen maken om de internationale dreigingen efficiënter af te weren vooraleer ze nationale uitwerking hebben.

2.6. Militaire C4ISR in een civiele organisatie of interdepartementele transitie in de Europese Unie?

Europese capaciteit staat niet in verhouding tot deze in de NAVO: de afwezigheid van een vergelijkbare commandostructuur en operationele procedures draagt zeker bij tot het verschil tussen de twee organisaties. Het weze duidelijk dat het niet het gebrek is aan bestaande technologie die daartoe bijdraagt. De inkrimping van defensiebudgetten op het continent is een bijkomende beperkende factor: de soevereine bijdragen en de voorkeur voor de nationale defensie-industrie kunnen leiden tot een trage besluitvorming betreffende capacitaire planning en uitvoering binnen de EU. De grootste vorderingen zijn vast te stellen in het domein van de ruimte, maar om sneller de transitie aan te vangen naar *joint* C4ISR, waarvoor tot op heden geen eindpunt is vastgelegd, is een vergelijkbare aanpak als in de NAVO vereist: de transformatie van de Alliantie is hierin een referentie. De maatstaf voor investeringen tot 2% van het bnp, vooropgesteld door de NAVO, wil aankoopprogramma's richten op de vastgestelde tekorten te weten onbemande platformen, transportcapaciteit, radars en linkverbindingen op schepen. Het gemeenschappelijke kader gaat natuurlijk niet voor op de beslissing van soevereine staten, maar interoperabiliteit en relevantie zullen wel in acht moeten worden genomen in toekomstige investeringen. De planning van capaciteiten in het NAVO-bondgenootschap heeft ook gevolgen voor de Europese structuren maar deze verschillen grondig in aanpak. Ieder land heeft eigen standaarden ontsproten uit voornamelijk industrie wat de interoperabiliteit op EU-vlak niet zal bevorderen. Geconcerteerde programma's als het strategische transport met de A400M zijn dan weer zodanig budgettair belastend dat ze de beschikbare ruimte in eventuele marges voor de komende jaren wegneemt. Met dit dilemma moet de EU een capacitair programma ontwikkelen dat noodgedwongen niet dupliceert wat in een ander kader beschikbaar is. Maar daarenboven dienen naast "procurement" op zich ook structuren en procedures voor inzetbaarheid afgebakend te worden. In Frankrijk bijvoorbeeld is een nationaal agentschap belast met de aankoop (Délégation Générale de l'Armement – DGA): deze dienst wil de bewapening van de Franse krijgsmacht beheren door de

ontwikkeling, de aankoop en de evaluatie van de wapensystemen die de krijgsmacht in gebruik heeft. Het bereik van dit agentschap behelst de ganse levensduur van het materieel. Daarnaast staat het ook in voor het schatten van de risico's en aan de hand daarvan de vereiste capaciteit te definiëren die de motivatie zal zijn voor technologische en industriële ontwikkeling. Het agentschap is ook resoluut exportgericht: de promotie van de defensie-industrie en haar ontwikkeling is markteconomisch gedreven: een taskforce werd opgericht van systeemontwikkelaars om onderzoek en ontwikkeling voor defensie af te stemmen en *cross-servicing maintenance* te garanderen. Hierin verschilt de Franse van andere nationale benaderingen in de organisatie dat het agentschap op regelmatige basis afstemt met defensie-industrie om de vereisten van de overheid te toetsen aan en af te stemmen op de planning van de private sector. Het prospectief plan van de komende dertig jaar verkent in het bijzonder de capacitaire krachtinspanning op langere termijn. In het bijzonder stelt het plan de vereisten in het licht op gebied van telecommunicatie, inlichtingen, C2, sensoren en onbemande platformen en hun mogelijke rol om het hoofd te bieden aan voormelde dreigingen. Het is het instrument bij uitstek om de behoefte te identificeren en de industriële ontwikkeling en het onderzoek dienaangaande. Uiteraard laat dit plan toe om op langere termijn de planning en de programmering van bewapeningsprogramma's te sturen. Het plan vermeldt onder meer:

> "Recouvrant la période des 30 ans à venir, avec une méthode d'analyse adaptée aux différents horizons considérés, il a pour rôle d'ouvrir des perspectives en identifiant les possibilités de ruptures techniques et opérationnelles et de donner des grilles de lecture pour préparer les choix relatifs à l'obtention ou au maintien de capacités opérationnelles adaptées aux besoins des armées… Il matérialise l'avancement des travaux prospectifs et capacitaires du collège des architectes de systèmes de forces (ASF), des officiers de cohérence opérationnelle (OCO) et des officiers de cohérence d'armée (OCA)." (http://www.ixarm.com/Le-plan-prospectif-a-30-ans)

Niets in de vermelding van het prospectieve plan laat blijken dat een supranationale integratie bij de prioriteiten behoort.

Het Verenigd Koninkrijk is zoals eerder vermeld het dichtst aangesloten bij het Amerikaanse project van volledige integratie in een C4ISR netwerk: de reductie van het *US Network-Centric Warfare*-concept (NCW) leidt door een budgettaire beperking en een latere aanvang tot het UK *Network Enabled Capability* concept (NEC) en kadert daarom al zijn operaties binnen een concept van netwerkcentriciteit, wat een integratie impliceert van alle bestaande en toekomstige platformen in één

gemeenschappelijk netwerk waarin systemen niet alleen als effectoren optreden, maar eveneens bijdragen tot het verrijken van de informatiecollectie. Aankoopdiensten werden daarom ook afgestemd op dit doel: het *Directorate for Equipment Capability-Command, Control and Information Infrastructure* (DEC-CII) is de grootste afdeling binnen het ministerie van defensie en heeft als voornaamste taak het invullen van tekorten in commando en controle en genetwerkte structuren. Het aanreiken van onbemande platformen is sinds 2006 een prioriteit maar staat de exploitatie van het bestaande platformenpark niet in de weg. De hoogtechnologische uitrusting van oudere platformen als Tornado, Nimrod en Canberra laat toe om interoperabiliteit te realiseren met NATO E3D en US Rivet Joint. De occasionele incompatibiliteit van nationale defensie-industrie met gemeenschappelijke projecten wordt binnen NAVO-verband geïllustreerd door het *Alliance Ground Surveillance* project (AGS) dat de ASTOR-voorstellen van British Aerospace en Raytheon niet heeft gekozen.

In Duitsland is men nog in transitie naar een *joint* architectuur hoewel er wel reeds samenwerkingsverbanden zijn met bijvoorbeeld Nederland op niveau van het binationale legerkorps onderverdeeld in de *earmarked forces* van de NAVO. Op langere termijn zet Duitsland zich ook in voor het gebruik van onbemande platformen, trend die zich in het overgrote meerderheid van de krijgsmachten doortrekt.

Italië maakt deel uit van de groep landen die de F-35 mee ontwikkelen samen met het Verenigd Koninkrijk, Nederland, Noorwegen en Denemarken in Europa. Niet alleen is Italië gericht op de transitie naar *jointness*, maar hebben budgettaire beperkingen dezelfde gevolgen als in andere Europese legers. De reductie van de personeels- en infrastructuurkosten zou de ruimte moeten creëren voor investeringen die passen bij het strategische kader van het land: de wil om in het Middellandse Zeegebied en omgeving bij te dragen aan stabiliteit tekent de krijtlijnen van de prioriteiten van de toekomst. De duurste programma's naast de aankoop van jachtvliegtuigen en onderzeeboten zijn gewijd aan C4ISR-integratie en *joint* integratie (http://www.aei.org/). Kleinere landen in de EU zijn vandaag meer geneigd tot samenwerking: ze hebben al langer de ervaring dat aankoopprogramma's van defensie een meerwaarde kunnen hebben indien ze gecoördineerd worden. Echter de aankoop van defensiematerieel en wapensystemen is nog een van de sterk nationaal gebonden sectoren waarin de soevereiniteitsgedachte zich concretiseert: waar het voor ieder land duidelijk is geworden dat dreigingen niet meer door één enkele actor het hoofd kunnen geboden worden, is de nationale defensie-industrie nog niet altijd afgestemd op deze grondtoon die samenwerking en interoperabiliteit vereist. De doelstellingen die de EU zich voorhoudt in dat kader, de strategie zeg maar, is essentieel. Zonder de

omschrijving van wat de politieke draagkracht van de EU kan zijn, kan men ook niet tot afspraken komen in zeer concrete materie als defensie-industrie: deze reiken immers verder dan een budgettaire uitvoering. Ze kaderen binnen de herhaaldelijke evaluatie van de relevantie van vorige en toekomstige programma's in de vrijwaring van vitale belangen van de EU (politieke, economische, sociale). Vandaag de dag is de EU voor de uitbouw van haar C4ISR-structuren nog te vaak afhankelijk van een bottom-up invulling. Er is nog geen substantie gegeven aan de strategische visie die de EU moet kunnen leiden in de materialisatie van de krijgsmacht-unie van morgen in het algemeen en de transitie naar C4ISR in het bijzonder. De opgelopen achterstand ten opzichte van de NAVO mede door het nationale belang voorrang te verlenen is niet meer goed te maken maar de EU kan wel haar specificiteit onderlijnen en voor haar eigen relevantie is het belangrijk dat het niet als een lichtere versie van de Alliantie wordt beschouwd. In dat opzicht, zowel voor de algemene visie als voor de realisatie van concrete projecten is het belangrijk dat aan een strategische visie op Europees niveau gestalte wordt gegeven: deze vormt een geactualiseerd dreigingsbeeld en zet tegelijk de vitale belangen van de EU in de kijker.

2.7. Deelbesluit

De militaire ervaring enerzijds en het duale karakter van de middelen, hebben ervoor gezorgd dat C4ISR zijn zuiver militaire rol is ontgroeid. In de VS heeft die transformatie zich voornamelijk laten drijven door de nood van en integrale verdediging van het thuisland tegen terroristische aanvallen: het departement Homeland Security werd hiervoor in het leven geroepen. Een van de andere leidende landen in het C4ISR domein, met name China, heeft hoewel in het bezit van de technologische mogelijkheden, nog niet de conceptuele en wettelijke transformatie uitgevoerd dat het op gelijke voet zou brengen met de VS in een extra-militaire rol. In dit gedeelte hebben we willen nagaan hoed het voorbeeld van de leidende landen in de materie zich al dan niet heeft doorgezet naar de Europese Unie.

We stellen vast dat de EU vandaag nog steeds niet ver genoeg gevorderd is naar een volwaardige interoperabiliteit, laat staan *jointness*: zoals eerder uiteengezet is dit een noodzakelijke stap in de transitie naar operationele C4ISR. Interoperabiliteit in defensieaangelegenheden is een zorg voor het Europees Defensieagentschap (EDA): het zijn de vaststellingen van de tekorten in operationele omstandigheden (al dan niet in multilateraal verband) die ervoor hebben gezorgd dat dit onderwerp überhaupt aandacht heeft gekregen.

Het zijn in het geval van de EU voorlopig kleinschalige projecten die de basis moeten werpen van wat later een architectuur zou kunnen worden. De overkoepelende visie die concrete projecten moet leiden ontbreekt echter. Concrete projecten moeten die genese echter zichtbaar maken en moeten ook als basis dienen voor de verdere uitbouw en de mogelijke exploitatie van het netwerk. In wat voorafging is die werkwijze aanwezig in de NAVO-benadering terwijl de EU-methodologie nog moet geschreven worden.

Cyberverdediging als ondersteuning van de C4ISR-architectuur vergen een samenwerking die de multilaterale coöperaties van vandaag overstijgen. Samenwerkingsverbanden vergen, naast de internationale invulling, de verruiming van het begrip interoperabiliteit naar departementen buiten de krijgsmachten. Belangrijker nog is het inzicht dat in dit domein louter capacitaire aspecten worden overstegen: synergie tussen verschillende

domeinen en departementen vraagt immers zowel capacitaire als procedurele afstemming.

Binnen het kader van de Europese Unie heeft iedere lidstaat eigen standaarden die vaak ontspruiten uit de industrie. Interoperabiliteit en jointness worden hier enkel moeilijker door. Voor de EU zij er in de materie twee opties: ofwel wordt een eigen C4ISR architectuur uitgewerkt die een top-down invulling krijgt. Bij deze optie moet men rekening houden dat de opgelopen achterstand ten opzichte van de leidende landen enerzijds maar ook ten opzicht van een militaire alliantie als de NAVO mogelijk nooit meer kan worden ingehaald. De tweede optie is die waarbij vanuit de concrete projecten en de initiatieven van de lidstaten een bottom-up benadering wordt uitgewerkt die verder enkel nog coördinatie en sturing nodig heeft om tot een bruikbaar operationeel netwerk te komen. Vandaag de dag is de EU voor de uitbouw van haar C4ISR-structuren nog sterk afhankelijk van een dergelijke bottom-up invulling, die de respectieve defensie-industrieën invullen in kleinschalige Europese projecten. Er is nog geen substantie gegeven aan de strategische visie die de EU moet kunnen leiden in de materialisatie van de krijgsmacht-unie van morgen in het algemeen en de transitie naar een volwaardig en zelfstandig C4ISR-netwerk in het bijzonder.

Deel 3

C4ISR in België en aanbevelingen

3.1. C4ISR: België

De verantwoordelijkheden voor de *joint ISR* (JISR)-capaciteit binnen de Belgische Defensie zijn gespreid over verschillende niveaus, gaande van de generale staf op strategisch vlak tot bij de componenten voor de tactische collecte en exploitatie van informatie, welke ook de bron ervan moge zijn. De collecte van informatie gebeurt door verschillende sensoren en verschillende diensten. De volledige beschrijving van de taken, het ambitieniveau, lees de verantwoordelijkheden van elke actor in de organisatie, staat buiten het bestek van deze studie.

De lijst van de belangrijkste C2ISR middelen in gebruik bij Defensie wordt hieronder gegeven: een exhaustieve lijst van de beschikbare middelen valt eveneens buiten het bestek van deze studie. Toch we trachten een overzicht te geven van wat aan grote commando- en controlesystemen (back-end C2ISR) en de digitale ISR systemen (front-end C4ISR). Het gedeelte computers, netwerken, interfaces, gateways en links worden niet in de lijst hernomen.

Tabel 3: C2ISR in België (informatie ACOS O&T, sectie D&R; 2014).

Component	***Systeem***	***Beschrijving***
JOINT		
	JCOP (viewer)	Joint Common Operation Picture, Joint C2 system
	Intel	OSINT/HUMINT/IMINT/IDINT/SIGINT (ELINT/COMINT)/MEDINTEL
	HELIOS II	Observatiesatelliet
	CBRN Analysis	CBRN analyse tool
	i2	Intelligence analysis platform
	RFIMS	Request for Information Management System
	ArcGIS	Geographic analysis tool
	CSD	Coalition Shared Data
	Collaborative Tools	Chat, MS Sharepoint
	SBO	Standaard Bureautica Omgeving (MS Office, MS Office, Acrobat Reader, Izarc, etc.)
LAND		
	ISIS	Integrated Staff Information system, Land C2 system

	OSIRIS	Battelfield Management System
	T-BMS	Battelfield Management System in PANDUR Veh
	SMV C4I	Belgian Soldier Transformation (BEST) C2 system
	AFSIS	Advanced Fire Support Information System, Artillerie C2 tool
	SVB/SCB	Battlefield surveillance radar (Bn ISTAR)
	PIRANHA/DINGO	Gev Vtg met sensoren (o.a. remotely operated selfdefence system (ROSS))
	PANDUR	Recce Vtg met sensoren (o.a. Waarnemings- en Inlichtingenplatform (WIP))
AIR		
	ICC	Integrated command&control , Air C2 system
	MASE	Multi AEGIS (Airborne Early Warning Ground Interpretation Segment) Site Emulator, aircraft control system
	ACCS	Air Command and Control System, Air C2 system
	F-16	Gev Vltg met sensoren (o.a. Modular Recce Pod (MRP) en SNIPER Advanced Targetting Pod (ATP), Radar Warning Receiver (RWR))
	A-109	Gev Heli met sensoren (o.a. Day Vision Optics Forward Looking Infra Red (DVO/FLIR), Radar Warning Receiver (RWR))
	NH90 NFH	Naval Frigat Helicopter met sensoren (o.a. Radar Warning Receiver (RWR), Electronic Support Measures (ESM), Forward Looking Infra Red (FLIR))
	NH90 TTH	Tactical Transport Helicopter met sensoren (o.a. Radar Warning Receiver (RWR), laser warning receiver (LWR), Missile Launch Detector (MLD))
	B-hunter	Unmanned Aerial Vehicle (UAV) met CCD en IR camera's
	NavAids	Navigatie hulpmiddelen
	MPR	Medium Power Radar (Glons)
	S-723	ATC Radar (Semmerzake)
	ASR	Airfield Surveillance Radars (Florennes-Kleine Brogel-Beauvechain)
NAVY		
	MCCIS	Maritime Command and Control Information System

	M-FF	Multirole fregat met sensoren (o.a. navigatieradar, luchtwaarschuwingsradar (LW08), 3D-radar (SMART), vuurleidingsradars (STIR), sonar, Surface Surveillance radar EO/IR) en een Combat Management System))
	MBV	Mijnenjager met sensoren (o.a. navigatieradar, sonar en een Integrated Mine Counter Measures System (IMCMS))
	MIK	Maritiem Informatie Kruispunt, bewaking BEL kust (COP op MARSUR Exchange System (MEXS), MCCIS, SAFESEANET, Longe Range ID and Tracking (LRIT), Automatic ID System (AIS))
MED		
	MIMS	Medical Information Management System, voornamelijk gebaseerd op Total Health en MS Office

De collecte van informatie gebeurt door verschillende sensoren en verschillende diensten. In overeenstemming met de wet houdende regeling van de inlichtingen- en veiligheidsdienst van 30 november 1998, zijn er vandaag in België slechts twee diensten erkent, zijnde de staatsveiligheid (binnen het nationale grondgebied) en ADIV (buiten het nationale grondgebied), de Algemene Dienst Inlichtingen en Veiligheid van de Krijgsmacht. Een hergroepering binnen Defensie van alle relevante actoren voor collecte van informatie binnen één component binnen één eenheid is niet noodzakelijk een goede optie: de collecte en verwerking van informatie gebeurt immers op twee niveaus. De spreiding van die middelen voor informatievergaring op tactisch en strategisch niveau heeft het voordeel dat die informatie van verschillende niveaus beschikbaar blijft. De centralisatie van deze competentie zou niet noodzakelijk ten goede komen aan de operationaliteit. Wel moeten de informatieverwerking, -exploitatie en, -fusie op een gecentraliseerde manier tot stand komen.

Merken we ook op dat België zowel met tactische als strategische capaciteit meewerkt aan voorbereidingen en oefeningen op internationaal vlak, bijvoorbeeld in het kader van de voorbereiding voor de EUBG-beurtrol. Maar zelfs op tactisch niveau moeten we vaststellen dat België in vergelijking met andere landen nog een lange weg van sensorintegratie te gaan heeft: zo is er bijvoorbeeld wel een mogelijkheid tot integratie van gegevens (plug-infunctie), maar beschikt ons land niet noodzakelijk over *assets* zoals tactische (mini- of micro-) UAV's. Als ons land dan al over *assets* kan

beschikken, kan het zijn dat we daarvoor de hulp moeten inroepen van bondgenoten of is de beschikbare informatie niet noodzakelijk integreerbaar of verwerkbaar. Zo is er vooralsnog geen mogelijkheid om AWACS-systemen te connecteren met tactische grondeenheden voor het volgen en identificatie van troepen of vectoren die in dezelfde zone opereren, noch door middel van Link 16, noch door middel van het NAVO BiCES-netwerk dat homologatie wacht. Het belang van inlichtingenvergaring en -verwerking is nochtans essentieel vanaf het tactische niveau, daar het voordeel voor de bescherming van troepen biedt. Samenwerking moet het gebrek aan *assets* compenseren en in dat opzicht is er wel een mogelijkheid om op informele wijze tussen verschillende landen ervaringen uit te wisselen: België heeft in een dergelijke groep uitwisselingen met Nederland, Noorwegen, Duitsland, Frankrijk, Denemarken, het Verenigd Koninkrijk en de Verenigde Staten (*Informal NATO ISR Commanders Group*).

In de nabije toekomst wordt de COTS-technologie niet meer weg te denken uit het beschikbare aanbod van militaire aankopen: het afzweren van eigen R&D in de meeste westerse defensies zorgt minstens voor het gebruik van commerciële onderdelen in militaire systemen of volledige commerciële producten in gebruik voor de informatievergaring (sensoren). Wel blijven de dataverwerking en -analyse vaak een door de gebruiker ontworpen concept. Toch heeft het stijgend aandeel van commerciële onderdelen in militaire systemen enkele belangrijke consequenties:

- Voor wat sensoren betreft, zal C4ISR in de toekomst de grens doen vervagen tussen militaire en civiele toepassingen. Ook het gebruik van meta-data analyse zal nog meer worden geëxploiteerd teneinde informatie te verkrijgen en doelaanduidingen mogelijk te maken. In de optiek dat eigen R&D wordt opgegeven ten voordele van COTS-technologie, zou dat aanleiding geven tot nieuwe zwaktes in de informatievergaring.

- Daarnaast zullen ook wapensystemen meer een meer samengesteld zijn uit componenten waarvan de exacte en exhaustieve compositie niet meer noodzakelijkerwijs is gekend. Hierdoor bouwt men een intrinsieke zwakte in de systemen zelf, die door eventuele tegenstrevers zouden kunnen worden uitgebaat wanneer zij daartoe nood hebben: een illustratie van de gevolgen daarvan wordt gegeven door de intrusies bij wapenhandelaars vanaf de aanvang van een nieuw ontwerp. Een gebrek aan informatiebeveiliging tijdens de ontwikkeling van nieuwe straaljagers bij Boeing, Lockheed Martin, Raytheon, Northrop Grumman werd deels geweten aan

netwerkconnectiviteit. De schaal van de intrusies evenals de tijdspanne ervan, zijn niet gekend.

Het mogelijk praktische gevolg voor betrokken systemen is dat de overleefbaarheid of de betrouwbaarheid ervan tijdens een crisis in twijfel kan worden getrokken. De connectie van objecten, sensoren en platformen kan om die reden ook een zwakte worden: een van de mogelijkheden die de Amerikaanse strijdkrachten in die omstandigheden hebben voorzien wordt teruggevonden bij hun kernwapenarsenaal. De overleefbaarheid van hun kritische massa wordt nagestreefd door een volledige loskoppeling van de C4ISR-architectuur: een aantal wapensystemen zal in dat geval moeten kunnen opereren zonder die architectuur en dat van bij aanvang van hun operationele periode. De loskoppeling van de genetwerkte structuur kan niet op latere tijdstippen worden beslist. Dit type isolement van uitrusting zal gedurende de hele levensduur van de wapensystemen moeten worden gehandhaafd, wat ook voor onderhoud een bijzonder probleem zou kunnen opleveren (zoals voor updates, technische diagnose etc…). Als men in de VS aan dergelijke oplossingen denkt om de overleefbaarheid van wapensystemen te garanderen, dan is het in de nabije toekomst misschien niet ondenkbaar dat ook in België ooit wordt gedacht aan het belang van loskoppeling: moderne systemen kunnen in die optiek vanaf het prille begin van de ingebruikname en zowel in kwantiteit (gedefinieerd als kritische hoeveelheid) als in kwaliteit (type wapensystemen) worden ontkoppeld van het netwerk om een "kritisch overlevingsisolement" te garanderen. Bovendien heeft België met zijn gevechtsvliegtuigen ook nog steeds een niet-conventionele rol: het is dus in dat opzicht belangrijk dat niet alleen de betrokken uitrusting, maar eveneens de opleiding van piloten en techniekers in die rol wordt vrijwaard indien ze worden toegewezen aan voornoemde kritische massa.

De meerwaarde van netwerkcentriciteit impliceert een snelle beslissingscyclus van planning tot uitvoering: dat is niet alleen in militaire omgeving vereist maar ook met betrokken civiele actoren. De aanvulling van civiele sensoren in de nationale luchtbeeldvorming is al decennialang een feit: de gegevens van de militaire radars van Glons en Semmerzake worden aangevuld met data van de civiele radars van Bertem en Saint-Hubert om een geïdentificeerd luchtbeeld boven het grondgebied te genereren. Maar deze integratie is niet in alle componenten van Defensie noch in alle omstandigheden (al dan niet ontplooid) mogelijk. Dit impliceert dat er voor het militaire netwerk nood is aan een uitbreiding van bestaande tactische mogelijkheden. Eenheden moeten de mogelijkheid hebben om zich aan te sluiten op de beeldvorming in hun operatiegebied. Dat betekent dat ze de mogelijkheid moeten hebben om de voor hun relevante informatie te beschikken van de sensoren in de regio. Het eerder aangehaalde element van

Link 16 is een sprekend voorbeeld dat de *situation* awareness van eenheden voor of tijdens ontplooiing moet mogelijk maken. Daarnaast moet dat beeld verruimd worden door eigen sensoren: tactische UAV's kunnen hiertoe zeker bijdragen. De aankoop van dergelijke sensoren is daarom op korte termijn te overwegen. Op strategisch vlak is er een korter termijn nodig tussen planning en uitvoering.

De integratie van de informatieverwerking van het strategische en het tactische niveau impliceert niet noodzakelijk een fysische verzameling van alle middelen (sensoren) voor die informatieverwerking: verspreiding garandeert immers een zeker niveau van overleefbaarheid en beschikbaarheid.

Het C4ISR-landschap kan ook in ons land niet uitsluitend door Defensie worden bepaald. Naar analogie met wat er in de VS en China is gebeurd, maar ook in organisaties zoals de NAVO en de EU, zullen ook wij de exclusieve militaire dimensie moeten overstijgen om naar een interdepartementale samenwerking te vloeien indien we een of andere vorm van Homeland Security gerealiseerd willen zien.

Bij wijze van illustratie wordt het belang van andere nationale departementen duidelijk wanneer we de nationale contactpunten van het eerder vermelde snelle waarschuwingsnetwerk van de EU in Homeland Security oplijsten (zie p.83): voor het ECURIE-netwerk is dat het FANC, voor het RAPEX-netwerk is dat de FOD Economie, voor de RASFF-EUROPHYT-, SHIFT- en ADNS-netwerken is dat het Federaal Agentschap voor Voedselveiligheid, voor het EWRS-netwerk is dat de FOD Volksgezondheid. Niet alleen het groot aantal actoren, maar ook het groot aantal systemen kunnen een hinder zijn voor sensor fusie en de centralisatie van de informatieverwerking. In ons voorbeeld van de snelle waarschuwingsnetwerken kan de nationale uitbating van de voorziene transmissiekanalen zeker verbeterd worden: zo kan men zich de vraag stellen hoe en waar men de informatie van deze netwerken dient te centraliseren: een tactische centralisatie zou naar analogie met het voorbeeld van Defensie niet noodzakelijk de beste interpretatie van de informatie genereren. De centralisatie van de informatie met het oog op de exploitatie ervan is echter ook hier een operationele vereiste en in dat geval zou dit kunnen gebeuren binnen de schoot van de crisiscel van de regering. Voor het ogenblik zijn dat enkel de systemen Bichat, MIC en ECURIE. Als bemerking moet men hier toevoegen dat enkel ECURIE over een eigen transmissiekanaal beschikt in het kader van radiologische incidenten. Bichat en MIC opereren via het Internet, wat het belang onderstreept van de beveiliging van ICT-capaciteit. Andere vermelde systemen komen niet rechtstreeks toe in het CGCCR-knooppunt: ECDC alarmering bijvoorbeeld vindt haar weg via de FOD Volksgezondheid.

Op zich is dit geen onlogische waarschuwingsketen. Toch kan men zich de vraag stellen of de waarschuwing niet in parallel zou kunnen gebeuren om de vertraging van de doorstroom van informatie tegen te gaan. Bovendien zou dit een garantie geven dat bij uitval van één systeem een back-up voorzien is die de centralisatie van de gegevens toch nog toelaat.

Het belang van andere dan militaire netwerken voor de collecte van bijkomende informatie kan in sommige gevallen een bijzondere meerwaarde genereren: we hebben al aangehaald dat voor de generatie van het luchtbeeld reeds jaren zo gebeurt en mee garant staat voor de veiligheid van het luchtruim. In dit bijzondere geval is een interdepartementale samenwerking dus een absolute vereiste die de veiligheid garandeert. We hebben ook gezien dat die interdepartementale samenwerking in andere gevallen garant staat voor de snelle transmissie van de juiste informatie, bijvoorbeeld voor snelle waarschuwingsnetwerken. Maar ook in die interdepartementale aanpak merken we dat onze buurlanden verder gevorderd zijn dan België: in multilateraal verband zoekt men naar een manier om het gebruik van civiele middelen te integreren in een allesomvattend netwerk dat een optimale exploitatie moet mogelijk maken. De snelle evolutie van de technologie heeft de gegevensuitwisseling exponentieel doen toenemen: het is dan ook noodzakelijk om compatibiliteit te garanderen teneinde die uitwisseling mogelijk te maken indien we in de toekomst een rol van betekenis willen spelen. Een combinatie van multidepartementale met een multilaterale aanpak zijn niet meer weg te denken uit het C4ISR-concept. Om tot die integratie te kunnen komen zijn echter ook investeringen vereist: in militaire middens zijn de investeringsniveaus vandaag op een niveau gekomen dat middelen enkel nog gemeenschappelijk kunnen worden aangekocht (pooling), of worden gedeeld in gebruik (sharing) om een multilaterale samenwerking toe te laten. Misschien moet men in de toekomst ook oog hebben voor een civiele benadering van begrippen *pooling* en *sharing* wil men meer rendement uit investeringen halen. De specificiteit van het C4ISR-netwerk laat een snelle, multilaterale integratie toe en vereist die zelfs.

Op nationaal vlak is een interdepartementale samenwerking niet altijd vanzelfsprekend: maar binnen het kader van een optimaal exploiteerbare nationale C4ISR-capaciteit is een fusie van de civiele en de militaire capaciteiten reeds jaren een feit. Naast de fusie van middelen of informatie is een samenwerking van militairen en burgers principieel niet altijd vanzelfsprekend te aanvaarden: civiele autoriteiten zijn niet altijd geneigd om militaire elementen in hun rangen toe te laten. De indruk zou immers kunnen worden geschept dat het militaire de overhand krijgt of dat alleszins die mogelijkheid wordt overwogen. Verschillende departementen kunnen echter pas goed samenwerken indien een structuur wordt geïntegreerd: niet enkel de

informatie is belangrijk maar ook de procedures, de opleiding en training. Een integratie van de civiele met de militaire capaciteiten kan enkel operationeel worden gecoördineerd in een centraal beslissingsorgaan en voorlopig vinden we enkel die mogelijkheid bij het crisiscentrum van de regering.

Veiligheid kan niet zonder militair instrument worden gegarandeerd. En militair vlak kunnen we geen rol meer van betekenis spelen zonder een multilaterale samenwerking. De middelen die daarvoor zijn vereist kunnen we niet anders meer verkrijgen/gebruiken zonder ze te bundelen (pooling) en te delen (sharing). Als klein land, en zelfs binnen een organisatie als de NAVO heeft België ondanks zijn actieve inzet een materiële achterstand opgelopen door jarenlange beperkingen van het defensiebudget. We hebben uit eerdere voorbeelden in deze studie gezien dat een achterstand niet enkel technologisch goed te maken is, maar ook organisatorisch moet worden gestuurd: de voorbeelden van de leidende landen hebben ons duidelijk gemaakt dat een dergelijke organisatorische transitie over decennia lopen en een dynamische evolutie kennen. Uit deze voorbeelden hebben we ook gezien dat een C4ISR-transitie niet beperkt blijft tot het militaire milieu, maar op zijn minst binnen het kader van Homeland Security ook binnen de civiele wereld is doorgedrongen. We zijn ook tot de vaststelling gekomen dat een volledig C4ISR-beeld in België niet tot stand kan komen zonder de insteek van die civiele wereld. Voorbeelden hebben ons getoond dat vele actoren hierbij dienen te worden betrokken. Voorlopig is een structurele aanpak daartoe nog niet tot stand gekomen: zowel een lijst van middelen als een gepaste structuur, zoals die uit het militaire milieu beschikbaar zijn, zijn niet voorhanden op het equivalente civiele niveau. Om tot een gemeenschappelijke meerwarde te komen is dus een inventarisatie en een structuur in de civiele organisatie vereist. Zoals het belangrijk is voor een supranationale operationaliteit dat zowel assets maar ook commando, controle communicatie en inlichtingen supranationaal wordt gestructureerd, is een nationale organisatie nodig die de werking ervan toelaat. Elk van de samenstellende delen heeft voorlopig echter zijn eigen departementale organisatie wat niet ten goede komt aan een geïntegreerde C4ISR-visie op nationaal vlak.

3.2. Aanbevelingen

We hebben in deze studie kunnen vaststellen dat netwerkcentriciteit een concept is dat een transitie heeft geïnitieerd naar nieuwe structuren in de krijgsmachten die noodzakelijk zijn om nieuwe technologie optimaal te benutten. Vooral de Verenigde Staten hebben deze transitie aangedreven en zijn daardoor in dat domein vandaag nog steeds een stap vooruit op andere krijgsmachten. Dit concept heeft hun geleerd een aantal voordelen optimaal te benutten zoals de snelheid van de commandoketen, de samenwerkingsverbanden, de engagementen *Beyond Line of Sight* (BLOS), de mogelijke reactiesnelheid op snel wijzigende gevechtssituaties. De uitbating van deze voordelen is echter verbonden aan het bestaan van een aangepaste doctrine: deze ontbreekt in vele Europese krijgsmachten zowel op nationaal als op supranationaal niveau. Het bestaan hiervan is nochtans een essentiële etappe in de aanpassingen die vereist zijn na het bereiken van *jointness*. Netwerkcentriciteit doet ons nog verder denken dan *jointness*, waarmee vele krijgsmachten vandaag nog worstelen. Shelton onderstreepte in zijn visie over *jointness* (Shelton, Henry H., 2000) het belang van de integratie van competenties van individuele krijgsmachtonderdelen, maar evenzeer op de intellectuele, operationele, doctrinaire en technische integratie die ervoor moet zorgen dat die krijgsmacht flexibel inzetbaar is. De krijgsmacht dient immers in staat te zijn om een heel gamma aan operaties te realiseren, verspreid in tijd en ruimte in een organisatie die niet noodzakelijk dezelfde commando- en controleketen behelst (coalitie, interdepartementaal, supranationaal): hiervoor moet men sneller, preciezer en accurater kunnen opereren, eigenschappen die na de *jointness*, enkel netwerkcentriciteit kan bereiken.

Op tactisch niveau wordt de neutralisatie van de juiste doelen op het juiste ogenblik belangrijker dan de vernietiging van een zo groot mogelijk aantal doelen: de concentratie van vuurkracht in tijd en ruimte is niet noodzakelijk meer de strategisch beste optie. Om die evaluatie te kunnen maken is kwaliteit van de informatie over de doelen en de uitwisseling van die informatie een beperkende factor: de verantwoordelijkheden met betrekking tot de exploitatie van informatie maakt echter ook het voorwerp uit van de eerder vernoemde doctrine. Door de juiste verdeling van verantwoordlijkheden ter afstemming van exploitatie van informatie kan men bovendien niet alleen de efficiëntie maximaliseren maar ook de kostprijs van een operatie drukken. Het drukken van de kosten is net belangrijk in het

huidige financiële en budgettaire klimaat: kostendrukking met verruiming van efficiëntie kan in de toekomst enkel nog in een netwerkcentrisch concept. Dit concept vereist echter een verkorting van de bestaande termijn tussen de plannings- en de uitvoeringsfase: de huidige toegepaste criteria zijn niet afdoend om een snel aanpasbare en reactieve krijgsmacht in een netwerk centrische omgeving te laten opereren.

De mate waarin die integratie zal bereikt worden is beïnvloed door twee factoren met name de overheersing van de informatie enerzijds en de intellectuele en technische innovatie anderzijds. Deze laatste draagt ook bij tot de snelheid waarmee het strategische landschap zal wijzigen en kan ook een effect hebben op de mate waarmee asymmetrische aanvallen kunnen worden gegenereerd. Maar dominantie kan alleen bereikt worden in die omstandigheden indien de beschikking over en de exploitatie (verwerking en verspreiding) van de informatie beheerst wordt. Dominantie van de informatie kan echter geen doel op zich zijn: het moet vertaald worden naar kennis en besluitvorming. Hiervoor zijn eveneens (zoals voor *jointness*) aanpassingen vereist in de organisatie, doctrine, opleiding en training en commando en controle. Het eerder aangehaalde transitie naar *jointness* mag dus zeker geen einddoel worden, maar moet een etappe zijn op weg naar de transformatie van de krijgsmacht naar een structuur die in staat zal zijn om aan de uitdagingen van de toekomst het hoofd te bieden.

Commando en controle die gebaseerd is op de correcte exploitatie van de informatie en de daaruit voortvloeiende besluitvorming maakt de effecten van *jointness* en netwerkcentriciteit tastbaar: een geconcentreerde uitwerking van het functioneren van eenheden die verspreid zijn in tijd en ruimte wordt zichtbaar. Alle technologische vooruitgang ten spijt blijft het menselijke element de sleutelrol spelen voor het behalen van de objectieven. Dit impliceert dat mensen worden ingezet die vertrouwd zijn enerzijds met nieuwe technologie en anderzijds de meerwaarde van netwerkcentrische operaties kunnen behalen (en tegelijk de voordelen alsook de beperkingen ervan kennen). In de Verenigde Staten is men bewust van het belang van het gebruik van overeengekomen terminologie, doctrine, organisatie, opleiding en training voor de operaties van de toekomst. De netwerkcentrische operaties nemen daarin een centrale rol en overschrijden het zuiver technische aspect ervan: het groot aantal betrokken actoren impliceert een interdepartementale en multinationale betrokkenheid en niet enkel een gemeenschappelijke woordenschat, maar ook op elkaar afgestemde procedures.

De operationele gevolgen van dit concept worden bovendien ook bepaald door de visie die men heeft en de keuze van de strategische opdrachten die men in de toekomst wenst uit te voeren: eerder vermelde

voordelen van de netwerkcentrische benadering en vereiste integratie van diensten en departementen kunnen in het gereduceerde budgettaire kader meer operationele slagkracht garanderen, maar de realisatie ervan vereist een visie die in het geval van de EU ontbreekt. Een benadering die zich beperkt tot het technische aspekt schiet tekort. De begeleidende concepten moeten de operationele inzet van bovenaan blijven sturen. De partnerschappen die kaderen binnen de realisatie van C4ISR kunnen daarom niet gebaseerd zijn op de eenzijdige input van commerciële partners, zelfs als de technische afhankelijkheid een frequenter contact zal vergen in de toekomst tussen private partners en overheid, in het bijzonder bij krijgsmachten die afstappen van eigen onderzoek en ontwikkeling. Operationele vereisten kunnen vaker en sneller veranderen, wat opnieuw een sneller en flexibeler samenwerkingsverband met private partners zal vergen. Maar meer nog dan voor de civiele toepassingen is de militaire operationaliteit afhankelijk van de goede en ook snelle werking van de opgestelde architectuur. Laat dit aspect nu net een element zijn waarvan EDA zelf aangeeft dat er nog ruimte voor verbetering bestaat (EDA (b), 2013): kleinschalige ad hoc projecten worden nog te vaak gemotiveerd door defensie-industrie van lidstaten en niet door ene gemeenschappelijke Europese visie terzake. De achterstand die de EU hierin heeft opgelopen ten opzichte van andere fora (zoals de NAVO) is niet meer goed te maken maar de exploitatie van een complementariteit (in opdrachten of regio) kunnen ervoor zorgen dat duplicatie wordt vermeden.

Op nationaal vlak zijn we tot dezelfde vaststelling gekomen dat er nood is aan een interdepartementale insteek: zowel technisch als organisatorisch is het C4ISR-beeld aan te vullen door een extra-militaire dimensie. Voor de *front-end* C4ISR-capaciteit weten we dat een nationale afstemming vereist is van drie belangrijkst actoren van informatievergaring te weten ADIV, de staatsveiligheid en het coördinatieorgaan voor de analyse van de dreiging. Waar de taak van de eerste duidelijk is afgebakend tot de operationele extraterritoriale informatievergaring, is de taak van de twee volgende overlappend voor de collecte van informatie (HUMINT/ OSINT) en inschatting van de dreiging op het nationale grondgebied. De technische aspecten van *front-end* C4ISR (SIGINT/ IMINT), worden automatisch door militaire en civiele middelen aangevuld. *Back-end* C4ISR betrekt dezelfde actoren voor het verwerken van de informatie. Maar naast de middelen betrekken de communicatie en de besluitvorming daaromtrent (C4) zowel de militaire als de civiele autoriteiten die in crisistijd de regering raad geven en de beslissingen van die regering uitvoeren. Een voorstel dat die samenwerking kan realiseren is een interdepartementaal informatiefusiecentrum gecolocaliseerd met de crisiscel van de regering. Dit behelst niet noodzakelijk een voortdurende uitwisseling van gegevens tussen voormelde actoren, maar een activatie in geval van crisis: enkel de samenwerking tijdens oefening kan

de samenwerking van middelen, procedures en personen verbeteren en de C4ISR interoperabiliteit optimaliseren. De internationale steun tijdens rampen biedt een bijkomende capacitief uitdaging die toelaat om het internationale kader verder af te stemmen.

3.3. Deelbesluit

Voor het gebruik van militaire middelen zijn we tot de vaststelling gekomen dat de bestaande technologische architectuur wel toelaat om sensoren te connecteren, maar dat het gebrek aan *assets* een beperkende factor kan zijn. Op tactisch niveau wordt de neutralisatie van de juiste doelen op het juiste ogenblik belangrijker dan de vernietiging van een zo groot mogelijk aantal doelen. Kwaliteit van de informatie en de uitwisseling ervan vereist ook op dit niveau het bestaan van wettelijke en doctrinaire referentiekaders. Dominantie in een snel wijzigend veiligheidslandschap kan alleen bereikt worden indien de beschikking over en de exploitatie (verwerking en verspreiding) van de informatie beheerst worden: hiervoor zijn niet alleen technische optionele *plug-in* mogelijkheden vereist maar ook eigen *assets* zijn nodig. Daarvoor uitsluitend berusten op de welwillende medewerking van bondgenoten zou betekenen dat we voor de beschikbaarheid van informatie afhankelijk worden van anderen. Technische afhankelijkheid heeft in dit geval geen uitsluitend technische oplossing. Deze afhankelijkheid betekent echter wel dat commerciële partners in de toekomst een nog belangrijkere rol zullen spelen vooral in een context waarbij men de keuze maakt commercial-off-the-shelf aankopen te bevoordelen ten opzichte van eigen R&D (Research and Development).

Het gebrek aan eigen R&D of assets kan misschien tijdelijk gecompenseerd worden door samenwerking in multilateraal verband: een multilateraal kader kan zich echter niet uitsluitend verechtvaardigen door het gebrek aan investeringen. De technische vooruitgang in et domein vereist trouwens een snellere beschikbaarheid van systemen na de planningsfase. In de toekomst zal ook in België een multi departementaal kader uitgewerkt moeten worden zoals dat bij onze buurlanden het geval is wil men een operationele Homeland Security kunnen operationaliseren: een stuwing van de militaire dimensie naar de extra-militaire dimensie vergt immers een coördinatie met de civiele wereld zowel voor wat *front-end* C4ISR als voor back-end C4ISR betreft. In een aantal beperkte gevallen is een front-end integratie gerealiseerd (zoals dat voor het luchtbeeld en sommige snelle waarschuwingssystemen). De organisatie van *back-end* C4ISR, die een besluitvorming toelaat op een geïntegreerd niveau is echter nog niet realiseerbaar: zowel de technische middelen als de organisatie van het de

civiele actoren is nog niet van die aard om de besluitvorming in de crisiscel van de regering te vereenvoudigen.

Homeland Security is het resultaat van de extra-militaire dimensie die men in de leidende landen en op supranationaal niveau tracht to stand te brengen. In België zijn we nog niet tot dat niveau gekomen. De snelle evolutie van de technologie en de kwantiteit van de gegevens die worden gecollecteerd hebben de complexiteit van de problematiek niet eenvoudiger gemaakt. Een overkoepelend C4ISR-concept met de noodzakelijke *assets* zijn noodzakelijke voorwaarden om de operationaliteit te garanderen. Enkel een structuur die multi departementale en multilaterale samenwerking toelaat zal daarom zowel op strategisch als op tactisch niveau in de toekomst een rol van betekenis kunnen spelen.

Netwerkcentriciteit is een concept dat een transitie naar nieuwe structuren van krijgsmachten heeft mogelijk gemaakt: deze laten toe om nieuwe technologie optimaal te benutten. De uitbating van deze technologie is echter onlosmakelijk verbonden met het bestaan van een aangepaste doctrine en wettelijk kader enerzijds, maar ook de noodzakelijke investering om een multilaterale operationaliteit te garanderen. Met een structurele transitie naar jointness, bereikt men echter niet het niveau van netwerkcentriciteit die in de leidende landen reeds wordt nagestreefd. De uitoefening van adekwate commando en controle zal zowel de *jointness* als de netwerkcentriciteit materialiseren: het groot aantal betrokken actoren bevestigt de nood aan een interdepartementale en multinationale betrokkenheid in de gehanteerde architectuur.

Algemeen Besluit

Algemeen Besluit

In dit werk gingen we na in welke mate netwerkcentriciteit en cyberoperaties belangrijk zijn op het pad naar de C4ISR-transitie: een louter gebruiker centrische of technische benadering schieten tekort voor structurele operationele noden. Zowel *front-end* als *back-end* C4ISR zijn daarom onderhevig aan een structurele ondersteuning: de C4ISR transitie is even veel afhankelijk van de organisatie als van de technologie. Een gevolg daarvan is dat de operationele militarisatie van het cyberdomein *jointness* zal afdwingen. We zijn in tot de vaststelling gekomen dat die transitie door militaire behoeften werd gestuurd: langdurende operaties in verre strijdtonelen hebben zowel de noden als de eisen blootgelegd voor operaties van de toekomst. Niet alleen de ervaring van de NAVO maar ook de structurele aanpassingen in leidende landen als de VS en China tonen aan dat de ondersteuning van een cyberarchitectuur onlosmakelijk verbonden is met de operationele vereisten van de vooropgestelde C4ISR-architectuur. Landen die het verst gevorderd zijn in die transitie hebben een visie en een organisatie die die visie weerspiegelt.

Na de militaire stand van zaken hebben we ons de vraag gesteld of de evolutie in de militaire C4ISR-architectuur beperkt is gebleven tot dat militaire domein, dan wel of er een extra-militaire dimensie bij de bestaande architectuur is gevoegd. Hier opnieuw zien we dat het de leidende landen zijn geweest die de aanzet hebben gegeven om de C4ISR transitie vanuit de militaire dimensie naar de civiele dimensie te stuwen. In het post 9-11 denkpatroon groeide in de VS het idee dat C4ISR en de cyber-ondersteuning ervan een plaats had in de beveiliging van de samenleving en heeft dit ook een structuur opgeleverd voor de organisatie van “homeland security”. Bovendien schept een dergelijk kader de mogelijkheid om de mandaten van nationale actoren te verankeren en taken af te stemmen op elkaar. China daarentegen, heeft nog niet de conceptuele en wettelijke transformatie uitgevoerd dat het op gelijke voet zou brengen met de VS in een extra-militaire rol. De EU, hoofdzakelijk een civiel actor van herkomst, is vandaag nog steeds niet ver genoeg gevorderd op weg naar volwaardige interoperabiliteit, laat staan *jointness*: zoals eerder uiteengezet is dit een noodzakelijke stap in de transitie naar operationele C4ISR.

Waar we vastgesteld hebben dat er binnen de NAVO een visie aanwezig te blijkt zijn voor het gebruik en de aanwending van een C4ISR-netwerk zijn het in het geval van de EU kleinschalige projecten die de basis

moeten werpen van wat later een architectuur zou kunnen worden. De overkoepelende visie die concrete projecten moet leiden ontbreekt echter. Ook de ondersteuning van een dergelijke architectuur in de vorm van cyberverdediging vergt een samenwerking die de multilaterale coöperaties van vandaag overstijgen. Samenwerkingsverbanden vergen, naast de internationale invulling, de verruiming van het begrip interoperabiliteit naar departementen buiten de krijgsmachten. De EU heeft hiertoe twee opties: een eerste optie bestaat erin een eigen C4ISR architectuur uit te werken (visie, strategie en capacitaire invulling) die een top-down invulling krijgt. De tweede optie is die waarbij vanuit de concrete projecten en de initiatieven van de lidstaten een bottom-up benadering wordt uitgewerkt die door de EU wordt gecoördineerd. In de praktijk blijkt de EU voor de uitbouw van haar C4ISR-structuren vandaag bij gebrek aan een andere optie afhankelijk van een dergelijke bottom-up invulling. Er is nog geen substantie gegeven aan een dergelijke visie van de EU. Actuele capaciteit in haar extra-militaire dimensie is nog onvoldoende ontwikkeld. De opgelopen achterstand binnen de EU overstijgt bovendien de louter capacitaire aspecten: synergie tussen verschillende domeinen en departementen vraagt immers zowel capacitaire interoperabiliteit als procedurele afstemming. De afwezigheid van een NAVO-achtige commandostructuur en bijpassende operationele procedures draagt bij tot eenachterstand met betrekking tot de operationele aanwending van C4ISR-capaciteit binnen het EU-kader.

Naast enkele concrete projecten binnen het domein C4ISR werd ook voor de ondersteunende cyberdimensie door lidstaten inspanningen gedaan: ze hebben gebruik gemaakt van hun respectieve strafwetgeving waardoor *de facto* samenwerking vereist wordt tussen veiligheidsdiensten (politie, inlichtingen), de krijgsmacht en private partners. Een toegenomen aandacht voor cybercriminaliteit en cyberverdediging heeft ook het inzicht doen groeien voor het belang van de eigen gevoeligheid voor externe (statelijke of niet- statelijke) aanvallen op kritieke infrastructuur via het netwerk, waardoor economische schade kan ontstaan.

In een laatste deel hebben we oog willen hebben voor de stand van zaken in België. Een niet exhaustieve lijst van capaciteiten binnen de krijgsmacht werd vergeleken met de situatie van de civiele wereld: een gemeenschappelijk beperkende beperkende factor aan de architectuur is het gebrek aan *assets*. Daarnaast is de groei van de extra-militaire dimensie of "homeland security" zoals die op andere niveaus werd uitgewerkt nog niet tot een vergelijkbare maturiteit gekomen. Voor een deel draagt een ontbrekend organisatorisch equivalent en een gebrek aan middelen tussen actoren daartoe bij. Daarnaast is een gemeenschappelijk werkingskader niet noodzaklijk afgestemd om zich te kunnen integreren in een multilateraal kader waaraan de

nationale organisatie zich kan spiegelen. Een aantal aanbevelingen werden hieruit gedistilleerd:

-integratie van technologie maar ook intellectuele, operationele, en doctrinaire synergie moeten de C4ISR architectuur ondersteunen;

-uitlsuitend kosten willen drukken laat geen marge voor technologische vooruitgang. Investeringen en een kortere uitvoeringstijd vanaf de plannningsfase zijn noodzaklijke voorwaarden om een C4ISR-architectuur te kunnen onderhouden;

-C4ISR-transitie kan niet herleid worden tot technologische innovatie maar moet interdepartemantale samenwerking toelaten;

-deze interdepartementale benadering vergt de uitwerking van een gemeenschappelijke woordenschat en procedures;

-op niveau van de EU is een uitgewerkte visie nodig in de plaats van enkele concrete initiatieven zonder overkoepelend C4ISR kader;

-een nationaal informatiefusiecentrum ter hoogte van de crisiscel van de regering is vereist.

Om terug te grijpen naar de titel van deze studie kunnen we besluiten dat C4ISR-transitie in alle opzichten meer is dan een louter technologisch vraagstuk: het vergt zowel operationeel, juridisch als organisatorisch aanpassingsvermogen om de transitie te vervolmaken die begon bij de *joint* herstructurering van Defensie. Deze was echter geen eindpunt: hooguit een keerpunt. Vanaf daar kan de integratie van middelen en diensten zich enkel nog meer vertakken.

Afgeleide problematieken die in de toekomst sturing zullen vereisen kunnen onderwerp worden van toekomstig onderzoek: een praktisch voorbeeld van een toepassing waar dergelijke sturing is vereist vindt men bij kritieke energie infrastructuur, een domein waarvan de beschrijving buiten het bestek van deze studie valt. Een ander element dat in dezelfde context aandacht kan genieten behelst de gevolgen van nieuwe afhankelijkheden: een netwerk centrische organisatie wijzigt de soevereiniteitsperceptie. Dit begrip zal in de toekomst niet meer dezelfde betekenis hebben, maar zal zowel materieel als juridisch herdefinieerd moeten worden.

Bijlagen

Bijlage 1: Perceptie van de cyberdreiging

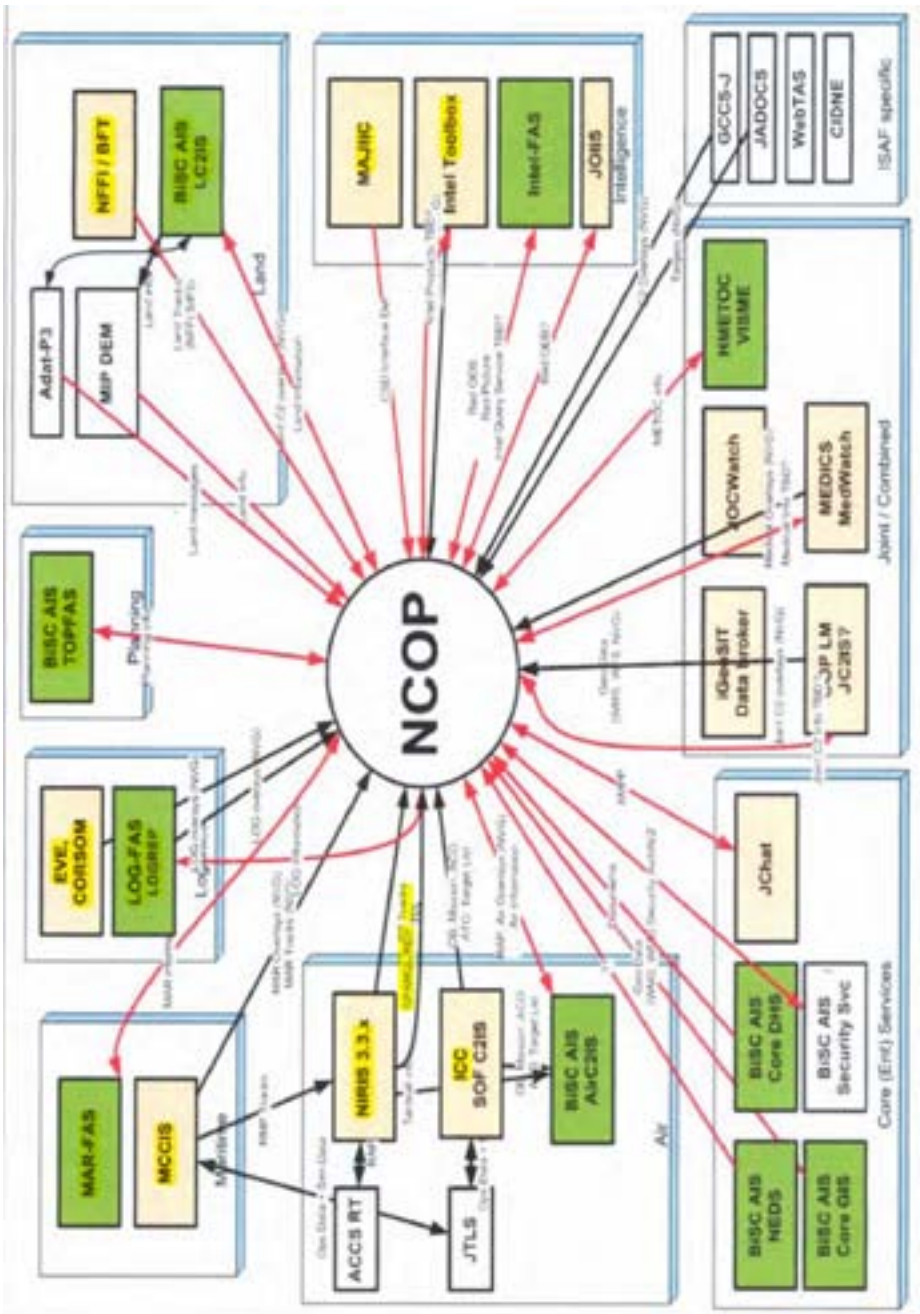
Comparator	Level of prioritisation	Characterisation of threat	Lead responding authority
Canada	One of seven highest	States (military and espionage) Cybercriminals Terrorist groups	Coordinating team within Public Safety Canada
Denmark	Highly likely	Financial damage Disruption or control of IT infrastructure and electronic warfare Espionage Cyber-relevance of terrorist threats	Sector responsibility, but leadership through the Danish Security and Intelligence Service and the National High Tech Crime Centre
Estonia	High (4 on a 5x5 matrix of impact and likelihood)	Focus on effects of threat actors	Estonian Authority for Information Systems
Finland	–	No typology available	Distributed among government departments
France	Major threat	No typology publicly used	Prime ministerial-level organisation (Agence Nationale de la Sécurité des Systems d'Information, ANSSI)
Germany	–	Terrorism, crime and war; natural hazards and technical failure or human error	Federal Ministry of the Interior and National Cyber Defence Centre (NCAZ)
The Netherlands	High priority	States Private organisations Professional criminals Terrorists Hacktivists Script kiddies Cyber-researchers Internal actors Non-actor	National Cyber Security Centre
Russian Federation	Most prominent	Internal (crime and corruption) External (state, terrorists, foreign competition)	Security Council of the Federation/Ministry of Defence National system of information protection and intelligence community
UK	Tier 1 (highest level)	Criminals Nation-states Patriotic hackers Terrorist groups Hacktivists	Cabinet Office level entity: Office for Cyber Security and Information Assurance
USA	Priority (one of four)	Criminal hackers Organised criminal groups Terrorist networks Advanced nation	Distributed across a number of organisations with inter-agency policy committee

		states	
NATO	Priority challenge (alongside four others)	None publicly available	Cyber Defence Management Board Cyber Defence Management Agency NATO's Computer Incident Response Capability
EU	–	None publicly available	Separate institutional mandates across protection of infrastructure of the EU (Computer Emergency Response Team, CERT-EU) Policy to tackle cyber-crime (DG HOME/Europol) International security and defence (European External Action Service/European Defence Agency) and business/government security (Directorate-General for Communications Networks, Content and Technology [DG CNCT]/European Network and Information Security Agency [ENISA])

Bron:
Rand, 2013. *Cyber-security Threat characterisation. A rapid comparative analysis*. RAND Europe. Cambridge.

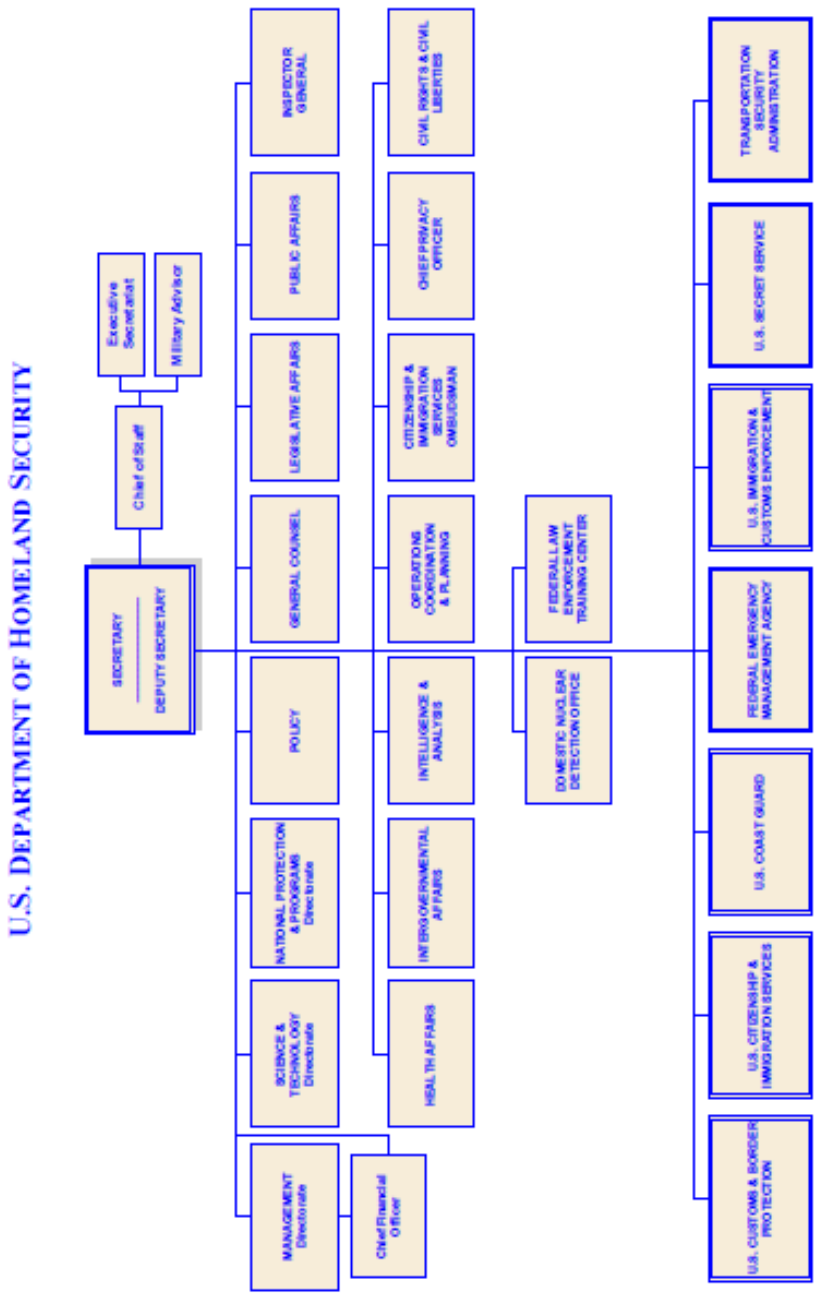
.

Bijlage 2: NATO Common Operating Picture -NCOP



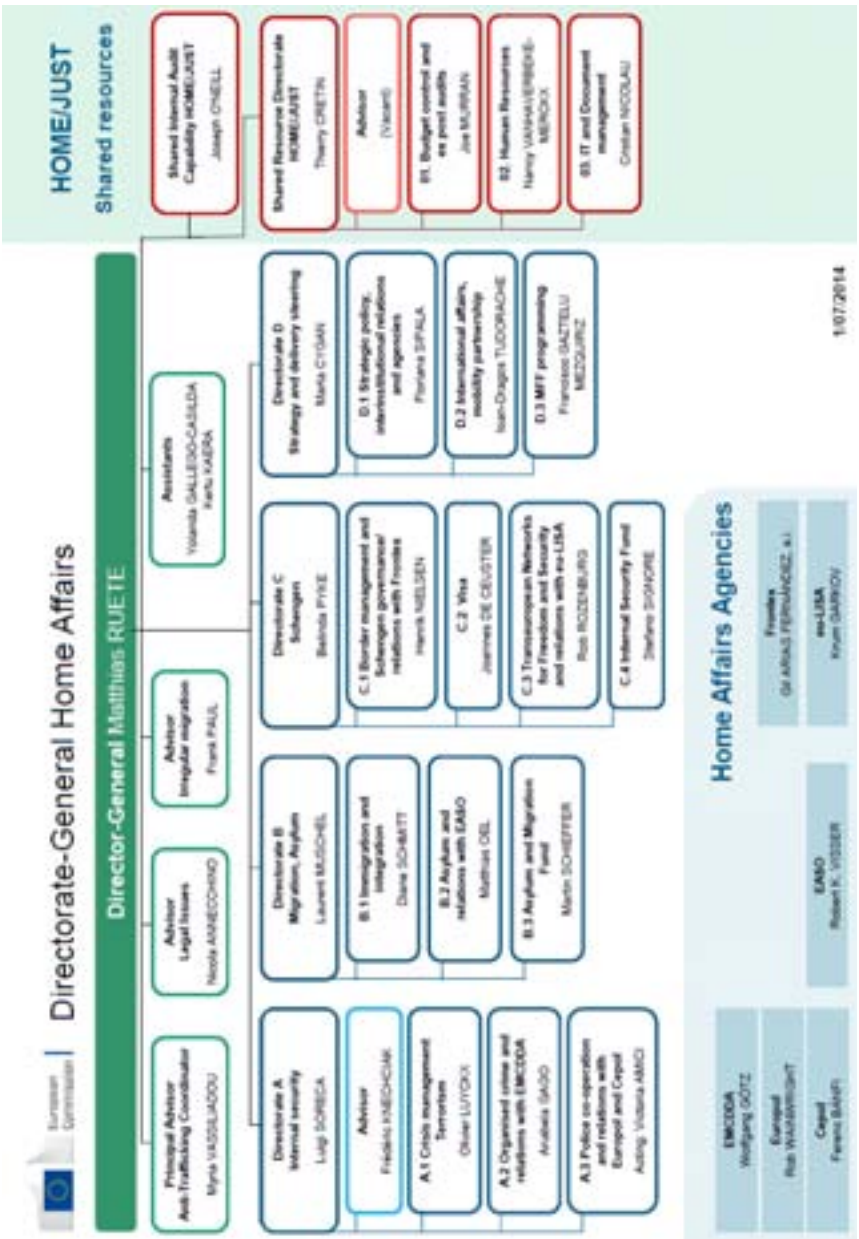
Bron:
Situational Awareness-Interoperability working group. 25-26 september 2014.

Bijlage 3: Organisatie US Department of Homeland Security



Bron:
http://www.dhs.gov/organizational-chart . Geraadpleegd op 20 oktober 2014

Bijlage 4: Organisatie EU Directoraat-generaal HOME



Bron:
http:// ec.europa.eu/dgs/home-affairs. Geraadpleegd op 27 oktober 2014.

Bibliografie

Bibliografie

AAP-06. NATO Glossary of Terms and Definitions. Edition 2012. North Atlantic Treaty Organization. NATO Standardization Agency (NSA).

Adams, Gordon and Guy Ban-Ari, John Logsdon, Ray Williamson. *Bridging the Gap. European C4ISR Capabilities and Transatlantic Interoperability*. The George Washington University. National Defense University. Octobre 2004.

Agence Nationale de la Sécurité des systèmes de l'Information (ANSSI). 2011. *Défense et sécurité des systèmes d'information. Stratégie de la France*. Février 2011.

Alberts, David S. and John J.Gartska. 1999. *Developing and Leveraging Information Superiority*. CCRP Press, 1999.

Anderson, R., & Fuloria, S. (2009), "Security Economics and Critical National Infrastructure,"in Workshop on the Economics of Information Security 2009.

Betz, David J; & Tim Stevens. 2011. Chapter Two: Cyberspace and sovereignty. Adelphi Series 51:424, 55-74.

Cabinet Office, 2011. The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. London. November 2011.

CNSS, 2010. National Information Assurance Glossary. Committee on national security systems. Instruction CNSSI-4009 van 26 april 2010.

Dai Qingmin, 2007. Ensure Historical Orientation and Promote Comprehensive Innovation of Military Informationization. China Military Science, 2007/1.

Development, Concepts and Doctrine Centre (DCDC). *Future Character of Conflict*. UK Ministry Of Defence. 2010. Beschikbaar via https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33685/FCOCReadactedFinalWeb.pdf. Geraadpleegd op 12 juli 2013.

Direction de l'information légale et administrative. 2013. Livre Blanc-Défense et Sécurité Nationale. Paris, 2013.

DiMichele, Bob. 2013. *State of C4ISR, Explains Prioriteies and Challenges During Time of Budget Uncertainty*. Army News Service. Beschikbaar via http://www.grlobalsecurity.org. Geraadpleegd op 20 oktober 2014.

EDA (a), 2013. IAP4 ISRTA-WTM Cluster Proposal. EDA R&T Directorate. Brussels, 24 April 2013.

EDA (b), 2013. *EDA Study Identifies Cooperation Prospects in Cyber Defence*. EDA News. Beschikbaar via via http://www.eda.europa.eu. Geraadpleegd op 12 juni 2013.

EEAS. 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. JOIN(2013) 1 final. Brussels 7.2.2013.

EFET. 2007. Pan-European Survey amongst energy traders about market distortions. Beschikbaar via: http://www.efet.org. Geraadpleegd op 27 februari 2013.

ENTSO-E (European Network of Transmission System Operators for Electricity). 2012. Interconnected system operation conditions in Continental Central Europe. A briefing paper to the European Commission. 13 March 2012. Beschikbaar via https://www.entsoe.eu/ . Geraadpleegd op 27 februari 2013.

EU Commission. 2012. Joint Declaration between the Department of Homeland Security and the European. Geraadpleegd op 27 oktober 2014. Beschikbaar via http://ec.europa.eu/digital-agenda/en/news/department-homeland-security-and-european-commission-joint-declaration

Farwell, James and Rafal Rohozinski. 2011. *Stuxnet and the Future of Cyber War*. Survival, 53:1, 23-40.

Foltz, Andrew, C. 2012. *Stuxnet, Schmitt analysis and the Cyber "Use of Force" debate*. Joint forces quarterly. Issue 67; 4th quarter 2012. Beschikbaar via http://www.ndu.edu/press/cyber-use-of-force.html. Geraadpleegd op 7 mei 2013.

Frost & Sullivan. 2012. *Market Insight: European C4ISR- Towards Integrated C2 at coalition level.* Beschikbaar via http://www.frost.com. Geraadpleegd op 11 juni 2013.

Future ISR. 2012. *The Collaborative Forum for Multinational JISR Transformation. Architecture, Governance and Interoperable Systems to Enable Joint ISR*. Working Group Discussion: Challenges of Future and Joint Mission Networks. 2 October 2012. Conference organized by Worldwide Business Research, Brussels.

Hanser Risk Group. 2012. *The Financial Aspects of the Security of Assets and Infrastructure in the Energy Sector*. A Set of Guidelines Prepared by the Harnser Group for the European Commision. Contract N° ENER/B1/ETU/42-2011/S12.611505. Autumn 2012.

Homeland Security Market Research. 2014. Beschikbaar via http://homelandsecurityresearch.com/wp-content/uploads/2014/04/GlobalChart_large.jpg. Geraadpleegd op 23 oktober 2014.

ICS-CERT, 2012. *Incident response summary report*. Beschikbaar via http://www.infosecisland.com/documentview/21847-ICS-CERT-Incident-Response-Summary-Report.html. Geraadpleegd op 31 mei 2013.

Innovasec. 2013. Mapping company markets and R&D. Presentation by Dr. Richard Chisnall for the European Security Innovation Network on 22 March 2013. Beschikbaar via http://www.europeansecuritydatabase.com/pdf/8_innovasec.pdf geraadpleegd op 24 april 2013.

Island of Palmas, 2 R.I.A.A. 829, 838 (Perm.Ct.Arb. 1928) en Corfu Channel Case at 43 (jurisprudentie Alvarez).

Joint Air Power Competence Centre (JAPCC) Roadmap for AIR C4ISR in NATO. Version 1.0 dated Nov 2007.

Kahn, Robert. E. 2011. *The role of architecture in internet defense* in: *America's cyber future. Security and prosperity in the Information Age*. Centre for a New American Security. Washington D.C. June 2011.

Kanselarij van de Eerste Minister, 2012. *Cyber Security Strategy. Securing Cyberspace*. Communicatiedienst van de Federale Ministerraad. Beschikbaar via https://www.presscenter.org. Geraadpleegd op 14 juni 2013.

Kopp, Carlo. 2014. *Advances in PLA C4ISR Capabilities*. In: China Brief, Volume 10, Issue 4.

Krasner, Stephen D. 2001. *Problematic Sovereignty: Contested Rules and Political Possibilities*. Columbia University Press.

Lakey, P.B. & .Neufelder, A.M. (1997). *System and Software Reliability Assurance Notebook*. Rome Laboratory Report. Rome, NY: Griffins Air Force Base.

Luiijf, Eric et al. 2008. *Empirical Findings on critical infrastructures dependencies in Europe*. TNO Defence, Security and Safety; TU Delft.

Luft, Gal. 2007. *Energy Security-What does it really mean?* In: Energy Security and Security Policy: NATO and the Role of International Security Actors in Achieving Energy Security. Ed. Phillip Cornell.

Malik, A. Mahboob, A. Khan, J. Zubairi "Application of Cyber Security in Emerging C4ISR Systems" chapter in process, IGI Global Handbook on Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies" . 2012, IGI Global Publishers.

Mandiant. 2013. *APT1. Exposing One of China's Cyber Espionage Units*. Beschikbaar via: https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/ . Geraadpleegd op 20 februari 2013.

Money, Arthur L. and David S. Alberts, 2000. *Network Centric Warfare: Developing and Leveraging Information Superiority*. DoD Cooperative Research Program. CCRP Publication Series. April 2000.

The Joint Air Power Competence Centre (JAPCC) Roadmap for Air C4ISR in NATO. Version 1.0 dated Nov 2007.

National Academies Press. 2006. *C4ISR for future naval strike groups*. Naval Studies Board (NSB) Division on Engineering and Physical Sciences, National Research Council of The National Academies. Washington DC: The National Academies Press. Beschikbaar via http://www.nap.edu/openbook.php?record_id=11605&page=152. Geraadpleegd op 05 april 2013.

NATO, 2012. *Future Mission Network Concept*. V2.0. NATO Headquarters, Supreme Allied Commander Transformation. Norfolk, Virginia. 10 October 2012.

NATO C3 Agency, 2011. *NATO C4ISR System Design Principles*. Agency Technical Directive 00.01.02. 1 October 2011.

NATO C&I Agency, 2012. *NATO Agency announces over 2 billion Euro of potential C4ISR investments in 2012-2013*. Beschikbaar via: http://www.ncia.nato.int/news geraadpleegd op 25 april 2013.

NATO RTO, 2004. *Coalition C4ISR Architectures and Information Exchange Capabilities*. Papers presented at the Symposium organized by the Information Systems Technology Panel (IST) in The Hague (The Netherlands), 27-28 September 2004. RTO-MP-IST-042. December 2005.

OECD. 2011. *Future Global Shocks: Improving Risk Governance*. Paris, June 2011.

Pollpeter, 2010. *Towards an integrative C4ISR system: Informationization and Joint operations in the People's Liberation Army*. In: The PLA at home and abroad. Strategic Studies Institute of the US Army War College. Carlisle. June 2010.

Presidential Policy Directive 21 "*Critical Infrastructure Security and Resilience"*. 12 February 2013. Bron: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity geraadpleegd op 20 februari 2013.

President's Commission on Critical Infrastructure Protection (PCCIP). 1997. *Critical Foundations: Protecting America's Infrastructures*. Washington D.C., October 1997. Beschikbaar via http://www.cyber.st.dhs.gov geraadpleegd op 21 februari 2013.

Pressreview Defensie, 2013. L'Otan s'attaque à la cyberdéfense et prépare sa nouvelle mission afghane. Bruxelles (OTAN) 29/05 (BELGA-DPA). 291601 MAY 13.

Rand, 2013. *Cyber-security Threat characterisation. A rapid comparative analysis*. RAND Europe. Cambridge.

Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie en Europese kritieke infrastructuur, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren.

Rigole, Tom en Koen Vanthournout en Geert Deconinck. 2006. *Intredependencies between an electrical power infrastructure with distributed control, and the underlying ICT infrastructure.* 2006 IEE conference. Taiwan.

Rinaldi, Steven M. et al. 2001. *Critical Infrastructure Interdependencies*. IEEE Control Systems Magazine. Washington. December 2001.

Robinson Neil, Luke Gribbon, Veronika Horvath and Kate Robinson. 2013. *Cyber Security threat characterization. A rapid comparative analysis*. RAND Europe. 2013.

Secretariat of the Security Committee. 2013. Finland´s Cyber Security Strategy. Government Resolution 24.1.2013 Ministry of Defense, Helsinki. January 2013.

Security and Defense Agenda (SDA). 2012. *Cyber-security: the vexed question of global security*. February 2012.

Shelton, Henry H., 2000. Joint Vision 2020. Chairman of the Joint Chiefs of Staff. US Government Printing Office. Washington DC, June 2000.

Smedts, Bart. 2010. Bescherming van de nationale kritische infrastructuur tegen een dreiging van asymmetrische proliferatie. Veiligheid en Strategie N°105. Koninklijk Hoger Instituut voor Defensie. April 2010.

Strategic Studies Institute, 2009. *Beyond The Strait: PLA Missions Other Than Taiwan*. Editor: Roy Kamphausen, David Lai, Andrew Scobell. Carlisle, April 2009.

Stokes, Mark A., 2012. *China's Quest for Joint Aerospace Power: Concepts and Future Aspirations*. In: The Chinese Air Force. Evolving Concepts, Roles, and Capabilities. Institute for National Strategic Studies. Washington, D.C.

Symantec, 2011. *W32. Stuxnet Dossier*. Version 1.4 (February 2011). USA, 2011. Beschikbaar via http://www.symantec.com geraadpleegd op 28 februari 2011.

Symantec, 2011. *W32. Duqu. The precursor to the next Stuxnet*. Version 1.2 (October 2011). USA, 2011. Beschikbaar via http://www.symantec.com geraadpleegd op 30 october 2011.

TAB. 2011. Office of the Technology Assessment at the German Bundestag. *What Happens During a Blackout*. Technology Assessment Studies Series N°4. Berlin, 7 April 2011.

Talinn Manual. 2013. *Talinn Manual on The International Law Applicable to Cyber Warfare*. Cambridge University Press. 2013.

Thales, 2010. *Thales defence and security C4I systems division (DSC) research and contribution to cyber security*. Beschikbaar via http://www.nis-summer-school.eu/nis10/presentations/Daniel_Gidoin.pdf geraadpleegd op 06 mei 2013.

Tuomioja, Erkki. 2012. Speech door Erkki Tuomioja, Minister van buitenlandse zaken van Finland op 4 april 2012 ter gelegenheid van het bezoek aan het Armenian Diplomatic Academy.

Tuukkannen, Topi. 2013. *Sovereignty in the Cyber Domain*. In: *The Fog of Cyber Defence*. Jari Rantapelkonen & Mirva Salminen eds. National Defence University. Helsinki 2013.

US Department of Energy (US DoE). Audit Report. *The Department's Management of the Smart Grid Investment Grant Program*. 0AS-RA-12-04. Washington D.C., 20 January 2012.

Umbach, Frank. 2012. *Critical Energy Infrastructure at Risk of Cyber Attack*. CKAS International Reports, 9/2012, pp.35-66.

Vandenberghe. 2012. *How to do business with NATO*. NATO Communication and Information Agency. Briefing to Belgian Industry. 26 november 2012. Beschikbaar via http://economie.fgov.be/nl/binaries/VANDENBERGHE_PPT_tcm325-205452.pdf geraadpleegd op 25 april 2013.

Vasilescu, Cesar. 2012. *Modeling the reliability of C4ISR systems hardware/software components using an improved Markov Model*. Technical Sciences and Applied Mathematics. Review of the Air Force Academy, the Scientific Informative Review, Vol IX, Issue 2(21)/2012.

Wolfram, Catherine. 2012. Measuring the economic cost of electricity outages. Energy Economics Exchange. Beschikbaar via http://energyathaas.wordpress.com. Geraadpleegd op 25 februari 2013.

C4ISR: een transitie naast de technologie?

Kapitein-commandant van het vliegwezen Bart Smedts
is onderzoeker Proliferatie, Kritieke Infrastructuur
en Cyberdreiging binnen
het Koninklijk Hoger Instituut voor Defensie
Bart.Smedts@mil.be

Is het vandaag nog mogelijk om militaire C4ISR-operaties uit te voeren zonder een impact te genereren in civiele netwerken of op infrastructuur? De organisatie enerzijds en de koppeling van platformen en sensoren anderzijds maken dit als maar moeilijker: waar de C4ISR-genese tot stand kwam uit militaire behoefte, is de verankering in de civiele maatschappij steeds groter geworden en stellen we vast dat de C4ISR-transitie verder gaat dan een technologische aanpassing. Een dynamische C4ISR- en ondersteunende cyberarchitectuur zijn wenselijk. In deel een van deze studie benaderen we de militaire oorsprong van C4ISR-evolutie en de ondersteunende cyber-dimensie. Vervolgens verkennen we de extra-militaire dimensie en de vereisten van toekomstige operatietonelen. In een laatste deel trachten we aanbevelingen te distilleren voor België.

Voor deze en andere publicaties:
www.khid.be