VEILIGHEID & STRATEGIE NR 124
Mei 2016

Koninklijk Hoger Instituut voor Defensie

Kritieke energie infrastructuur: kadrering en afhankelijkheden

Kapitein-commandant van het vliegwezen Bart Smedts

DEFENSIE

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

Kritieke energie infrastructuur: kadrering en afhankelijkheden.

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

A comprehensive and uniform definition of critical energy infrastructure lacks and should include the influence of cross-domain dependencies. The degree of criticality thus exceeds the identification of individual vital energetic elements of infrastructure but should rather be defined as the degree to which an incident may cause a cascade of effects in other domains. The importance of energy distribution systems increases with that regard in the future and therefore the protection of critical energy infrastructure cannot be reduced to the sole physical protection but encompasses a cybernetic aspect as well as other structural measures.

The physical protection of critical energy infrastructure gives relevance to the involvement of security actors as Belgian defense. Internally, a physical protection is only possible in a dynamic way by sketching an evolutionary picture of the threat on the one hand and involvement of private as well as public partners: therefore a long term investment climate is needed. In addition, the conformity to standards and connectivity are key to successful protective measures. In addition dependencies can be decreased by diversified sources and diversified origins of one energy resource: countries like Turkey, the Middle East and Norway will remain regions of interest for Europe to that aim.

The US as a model for European cybernetic protection is insufficient: institutionalized standards and procedures for the cyber protection of critical infrastructure, should also be enforceable on public and private partners within the EU. The involvement of defense actors in the cyber protection has legal constraints and consequences for critical infrastructure amongst which nuclear installations.

Diversification of resources and increasing energy efficiency will reduce the overall vulnerability while increasing the need for connectivity and protection of distribution systems. Artificial subsidies as well as the absence of long term investment climate, and the irrational comparison of maximum output power as compared to actual energy availability leave no rational cost-

benefit analysis between available resources. A common energy policy at European level could facilitate a stable investment climate.

In Belgium, the improved protection of critical energy infrastructure is regulated by the law of July 2011 as well as the Royal Decree implementing it for the energy sector: Belgian Defense's role herein, next to the support for the physical protection, lies in the exchange of information with security and intelligence services and in the coordination of the military with the civil list of critical infrastructure. The need to broaden the scope of the Law of 11 July 2011 beyond the energy and transportation sector is exemplified by the empiric relevance of the cybernetic domain to run and control critical energy infrastructure. The mandate of the Cyber Security Centre of Belgium should be extended to that aim and a cyber-incident response plan that allows for interaction between existing emergency plans on the one hand and planning for cyber incidents at the advent of failure of critical energy infrastructure in particular will be needed. A-dogmatic diversification of resources and capacity is necessary but will not suffice as the junction of cross-border distribution systems will reduce vulnerability while at the same time increase the complexity of the protection problem.

Both in terms of definition of criticality of critical energy infrastructure as well as in the quest for solutions, it appears that the protection problem holds multi-departmental, multi-disciplinary and multilateral parameters which increase the complexity in time. This thrives to the conclusion that the tendency to disinvest in research and development is contrary to the rational genesis of a solution: the partnership between defense, industry and science, is a prerequisite and should therefore be restored. This approach will ensure the protection of this complex issue to reach a successful conclusion at regional, national and supranational level.

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

Lijst van afkortingen

ADCC	Algemene Directie van het Crisiscentrum
ADIV	Algemene Dienst Inlichtingen en Veiligheid
CCB	Centre for Cyber Security Belgium
CEP	Civil Emergency Planning
CERT	Cyber incident Emergency Response Team
CEDS	Cybersecurity for Energy Delivery Systems
CIWIN	Critical Infrastructure Warning Information Network
COTS	Commercial off the shelf
CSET	Cyber Security Evaluation Tool
DAR	Design Architecture Review
DHSOIP	DHS Office for Infrastructure Protection
DHS	Department of Homeland Security
DoD	Department of Defence
DoE	Department of Energy
ECI	European critical infrastructure
EDA	Europees Defensieagentschap
EFTA	European Free Trade Association
EGCI	Electric Grid Cybersecurity Initiative
EMP	Elektromagnetische puls
ENISA	European Network and Information Security Agency
ENSEC COE	Energy Security Center of Excellence
ENSREG	European Nuclear Safety Regulators' Group
ENTSO	European Network Transmission System Operators
EPCIP	European Program for Critical Infrastructure Protection
ES-ISAC	Electricity Sector Information Sharing and Analysis Centre
Euratom	European Atomic Energy Community
FANC	Federaal Agentschap voor Nucleaire Controle
FERC	Federal Energy Regulatory Commission
KEI	Kritieke Energie Infrastructuur
IAEA	International Atomic Energy Agency
ICS-CERT	Industrial Control Systems Cyber incident Emergency Response Team
INPO	Institute for Nuclear Power Operations
NAVV	Network Architecture Verification and Validation
NCCIC	National Cybersecurity and Communications Integration Centre
NERC	North American Electric Reliability Corporation
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NRF	National Response Framework

OVSE	Organisatie voor Veiligheid en Samenwerking in Europa
PPD	Presidential Policy Directive
RoE	Rules of Engagement
SCI	Supplier Concentration Index
TNCEIP	Thematic Network on Critical Energy Infrastructure Protection
TWh	TeraWatt hours

Inleiding

Vooreerst willen we in dit werk tot een bruikbare definitie of omschrijving komen van wat men onder kriticiteit verstaat: aan de hand van bestaande definities en empirisch onderzoek, wil men in een eerste deel alle mogelijke elementen omschrijven die van dichtbij of ver enige invloed hebben op voornoemde term. Meteen zullen we zien welke de gevolgen een dergelijke omschrijving inhouden: van wat vroeger werd omschreven als bescherming kritieke infrastructuur dienen we dus zowel de aard van die infrastructuur als de aard van de bescherming in vraag te stellen. Van de bij aanvang zuiver fysische aard van de bescherming, komt men tot de vaststelling dat kriticiteit, zowel door de aard van de dreiging als de grotere complexiteit door afhankelijkheden in verschillende domeinen, niet meer herleid kan worden tot één enkel domein of een opsomming van domeinen, maar dat kriticiteit moet omschreven worden als de mate waarin een incident een cascade aan effecten kan veroorzaken in andere domeinen.

In een tweede wordt aandacht geschonken aan de domeinen die vermoedelijk de oorzaak zullen zijn van voormelde cascade effecten: in dit specifieke geval doen we dat voor de energie sector door de organisatie van de bescherming in de VS, de EU en de NAVO nauwer onderzoeken. We zullen ook merken dat van de initiële en verouderde aanvangscriteria tot bescherming, herleidbaar tot fysische bescherming, nieuwe elementen tot bescherming in rekening dienen te worden gebracht die de complexiteit van de opdracht nog bemoeilijken, maar die de bescherming van kritieke energie infrastructuur robuuster maken: komen hiervoor in aanmerking cybernetische bescherming maar ook diversificatie en energie-efficiëntie.

Het cybernetische aspect is het onderwerp van deel drie waarin men aandacht wil schenken aan de verschuiving van het initieel zuiver fysisch aspect van die beveiliging van kritieke energie infrastructuur naar de aanvulling met meer cybernetische beveiliging. We gaan in dit deel na welke de maatregelen en organisationele aanpassingen zijn geweest die daartoe geleid hebben. Vervolgens gaan we na in hoeverre in de EU die trend al dan niet is gevolgd. In een volgend hoofdstuk worden de juridische implicaties van een dergelijke verruiming van de omschrijving van kritieke energie infrastructuur en in het bijzonder voor de bescherming ervan belicht. Als slot van dit gedeelte wordt een hoofdstuk gewijd aan een energie infrastructuur die van bij aanvang

bijzondere bescherming genoot omwille van de catastrofale gevolgen die na de ramp van Fukushima nog meer op de voorgrond zijn getreden.

In deel vier wil men oog hebben voor de aanvullende structurele elementen ter bescherming van kritieke energie infrastructuur te weten diversificatie en energie-efficiëntie. We gaan in dit deel na welke de uitdagingen zijn voor de EU rekening houdend met het kader van reductie van de uitstoot van broeikasgassen.

In een laatste deel gaan we na hoe ons land zich positioneert in deze problematiek en trachten we te identificeren welke de uitdagingen zijn die ons op middellange tot op lange termijn te wachten staan.

De standpunten van de auteur geven niet noodzakelijk de standpunten van Defensie of het Koninklijk Hoger Instituut voor Defensie weer.

Deel 1

Definities, kadrering en belang van kritieke energie infrastructuur

Definities, kadrering en belang van kritieke energie infrastructuur

Definities met betrekking tot wat we verder in dit werk zullen omschrijven met de term kriticiteit, en in de Angelsaksische literatuur omschreven door de gemeenschappelijke term "criticality", worden al naargelang de geraadpleegde bronnen anders ingevuld. Kritische functies behelzen hoofdzakelijk leveringsdistributiesystemen voor energie, diens operatie, dienst of een opdracht die wanneer ze worden onderbroken of gecompromitteerd, ernstige schade zouden toebrengen in andere domeinen zoals veiligheid, gezondheid, operaties en economie (Energy Sector Control System Working Group, 2011; p.21). De ernst van die gevolgen zou dan meteen ook een maat zijn voor de kriticiteit die hiermee is gedefinieerd en zelfs een kwantitatieve benadering mogelijk zou maken door een schatting van het aantal dagen dat een systeem niet operationeel blijkt of de kosten die ermee gepaard gaan.

De jongste definitie van de term kritieke infrastructuur vloeit voort uit de USA Patriot Act van 2001 (42 U.S.C. 5195c(e)), met als definitie "systemen of instrumenten die, zowel fysisch als virtueel, zo essentieel voor de Verenigde Staten dat het onvermogen of de vernietiging van dergelijke systemen een slopende impact zouden hebben op de veiligheid, nationale economie, gezondheidszorg of enige ander combinatie van voorgaanden." (eigen vertaling)[1]. Dit stemt overeen met de geest van artikel 2 van de 2008-richtlijn van de Europese Raad stellende dat het een "voorziening, systeem of een deel daarvan [betreft] op het grondgebied van de lidstaten dat van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, waarvan de verstoring of vernietiging in een lidstaat aanzienlijke gevolgen zouden hebben doordat die functies ontregeld zouden raken." (eigen vertaling)[2]. De europese kritieke infrastructuur is dan enkel een verwijzing naar

[1] systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

[2] an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a

de geografische locatie van die infrastructuur en zijn grensoverschrijdende impact bij uitval: om beschouwd te worden als 'European critical infrastructure' (ECI) moet een infrastructuur gelokaliseerd zijn in een van de lidstaten en tegelijk moet de uitval of de vernietiging ervan een impact hebben op minstens twee lidstaten, met inbegrip van effecten die te wijten zijn aan afhankelijkheden tussen verschillende sectoren onderling.

Een aanzet tot definitie wordt gegeven in het verslag van de Amerikaanse presidentiële commissie voor bescherming van kritieke infrastructuur. Deze definieert infrastructuur als "een netwerk van onafhankelijke, meestal private, door de mens gemaakte systemen en processen die samenwerken om een continue stroom van essentiële goederen en diensten te genereren" (PCCIP, 1997; p.3 - eigen vertaling). Het addendum dat slaat op de kriticiteit heeft betrekking op "het onvermogen of de vernietiging van die infrastructuur een verzwakking van defensie en de economische veiligheid tot stand zou brengen (op.cit.)". In de Verenigde Staten, waar de cultuur voor bescherming van infrastructuur door gekende gebeurtenissen gedrevener is dan in de Europese Unie, zien we dat de identificatie zelfs in haar omschrijving in de mogelijkheid voorziet van aanpassingen indien noodzakelijk geacht: "De minister van Binnenlandse Veiligheid (Homeland Security) zal periodisch de noodzaak evalueren om veranderingen aan te brengen en veranderingen goed te keuren aan sectoren die behoren tot kritieke infrastructuur. Hij zal daartoe overleg plegen met de raadgever van de President inzake binnenlandse veiligheid en contraterrorisme vooraleer een sector van kritieke infrastructuur te veranderen of een daaraan gehecht sectorspecifiek Agentschap" (The White House, PPD 21 – eigen vertaling). De kriticiteit zoals ze in de Amerikaanse definitie kwantificeerbaar is, hangt af van de gevoeligheid van systemen enerzijds en is ook afhankelijk van de nationale energieveiligheid. In wat volgt zullen we onderzoeken of die definitie met uitsluitend nationale insteek volstaat, dan wel of die gestoeld is op een internationaal netwerk van bronnen, infrastructuur en beschikbaarheden van voorgaande, moet ze worden aangevuld.

In de Verenigde Staten werd een concrete invulling gegeven aan de definitie van kritieke infrastructuur: onder de vorm van Presidential Policy Directive 21 van februari 2013[3] als aanvulling op de US Patriot Act waarin 16 domeinen worden gedetailleerd die in aanmerking komen voor bijzondere

---

significant impact in a Member State as a result of the failure to maintain those functions.

[3] Critical Infrastructure Security and Resilience beschikbaar via https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. Geraadpleegd op 7 april 2015.

aandacht omwille van het feit dat de onderbreking van functionaliteit, het leven, bezittingen, het milieu en de volksgezondheid in gevaar zouden kunnen brengen. De betere bescherming ervan zou moeten zorgen voor de beperkte impact op de goede werking van de overheid en simultaan sociale en economische consequenties beperken. De domeinen die hierin worden gelijst gaan van chemie, commerciële infrastructuur, communicatie, kritieke manufactuur, dammen, defensie-industrie, nooddiensten, energie, financiële diensten, voeding en landbouw, overheidsgebouwen, gezondheidszorg en volksgezondheid, informatietechnologie, kernreactoren, -materiaal en –afval, transport, water en afvalwaterbehandeling. Ter vergelijking is er in de EU een veel kortere lijst weerhouden te weten: chemie, energie, financiën, voedselveiligheid, gezondheid, informatie- en communicatietechnologie (optioneel), nucleaire industrie, transport, water, ruimtevaart en onderzoeksfaciliteiten[4].

Mogelijke oorzaken voor het in gevaar brengen van de goede werking van die domeinen omvatten natuurlijke rampen, cyberincidenten, industriële ongevallen, pandemieën, terroristische activiteiten, sabotage en vernietigende criminele activiteiten.

Het is de gevoeligheid van systemen die aan de basis ligt van deze formulering als definitie van kriticiteit en de reden daarvoor is terug te vinden in de afhankelijkheid van verschillende domeinen onderling. De belangrijkste reden daarvoor is de vaststelling dat een verstoring in de energie-infrastructuur ernstige schade kan berokkenen. Het gebrek aan strategisch onderzoek en inzicht vooraf wordt door Lovins als ‘ad-hocratie’ (Lovins, 1982; p.2) bestempeld en is tevens de oorzaak van een groeiend aantal onaangepaste afhankelijkheden. Het adjectief ‘onaangepast’ duidt in de richting van een gebrek aan onderzoek van de mogelijke implicaties van het ontstaan van afhankelijkheden: dat er steeds meer afhankelijkheden bestaan is niet vreemd aan een steeds complexer netwerk van diensten en toestellen. Maar een dergelijk netwerk kan ook tot stand komen zonder echt rekening te houden met de gevolgen van die afhankelijkheden noch de gevolgen van nieuwe connecties van domeinen op langere termijn. Indien het toenemen van afhankelijkheden eigen is aan de grotere mate van complexiteit die van netwerken voortvloeit, komt dat in het onderwerp dat ons aanbelangt concreet zowel fysisch als cybernetisch tot uiting: een voorbeeld daarvan is de onmiddellijke commerciële return die wordt nagestreefd door private actoren en daarom als voldoende reden wordt beschouwd om apparatuur te connecteren en zo netwerken voor gebruikers en exploitanten te ontwerpen (‘network of things’) dat in de toekomst beter zal kunnen inspelen op de specifieke noden van ieder gebruiker

[4] Ontwerp van richtlijn van 2006 en richtlijn van 8 december 2008: 2008/114/EC

afzonderlijk in tegenstelling met het standaardpakket dat vandaag aan een collectief van gebruikers wordt afgeleverd. Deze flexibele benadering van dienstverlening vergt echter een informatiestroom die in twee richtingen loopt: van de producent naar de gebruiker en omgekeerd. En net hierdoor kan een bijkomende gevoeligheid tot stand komen: daar waar vroeger alleen het al dan niet beschikbaar stellen van voormelde goederen en diensten een probleem kon vormen, is dat nu te moduleren door een onaangepaste kwantificatie. Een voorbeeld hiervan kan gevonden worden bij de variabele output van energiestromen afkomstig van alternatieven energiebronnen op een onaangepast distributienetwerk.

Voorgaand voorbeeld stelt meteen ook de vraag in welke mate het commerciële voordeel te rijmen valt met het collectief belang of met andere woorden welke de gevolgen van deze vaststelling zijn voor het definiëren van kritieke infrastructuur en welke bijgevolg ook de perimeter is die men in het kader van de bescherming dient te beveiligen. Ook empirisch onderzoek toont tal van pogingen (voornamelijk na de aanslagen van 9/11) ter identificatie ervan: een oplijsting van sectoren die men in beschouwing wil nemen schiet in dit plaatje tekort. Op zich is het een noodzakelijke maar niet voldoende voorwaarde: elke poging tot exhaustieve lijst bleek al snel tekort te schieten. De pogingen om na de aanslagen in de VS een exhaustieve lijst op te stellen van sectoren en hun respectieve infrastructuur, bleek in de VS moduleerbaar en interpreteerbaar te zijn al naar gelang de noden en vooropgestelde doelen: een eerste poging tot inventarisatie bleek vooral respons te genereren door de extra financiering die een dergelijke inventarisatie met zich meebracht. Het bureau dat verantwoordelijk was voor de inventarisatie van alle kritieke infrastructuur in de VS (National Asset Data Base-NADB) moest verschillende fazen doorlopen waarvan een eerste bestond uit zelfrapportage. In 2006 kwam men tot de vaststelling dat een eerste product dat tot stand was gekomen niet bruikbaar was omwille van een verkeerde interpretatie van het begrip kriticiteit: in de richtlijnen voor rapportage was immers gemeld door het verantwoordelijk agentschap (DHS Office for Infrastructure Protection- DHSOIP) dat ‘elk systeem of element in beschouwing moest worden genomen dat, indien aangevallen, aanleiding zou geven tot een catastrofaal aantal doden of catastrofale economische schade’ (Clemente, 2013; p.19). Elk van de gebruikers bleek uit te gaan van een ander niveau van schade met als gevolg dat datgene wat lokaal of zelfs privé een onaanvaardbare schade zou zijn, op nationaal vlak irrelevant blijkt voor verdere exploitatie. De positie van DHS hierin is duidelijk en omvatte van bij aanvang een benadering die niet alleen nationale exploitatie zou mogelijk maken maar een risicoanalyse zou toelaten die verder reikt dan het lokale niveau (DHS, 2006; p.20): “DHS has begun developing, but has not yet completed, a framework to help agencies and the private sector develop a consistent approach for analyzing and comparing risks

to transportation and other sectors. Until this framework is finalized and shared with stakeholders, it may not be possible to compare risks across different sectors, prioritize them, and allocate resources accordingly." Presently, the NADB enables DHS to conduct consequence-based prioritization through "simple analytical normalization tools to convert risk assessment results into comparable units" (Department of Homeland Security, Office of the Inspector General, 2006; p.20). Niet enkel de andere interpretatie van wat kriticiteit zou moeten inhouden, maar ook de geografische beperking bleek een tekortkoming voor de definitie. De illustratie ervan werd duidelijk toen vanaf 2008 kritieke afhankelijkheden moesten worden gelijst op gezamenlijk initiatief van DHS en het State Departement met als richtlijn de inventaris op te stellen van alle kritieke infrastructuur dat gelegen zou zijn buiten de geografische grenzen van de VS en waarvan het verlies een kritieke impact zou hebben op de gezondheid en/of de economische veiligheid en/of nationale veiligheid van de VS.

Door de vaststelling van de evolutie in de benadering van een meer lokale naar een internationale input, komt men automatisch tot op een punt waar men moet besluiten dat de tekorten van de initiële benadering werden erkend en dat men van een exhaustieve lijst infrastructuur is geëvolueerd naar een meer generieke benadering van goederen, diensten en infrastructuur: de gebruikte methodologie en de consequenties ervan hebben als gevolg gehad dat een dergelijke exhaustieve lijst niet meer uitbaatbaar is. En dat is nog niet eens het eindpunt van de redenering: zowel de fysische connecties maar ook de input van kritieke goederen en diensten, kritiek voor de goede werking van de economie, zouden sinds de crisis van 2008 mee hun rol hebben in een dergelijke lijst. De bijdrage van elk van de domeinen in de uiteindelijke internationale lijst wordt meegegeven in bijlage één. Naast de relatieve toedracht van elk domein in het complete plaatje, stelt men vast dat de connectie zelf tussen de verschillende domeinen en sectoren aan belang won: omwille van marktvereisten moet immers de tijd voor informatieverwerking gereduceerd worden en wordt vandaag hiervoor bijvoorbeeld gebruik gemaakt van het cyberdomein voor al wat vroeger nog door telecommunicatiemiddelen moest worden gerealiseerd.

Het besef van de complexiteit van de problematiek beperkte zich niet tot de VS. Afhankelijkheden werden door Rinaldi et al. reeds omschreven als het verband of de connectie tussen twee infrastructuren, waardoor de toestand van één infrastructuur de toestand van een andere beïnvloedt (Rinaldi et al., 2001; p.14). Een geïsoleerde sector op zichzelf als kritiek beschouwen is dus duidelijk ontoereikend. Laat dat nu net het problematische zijn in de methodologie die de Europese Unie gebruikte voor de definitie en de identificatie van kritieke infrastructuur (2008/114/EC): kritieke sectoren

werden als geïsoleerde entiteiten omschreven. Vandaag de dag zijn de sectoren fysisch of virtueel (cybernetisch) met elkaar verbonden. Deze connectie is noodzakelijk voor de optimale benutting van mogelijkheden en voor het bereiken van commerciële doelstellingen. Deze opportuniteit zorgt echter voor het concomitante voorkomen van nieuwe gevoeligheden en afhankelijkheden. Men kan in dat geval een effect-orde definiëren als het aantal connecties dat tussen twee niet-rechtstreeks geconnecteerde netwerkelementen bestaat. In ons voorbeeld kan men spreken van tweede, derde, etc. ordeconnecties. Het belang van de netwerkstructuur en de orde van connecties komt naar voren bij de bestudering van cascade-effecten waarbij een incident niet meer geïsoleerd moet beschouwd worden maar aanleiding kan geven tot incidenten in andere domeinen. In het bijzonder voor het domein energie is dat merkbaar en hiertoe werd sinds 1982 al onderzoek gedaan in de VS: doel van het onderzoek was om alle factoren in kaart te brengen die energiesystemen zouden verstoren, oorzaken van die verstoringen, de gevolgen ervan en de interacties van verschillende systemen; aan te tonen waarom sommige systemen die betrouwbaarder zouden worden in een geïnterconnecteerd systeem plots ook minder veerkrachtig kunnen worden ten opzichte van incidenten; mogelijke ontwerpen te construeren die niet onderhevig zouden zijn aan pannes of verstoringen; ervoor te zorgen dat de veerkracht van die combinatie van systemen niet noodzakelijk duurder zou uitvallen wanner het systeem *ab initio* in een dergelijke configuratie wordt ontworpen. De bedoeling hiervan was te onderzoeken in welke mate een technologische verbetering de samenleving gevoeliger heeft gemaakt voor de gevolgen van rampen en noodsituaties waarover geen controle kan worden gewonnen door de toegenomen complexiteit en technologisch afhankelijkheid.

In feite kan een dergelijk complex netwerk elke actor ontdoen van een volledige controle van de dynamiek van het netwerk en kan slechts bij benadering het belang van orde-effecten worden bepaald. De tendensen in de markteconomie willen wel dat meer en meer fluxen in real-time kunnen worden opgevolgd, en dat reactie op veranderingen zo snel mogelijk plaatsgrijpen om niet de indruk te scheppen dat een dergelijke dynamiek volledig buiten de controle van alle actoren plaatsgrijpt, in het bijzonder de politieke leiders: feit blijft dat de maximalisatie van de economische return (het vergroten van de efficiëntie en de tijdswinst) aanleiding heeft gegeven tot meer complexe systemen met meer inter-connecties die voor meer efficiëntie moesten zorgen. Tegelijkertijd gaat de stuwing om meer en meer economische efficiëntie na te streven samenvallen met het bereik van de limieten van de controleerbaarheid en dus de beveiliging van alle sectoren in het netwerk op een exhaustieve manier. Het verlies van de controle heeft volgens Clemente als gevolg dat men geneigd is om de perimeter voor controle meer en meer uit te breiden en meer

en meer elementen en/of processen daarom als kritiek te gaan beschouwen (Clemente, 2013; p.26). Het zal er dus op aan komen om, in de zoektocht naar een definitie of identificatie van kriticiteit, om die verbanden en/of structuren aan te duiden die zowel privaat als publiek consensus genieten in het feit dat onvoldoende bescherming of faling ervan tot onherstelbare menselijke en/of economische schade zou leiden: in dat opzicht kan men stellen dat de vrije markt ergens haar eigen grenzen bepaalt wanneer, wil het de gevolgen van de complexiteit kunnen dragen en de beveiliging ervan mogelijk blijven maken, het beperkt wordt door investeringen die moeten worden gedaan om de controle op een geïnterconnecteerd netwerk van domeinen tot stand te kunnen brengen. In elke dimensie die moest worden geordend (land, water, lucht, ruimte) is men in staat geweest om dit op een aanvaardbare manier te reguleren. De vraag rijst nu of het vijfde domein, cyber, nog in volle ontwikkeling en dienst doend als connector tussen alle bestaande domeinen, op een gelijkaardige manier zal kunnen worden gereguleerd en/of beveiligd als de overige, dan wel of een zekere oncontroleerbaarheid of onvoorspelbaarheid van de domeinen in dit geval moet worden aanvaard. In dat geval kan geen algemene beveiliging worden verzekerd en moeten zekere prioriteiten worden gesteld aan de verzekering van die elementen die men als kritiek zal willen erkennen. Zoals men in het domein van de beveiliging tegen terrorisme heeft gezien dat een grotere bescherming synoniem kan zijn van een grotere vorm van fysieke controle, is het mogelijk dat dit ook in andere domeinen het geval zal zijn.

Als gevolg van voorgaande kan men stellen dat de omschrijving van kriticiteit niet in eerste instantie zal bestaan uit een exhaustieve lijst van domeinen en installaties maar eerder uit verbanden tussen domeinen en de impact van cascade-effecten. De vraag die we ons dan moeten stellen is te weten of alle domeinen even belangrijk zijn, dan wel of er een geprivilegieerde keuze te maken is in het belang van domeinen en/of verbanden ertussen? In 2008 onderstreepte Luijf (TNO, 2008) reeds het belang van slechts een beperkt aantal sectoren voor het genereren van die cascade-effecten: voornamelijk energie- en telecommunicatiestoringen zouden aan de basis liggen van domein-overschrijdende incidenten. Dit is opmerkelijk daar de EU in eerste instantie slechts optioneel het belang van communicatietechnologie heeft vastgelegd. De afhankelijkheden worden in de Europese richtlijn nochtans expliciet vermeld en het grensoverschrijdende karakter van incidenten erkend. Deze worden in artikel 2 beoordeeld door domein-overstijgende criteria met inbegrip van afhankelijkheden van andere soorten infrastructuur, waaronder verstaan wordt dat die niet noodzakelijk zelf opgenomen worden in de lijst van kritieke infrastructuur. De studie van Luijf et al. (TNO, 2008) wees uit dat, op een totaal van 1.749 incidenten met impact op één of meerdere domeinen in 29 Europese landen, 268 aanleiding gaven tot cascades: 60% daarvan was te wijten aan

energie, 24% aan telecommunicatie, 5% aan transport en 3% aan water. Energie neemt de belangrijkste plaats in deze incidenten en het spreekt dus vanzelf dat in een niet-exhaustieve benadering een prioritaire aandacht dient te gaan naar het belang van kritieke energie-infrastructuur. De kans op cascadegeneratie voor de energiesector werd geschat op 50% terwijl dat voor telecommunicatie 40% is. Wetende dat na de aanslagen van Brussel communicatie, al dan niet moedwillig, een van de eerste getroffen domeinen bleeg rijst de vraag te weten of dergelijke incidenten in de toekomst mogelijke gevolgen kunnen hebben onder de vorm van cascade-effecten. De connectiviteit met andere sectoren is tegelijk een mogelijkheid van groter penetratievermogen in het dagelijkse leven: in 24% van de incidenten is die connectiviteit van eerste orde, waaronder moet worden begrepen dat een incident in één domein ook gevolgen genereert in een ander domein. In 4% van de gevallen was de penetratiegraad van tweede orde (een incident in één domein genereert een gevolg in minstens twee andere domeinen) en 0,2% onder te brengen als derde orde (een incident in één domein genereert een gevolg in minstens drie andere domeinen). Hogere dan derde orde-incidenten werden niet waargenomen in voormelde studie. Merk op dat het bestaan van een cascade een hogere orde dan één impliceert dat versterkende terugkoppelingen mogelijk worden. Een illustratie van hogere ordecascades en terugkoppelingsvoorbeelden werden uitgewerkt in bijlage 2. Maar belangrijke nog dan de terugkoppeling die de complexiteit van de gevolgen doet toenemen, is het onderscheid te maken tussen domeinen die voornamelijk door de inputs van andere domeinen (receptoren) ondergaan terwijl andere domeinen voornamelijk outputs genereren (donoren). Teruggrijpend naar ons voorbeeld stellen we vast dat energie, ICT en financiën kritische donoren zijn terwijl volksgezondheid en industrie eerder onder te brengen zijn onder de noemer kritische receptoren. Zowel de studie van Luijf als het voorbeeld van de connectie van domeinen geven aan dat energie de belangrijkste plaats inneemt en dus de aandacht dient te krijgen in een studie omtrent kritieke infrastructuur en de gevolgen van incidenten op de maatschappij.

Na de empirische vaststelling van de prioriteit die energie geniet in de nationale benadering dient men vast te stellen dat energie ook bij de internationale strategische prioriteiten hoort die grootmachten nastreven: in dat kader vindt men, zowel in de vooruitzichten op lange termijn, als de strategische prioriteiten van krijgsmachten dat oplossingen voor energetische vraagstukken nog grote onzekerheden blijven bevatten: zowel energiezekerheid als een efficiënte vorm van bescherming van kritieke infrastructuur moet immers worden tot stand gebracht. In dat kader wil men in de eerste plaats energetische veiligheid garanderen, waaronder moet worden verstaan de beschikbaarheid van de bronnen enerzijds als ook de technische mogelijkheid

om die te exploiteren. We zullen verder zien welke elementen daartoe kunnen bijdragen. We zullen ook merken dat de energetische vraagstukken in hun antwoord ook interferentie ondervinden van andere domeinen. Bovendien laat voornoemde penetratie van andere sectoren ook toe dat rekening dient te worden gehouden met parameters die, extern energie, toch een invloed kunnen hebben op het strategische belang: zo zijn in dit geval ook cascade-effecten mogelijk door de gevolgen van incidenten in het cyberdomein die effecten veroorzaken in het domein energie. Risicoberekening van staten houden daar de dag van vandaag wel degelijk rekening mee maar in private bedrijven wordt nog niet systematisch rekening gehouden met de mogelijke gevolgen van een (buitenlands) cyberrisico op energie-infrastructuur. In het officiële verslag van de directeur nationale inlichtingen wordt het nochtans vermeld als de eerste globale dreiging van de reeks met mogelijke gevolgen voor het distributiesysteem voor elektriciteit (maar ook voor olie en/of gas) en ook luchtvaartveiligheid, respectievelijk overeenkomend met de domeinen energie en transport uit de EU richtlijn en Presidential Policy Directive (SASC, 2015). Onze werkdefinitie van kriticiteit kunnen we dus aanpassen als volgt: de mate waarin aan een energievraag niet kan worden voldaan door een niet voorzienbare omstandigheid en die over de domeingrenzen heen invloed heeft op het genereren van energie of de weerbaarheid van connexe domeinen. De onvoorziene omstandigheid die we hier aanhalen beperkt het aantal oorzaken waarmee moet worden rekening gehouden.

Onder de voorzienbare omstandigheden (oorzaken), waaronder men veronderstelt dat men zich kan voorbereiden op dergelijke evenementen, dienen volgende omstandigheden in rekening worden genomen: niet door de mens veroorzaakte omstandigheden (weer, rampen[5]), door menselijke tussenkomst veroorzaakte rampen (oorlog, terrorisme, sabotage[6]), falen van een complex systeem (technisch, logistiek, economisch), het falen van een controlesysteem van die energiedistributie (cyberaanval). Elk van deze oorzaken kan ernstige economische gevolgen hebben. Meer zelfs, ze kunnen vanuit geostrategisch oogpunt worden beschouwd als een dreiging. We zullen later zien dat het niet vanzelfsprekend is omwille van de kennis van mogelijke oorzaken, toch te kunnen voorzien in energiedistributie omdat, ondanks de kriticiteit geen exclusieve beveiliging kan worden verzekerd door één enkel departement (zoals, bijvoorbeeld, de krijgsmacht) zelfs voor voorzienbare incidenten en dit

[5] Nuttige data met betrekking tot de epidemiologie van rampen en hun impcat kunnen bekomen worden via de website http://www.cred.be/

[6] Nuttige data die een idee kunnen geven van het aantal aanvallen en de gevolgen ervan kunnen worden bekomen via de website http://trackingenergyattacks.com/EIAD

uitsluitend omwille van de complexiteit van het netwerk dat tot stand is gekomen door afhankelijkheden. Afhankelijk van de analyse van de dreiging en de structuren die er het voorwerp van zijn, zullen we als vertrekhypothese stellen dat mogelijk een samenwerking moeten worden voorzien tussen meerdere departementen. In het besluit van dit werk zullen we op deze stelling terugkomen om een meer duidelijke invulling te geven aan dit concept voor België. Als gevolg daarvan komt men tot de conclusie dat een beveiliging niet meer uitsluitend kan worden gereduceerd tot de fysische beveiliging van bijvoorbeeld bronnen of installaties, maar dat we vandaag ook moeten terugvallen op de cybernetische beveiliging en een strategie voor de optimale exploitatie en gebruik van energie.

In de VS blijkt die hypothese alleszins steek te houden: de mogelijke oorzaken voor het wegvallen van essentiële energievoorziening moesten door een strategie het hoofd worden geboden. De lange termijn visie voor de energiesector werd daarom in die richting herbekeken: "The Energy Sector envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government" (Homeland Security, 2007). Teneinde deze visie te verwezenlijken zijn een aantal doelstellingen vooropgesteld waarin duidelijk de interdepartementale connectie naar voren treedt en afhankelijkheden ook in de praktijk worden erkend: de verschillende installaties worden immers verbonden door exploitatie of distributiesystemen en netwerken.

1.Doelstelling 1 legt de nadruk op het belang van informatie-uitwisseling tussen de publieke en de private sector om over een geactualiseerd beeld te beschikken van mogelijkheden en beperkingen van het systeem ("Establish robust situational awareness within the Energy Sector trough timely, reliable, and secure information exchange among trusted public and private sector security partners").

2.Doelstelling 2 legt de nadruk op het feit dat zowel de fysische als de virtuele veiligheid moeten worden verzekerd ("Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security and resiliency").

3.Doelstellingen 3 tot en met 5 beogen ook de continuïteit van de bescherming tot stand te brengen ("Conduct comprehensive emergency, disaster and continuity of business planning, including training and exercises, to enhance reliability and emergency response; clearly define

critical infrastructure protection roles and responsibilities among all Federal, State, local and private sector security partners; understand key sector interdependencies and collaborate with other sectors to address them, and incorporate that knowledge in planning and operations").

4.De laatste doelstelling beoogt het publieke vertrouwen in energieveiligheid te herstellen ("Strengthen partner and public confidence in the sector's ability to manage risk and implement effective security, reliability, and recovery efforts").

De zoektocht naar de redenen van het falen van kritieke energie-infrastructuur heeft geleid tot de vaststelling dat vele oorzaken van falen evenzeer effecten veroorzaken aan een bepaald type infrastructuur, maar evenzeer op de complexere interacties die eerder werden aangehaald en in figuur van bijlage 2 worden geïllustreerd. De kwetsbaarheid van het volledige systeem kan bijgevolg niet geëvalueerd worden door de som van alle mechanische individuele en infrastructurele kwetsbaarheden van energie-infrastructuur alleen. Kwetsbaarheden worden duidelijk door de aard van de falingen die ze veroorzaken: het falen van één onderdeel (common-mode[7], common-cause[8]); falen door onvoorspelbaarheid te wijten aan de complexiteit van het systeem en de interacties van de verschillende onderdelen; falen door hogere orde gevolgen (cfr figuur in bijlage 2); verrassingen.

1.Falen van één onderdeel door common-mode of common-cause heeft de neiging om meer schade te veroorzaken bij incidenten bij kernreactoren.

2.Falen door complexiteit wordt vaak uitgelegd aan de hand van biologische of sociale interacties en met volgende kenmerken: ze zijn voorzien van feedback interacties waardoor de voorgeschiedenis ook een rol speelt in de actuele werking van het systeem; ze reageren op gebeurtenissen die een gespreide geografische verdeling hebben; door geregeld te worden door niet één discrete parameter maar drempelwaarden is een niet-lineaire respons vaak vastgesteld. Deze eigenschappen hebben volgens Lovins een zeer belangrijk gevolg voor de beveiliging van dergelijke systemen omdat men de gehele structuur niet kan beveiligen door één enkel onderdeel of één enkele locatie te

[7] Common-mode faling verwijst naar de faling van identieke en redundante onderdelen door een enkele gebeurtenis (Lovins, 1982; p.20).

[8] Common-cause faling verwijst naar verschillende onderdelen die eenzelfde taak uitvoeren en die onder de zelfde omstandigheden op een identieke manier falen (Lovins, op.cit.).

beveiligen. Dit wordt zeer goed geïllustreerd door veiligheidsaspecten louter te beperken tot één enkel domein (te weten de krijgsmacht) terwijl men ondertussen weet dat de krijgsmacht alleen niet kan instaan voor de beveiliging van het elektriciteitsdistributie-netwerk bijvoorbeeld.

3.Falen door het bestaan van hogere orde cascades werd reeds in de aanvang van deze inleiding aangehaald als het gevolg van afhankelijkheden en tevens een nieuwe maatstaf voor het bepalen van de kriticiteit: domeinen die steeds terugkomen (als donor of als receptor) zijn belangrijke knooppunten die de gevoeligheid van het hele systeem zullen bepalen.

4.In de beveiliging van systemen moet niet alleen rekening worden gehouden met de redundantie van onderdelen en de uitvoerbaarheid van processen die men kent maar ook met onvoorzienbare omstandigheden: de ramp van Fukushima heeft voldoende aangewezen de oorzaak te zijn geweest van een samenloop van omstandigheden die, indien ze zich afzonderlijk zouden hebben voorgedaan, perfect het hoofd zouden kunnen worden geboden. De ontwikkeling van een systeem dat veerkracht kan vertonen in omstandigheden waar men nog niet is mee geconfronteerd, is het best bereikbare.

Redenen die men kan aanhalen voor de kwetsbaarheid van het energie-onderdeel of op zijn minst die de perceptie van kwetsbaarheid vergroot lopen uiteen. We zetten er hier enkele op een rij:

- gevaarlijke materialen: dit geldt zowel voor het gevaar van toxiciteit (na de rampen als Fukushima en Seveso behoeft dat geen verdere uitleg) als voor het gevaar om aangewend te worden voor andere doeleinden dan waarvoor het materiaal initieel was bestemd (zoals in een militair programma bijvoorbeeld),
- beperkte aanvaarding door het publiek: afhankelijk van de ligging van de installatie en de hinder en de onmiddellijke voordelen voor omwonenden zal de weerstand gemoduleerd kunnen worden,
- centralisatie van bronnen: niet enkel de centralisatie van een grote hoeveelheid bij exploitatie (zoals een oliebron), maar ook bij de distributie (bijvoorbeeld transit door logistieke choke points) wordt een mogelijke aanleiding voor kwetsbaarheid,
- lange afstanden: de nood aan distributie over lange afstanden zorgt voor een kwetsbaarheid die mogelijk over dezelfde lengte van de distributie aanwezig is, of die extra middelen zal vergen voor de bescherming ervan,

- beperkte alternatieven of vervangingsoplossingen: het gebruik van alternatieve bronnen bleek vooral sinds Fukushima een goede optie om nieuwe rampen te vermijden in de toekomst maar in Japan en Duitsland is deze optie ontoereikend gebleken om aan de vraag te kunnen voldoen,
- nauwe marges van operationele werking: fluctuaties veroorzaakt door wegvallen van alternatieve bronnen (bijvoorbeeld windenergie) kunnen aanleiding geven tot een instabiliteit van het hele elektriciteitsnetwerk dat slechts operationeel blijft binnen nauwe marges (zie verder). Een gelijkaardige vorm van instabiliteit ontstaat in de gasdistributie wanneer drukken te veel schommelen en pompen niet optimaal meer kunnen functioneren,
- niet soepele werking van distributienetwerken, wisselwerking tussen verschillende systemen die verondersteld waren onafhankelijk te zijn van elkaar: zo is de uitval van stroom ook de oorzaak voor het wegvallen pompcapaciteit van olieproducten,
- concentratie van groot kapitaal/investeringen: de aanbouw van een nieuwe centrale vanaf de planning tot de uitvoering kan al gemakkelijk tien jaren in beslag nemen. De motivatie van investeerders kan in een dergelijk scenario enkel aangewakkerd worden door een stabiele financieel beleid op langer termijn,
- lange wachttijden: naast de financiële onzekerheid is er door de wachttijd vanaf concept tot uitwerking een evolutie in de beschikbare technologie die niet noodzakelijk in het laatste gefinancierde plan wordt weerhouden waardoor het concept niet finaal de beste bescherming geniet tegen nieuwe dreigingen die kunnen opduiken,
- gespecialiseerde operatie en nazicht-vereisten: de moderne controle van distributie van energie wordt beheerd door geautomatiseerde systemen (wat intrinsiek een nieuwe kwetsbaarheid introduceert in alle vormen ervan) en vereist daarvoor speciaal opgeleid personeel dat zowel met die controlesystemen als met de betreffende energetische technologie te maken heeft (welk niet altijd voor handen is),
- mogelijkheid van sabotage aan de bron of over de lange keten van het distributienet: de verlenging van de distributiekanalen van de bron naar de gebruiker zorg voor een mogelijke kwetsbaarheid over de hele lijn.

De maatregelen die ervoor moeten zorgen om voormelde kwetsbaarheden te verminderen kosten natuurlijk veel geld. De effecten voor de (on)beschikbaarheid als last voor de economie zal moeten worden afgewogen ten opzichte van de kost van onderbrekingen. Dat is een politieke keuze die moet ingeschreven worden in een beleid dat overeenkomt met de prioriteiten van het ogenblik. In de VS is dat het geval sinds de aanslagen van

11 september 2001. Drie strategische imperatieven vertalen die behoefte, te weten (The White House, PPD 21):

> 1.Het afstemmen en uitklaren van verantwoordelijkheden binnen de federale overheid teneinde de nationale eenheid omtrent de versteviging van de beveiliging omtrent kritieke infrastructuur in de hand te werken,
> 2.Het efficiënt uitwisselen van informatie mogelijk maken door de minimale vereisten te definiëren voor systeemvereisten binnen de federale overheid,
> 3.Het implementeren van een integratie en analysefunctie om op de hoogte te blijven omtrent planning en operationele beslissingen met betrekking tot kritieke infrastructuur.

Deze visie wordt vertaald in concrete maatregelen om de veiligheid en veerkracht van kritieke infrastructuur te vrijwaren: deze maatregelen omvatten de evaluatie van publieke-private partnerschappen, de bepaling van minimale vereisten voor natiestaten voor een optimale informatievergaring, de ontwikkeling van een capaciteit die *real-time situation awareness* genereert met betrekking tot kritieke energie-infrastructuur met inbegrip van zowel fysieke als cybernetische elementen die daar kunnen toe bijdragen, de actualisatie van beschermingsplannen en het onderzoek naar veiligheid en veerkracht. Het gebrek aan internationale standaarden voor cybernetische veiligheid is nochtans een gebrek vanuit het standpunt van menig nationaal veiligheidslandschap (U.S. DoE, 2012): bestaande plannen zijn vaak ontoereikend of schieten tekort in een relevant risicobeoordeling en/of het inschatten van zwakten. In het bijzonder is er een gebrek aan cyberveiligheid-standaarden bij processen voor energiedistributie.

Een deel van die kwetsbaarheid is duidelijk geworden als gevolg van de ramp van Fukushima: de ramp heeft immers niet alleen aangetoond dat men voor een nucleaire installatie ook multipele risico's in beschouwing moest nemen voor de bescherming van andere kritieke infrastructuur, maar ook dat de alternatieve vormen van elektriciteitsproductie niet altijd adequaat blijken te zijn in hun huidige configuratie of aanwending. Zowel het distributienetwerk van fluctuerende energie-inputs als de cybernetische regulatie ervan zijn cruciaal indien men een geloofwaardig alternatief in plaats wil stellen voor een energievorm die (misschien tijdelijk) niet meer tot de keuzes van het beschikbare pallet behoren: als gevolg van een dergelijke keuze zijn fluctuaties in netwerkbelasting toegenomen sinds het steeds toenemend aantal hernieuwbare energie (ENTSO-E, 2012). De onvoorspelbaarheid van de precieze hoeveelheid beschikbare alternatieve energie afkomstig uit zones zoals noord-Duitsland, Denemarken, de Noordzee en de Baltische zee, kan

fluctuaties op het distributienet veroorzaken in die mate dat de fysische limieten van de materialen niet meer kunnen voldoen aan de schok die een nationaal netwerk op een gegeven ogenblik moet verwerken door de fluctuaties op het internationale net. Dergelijke afwijkingen van het geplande transmissie-vermogen ten opzichte van het werkelijke vermogen wordt in de grote meerderheid van de gevallen waargenomen in landen van Centraal Europa zoals Duitsland, Polen, Tsjechische Republiek, Slovakije, Hongarije. Het subsidiariteitsbeginsel dat in het verdrag van Lissabon wordt onderschreven (artikel 5), bepaalt dat in de EU de besluitvorming zo dicht mogelijk bij de burgers dient te worden genomen. In zaken energie zijn dat dan ook vaak lokale besturen en private partners die voor de opvang van voormelde fluctuaties moeten kunnen zorgen: door een gebrek aan transnationale coördinatie is het echter niet eenvoudig om aan die fysieke beperkingen te verhelpen. Het afstemmen van procedures, ongecoördineerde regionale en nationale netwerkuitbreiding en de onvoorspelbaarheid van de flux op het netwerk zijn elementen die daartoe bijdragen. De kost van een onderbreking van de distributie is een essentiële parameter die mee zal bepalen in welke mate aan dit euvel kan worden verholpen en dient daarom in rekening te worden genomen bij de evaluatie van de nood aan nieuwe infrastructuur. Kwalitatieve factoren die mee die kost zullen bepalen kan men vinden in fysische schade, virtuele netwerkschade (bijvoorbeeld door overbelasting of cyber-aanvallen), kost door schade aan de reputatie van het energiebedrijf of bedrijven die geen leveringen kunnen realiseren door het wegvallen van energie en het verlies aan klanten, verlies van competitiviteit, kosten van verzekering, kosten voor de opleiding van operatoren, kosten van wettelijke claims en vergoedingen, enz. Een algemeen aanvaardde methode om die kost te schatten is niet voorhanden. Al naar gelang de bron zal een ander methodologie en een ander resultaat worden gevonden: grote speelmarges bestaan en kunnen zelfs een veelvoud zijn. Dit maakt het onmogelijk om een schatting in de VS zonder meer te extrapoleren naar eigen streek of te veralgemenen naar de Euregio. Kost is bovendien tijdsafhankelijk: vraag fluctueert immers in de tijd. Een illustratie daarvan is het feit dat de vraag en dus de prijs in de winter hoger zal zijn dan in de zomerperiode of wanneer de productie toeneemt. Zowel de impact, de perceptie als de prijsschatting is zeer verschillend aan beide zijden van de Atlantische oceaan. Een voorbeeld zal dit duidelijk maken: in 2003 werden 50 miljoen klanten, zowel private personen als olie- en gasindustrie raffinaderijen en distributiebedrijven van de stroomvoorziening afgesloten, zowel in de VS als in Canada: de kost van die onderbreking werd geraamd tussen de 4,5 en 10,3 miljard USD. De raming werd geschat op de prijs die gebruikers (publiek of privaat) zouden bereid zijn om te betalen voor het geval de onderbreking zou kunnen worden vermeden: dat totaalbedrag tot 100 maal hoger kon uitvallen per kWh van de geschatte prijs van de geleden schade (TAB, 2011, p.64). De orde van grootte schijnt overeen te komen met eerdere ramingen die een panne

kost schatte op 1 miljard USD (New York -1977; Lovins, 1982; p.65). Een andere methode bestaat eruit om de aankoopwaarde van alternatieve leveranciers of de vervangkost te schatten: om de spreiding te evalueren van de mogelijkheden, ligt die waarde in de VS en Australië rond de 8,6€ per kWh terwijl een gelijkaardig Duits voorbeeld die kost tussen de 8-16€ per kWh schat (TAB, 2011, p.65). Eenvoudige vuistregels liggen soms aan de basis van die schattingen en maken gebruik van extrapolatie die niet zonder beperkingen kan worden toegepast (als voorbeeld citeren we het gebruik om de vraag bij een panne van 10kW een factor 10 te verhogen bij een panne van 100kW- Lovins, 1982; p.64). Vraag en aanbod verhouden zich echter niet in alle omstandigheden lineair.

Deel 2

Meer dan fysische bescherming?

2.1. Inleiding

Gezien de verschillende oorzaken en de kosten verbonden aan faling van energie-infrastructuur, moet worden gezocht naar gepaste maatregelen voor de bescherming ervan. Tussen centralisatie of decentralisatie bestaan verschillende benaderingen met betrekking tot de beste bescherming die men voor kritieke energie-infrastructuur kan voorzien en in het verleden is trouwens gebleken dat naargelang de culturele achtergronden en oorlogen, andere benaderingen worden geadviseerd. Als voorbeeld kan men vermelden dat een concentratie van al te grote industriële capaciteit een vooropgesteld doelwit kan worden voor militaire operaties. Een vorm van bescherming kan net daarom de verspreiding zijn van de installaties: in het geval van stroomvoorziening in het algemeen en zijn distributienetwerk in het bijzonder is die verspreiding in elk geval een noodzaak. De spreiding kent hier echter zijn grenzen in die zin dat de opwekking in een centrale moet gebeuren waarvan de verdeling van de geleverde stroom wordt uitgevoerd. Twee oplossingen zijn mogelijk: ofwel centraliseert men alle centrales en maakt men een grotere capaciteit in één punt, waarvan men de bescherming optimaal regelt, ofwel zorgt men net voor de grotere spreiding door een groter aantal kleinere centrales. Beide gevallen kwamen tijdens de tweede wereldoorlog voor. Als illustratie van de centralisatie kan men het Duitse voorbeeld aanhalen, waar de volledige zware industrie en energieopwekking werd gecentraliseerd in het Roergebied. Daartegenover staat de benadering van Japan, dat weliswaar door geografische, maar ook door de bijkomende seismische activiteit beperkt was in de keuze van het aantal sites en eerder gedwongen werd tot spreiding: op individuele basis waren die centrales of dammen in het Japanse geval geen aantrekkelijke doelen omdat te veel inspanning moest worden geleverd voor een te klein resultaat bij vernietiging. Spreiding kan daarom een mogelijke aantrekkelijke strategie vormen voor de bescherming van infrastructuur: tot in de jaren tachtig werd die benadering trouwens ook door China gebruikt. Een derde van de door het land opgewekte stroom in landelijke gebieden, en meer dan een derde van zijn hydro-kracht gegenereerde stroom was afkomstig van kleine centrales die niet meer dan enkele tientallen kW bedroegen.

De keuze tussen centralisatie en decentralisatie is een strategische keuze maar die fundamenteel is voor de bescherming en de veerkracht van de energievoorziening. Eenzelfde redenering kan immers worden gemaakt voor de opslagcapaciteit van ruwe en/of geraffineerde olie. Die wetenschap en een

daaropvolgende faling van de volledige stroomvoorziening in Frankrijk heeft er in 1978 (Lovins, 1982; p.72) voor gezorgd dat men zich ernstige vragen begon te stellen omtrent de gevoeligheid van het energienetwerk, waaronder voortaan zowel de opwekking als de distributie moeten rekenen. Vanaf dan werd het pad van de decentralisatie bewandeld, mede gesteund door het groeiende belang van hernieuwbare energiebronnen: vele verspreide opwekcapaciteit zou via het bestaande distributienet in staat zijn om voldoende energie op te wekken en toch de gevoeligheid voor schokken verminderen. Het spreekt voor zich dat de opkomst van nieuwe technologie deze tendens kracht heeft bijgezet maar ook dat het a priori niet werd beschouwd als een wondermiddel om bestaande vormen van energieopwekking te vervangen. Er moest dus nog steeds gezocht worden om de bestaande en waargenomen gevoeligheden te beperken. Gevoeligheden van elektronische aard waren reeds gekend sinds het einde van de tweede wereldoorlog en beperkten zich tot de bescherming tegen stroompannes of elektromagnetische puls (EMP). De opkomst van alternatieve stroombronnen heeft er echter voor gezorgd dat ook de beschikbaarheid op het distributienet aan bepaalde voorwaarden moest voldoen om de stabiliteit van de verdeling niet in het gedrang te brengen. En sindsdien weten we dat ook de controle van die distributie enkel door slimme netwerken kan geschieden indien men in staat wil zijn om een reële kostprijs aan te rekenen aan de consument. Hierdoor wordt een gevoeligheid bij-gecreëerd voor cybernetische dreiging. Binnen de komende tien jaren kan men enkel een toename van die dreiging verwachten door een grotere connectie van instrumenten aan het intelligente distributienetwerk. De energiesector wordt vandaag gerekend onder de top vijf van de meest bedreigde sectoren te wijten aan cybernetische aanvallen (Symantec, 2014; p.3). De toename van de aandacht voor cybernetische dreiging in het domein van kritieke energie infrastructuur is onlangs toegenomen in de nasleep van twee ongevallen: ten eerste de ramp van Fukushima en de cascade van gevolgen die ervoor hebben gezorgd dat de kerncentrales niet meer onder controle konden worden gehouden. Vervolgens de bekendmaking van de gevolgen van het Stuxnet virus op het kernprogramma van Iran, waarvan de industriële cowaren aangesloten. De wetenschap dat de werking van kritieke energie infrastructuur (KEI) vandaag ondenkbaar zou zijn zonder ICS, maakt dat de mogelijkheid van cyberdreiging op deze systemen vragen losweekt met betrekking tot impact en penetratievermogen in onze dagelijkse werking van dergelijke incidenten en de cascade die ze kunnen veroorzaken (Butrimas et al., 2012; p.13). We komen in de feiten terug op de vaststelling van interconnectie van sectoren: energieproductie hangt af van telecommunicatie voor de controle en het beheer en bovendien is de werking van gasproductie en transport afhankelijk van de stroomvoorziening. Een specifieke eigenschap van die ICS is de snelle beschikbaarheid door afstandscontrole: beveiliging van dergelijke systemen is

niet noodzakelijk de primaire behoefte geweest tijdens de uitwerking ervan. De ramp van Fukushima als voorbeeld of vertrekpunt van de denkoefening is daarom niet eens ver gezocht: het is niet de aardbeving of de vloedgolf op zich die de ramp hebben veroorzaakt, maar de ontoereikende beveiliging en de cascade aan opeenvolgende gebeurtenissen die tot de *black out* van de controlemogelijkheid heeft geleid.

2.2. Bescherming in de VS

In de VS is een struktuur samengesteld om de Staat in de mogelijkheid te stellen om te reageren tijdens incidenten die catastrofale gevolgen hebben of die mogelijk aanleiding geven tot cascades die het eerste incident buiten proportie aanzwellen en oncontroleerbaar maken. Zowel de fysische bescherming van kritieke infrastructuur als de cybernetische bescherming ervan, en in het bijzonder van KEI worden in beschouwing genomen: zelfs de krijgsmacht is door jarenlange inkrimping van budgetten niet meer in staat om alleen in te staan voor die bescherming en het herstel van functies indien een incident grote delen van de burgerbevolking en de krijgsmacht zelf zouden treffen. Toch staat het onomstotelijk vast dat men steeds beroep zal blijven doen op één departement dat in alle omstandigheden het langst zou moeten kunnen blijven functioneren en dat is het *Department of Defence* (DoD): de ramp na de storm Katrina heeft dat onomstotelijk bewezen. Twee elementen dragen bij tot een efficiënte respons op federaal vlak, te weten het *National Response Framework* (NRF) en het *National Infrastructure Protection Plan* (NIPP). Beiden moeten toelaten om de regionale middelen te coördineren en te ondersteunen, maar bieden op zich geen alleenstaande oplossing voor het probleem. Het is in de VS zelfs duidelijk geworden dat in het geval van een grote ramp buiten normale proportie, een belangrijke bijdrage zal moeten worden gevraagd aan de private sector om de onmiddellijke en de lokale noden op te vangen. Meeste plannen of noodplannen ter bescherming van kritieke infrastructuur maken niet noodzakelijk afzonderlijk de oefening voor KEI en dat is nog minder het geval voor de cybernetische bescherming ervan. De cybernetische dreiging en kritieke infrastructuur worden vandaag nog te veel als afzonderlijke entiteiten beschouwd: in de Verenigde Staten is men echter tot het inzicht gekomen dat de combinatie van beiden een noodzaak is en werd als gevolg daarvan een Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[9] in het leven geroepen: het maakt deel uit van het Department of Homeland Security en is verantwoordelijk voor

- analyse en respons op incidenten met controle-systemen;

[9] https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team geraadpleegd op 04 mei 2015.

- analyse van gevoeligheden en gebruikte malware;
- on site incident respons;
- inlichtingenvergaring met het oog op situational awareness;
- bekendmaking van gevoeligheden beheren en controleren;
- informatievergaring en verspreiding controleren door alarmen.

Sinds het begin van de eerste dreiging met elektromagnetische interferenties, te weten een elektromagnetische puls (EMP) waarvan de opwekking wordt bevestigd door de doctrines en/of de experimenten van landen als Rusland, China, Iran en Noord-Korea, is de cybernetische beveiliging van KEI hoogst noodzakelijk gebleken: informatica van vandaag blijkt immers veel gevoeliger te zijn voor gevolgen van EMP in het algemeen en gerichte cyberaanvallen in het bijzonder dan dertig jaren terug (Cogan, 2011; p.18). Indien militaire communicatiemiddelen daartoe worden beschermd, is het helemaal anders gesteld met de civiele communicatiemiddelen en bijgevolg zijn moderne ICS ook kwetsbaarder voor dit fenomeen dat aan de basis kan liggen van cascade-fenomenen. De lijsting van de kritieke infrastructuur en hun onderlinge afhankelijkheden in de VS is slechts een oefening die door het Department of Defense (DoD) sinds 2011 is gestart en deze oefening lag aan de basis van een aanpassing aan catastrofale scenario's waarop moest worden getraind. Tot hiertoe werden die beperkt tot één staat, maar nieuwe catastrofale scenario's moesten rekening houden met een getroffen populatie van 7 miljoen inwoners, betrokkenheid van meerdere staten, 190.000 doden bij aanvang van een cascade-ramp en nog eens zo veel gekwetsten. De aard van de schade wordt in die scenario's zo groot dat het betreden van het getroffen gebied voor civiele hulpverleners bijna onmogelijk maakt. De departementen die in dergelijke gevallen moeten tussenkomen zijn het Department of Homeland Security (DHS) en het Department of Defence (DoD). Dit laatste departement kan enkel door de president van de VS worden gevraagd om op te treden om KEI te beschermen (Cogan, 2011; p.15). Te onthouden is dat militaire planning in de VS ook rekening houdt met een ramp van catastrofale omvang op kritieke infrastructuur, in het bijzonder voor de sectoren communicatie en elektriciteit. De twee scenario's bij uitstek waarvoor dit voor het ogenblik wordt geoefend door DoD zijn van elektromagnetische aard (EMP door kernexplosie en zonnestormen), maar vormen de basis van hoe men de betrokkenheid van meerdere departementen in het kader van de bescherming van KEI kan verwachten in het geval van niet beheersbare rampen.

2.3. Bescherming in de EU

Sinds 2006 is men gekomen tot een definitie van kritieke infrastructuur via het EPCIP programma dat uiteindelijk heeft geleid tot het opstellen van de richtlijn[10] die we eerder in dit deel hebben besproken. In de genese van de volledige lijst kritieke infrastructuur, werden energie en transport als eerste weerhouden maar wordt echter geen verduidelijking gegeven over het al dan niet bestaan van een lijst kritieke energie infrastructuur. De richtlijn heeft betrekking op bronnen, opslag, en distributie van olie en gas, centrales en hun transmissie- en distributienetwerk. Verduidelijkingen en aanvullingen worden pas duidelijk in fora die door de EU worden georganiseerd of waaraan het directoraat-generaal energie deelneemt. Zo blijken ook toegang tot energiebronnen, de distributie- en/of netwerkinfrastructuur en de opwekkingsinfrastructuur (centrales) allen onder de aandachtspunten van de KEI beschermingsmaatregelen te vallen (Egmont conference. *Energy transition: A Multifaceted Challenge for Europe. Securing Europe's electricity supply*. 05 Mai 2015). De Europese Commissie heeft in het verlengde van de EPCIP- richtlijn van 2008, het zwaartepunt van de organisatie verlegd naar de samenstelling van een netwerk van eigenaars en operatoren van elektriciteit-, olie- en gasinfrastructuur. Dit netwerk zou zowel het beleid als de praktische organisatie ervan onder de loep nemen: deze uitwisseling van ervaring heeft vooral betrekking op veiligheidsincidenten (Thematic *Network* on Critical Energy Infrastructure Protection- TNCEIP-network). In de kadrering van het project wordt de nationale verantwoordelijkheid onderstreept van de bescherming van energie-infrastructuur, voornamelijk in geval van rampen, terroristische en/of criminele activiteit. Daarenboven wordt het transnationale karakter van de effecten onderstreept en het daaruit voortvloeiende belang van de Europese Commissie voor het afstemmen van de nationale inspanningen die voornamelijk gericht zijn op de bescherming van energie infrastructuur. De visie die binnen het kader van het netwerk wordt verkondigd is gebaseerd op drie pijlers:

[10] Richtlijn 2008/114/EC van 8 december 2008 betreffende de identificatie van Europese kritieke infrastructuur en de bescherming ervan. Deze richtlijn is ook beter bekend als de EPCIP richtlijn.

- een gemeenschappelijke en holistische benadering voor de bescherming van infrastructuur dat (grensoverschrijdende) van strategisch belang blijkt in Europa;
- gebaseerd op de vaststelling dat alle leden van het netwerk een toegenomen aantal aanvallen en beschadigingen hebben moeten vaststellen te categoriseren als vandalisme of cyberaanvallen;
- gelijke kansen en opportuniteiten voor ieder lid van het netwerk, hetgeen betekent dat operatoren en eigenaars hetzelfde doel nastreven, te weten de veilige en doeltreffende opwekking en distributie van energie.

Deze visie veronderstelt een voortdurende uitwisseling van gegevens tussen eigenaars van infrastructuur, hun operatoren, en de betrokken overheden. Deze infrastructuur is onderhevig aan zowel nationale wetgeving als aan de internationale inschatting van de risico's die de kriticiteit ervan bepalen (overeenkomstig de definitie die we aan deze term eerder in dit werk hebben gegeven). Door de afhankelijkheden is de internationale dimensie minstens van even groot belang als de nationale en regionale visie van die infrastructuur en is het pas op dat niveau dat men de impact van kritieke elementen kan inschatten voor de distributie naar de gebruiker: daartoe werden een aantal maatregelen voorgesteld waaronder het beschikbaar stellen van het waarschuwingsnetwerk voor kritieke infrastructuur (Critical Infrastructure Warning Information Network –CIWIN) aan de energieleveranciers, de grensoverschrijdende ondersteuning door lidstaten in geval van distributieproblemen in een naburige lidstaat, het vastleggen van gemeenschappelijke criteria voor het schatten van dreigingen ten aanzien van en risico's voor KEI, de integratie van het ICT domein in het EPCIP project en de actualisatie van de wettelijke voorzieningen daaromtrent[11]: we zullen in wat volgt nagaan in welke mate ook vooruitgang in die richting werd geboekt. Naast deze informatie-uitwisseling is ook een platform voorzien voor laboratoria en kenniscentra waar de kriticiteit kan getest worden en onderzoek gevoerd naar de efficiëntie van verschillende configuraties van energie-infrastructuur zowel voor wat energiedistributie als SCADA beveiliging betreft[12].

[11] Deze benadering vertrekt van het standpunt dat ICT onontbeerlijk is voor het beheer van SCADA systemen. Als dusdanig wordt vanaf de synergie tussen beiden in KEI zodanig dat men vanaf nu KEI zou kunnen opsplitsen in operationele technologie (OT) en informatietechnologie (IT).

[12] ERNCIP is een Europese databank die informatie herneemt over testfaciliteiten die betrekking hebben op kritieke infrastructuur en kritieke energie infrastructuur. Alle belanghebbenden van dergelijke installaties kunnen via een dergelijk platform onderzoekscentra in hun domein identificeren en deze contacteren met zeer specifieke vragen of zelfs onderzoeksprojecten. Sectoren die worden betrokken in het project

Een belangrijke aanpassing ten opzichte van de initiële ontwerprichtlijn van 2006 en de uiteindelijke richtlijn van 2008, is het besef op Europees niveau gegroeid dat een dergelijk project zich niet kan beperken tot de identificatie van kritieke infrastructuur (noch enkele domeinen die hiervoor het meest kritiek zijn) maar dat de interconnecties tussen de domeinen worden erkend. Het werkdocument van de Europese Commissie legde die visie vast op een zeer pragmatische wijze om de restrictieve initiële aanpak van 2008 te verbeteren (SWD(2013) 318 final): vier domeinen vormen, omwille van het grensoverschrijdende en Europese karakter, de grondlaag van wat de samenwerking in dit domein kan voorstellen: Eurocontrol, Galileo, het elektriciteitsnetwerk en het gasdistributienetwerk. De kritieke infrastructuur die aan de hand van de eerste richtlijn werd geïdentificeerd, beperkte zich tot de domeinen energie en transport. Minder dan twintig Europese kritieke infrastructuren werden aldus aangeduid en bijgevolg even weinig operationele veiligheidsplannen voor de betrokken infrastructuur. Tot hiertoe werden grote infrastructuren, zoals het elektriciteitsdistributienetwerk niet als Europese kritieke infrastructuur erkend. De Commissie is van nu af aan echter wel geneigd om een systeembenadering te bevoordelen waarin kritieke infrastructuren worden beschouwd als een verbonden netwerk. Eerder was de methodologie beperkt tot een sectorale benadering die eruit bestaat iedere sector afzonderlijk te beschouwen en de risico's van het beschouwde domein onafhankelijk te evalueren naar de aan te wenden maatregelen toe. Dit had als gevolg dat enige vorm van Europese dimensie van coöperatie tussen buurlanden werd tot stand gebracht.

Hoewel die interconnectie nu wordt erkend op Europees niveau, moet men er zich van bewust zijn dat die ook verder reikt dan de Europese grenzen. In het bijzonder voor de bescherming van kritieke infrastructuur, en als afgeleide daarvan KEI, wordt een bijzondere samenwerking vooropgesteld met de landen aangesloten aan de vrije handelszone (European Free Trade Association - EFTA). Deze landen omvatten Liechtenstein, Zwitserland, IJsland en Noorwegen. De laatste twee zijn belangrijk voor de gaswinning en de bevoorrading in Europa en uiteraard ook voor de elektriciteitsdistributie aangezien ze deel uitmaken van het netwerk. De samenwerking die met deze landen door de EU op touw is gezet voorziet in alle operationele gevolgen voor de uitbating van voormelde bronnen, in het bijzonder voor wat de infrastructuur, het beheer en de controle ervan noodzakelijk kan zijn met

---

omvatten alle domeinen die terug te vinden zijn in de lijst van kritieke infrastructuur die in de EPCIP-richtlijn worden hernomen voor dreigingen die voortvloeien uit rampen van natuurlijke of technologische oorsprong of die moedwillig werden veroorzaakt.

inbegrip van de cybernetische beveiliging van die uitrusting en controlesystemen. In het verlengde van die samenwerking heeft de Commissie ook geoordeeld dat de strijd tegen het terrorisme en andere gerelateerde risico's aanleiding zou moeten kunnen geven tot een schatting van de veerkracht tegen de dreiging op elektriciteitsnetwerken: door deze benadering worden ook de cyberbeveiliging en de beveiliging tegen terroristische aanslagen het voorwerp van aandacht. De motivatie van de Commissie is bovendien duidelijk in deze dat de opkomst van Slimme Netwerken een nauwere samenwerking tussen energie en cyberveiligheid zal vereisen en de facto de link met cyberveiligheid is gelegd. Een speciale Task Force werd tot dit doeleinde opgericht.

In het beschikbare wettelijke instrumentarium voor de organisatie van Europese energie-infrastructuur vindt men de verordening van het Europees parlement van 17 april 2013[13] die de richtlijn van 2008 aanpast en waar nodig aanvult. Hierin wordt de strategie van de Commissie voor Europa 2020 onderschreven die de energie-infrastructuur als een vlaggenschipinitiatief naar voren stelt als ondersteuning van het groeiend besef van de noodzaak aan een energiepolitiek. Volgende krachtlijnen hebben belang in het argumentarium ten voordele van de organisatie van die infrastructuur (European Commission, 2013; p.L115/39):

- aan de fragmentatie of tenminste de ontoereikendheid van het bestaande netwerk moet worden verholpen door alvast op continentaal niveau de netwerken aan elkaar te koppelen en te moderniseren (waaronder men verstaat de noodzakelijke aanpassingen door te voeren die het netwerk resistent maken voor de variabele output van alternatieve energiebronnen voor elektriciteitsnetwerken).
- de drie beleidsdoelstellingen in zake energie die een dergelijke strategie rechtvaardigen, te weten duurzaamheid, concurrentiekracht en energievoorzieningszekerheid worden ook in dit document onderstreept.
- geen enkele lidstaat van de EU mag nog geïsoleerd zijn van het gas- en elektriciteitsnetwerk of zijn energievoorziening in gevaar zien komen doordat het ontbreekt aan de nodige geschikte interconnecties.
- niet alleen het bestendigen tegen defecten maar ook tegen natuurrampen of door de mens veroorzaakte rampen, de gevolgen van klimaatverandering maar ook de bedreiging voor de veiligheid van die infrastructuur moet aanleiding geven tot een verbetering ervan.

[13] Richtlijn betreffende richtsnoeren voor de trans-Europese energie-infrastructuur en tot intrekking van de Beschikking nr.1364/2006/EG en tot wijziging van de Verordening (EG) nr.713/2009, (EG) nr.714/2009 en (EG) nr.715/2009.

In het verlengde van deze argumentatie is een raming gemaakt van de kosten die gepaard gaan met de noodzakelijke aanpassingen op het bestaande distributienetwerk: in de periode tot 2020 zijn deze investeringen op gas- en elektriciteitsdistributie, gecatalogiseerd onder de hoofding "Europees belang", vastgesteld op 220 miljard €. 12 prioritaire infrastructuurprojecten werden door het Europese parlement geïdentificeerd als essentieel voor de verwezenlijking van de energie- en klimaatdoelstellingen van de Unie: projecten beslaan elektriciteitstransmissie en -opslag, gastransmissie, aardgasopslag, infrastructuur voor het transport van vloeibaar aardgas en de installatie van slimme netwerken, zogenoemde elektriciteitssnelwegen, transport van koolstofdioxide en olie-infrastructuur. De zones die geografisch belangrijk zijn voor die projecten worden gegeven in bijlage drie (Corridors van energie-infrastructuur -Verordening (EU) Nr.437/2013 van het Europees parlement en de Raad van 17 april 2013; Bijlage I p.115/62) terwijl de categorieën van de infrastructuur gedetailleerd worden in bijlage 4 (Categorieën energie-infrastructuur -Verordening (EU) Nr.437/2013 van het Europees parlement en de Raad van 17 april 2013; Bijlage II p.115/64).

Het geheel van de maatregelen dient echter te passen binnen het kader van de 2020 doelstellingen die een zo groot mogelijk percentage aan hernieuwbare bronnen in het beschikbare energiepallet operationeel in gebruik wil zien tegen 2020. De nood om te "decarboniseren" is de rode draad van de beslissing tegen de klimaatopwarming en geeft voorrang aan hernieuwbare bronnen waardoor een evolutie in gang moet worden gezet van grote gecentraliseerde systemen en centrales naar een meer gedecentraliseerd netwerk van kleinere eenheden. Het geheel past in een commerciële benadering van de marktinvulling en de nood om ten allen tijde aan de vraag te kunnen voldoen. Daartoe is men zich bewust dat in de nabije toekomst inzet noodzakelijk is voor zowel hardware als software: in het gedeelte hardware, zijn investeringen vereist voor de uitbouw van nieuwe transmissielijnen en centrales, in het gedeelte software dient de regelgeving te worden aangepast zodat nationale regels worden geleest op een supranationaal model dat kan voldoen aan de vraag van de energiemarkt en tegelijk een sturing van die markt mogelijk maakt. Bovendien worden de vereisten van de nieuwe investeringen gekaderd op een infrastructuur die uitbating mogelijk maakt tot 2030 en daarna. Die visie is vandaag nog te weinig te rijmen met de huidige marktstructuur die nog te veel is gestoeld op de nationale benadering: deze kent aan KEI hoofdzakelijk een nationale rol waardoor lokale politici rekenschap moeten kunnen geven voor een lokaal kiezerspubliek. Bovendien is de nood aan slimme netwerken voor de integratie van alternatieve bronnen nog niet voldoende doorgedrongen tot de politieke geesten, om nog niet te spreken van de cyberverdediging in datzelfde domein. De nog bestaande barrières voor een geïntegreerde markt met de nodige bescherming van KEI

zijn te herleiden tot de nationale politiek die nog steeds voorrang krijgt op de marktvraag. De stappen die noodzakelijk zijn om hierin vooruitgang te boeken zijn design van het nieuwe netwerk-concept, investeringen voor de realisatie ervan, en uiteindelijk regulering in operationele fase. Die nationale insteek verklaart ook de verschillende posities die ten aanzien van kernenergie in West-Europa werden ingenomen, al naargelang de historische achtergrond en de geopolitieke keuzes van weleer in ieder land. De tendens die eruit bestaat om in West Europa het nucleaire terug te dringen na de ramp van Japan, wordt gecompenseerd door een toegenomen vraag in groeilanden, landen uit Oost-Europa en landen uit het Midden-Oosten. In dat opzicht en zelfs indien er een regionale terugdringing van een technologie tot stand komt die voor een deel door politieke of ideologische motieven wordt verklaard, moet men toch rekening houden met het feit dat een dergelijke technologie niet overal op een gelijkaardige wijze aan densiteit zal verliezen, omwille van het aandeel dat ervoor zorgt dat een koolstofvrije energieproductie op die manier kan worden gerealiseerd. Het nucleaire zal in een scenario van gedecarboniseerde energieproductie steeds zijn plaats hebben: in die gebieden waar men er nog gebruik wil van maken zal men dus ook voor een veilige en beveiligde manier van energieproductie moeten voorzien. De tekorten die in ons land zijn ontstaan en die sinds de afkoppeling van onze eigen centrales hebben gezorgd voor een hivernaal ontkoppelingsplan hebben de noden voor een betere distributie binnen Europa in de verf gezet.

Nochtans is de samenwerking over de grenzen heen al ruim verbeterd in vergelijking met 10 jaar geleden. Een overschot aan capaciteit was destijds bijna niet te transfereren naar landen die verder gelegen waren dan de onmiddellijke buurlanden. Sinds 2008 en het creëren van het netwerk van Transmission System Operators voor elektriciteit (European Network Transmission System Operators – ENTSO-e), operationeel sinds juli 2009, blijkt dit probleem van de baan: het doel van dit netwerk was een operationeel transmissienetwerk tot stand te laten komen. Een dergelijke organisatie bestaat in Europa zowel voor gas (ENTSO-g) als voor elektriciteit (ENTSO-e) en gebruikt de vaste infrastructuur voor de verdeling van energie. Door het gebruik van die vaste infrastructuur heeft een TSO de facto een soort van monopolie positie en is er bijgevolg regulering door de Europese commissie[14]in principe mogelijk. Een TSO zorgt voor de verdeling van elektriciteit vanaf opwekking naar regionale distributieoperatoren (DSO).

[14] Een gelijkaardige verdeling van verantwoordelijkheden bestaat in de Verenigde Staten waar een Independent System Operator (ISO) voor de nationale (interstatelijke) coördinatie zorgt van de regionale systeemoperatoren (Regional Transmission Organization -RTO).

De integratie van hernieuwbare bronnen is in deze organisatie noch steeds een probleem omdat sommige delen van het Europees netwerk worden beladen met een overcapaciteit terwijl in andere delen een tekort ontstaat. De beperkte transmissiemogelijkheden aan de grenzen van landen kan de transit beperken en heeft de laatste winter gezorgd voor afkoppelingsplannen in vele landen van Europa en uiteraard ook bij ons. Het zijn net die transmissiesysteembeheerders die een cruciale rol gaan spelen in de operationele coördinatie voor de realisatie van een dergelijk ge-interconnecteerd netwerk: deze moeten de operationele interoperabiliteit weten te realiseren en mede hierdoor wordt duidelijk dat het supranationale niveau enkel een sturende rol heeft. Deze organisatie wordt volledig in handen van de operatoren gelaten en voldoet ook hiermee aan het subsidiariteitsbeginsel, waaronder men veronderstelt dat men geen organisatie of beheer op een niveau hoger moet tillen dan het strikt noodzakelijk voor de goede werking ervan. Dit vergt echter ook engagelment van commerciële exploitanten die, in een periode van laagconjunctuur en politieke onzekerheid niet echt geneigd zijn tot nieuwe investeringen. Hiervoor is immers stabiliteit en een terugverdieneffect op redelijk termijn vereist. Dit is wat de verordening tot stand wil brengen waarin een stabiele en voorspelbare regelgeving voor projecten die worden beschouwd als behorend tot het gemeenschappelijk Europees belang. De criteria die hiervoor moeten worden vervuld zijn:

- zich bevinden in ten minste één van de geografische corridors die in bijlage drie worden hernomen;

- de voordelen van het project zijn belangrijker dan de kosten die eruit voortvloeien;

- het project moet betrekking hebben op twee lidstaten of een grensoverschrijdend effect te hebben of gemeenschappelijk zijn aan één lidstaat en een land uit de Europese Economische ruimte.

De energetische politiek die de EU tot stand wil brengen kadert in het ruimer geheel dat door geostrategische behoeften wordt gedreven: de vaststelling van twee ontwrichtende bewegingen op geografische zones die voor Europa van uitermate groot belang zijn heeft de EU doen inzien dat een energetische politiek van de unie de enige moeilijkheid is om de lidstaten een vorm van energiebevoorrading te garanderen. De regio's die de EU daartoe zorgen baren zijn het Midden-Oosten en Oekraïne. De gebeurtenissen/actoren die voor de EU verantwoordelijk zijn voor een verstoring van de normale distributie zijn IS enerzijds en de crisis met Rusland anderzijds. Maar niet alleen de beschikbaarheid van de grondstoffen voor de energieproductie baart de EU en zelfs de VS zorgen: ook de conceptuele uitrusting van de

infrastructuur voor energie is zowel in de EU als voor de VS op aardgas gericht, waarvan distributie hoofdzakelijk door pijpleidingen gebeurt (in Azië en in de regio rond de Stille Oceaan is dat eerder LNG). Daarnaast heeft de situatie na de ramp van Fukushima in vele landen van de EU bovendien voor een moratorium of een herziening van het gebruik van kernenergie gezorgd. In Duitsland heeft een dergelijk "Energiewende" gezorgd voor een nog grotere afhankelijkheid van voormelde regios: petroleum moet in dit geval dienst doen als strategische buffer voor de opvang van fluctuaties in leveringen enerzijds en de beschikbaarheid of de ontoereikendheid van alternatieve energievormen anderzijds. Naast de beschikbaarheid van bronnen en de grote infrastructurele werken, is een derde en niet te verwaarlozen element de oorzaak van een europeanisering van de energiepolitiek: de prijs. Het voorbeeld van de gasafhankelijkheid is hier veelzeggend: om de gasprijs los te koppelen van petroleum en meer te kunnen inspelen op interne vraag en aanbod, is een dergelijke politiek noodzakelijk. Voor het ogenblik is de Unie veel te veel afhankelijk van een beperkt aantal "suppliers" per beschikbare distributielijn (pijplijninfrastructuur is de beperkende factor), is het netwerk niet voldoende geïnterconnecteerd met andere woorden is er een fragmentatie van de netwerkinfrastructuur, en is er extern aan de Unie een artificiële concentratie van externe staatsleveranciers. De Unie moet als gevolg hiervan kampen met een prijsspagaat tussen de goedkope traditionele bronnen en de duurdere hernieuwbare bronnen. Intern gebruik van nieuwe en hernieuwbare bronnen blijft nog veel te duur (al dan niet door het voorzien van staatssteun) terwijl het zich van de afhankelijkheid van de traditionele bronnen wil loskoppelen. Het overaanbod van die bronnen en het beperkt aantal leveranciers zal de geostrategische spanningen hetzij in het Midden-Oosten, hetzij aan de grenzen van de Unie niet doen afnemen, wel in tegendeel: de concurrentie voor het resterende marktaandeel van de EU in het Midden-Oosten enerzijds en anderzijds de terug plooiing van de VS uit de regio naar aanleiding van een groter gewaande reserve schaliegas zullen de spanningen tussen Saoedi-Arabië en Iran doen toenemen. De betrokken actoren in de regio speculeren trouwens dat die Amerikaanse terugtrekking slechts van tijdelijke aard zal zijn aangezien schaliegaswinning veel duurder blijkt dan de winning van traditionele oliereserves. De vraag blijft de drijvende factor in de economie van de bronnen: aangezien die niet onmiddellijk aantrekt is het meer dan waarschijnlijk dat de prijs van traditionele olieproducten nog een tijd laag zal blijven en de inkomsten van de olieproducerende landen hierdoor lager zullen uitvallen dan gebudgetteerd: geostrategische spanning verzekerd.

Het besluit van de geostrategische context voor de Unie is duidelijk: de huidige trend van de voortzetting van bilaterale overeenkomsten om een grensoverschrijdend beleid tot stand te brengen is ontoereikend. Om een concurrentiële en tegelijk veerkrachtige energiemarkt in werking te laten

treden moet een gemeenschappelijk energiebeleid op de sporen worden gezet. Drie elementen dragen daartoe bij:

1.de technische aanpassingen en verbeteringen voor een aangepast distributienet, zowel voor de traditionele bronnen (gas, olie, kernenergie) als hernieuwbare technologie zijn daarvoor noodzakelijk over de hele Europese ruimte;

2.het veiligstellen van de beschikbaarheid van energiebronnen is op langere termijn een essentiële stap in de realisatie van een energiemarkt die een groeiende economie moet kunnen ondersteunen: dit aspect van energieveiligheid is een nieuwe benadering die in de EU nog pas sinds kort haar intrede heeft gedaan. Dit aspect wordt in deel 4 besproken.

3.ook institutioneel moet een kader worden geschept dat vertrouwen schept bij kandidaat investeerders om zware infrastructuurwerken uit te voeren voor het opwekken en het verdelen van energie: richtlijnen en gemeenschappelijke wettelijke garanties kunnen hiertoe bijdragen.

Uit de keuzes van leidende landen in de EU (zoals Duitsland) is gebleken dat een Energieomschakeling niet uitsluitend een electorale of ideologische keuze kan en mag zijn in de toekomst. De keuze van Duitsland heeft er bijvoorbeeld voor gezorgd dat een groter afhankelijkheid van het Russische gas tot stand werd gebracht en dat tegelijk een stap terug werd gezet in koolstofarme energieproductie.

Een beleid met een eengemaakte energetische markt kan dergelijke beslissingen rationaliseren. Maar een dergelijke interne energiemarkt moet ook rekening houden met de externe factoren die deze markt zullen bepalen te weten de crisis in Oekraïne, de toekomst van de bronnen die gecontroleerd worden door of bedreigd worden door IS, de relatie die men zal ontwikkelen met Iran na de totstandkoming van een akkoord met dat land. De grootste struikelblok tot hiertoe voor de totstandkoming van een dergelijke gemeenschappelijke energiemarkt blijkt de nationale soevereiniteit te zijn en de incompatibiliteit van de nationale prioriteiten die in lidstaten in de loop der jaren is gegroeid: de ondersteuning van de nationale industrie en de fundamentele keuzes zoals Frankrijk dat de voorkeur geeft aan het nucleaire terwijl in Duitsland net van die optie afstand is genomen, zal een gemeenschappelijk intern beleid niet eenvoudiger maken: ene en andere optie heeft immers technische implicaties die niet noodzakelijk aanvulbaar zijn (bijvoorbeeld voor opvang van tekorten en netwerkstabiliteit). Rusland zal een belangrijke leverancier blijven in de toekomst, maar de verderzetting van handelsrelatie zoals die voor de Oekraïense crisis bestond zal niet mogelijk zijn. De veiligheid van de energievoorziening zal uiteindelijk het gevolg zijn van de politieke keuzes en de gevolgen van de politieke crisis met Rusland. Zoals eerder vermeld zullen de politieke verhoudingen ook bepalen wat de

relaties en de uitwisselingen met andere belangrijke partners in het vraagstuk zijn. Infrastructuur en bestaande bilaterale akkoorden zijn reeds beter dan een tiental jaren geleden. Echter voor het voeren van een coherent extern beleid inzake energievoorziening en infrastructuur zijn een aantal elementen in rekening te nemen op Europees vlak:

1.voor wat infrastructuur betreft is 20% meer opslagcapaciteit voor gas beschikbaar binnen de Unie in vergelijking met 10 jaar geleden;

2.voor vergassingscapaciteit is er 25% meer beschikbaar dan in dezelfde periode;

3.de interconnectie en distributie-infrastructuur is nog ontoereikend om tegemoet te komen aan punctuele tekorten zowel voor gas als elektriciteit;

4.voor het bepalen van een strategie als concretisatie van een visie is het protectionisme van de lidstaten nog te groot zoals blijkt uit de tegenstellingen tussen de Franse en de Duitse benadering;

5.daarom zal intern de EU een "energetische diplomatie" tot stand moeten komen die erin zal moeten slagen om een gemeenschappelijke noemer te vinden in de vaak te uiteenlopende standpunten van de lidstaten;

Het kan op het eerste gezicht een evidentie lijken om een dergelijke gemeenschappelijk standpunt in te nemen, maar niet enkel het corporatisme heeft dit tot nog toe in de weg gestaan in Europa. De aanwending van die energie heeft een zeer uiteenlopend spectrum binnen de Unie (Donnelly, 2015) dat een volgende verdeling vertoont: verwarming en afkoeling maken reeds 40% uit van de energetische behoeften, mobiliteit nog eens 33% en slechts 21% voor de opwekking van stroom. De verschillende behoeften en marktaandelen voor het gedeelte verwarming binnen de EU alleen al gaan zorgen voor andere prioriteiten in het Noorden dan in het Zuiden van de Unie. Deze tegenstelling werd ook door Etienne Davignon onderstreept (Davignon, 2015): volgens hem blijft regionaliteit belangrijk in het debat omdat iedere regio een specificiteit heeft die een andere politieke benadering vergt. Dit creëert een immanente ambiguïteit die er enerzijds uit bestaat om een collectief doel na te streven maar tegelijkertijd de wetenschap dat één enkele benadering niet zal tegemoet komen aan de betrachtingen van alle particulieren, industrieën en overheden van de Unie. Tegelijk zal een zekere rationalisatie moeten worden bereikt: zones in de EU hebben een grotere toegang tot bronnen en kunnen beter aan hun lokale vraag tegemoet komen dan andere. In de praktijk is voor het ogenblik een lokale nominale overcapaciteit niet vertaalbaar naar een gegarandeerde bevoorradingszekerheid. Deze paradox moet men zien te overbruggen maar op korte termijn is hiervoor niet noodzakelijk een terugwineffect voor te verwachten. De oplossing in dit geval is een dubbel spoor na te volgen:

- Intern de EU door investeringen in een beter distributienetwerk en de verbinding van energie infrastructuur hiermee.
- Extern de EU door een gemeenschappelijke visie na te streven die ook binnen de EU door de prioriteiten die eraan worden gegeven aanvaardbaar is voor iedereen.

De enige manier om een dergelijk gemeenschappelijk doel na te streven past in een globaal kader. Het is precies dat kader dat de internationale klimaatconferenties ons bieden voor de strijd tegen de klimaatverandering. Met dit doel voor ogen is het eenvoudiger om de vraag trachten te beperken, en het overblijvend gedeelte meer te laden met hernieuwbare energie. Tegelijk heeft deze benadering het voordeel dat het aandeel van traditionele bronnen wordt verlaagd, waardoor de afhankelijkheid minder wordt en de gevoeligheid voor regionale instabiliteit maar ook prijsfluctuaties minder grote gevolgen hebben. Bij aanvang van onze problematiek zijn we vertrokken van een hypothese waarbij we de definitie van kriticiteit moesten aanpassen omwille van de gevolgen van interconnecties enerzijds en de gevolgen van energetische onbeschikbaarheden anderzijds. Op dit punt in onze redenering gekomen stellen we in de feiten vast dat de politieke invulling op supranationaal niveau ons tot dezelfde conclusie drijft: tot hier toe ging men ervan uit dat het vooral technische falingen waren (al dan niet door de mens veroorzaakt) die aan de basis lagen van het energieveiligheidsprobleem. Nu stellen we vast dat naast de uitbreiding van de definitie van kriticiteit ook de oorzaken ruimer moeten worden gezien en in dit geval "politieke disrupties" evenzeer aan de basis kunnen liggen van een energetische onbeschikbaarheid. We komen bijgevolg via twee onafhankelijke redeneringen tot dezelfde besluiten: zowel een zuiver technische benadering als een supranationale politieke insteek leiden tot de conclusie dat een energetische problematiek niet tot één of ander te herleiden valt. Een veiligheidsplan moet dus niet enkel rekening houden met technische oorzaken van een onderbreking maar ook met de politieke oorzaken ervan. Hierdoor moet men niet allen oog hebben voor de interne vraag van de EU, maar ook voor de upstream-beschikbaarheid en de diversificatie op een dergelijke manier organiseren dat die aan de interne vraag kan voldoen: hiervoor is ook een extern distributienetwerk te operationaliseren.

Kijken we naar de mogelijke oplossingen die de EU kan hanteren, zijn we vanwege de verruiming van de oorzaken uit het uitsluitend technische of politieke aspect, tot het besluit gekomen dat deze oplossingen zowel een interne als een externe dimensie moeten omvatten en in ieder van deze gevallen zowel een politieke als een technologische benadering:

<u>Oplossingen voor de EU voor de externe dimensie</u>:

Vanuit technologisch oogpunt, zal het voor de EU belangrijk zijn om voor een langer termijn de mogelijkheid te hebben aan de grenzen van de unie de noodzakelijke verbindingen te voorzien die moeten toelaten aan te sluiten op de aangrenzende distributienetwerken. Ook aanvoerlijnen moeten de aanvoer van verschillende bronnen toelaten en uitbreiding mogelijk maken in de toekomst: in het bijzonder moet vandaag al aandacht worden gegeven aan de technologische uitdagingen die de exploitatie en het transport van Arctische bronnen aan de Unie zullen stellen. Bovendien heeft die externe technologische dimensie een onmiddellijk gevolg voor de interne technologische capaciteit omwille van compatibiliteit van capaciteit enerzijds en de vermenigvuldiging van het aantal aansluitingspunten door de toename van de verschillende aanvoerlijnen.

Op extern politiek vlak is het noodzakelijk om rekening te houden met de geostrategische evoluties in de materie en de landen die voor Europa de energie-hub van de toekomst zullen zijn:

- Rusland zal een belangrijke bron blijven voor traditionele energiebronnen van Europa ook al is de Chinese markt een grotere afnemer van dat land in de toekomst.
- Naast Rusland zal Turkse regio beschouwd moeten worden als een energie-hub van Europa en de Unie en als transitcorridor van de grondstoffen die van het Midden-Oosten afkomstig zijn.
- De associatie van de Centraal-Aziatische landen met Rusland of Turkije verlegt bovendien de aandacht van de EU nog verder naar het Oosten

Dit heeft voor gevolg dat een sterk Europees beleid zal moeten worden uitgebouwd naar die landen toe (externe dimensie). Het idee om ook stroom in Noord-Afrika op te wekken uit hernieuwbare bronnen en te exporteren naar Europa lijkt niet de beste optie: als alternatief zou in dit deel van de wereld stroom moeten worden opgewekt uit hernieuwbare bronnen voor lokale consumptie en de traditionele energiebronnen eventueel gebruikt worden voor uitvoer naar Europa dat op die manier de bronnen van het beschikbare pallet kan verruimen.

<u>Oplossingen voor de EU voor de interne dimensie</u>:

De interne technologische dimensie bestaat eerst en vooral uit de keuze van de exploitatie van bronnen en de centrales die erbij horen. Maar bovendien staat het actuele distributienet niet in voor de adequate verdeling van de totale capaciteit: daartoe moeten regionale verschillen die een fundamentele andere benadering genereren over het geheel van de Unie worden overwonnen door protectionistische en corporatistische reflexen te overstijgen. Dit is mogelijk door een flexibel distributienet voor zowel gas als elektriciteit dat ook toelaat om hernieuwbare bronnen op een flexibele manier

op het net te gebruiken en regionale tekorten op te vangen door een grotere netwerking (minder shoke points) dan vandaag het geval is.

De interne politieke dimensie zal eruit bestaan om op niveau van de Unie een gemeenschappelijke basis te vinden, een energetisch beleid dat meer dan een exhaustieve identificatie van de kritieke energie-infrastructuur, het budgettair kader moet bepalen dat potentiële investeerders de mogelijkheid geeft om zicht te hebben op een redelijke terugverdientijd. In het verlengde van het technische aspect dringt zich een dynamisch luik op van de identificatiebehoeften aan kritieke infrastructuur: in eerste instantie is die aanzet gegeven na het bestaan van de richtlijn van 2008 (waarvan we het gebrek om afhankelijkheden en cascade-effecten in beschouwing te nemen reeds werd vermeld). Echter een bijkomende dimensie werd aangehecht aan die benadering door de evolutie van de technologie en vergt daarom een regelmatige herziening van wat we hier in beschouwing nemen in het domein kritieke energie infrastructuur[15] en wat de beperkingen zijn van het begrip soevereiniteit zoals dat nu wordt beschouwd en welke invulling we er in de toekomst aan willen geven.

Eén van de concrete aspecten van deze problematiek vinden we bijvoorbeeld terug in de constructie van het elektriciteits-distributienetwerk: in niet alle landen van de Unie wordt die op een gelijkaardige wijze uitgevoerd. Frankrijk en het Verenigd Koninkrijk geven er de voorkeur aan om het monopolie van de staat hierin te vrijwaren terwijl Duitsland, Nederland en Zweden de voorkeur geven aan een regionale insteek en bijgevolg regionale verschillen kunnen opduiken. Het bestaan van een Europees netwerk van transmissie-operatoren (ENTSO-e) voor het elektriciteitsnetwerk moet er op termijn voor zorgen dat de actoren op de markten gecoördineerd worden zodat ze toegang krijgen tot het bestaande distributienet (dit behelst de participatie van zowel elektriciteitsopwekking door grote bedrijven als particulieren). De veiligheid van bevoorrading in dit domein moet voor dat netwerk bestaan uit een veilige output en de maintenance van het systeem. Binnen deze organisatie werden de punten

[15] Een voorbeeld daarvan wordt geïllustreerd door de afhankelijkheid van controlesystemen voor energiedistributie en opwekking van het cyberdomein. Het besef binnen de EU dat een nieuwe invulling moest worden gegeven aan het begrip soevereiniteit, steunt op de verantwoordelijkheid om in dit domein de veiligheid te vrijwaren en er tevens voor te zorgen dat het gebruik van dit domein geen concomitante veiligheidsincidenten veroorzaakt in andere domeinen als gevolg van het gebruik van de cybernetische vector (Hohlmeier, 2015). Een discussie ten gronde met betrekking tot deze problematiek werd in de schoot van de EU gehouden in juni 2015.

aangewezen die zowel de organisatie van de energie-unie als de operationele implementatie ervan kunnen bewerkstelligen:

1.41 ENTSO-e in 34 landen moeten hiervoor 10 verschillende technische codes op elkaar afstemmen zonder dewelke het niet mogelijk is om de klimaatdoelstellingen noch de beleidsdoelstellingen (decarboniseren en voorzieningszekerheid) van een eengemaakte energiemarkt te bewerkstelligen.

2.het in kaart brengen van alle bestaande instrumenten voor het financieren van nieuwe infrastructuur. Lidstaten worden daarvoor aangemoedigd om hun energetische beleidsvisie horizon 2030 bekend te maken tegen volgend jaar: de bekendmaking hiervan moet het potentiële investeerders mogelijk maken om op basis van de transittarieven van ENTSO-e een schatting te maken van de haalbaarheid en de mogelijke return van toekomstige projecten.

3.coördinatie en inschatting van gevolgen van nationaal beleid van lidstaten met betrekking tot het verzekeren van energiezekerheid: zowel de opportuniteiten van iedere lidstaat als de schatting van de gevolgen van beleidsbeslissingen kunnen in dit gemeenschappelijk netwerk worden geëvalueerd. In het bijzonder wordt aandacht geschonken aan de grensoverschrijdende gevolgen van nationale beleidsbeslissingen en de controle van eventuele marktbeïnvloeding hierdoor.

4.de technische coördinatie in geval van tekorten op de energiemarkt is niet voldoende: ook moet de strategische visie op langere termijn soms worden afgewogen (bijvoorbeeld in het geval van een internationaal tekort) ten opzichte van de marktgerichte prioriteiten die men op dat moment geneigd zou zijn te verkiezen of waar men bij voorkeur de elektriciteit zal laten toekomen.

5.het heroriënteren van de energiemarkt naar een markt die meer afgestemd is op de vraag dan de constante output van vandaag en daarbij een optimale en dynamische prijsberekening kan bewerkstelligen: integratie van een groter aandeel van hernieuwbare bronnen is daarvoor aangewezen maar een te grote subsidie van staten in dat kader is op lange termijn nefast voor het realiseren van een eengemaakte energiemarkt door een artificiële prijsondersteuning.

6.niet alleen het nationale beleid op langer termijn moet kunnen worden gegarandeerd voor een efficiënte investeringscapaciteit, maar ook de investering in onderzoek moet door de lidstaten blijvend worden gevrijwaard: private investeringen volstaan niet voor onderzoek en daarom is een blijvende inzet van de lidstaten noodzakelijk.

Het komt erop neer dat zowel micro-economische parameters van vraag en aanbod worden verzoend met macro-economische vooruitzichten (economische groei, inflatie en werkloosheid) en strategische overwegingen (energiezekerheid en bescherming van infrastructuur). De positie van private-

en overheidsbedrijven hierin is duidelijk: het bestaan van hindernissen voor het één maken van de energiemarkt is te wijten aan nationale accenten die fragmentatie onderhouden en de veiligheid van kritiek energie infrastructuur in het gedrang brengen. De fragmentatie waarvan sprake is eerder een verdubbeling van de inspanningen en is enkel te wijten aan een gesponsorde maar ongecontroleerde input van alternatieve energiebronnen op nationaal vlak. Hierdoor worden duplicaties vanzelfsprekend: om dit probleem van de baan te helpen moeten volumes (en dus de subsidies voor alternatieve bronnen worden gecontroleerd). Het gebrek aan coördinatie op supranationaal niveau zorgt voor meer potentiële zwakheden in het gehele netwerk: een nieuwe aanpak zal in het distributienet moeten zorgen voor de levering van de juiste capaciteit op de juiste plaats wanneer die wordt gevraagd. De aanpak om daarom 20% hernieuwbare bronnen in het totale aanbod te hebben kan een beleidsdoelstelling zijn die niet noodzakelijk vereist dat die wordt doorgetrokken naar alle lidstaten van de EU: regionale verschillen kunnen een meer operationeel resultaat geven en daartoe is een coördinatie vereist op niveau van de TSO's (Matheu, 2015). Het beste operationele voorbeeld dat hiervoor kan worden gegeven is weergegeven door de gevolgen van een zonsverduistering voor de opwekking van energie door hernieuwbare bronnen, in casu zonnepanelen, en de gevolgen ervan voor het hele netwerk. De vraag/aanbod parameters zijn daarom cruciaal in de benadering die het moet mogelijk maken om incidenten van een andere orde in de toekomst op te vangen in de plaats van een vooropgesteld doel te uniformiseren over het territorium van de Unie. Kosten baten analyses van infrastructuur bieden daartoe nuttige informatie maar de kosten/baten analyse van een distributielijn werd nog niet uitgevoerd: de moeilijkheid van een dergelijke oefening is voor een deel te wijten aan de internationale implicaties van een dergelijke infrastructuur en dus zijn de kosten en de gevolgen van de vooropgestelde nieuwe regels moeilijk in te schatten. In de configuratie van de markt en onafhankelijk van het feit of een enkele energiemarkt wordt tot stand gebracht of niet, heeft iedere beslissing, zowel nationaal als internationaal, gevolgen voor andere marktspelers.

Dit beperkt zich bovendien niet tot de elektriciteitsmarkt: ook voor gas zijn drie elementen essentieel voor een efficiënte bescherming van kritieke energie infrastructuur te weten de beschikbaarheid van grondstoffen (problematiek die steeds aan nationale prioriteiten zal onderworpen blijven), distributie infrastructuur, opwekkingsinfrastructuur (centrales; problematiek die ook, deels historisch gegroeid, onderhevig zal zijn aan regionale verschillen en nationale prioriteiten). Ook in dit geval is het distributie netwerk een cruciaal element in de beveiliging van KEI en moet een antwoord gevonden worden op volgende vragen: wie beslist welke keuze wordt gemaakt, wie betaalt voor die keuze, wie neemt deel aan het project, op welke

manier wordt over de grenzen gewerkt, stelt de nieuwe infrastructuur niet te veel vereisten aan het geheel (met andere woorden is er flexibiliteit in het gebruik mogelijk) en ten slotte hoe worden mogelijke gevoeligheden of tekortkomingen van nieuwe systemen en technologieën in rekenschap genomen? Een antwoord op die vragen zou deel moeten uitmaken van elke kosten batenanalyse die in het domein van energie in de toekomst nog wordt gemaakt.

Men komt tot de vaststelling dat bescherming van kritieke energie-infrastructuur verder reikt dan de fysische bescherming van een lijst installaties. Om te beginnen met de verruiming van het beeld dat men in de toekomst zal moeten hanteren met betrekking tot bescherming van kritieke energie- infrastructuur is die voortaan niet meer te herleiden tot de bescherming van bronnen en/of producerende eenheden, maar is er een essentiële toevoeging met name in de distributienetwerken. Verder zal men binnen de Unie deze fysische bescherming moeten aanvullen met een essentieel onderdeel van cybernetische beveiliging van zowel de energie producerende eenheden en bronnen als het distributienetwerk. Vervolgens zal men een betere veerkracht kunnen bewerkstelligen door een diversificatie van de verschillende bronnen van energie die in de Unie worden gebruikt. Met betrekking tot de essentie van de beveiliging van het distributienet is men in deze context verplicht toe te voegen dat het voor de Unie belangrijk zal zijn om ook de aansluiting aan het netwerk aan de grenzen van de Unie te optimaliseren. Ten slotte zal een energie efficiëntie ervoor zorgen dat de exploitatie van de bestaande bronnen duurzamer wordt en dat hierdoor minder afhankelijkheid wordt in de hand gewerkt, of ten minste dat minder grote volumes grondstoffen nodig zijn voor een gelijkaardige hoeveelheid geproduceerde energie. In wat volgt zullen we merken dat een zuiver civiele benadering in deze ook tekort schiet en dat ook binnen een organisatie, die a priori een militaire samenwerking nastreeft, gelijkaardige doelen prioritair worden.

2.4. Bescherming in de NAVO

Bij afloop van de NAVO-top van Wales in september 2014 werden de belangrijkste prioriteiten van de Alliantie voor de nabije toekomst op een rij gezet. Met betrekking tot energie leest men (NATO, 2014):

> "A stable and reliable energy supply, the diversification of routes, suppliers and energy resources, and the interconnectivity of energy networks remain of critical importance. While these issues are primarily the responsibility of national governments and other international organisations, NATO closely follows relevant developments in energy security, including in relation to the Russia-Ukraine crisis and the growing instability in the Middle East and North Africa region. We will continue to consult on and further develop our capacity to contribute to energy security, concentrating on areas where NATO can add value. In particular, we will enhance our awareness of energy developments with security implications for Allies and the Alliance; further develop NATO's competence in supporting the protection of critical energy infrastructure; and continue to work towards significantly improving the energy efficiency of our military forces, and in this regard we note the Green Defence Framework. We will also enhance training and education efforts, continue to engage with partner countries, on a case-by-case basis, and consult with relevant international organisations, including the EU, as appropriate."

In de verklaring wordt niet alleen het belang onderstreept van energieveiligheid en beschikbaarheid van energiebronnen, maar wordt ook de bescherming van kritieke energie infrastructuur en de bijdrage van energie efficiëntie als belangrijk gewaardeerd. In het strategisch concept van de NAVO staat trouwens reeds in dit verband welke de dreigingen zijn die het toekomstig veiligheidslandschap zullen bepalen (NATO, 2010; pt.13):

> "All countries are increasingly reliant on the vital communication, transport and transit routes on which international trade, energy security and prosperity depend. They require greater international efforts to ensure their resilience against attack or disruption. Some NATO countries will become more dependent on foreign energy suppliers and in some cases, on foreign energy supply and distribution networks for their energy needs. As a larger share of world consumption is

transported across the globe, energy supplies are increasingly exposed to disruption."

Om die reden wil de NAVO actie ondernemen om de energieveiligheid te garanderen[16] ("develop the capacity to contribute to energy security, including protection of critical energy infrastructure and transit areas and lines, cooperation with partners, and consultations among Allies on the basis of strategic assessments and contingency planning- Op.Cit.pt.19). Die actie kan gericht zijn zowel op de fysische als de cybernetische beveiliging van energie-infrastructuur. Echter, binnen de schoot van de NAVO is er van de bondgenoten uit een zekere terughoudendheid om dit onderwerp aan te snijden. Volgens Rühle was de basis daarvoor te vinden in vier redenen (Rühle, 2011):

-de uiteenlopende nationale belangen en deelnames in energiebedrijven en/of exploitatie van bronnen;

-de afhankelijkheid van Rusland voor een groot gedeelte van gasvoorziening;

-het groot aantal actoren dat reeds in het zuiver civiele (en vaak commerciële) reeds dagdagelijks met de materie betrokken zijn;

-een te opmerkelijke betrokkenheid van de NAVO ter zake zou kunnen gepercipieerd worden als een militarisatie van het domein hetgeen opnieuw van andere partijen gelijkaardige reacties zou kunnen uitlokken of zelfs als een provocatie zou kunnen overkomen.

Een bijkomende reden voor die terughoudendheid is voor een deel te wijten aan de economische crisis en de implicaties ervan voor investeringen. Voldoen aan de basisbehoeften zoals functioneringskredieten, laat staan aan investeringskredieten is voor alle landen in de Alliantie een probleem geworden: hoe moeilijk zal het dan wel niet zijn om een volledig nieuw domein op te nemen in de openstaande werven voor de nabije toekomst? De samenwerking met partners maar evenzeer met supranationale instellingen als de EU, de OESO en private energieleveranciers wordt hiervoor dus belangrijk in de toekomst. De rol die de NAVO intern kan spelen is daarom te herleiden tot de expertise die de alliantie reeds rond andere taken heeft ontwikkeld.

[16] Het Central European Pipeline System (CEPS) is onderdeel van een veel breder netwerk van wat vroeger als een louter militaire infrastructuur werd ontplooid door de NAVO om de beschikbaarheid van energie voor vliegtuigen en voertuigen te garanderen. Sommige delen van het netwerk worden nu hoofdzakelijk nog door grote civiele exploitanten (bijvoorbeeld luchthavens) gebruikt.

Vooreerst is er de mogelijkheid om zowel kritieke infrastructuur voor energie en bevoorrading te beveiligen (in sommige gevallen zou dat een geconcentreerde, dan wel een verspreide infrastructuur of aanvoerweg kunnen zijn). Verder zal een dergelijke beveiliging ook een cybernetische beveiliging van industriële controlesystemen moeten behelzen. Vervolgens is een dialoog met partnerlanden vereist, zowel in het geval het over bondgenoten gaat die eventueel aandeel hebben in een bijzondere samenwerking met energiebedrijven, dan wel wanneer het over een partner maar geen bondgenoot zou gaan die op een doorvoerroute van de productie zou liggen. Ten slotte kan de NAVO ook terugvallen op haar expertise van samenwerking tussen civiele en militaire structuren, in het bijzonder in het geval van rampen (Civil Emergency Planning), maar dat tevens in dat kader een samenwerking is voorzien met betrekking tot cybernetische beveiliging: ook in dit domein wordt reeds sinds de Top van Lissabon onder de Civil Emergency Planning (CEP) koepel werk gemaakt van dialoog en samenwerking in het CIIP-domein, onder meer door middel van het Civil Communications Planning Committee (CCPC). Een bijkomend forum dat een uitwisseling van expertise met betrekking to energieveiligheid moet mogelijk maken is het creëren van het NATO Energy Security Center of Excellence (ENSEC COE). Het is een multilateraal expertisecentrum dat sinds 2012 werd opgericht met als doel experten-advies te kunnen leveren met betrekking tot de problematiek en operationele gevolgen van energieveiligheid. De opdracht van het centrum wordt weergegeven op de intropagina van hun website[17]:

> "The mission of the ENSEC COE is to assist Strategic Commands, other NATO bodies, nations, partners, and other civil and military bodies by supporting NATO's capability development process, mission effectiveness, and interoperability in the near, mid and long terms by providing comprehensive and timely subject matter expertise on all aspects of energy security. The mission includes cost effective solutions to support military requirements, energy efficiency in the operational field, and interaction with academia and industry."

Het centrum moet instaan voor technische en academische ondersteunging, in het bijzonder voor het uitvoeren van de risicoanalyse, voor het genereren van oplossingen die tegelijk milieuvriendelijk en afdoend zijn in een Smart Defence kader, voor analyse van oplossingen voor het verzekeren van energieaanvoer en bescherming van kritieke energie infrastructuur en zo NAVO-opdrachten te ondersteunen en energie-efficiëntie te verhogen, voor de identificatie van toekomstige dreigingen in de materie als gevolg van het

[17] http://www.enseccoe.org/en/about-us/centre-of-excellence.html

tekort aan energiebronnen en als gevolg van de complexiteit van de voorziening.

Maar naast de taken en de divisies die de NAVO zelf beheert, is de rol die de NAVO zal spelen met betrekking tot energie ook door externe factoren bepaald. Het zal immers het gevolg zijn van het aangepaste kader waarin de energieproductie zich in de toekomst op zal toespitsen: de spanningen die in het Midden-Oosten gerezen zijn, hebben in het Westen de angst voor de energievoorziening enkel maar onderhouden. Het opdrijven van conflictueuze spanning rond bronnen, infrastructuur en transitlijnen heeft bijvoorbeeld Polen ertoe aangezet om een concept als een energieartikel 5 te lanceren: een dergelijk concept zou erin bestaan om steun te verlenen aan een land dat ontwricht zou worden door de onbeschikbaarheid van energiebronnen. Het is in de eerste plaats de situatie rond Oekraïne die ervoor heeft gezorgd dat Polen een dergelijke wens heeft geuit. Nochtans is de situatie niet meer dezelfde als in de jaren ’70 en zijn marktprijzen van traditionele bronnen ernstig gezakt: twee redenen zijn daarvoor verantwoordelijk, te weten enerzijds de crisis in Oekraïne en het daaruit voortvloeiend embargo ten opzichte van Rusland en anderzijds het akkoord met Iran. Wat de toekomst zal brengen indien de spanningen tussen Turkije en Rusland aanhouden is onduidelijk: het wegvallen van een gegarandeerde doorvoercorridor zou aanleiding kunnen geven tot een nieuwe prijsstijging.

Een dalende prijs heeft nochtans de druk niet doen afnemen om een ander gewicht te leggen in het verbruik van energiebronnen. De klimaatverandering heeft de prangende noodzaak tot een lagere uitstoot van broeikasgassen aangetoond en verklaart mee de tendens van Westerse landen om zich enigszins los te weken van de afhankelijkheid van fossiele brandstoffen en daardoor de markt zodanig te beïnvloeden dat internationale veiligheid hierdoor anders zou worden ervaren. Mede wordt hierdoor een nieuwe rol weggelegd voor allianties als de NAVO: enerzijds als actor maar anderzijds als veiligheidsverschaffer. Als actor is het natuurlijk mee een verbruiker van energie, meer bepaald fossiele brandstoffen. Als veiligheidsverschaffer heeft de alliantie volgens sommigen een bijkomende rol als beschermer van kritieke energie infrastructuur, waaronder zowel de bronnen als de distributielijnen moeten worden begrepen. Een te grote nadruk leggen op die specifieke taak zou volgens Cornell een militarisering van het onderwerp als gevolg hebben (Cornell, 2013): het zou als gevolg hebben dat de markt een artificiële veiligheidsproblematiek wordt opgelegd waardoor potentiële investeerders niet meer de aantrekking zouden ondervinden om de infrastructuur uit te breiden en tegelijk van de noodzakelijke bescherming te voorzien. Naast de lagere aantrek voor investeringen zou dit bovendien kunnen leiden tot een nieuwe militarisering van zones die zowel de bron, de

distributiekanalen als de ontvangende landen zou kunnen treffen. Een grotere fysische betrekking van krijgsmachten in de bescherming van kritieke energie infrastructuur zou derhalve volgens hem op het einde van de rit de veiligheid en de beveiliging niet ten goede komen. Maar ruimer dan het standpunt van Cornell, kan men er niet onderuit dat het volledige energetische debat al een geostrategische lading dekt en dat hoewel zonder de fysische aanwezigheid van troepen naast bronnen of distributielijnen, wel de hete adem wordt gevoeld van alle staten die er belang bij hebben om bronnen te exploiteren, al was het maar omdat krijgsmachten relatief meer van die traditionele bronnen verbruiken met hun wapensystemen en dat dit in het komende decennium nog niet zal veranderen. Zowel de NAVO als Rusland hebben dat in hun respectieve doctrines en verklaringen met zo veel woorden duidelijk gemaakt: Rusland door energie zowel als een doel als een middel naar voren te schuiven in haar poging om de invloed van het land uit te breiden[18], de NAVO van zijn kant door energie veiligheid te willen bewerkstelligen[19]. De positie ten opzichte van het Midden-Oosten is dan ook kritisch indien men de dreiging op de energielevering uit die regio in beschouwing neemt: een aantal scenario's werden in dat opzicht vooropgesteld als mogelijke alternatieven voor het schatten van de risico's die verbonden zijn aan de onbeschikbaarheid van energiebronnen door terroristische aanvallen op installaties, door het wegtrekken van arbeiders in de sector omwille van de onrust in de regio, politieke instabiliteit, te wijten aan uitlopers van de Arabische Lente, de uitbreiding van de onrust in Irak naar andere regio's waar oliebronnen gelegen zijn, onder meer door de acties van de Islamitische Staat (IS) of een regelrecht militair treffen in de regio met de afsluiting van choke points zoals de straat van Hormoes tot gevolg. Elk van die scenario's kan in één of meer landen met de grootste olievelden tot stand komen (Saoedi-Arabië, Libië, Irak, de Kaukasus, Centraal-Azië) of in meerdere tegelijk. Eén van de voorgestelde oplossingen daarvoor bestaat uit de exploitatie van andere energiebronnen en zelfs alternatieve gasproductie uit te baten: op lange termijn zal dit echter soelaas bieden voor die landen die tot voor kort een te grote afhankelijkheid vertoonden voor de gas- en/of oliesector. Een andere oplossing bestaat er uit

[18] Russia's National Security Strategy to 2020. Beschikbaar via http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=154915. Geraadpleegd op 11 augustus 2015.

[19] We will continue to consult on energy security and further develop the capacity to contribute to energy security, concentrating on areas where NATO can add value. To this end, we will work towards significantly improving the energy efficiency of our military forces; develop our competence in supporting the protection of critical energy infrastructure; and further develop our outreach activities in consultation with partners, on a case-by-case basis. Uittreksel uit Chicago summit declaration beschikbaar via http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en geraadpleegd op 12 augustus 2015.

om transit van deze grondstoffen via alternatieve routes te voorzien (bijvoorbeeld vanuit Libië door de Middellandse zee of via Turkije) waarvoor betere of nieuwe distributielijnen moeten worden voorzien. Een duurzame oplossing voor de spanningen met Iran zou hiervoor een goed alternatief bieden. Een andere oplossing bestaat erin om het aandeel traditionele olieproducten te laten afnemen in het totale pakket (door gebruik van andere of alternatieve bronnen of zelfs te combineren met een betere energie-efficiëntie). Elkeen van de oplossingen die zonet voorgesteld werden hebben betrekking op ofwel de technologie, ofwel de consumptie, ofwel de productie en de verspreiding ervan. Een ideale oplossing zal meer dan waarschijnlijk een combinatie zijn van alle voormelde mogelijkheden en de beschermingsmaatregelen van infrastructuur die erbij passen: in een volgend hoofdstuk zullen we merken dat die maatregelen zowel de fysische als de cybernetische bescherming moeten kunnen behelzen.

De mogelijke alternatieve scenario's voor de consumptie van energie zullen mogelijk ook gevolgen hebben voor de opdrachten van de NAVO: Cornell beschrijft inderdaad drie scenario's voor de komende 20 jaren waarvan elkeen een verschuiving van de securitaire implicaties tot gevolg heeft:

-een eerste heeft als aanleiding een verschuiving van de vraag (wat men vandaag reeds vaststelt) met name dat de vraag voor traditionele olie en gasproducten toeneemt in groeilanden en meer bijzonder in het verre oosten, terwijl dat eerder afneemt in West-Europese landen. In een dergelijk scenario ziet men in de landen van het Midden-Oosten een toename van hun gasproductie en consumptie: de stijgende vraag zou de prijs doen stijgen terwijl de VS er tegelijk door hun alternatieve productie minder afhankelijk van worden. Een dergelijk scenario zou de laagconjunctuur in West-Europa kunnen onderhouden terwijl het oosten net meer kan investeren in militaire middelen. Het resultaat is een mogelijke militarisering van de oosterse zeeën waar de NAVO minder inspraak heeft en nog minder zal hebben in de toekomst.

-in een tweede scenario is het vooral gas dat de vraag drijft in een betrachting om toch een lagere uitstoot van CO_2 te kunnen bewerkstelligen. In dat scenario worden nieuwe zones zoals het Arctisch gebied bijzonder belangrijk en kan de rol van een land als Rusland en alle belanghebbenden in de regio op de spits worden gedreven. In een dergelijk geval ziet men ook voor de rol van de NAVO en de nabijgelegen zone van de Alliantie een rol, maar tegelijk zal men moeten voorzien in alternatieve aanvoer van gas, zoals bijvoorbeeld uit Iran via Turkije of via de Middellandse zee uit Libië of nog via het oostelijk deel van de Middellands zeegebied (Cyprus/Israël): in elk van de gevallen zal een belangrijke rol te

vervullen zijn voor transport- of exploitatie-infrastructuur en de beveiliging ervan: gezien de proximiteit van het NAVO-territorium kan hiervoor een rol vervuld worden door observatie (zoals satellietbeeldverwerking en drones) maar ook sensoren.

-een laatste scenario wil Europa nog steeds drijven naar het respect van de Kyotto norm en in het zicht daarvan meer koolstofarme bronnen zien gebruiken, waaronder ook kernenergie. Zowel de groeilanden als de OESO-landen staan in dit scenario aan de spits en in dat geval wordt een groter gedeelte van de kritieke energie infrastructuur samengesteld door kerninstallaties en alternatieve energiebronnen.

Maar geen enkel van die scenario's hoeft daarom ongewijzigd en exclusief te worden gerealiseerd: het is eerder waarschijnlijk dat een regionale mix van een en andere scenario zich zal voltrekken. Een veel betere manier om de bescherming te verbeteren zou er volgens Cornell uit bestaan om kapitaal intensieve observatie van bronnen en distributie te realiseren (bijvoorbeeld aan de hand van satellieten en andere sensoren) en opleiding en training te ondersteunen in transitlanden. Maar hiermee legt hij vooral de nadruk op de fysische bescherming als enig oplossing van het probleem: en het is ook inderdaad zo dat dit de meest vanzelfsprekende richting is waaraan, als gevolg van de vaststelling van de dreiging, wordt gedacht. Het zijn immers meestal infrastructuur van energiebronnen en/of distributiecentra die zowel door staatsactoren als niet-staatsactoren worden betracht. Maar ook in vredestijd kunnen ze door zowel menselijke als door de natuur veroorzaakte factoren getroffen worden en aanleiding geven tot een onderbreking van de voorziening. In operatietonelen is de bescherming ervan een element die een zware kost genereert, zowel in deviezen als in mensenlevens: operaties in Afghanistan hebben bijvoorbeeld naar schatting en enkel door het element 'force protection' van energiebronnen in rekening te brengen, het dubbele gekost van de nominale waarde per verbruikte liter brandstof (Petkevicius, 2012; p.4). In dezelfde bron wordt gewag gemaakt van het feit dat tussen 2003-2007 meer dan 3000 manschappen werden gewond of gedood tijdens aanvallen op brandstof of wateropslagcapaciteit.

Los van deze of gene oplossing die door verschillende bronnen worden naar voren geschoven, moet men zich de vraag stellen welke elementen kunnen bijdragen tot een betere beveiliging: het antwoord is niet triviaal en kan niet herleid worden tot één enkel element zoals fysische beveiliging alleen. Een oplossing voor het garanderen van energiezekerheid moet daarom de fysische beveiliging overstijgen en eerder een pallet van maatregelen inhouden en bijvoorbeeld volgende elementen bevatten:

-een deel van de oplossing kan er daarom uit bestaan om te diversifiëren (olie, gas, elektriciteit), waardoor men niet noodzakelijk

voor de meest commercieel voordelige optie kies: een keuze om te diversifiëren beperkt zich bovendien niet tot de gebruikte bron van energie maar ook het vermeerderen van de distributie van de beschikbare bronnen;

-de fysische beveiliging van bronnen, maar ook van het distributienetwerk zodat voor de alliantie een vorm van operationele energieveiligheid tot stand komt: deze moet in alle omstandigheden toelaten om operaties niet in het gedrang te brengen indien die zouden worden gepland;

-het gebruik van alternatieve energiebronnen aanmoedigen die toestaan dat een zekere autonomie wordt bekomen van de gebruiker;

-een dergelijke autonomie kan eveneens worden vergroot met traditionele bronnen, vooropgesteld dat de energie efficiëntie ook bij de Alliantie wordt vergroot: een verhoging van die efficiëntie is bovendien een element van synergie met de strategie die de Europese Unie eveneens in haar energetische politiek nastreeft en is dus een strategisch objectief dat te verkiezen is boven energetische onafhankelijkheid. Een essentieel verschil in aanpak tussen de twee organisaties verklaart onder meer waarom vele lidstaten in hun nationale politiek nog steeds energetische onafhankelijkheid verkiezen boven de energie-efficiëntie: in een commerciële benadering geeft het immers meer kans op een snelle return en landen met een historiek en capaciteit in ene of gene energievorm zullen niet snel geneigd zijn om de nationale voordelen ervan te herzien ten voordele van een collectieve oplossing;

-de voormelde fysische beveiliging van bronnen en/of distributielijnen is gezien de nieuwe dreiging niet meer voldoende: ook een cybernetische beveiliging moet in de hand worden gewerkt.

Men komt tot de deelconclusie dat de vrijwaring van de beschikbaarheid van energie niet meer louter te herleiden is tot de fysieke beveiliging van bronnen en aanvoerroutes, hoewel het er zeker toe bijdraagt (en waarvoor gelijkaardige middelen kunnen worden ingezet als diegene die voor force protection worden gebruikt), maar evenzeer afhankelijk is van diversificatie, energie-efficiëntie en de cybernetische beveiliging die zich in de loop van de komende jaren binnen de schoot van krijgsmachten maar ook de landen waarvoor ze worden ingezet zullen moeten voltrekken. De top van Wales herneemt in dat verband (NATO, 2014):

> “As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence

> responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."

We stellen vast dat de Alliantie in haar slotverklaring van de top van Wales het belang onderstreept van dat cyberelement in het verdedigen van de welvaart en dat het idee om daarvoor terug te vallen op artikel 5 van het verdrag van Washington onderworpen zal zijn aan overleg. In het bijzonder onderschrijft de alliantie het idee dat nationale netwerken cruciaal zijn voor het realiseren van een cyberverdediging. In wat volgt willen we daarom nagaan hoe de organisatie in de VS, de EU en ons land wordt georganiseerd met betrekking tot de cybernetische beveiliging van energieproductie en distributie.

2.5. Deelbesluit

Keuze tussen centralisatie of decentralisatie is fundamenteel voor de geschikte bescherming van kritieke energie infrastructuur: de energiesector wordt vandaag de dag immers tot de top vijf gerekend van de meest bedreigde sectoren. Nochtans is zelfs in de VS gebleken dat opeenvolgende budgettaire inkrimpingen ervoor hebben gezorgd dat zelfs het DoD niet meer in staat zou zijn om zowel zichzelf als de samenleving in de VS adekwaat te beschermen in geval van gerichte aanvallen op kritieke energie infrastructuur, mede ook door de uitbreiding van de distributiebutiekanalen ervan. Meer en meer worden daarom niet alleen de civiele actoren maar zelfs een beroep gedaan op de medewerking van private actoren in de organisatie van de bescherming.

In de EU dienen door de complexiteit van de problematiek zowel de interne als de externe dimensie, maar ook politieke als technologische factoren in rekening gebracht als insteek van oplossingen. Bescherming van kritieke energie-infrastructuur reikt verder dan de fysische bescherming van een lijst installaties: voor de beveiliging van het distributienet is het voor de Unie belangrijk om ook de aansluiting aan het netwerk aan de grenzen van de Unie te optimaliseren en binnen de Unie ervoor te zorgen dat energetische eilanden worden weggewerkt. Verder moet energie efficiëntie ervoor zorgen dat de exploitatie van de bestaande bronnen duurzamer wordt en dat hierdoor minder afhankelijkheid wordt in de hand gewerkt, of ten minste dat minder grote volumes grondstoffen nodig zijn voor een gelijkaardige hoeveelheid geproduceerde energie. Vervolgens zal men een betere veerkracht kunnen bewerkstelligen door een diversificatie van de verschillende bronnen van energie die in de Unie worden gebruikt.Verder zal men binnen de Unie deze fysische bescherming moeten aanvullen met een essentieel onderdeel van cybernetische beveiliging van zowel de energie producerende eenheden en bronnen.

Een zuiver civiele benadering van de problematiek schiet tekort en dat is merkbaar doordat een militaire organisatie als de NAVO gelijkaardige doelen als prioritair beschouwt. Nochtans zijn niet alle bondgenoten op dezelfde lijn op dat vlak: sommige gaan zelfs zo ver het concept van energieartikel vijf te willen creëren waarbij een bondgenoot de onmiddellijke hulp van andere zou worden verleend indien de energieveiligheid in gevaar zou worden gebracht. Bijkomende beschermingsopdrachten zullen in elk van

de open opties een bijkomende kost hebben in harde valuta of mensen, kost die zijn weerslag zal hebben op de brandstofprijs. De vrijwaring van de beschikbaarheid van energie is bovendien niet louter te herleiden tot de fysieke beveiliging van bronnen en aanvoerroutes, hoewel het er zeker toe bijdraagt (en waarvoor gelijkaardige middelen kunnen worden ingezet als diegene die voor force protection worden gebruikt), maar is evenzeer afhankelijk van cybernetische beveiliging, diversificatie en energie-efficiëntie. In wat volgt worden deze elementen belicht.

Deel 3

Cybernetische afhankelijkheid en -veiligheid

3.1. Algemeen

De eerste ervaringen met aanvallen op computersystemen werd gedemonstreerd in de militaire middens: gedurende de eerste Golfoorlog werd het luchtbeeld van Iraakse luchtmacht tijdens de eerste Amerikaanse aanval gewijzigd zodat luchtverdedigingseenheden niet in staat zouden zijn optimaal te reageren. Van deze uitsluitend militaire toepassingen is reeds lang afgegleden naar de civiele toepassingen. Niet noodzakelijk om militaire redenen, maar vooral vanwege financiële implicaties, werden olie- en gasproducenten recent vaak het slachtoffer van gerichte aanvallen (2012-2013): zodanig veel zelfs dat het de aandacht trok van het Department of Energy en Department of Homeland Security (DHS).

De bezorgdheid voor dergelijke aanvallen is alleszins in de VS doorgesijpeld en heeft over de partijpolitieke grenzen aanleiding gegeven tot debat. Van bij aanvang van ontwikkeling van industriële controlesystemen (ICS, SCADA) werden die geïsoleerd van het Internet. Een totale isolatie blijkt echter nooit mogelijk: al was het maar voor updates van de software configuratie of het "patchen" van fouten in het systeem, wordt vandaag connectie voorzien op een of andere manier waardoor blootstelling aan aanvallen wordt mogelijk gemaakt (tijdelijke connectie, USB-sticks).

Niets kan beter de actuele betrokkenheid weergeven van het cyberdomein voor de opwekking en voor de distributie van energie in het bijzonder, dan wat een bipartizaan initiatief in de VS erover heeft gerapporteerd in het kader van het Electric Grid Cybersecurity Initiative (EGCI, 2014; p.34):

> "From the perspective of federal policymakers, a key question is the degree to which cybersecurity events on distribution systems could have implications for the bulk power system, of for broader national security or economic interests. In some cases, cyber attacks on distribution system facilities could have consequences that extend beyond that system. For example, simultaneous attacks on multiple distribution utilities, or an attack on a single utility's distribution operations in multiple locations, could have broader ramifications for the bulk power system. In addition, electric distribution systems carry power to pipelines, water systems, telecommunications, and other critical infrastructure, while also serving critical government or military

> facilities. Distribution-level cyber attacks that disrupt electric service to such facilities could have important economic and security consequences. Finally, as the grid continues to modernize over the next few decades, the lines between transmission and distribution systems may become increasingly blurred, creating challenges for the management of cyber security risks and the traditional and jurisdictional divide. For example, many analysts are projecting an increased role for distributed generation systems that are engineered to accommodate two-way power flows. This evolution could increase the likelihood that cyber events at the distribution level would pose a risk to the bulk power system, and it points to a growing need for coordination across the entire electric power sector."

We stellen vast dat in de VS duidelijk de vraag wordt gesteld in welke mate de noodzakelijke evolutie naar nieuwe distributiesystemen niet meer gevaar oplevert voor incidenten die het hele netwerk in gevaar zouden kunnen brengen. In het bijzonder wordt de relevantie van de aandacht voor verschillende gelijktijdige cyberaanvallen of één aanval op verschillend locaties niet meer in vraag gesteld, noch de mogelijke implicaties ervan voor kritieke infrastructuur en zelfs overheids- en/of militaire installaties. Energieleveranciers beschouwen zichzelf nog als goed beveiligd, terwijl telecommunicatiefirma's het slechtst scoren in onafhankelijke enquêtes van experten (Symantec, 2012; p.6). In een "slim" netwerk waar niet alleen de energieleverancier belangrijk is maar ook de communicatie en het distributienetwerk, is dit een kritiek element dat mee te nemen is in de evaluatie van de kwetsbaarheden.

Als gevolg daarvan komt men automatisch tot de vaststelling dat men zich in geval van grootschalige incidenten waarin kritieke energie infrastructuur is betrokken, ook de vraag dient te stellen welke de impact zal zijn van het incident voor andere domeinen: naast het cyber incident zelf is er vaak een grote fysische implicatie aan verbonden. Een dergelijke extrapolatie is geen vanzelfsprekende oefening en daarom is het in ieder geval eenvoudiger te vertrekken van een op schaal vergelijkbaar impactmodel. De incidenten waarover sprake baren zorgen op alle continenten. In wat volgt zullen we zien hoe aan beide zijden van de Atlantische Oceaan op een andere manier maatregelen worden genomen om het hoofd te bieden aan gerichte aanvallen. De gevoeligheden van systemen worden nauwlettend in de gaten gehouden. Daarom worden alle technologische aspecten van het probleem reeds jaren onder de loupe gehouden, ook de mogelijke faling van back-up systemen: een voorbeeld ervan vinden we terug in het onderzoek naar gevolgen van gevoeligheden die reeds in 2007 werden vastgesteld op generatoren, welke vaststelling in vele domeinen tot ingrijpende gevolgen zou

kunnen leiden. Het project dat de naam Aurora draagt had als doel na te gaan welke de gevolgen konden zijn van een softwarematige programmatie van connectoren die op een abrupte manier zouden opengesteld worden en mechanische delen daardoor op een niet voorzien frequentie te laten draaien, hetgeen zou resulteren in mechanische schade aan motoren, generatoren en compressoren. De Aurora aanval zou eruit bestaan om interruptoren van circuits kortstondig aan en uit te schakelen zodat de synchrone werking van mechanische delen wordt verstoord en voor mechanische torsie zorgt die tot irreversibele schade kan leiden. De fysische schade die op een cybernetische wijze zou worden gegenereerd, zou op die manier gevolgen hebben voor alle sectoren die mechanische onderdelen op de een of andere manier door SCADA systemen in het algemeen en Industriële Controle Systemen in het bijzonder worden aangestuurd: raffinaderijen, spoorwegtransport, waterpompen, krachtcentrales en alle generatoren die elektriciteit moeten genereren. Het weze duidelijk dat het in geenenkel opzicht gaat over een banale ontkoppeling van generatoren maar een fysische vernietiging als gevolg van een cybernetische interventie in industriële controlesystemen die mechanische rotatie elementen aansturen. Het incident werd in 2007 eerst gemodelleerd en getest om in reële condities in staat te zijn om de aan het licht gebrachte zwakheden te testen en eventuele maatregelen te kunnen treffen om de beveiliging ervan in de hand te werken: hiervoor werden alle fabrikanten betrokken om een systeem uit te werken dat de mechanische beveiliging zou kunnen garanderen, waarna zowel de overheid in de VS als de betrokken diensten, die mogelijk het slachtoffer van een dergelijk incident zouden kunnen worden, te sensibiliseren voor het gevaar. Tegelijkertijd werden de resultaten en de conclusies van de modelisering bekend gemaakt over de grenzen en aan bondgenoten, en werden technische briefings georganiseerd in de betrokken domeinen en sectoren om maatregelen te kunnen treffen (de installatie van hardware beveiliging en onderbrekers, de installatie van detectie van mogelijke 'Aurora type aanvallen') die ervoor moeten zorgen dat een aanval tijdig wordt vastgesteld en dat de geviseerde uitrusting tijdig kan worden ontkoppeld vooraleer er onherroepelijke schade wordt toegekend. De wetenschappelijke studie van het probleem heeft geleid tot de identificatie van een aantal voorwaarden om tegen een dergelijk schadegeval beschermd te zijn (Salmon et.al., 2010):

-een kennis van alle communicatiemiddelen van het systeem (waaronder SCADA);

-gebruik van paswoorden die voldoende variatie en beveiliging vertonen (geen standaard paswoorden voor het beheer van het systeem);

-encryptie van communicatie of zelfs gebruik van glasvezel voor communicatie;

-beheer van kennis en beperking tot toegang ervan tot diegene die er echt nood toe heeft;

-geen gebruik van redundante paswoorden;
-gebruik van beveiligde monitoring met alarm voor intrusie;
-kennis van alle gebruikers van het systeem;
-combinatie van fysische met cybernetische veiligheid.

We gaan in wat volgt na welke de initiatieven in de VS, respectievelijk de EU en ook in ons land werden tot stand gebracht om dergelijke en andere dreigingen onder controle te houden.

3.2. De Verenigde Staten als model?

In de VS werd daartoe de vergelijking gemaakt tussen de gevolgen van een cyber incident enerzijds en een cyber aanval met fysische gevolgen anderzijds. Tot voor kort waren enkel de plannen voor noodtoestanden bij natuurrampen relevant en houden zij op een voldoende grote schaal rekening met de gevolgen van interdepartementale onderbrekingen of malfuncties waarbij energie een centrale rol speelt. De kans om terug operationeel te worden in omstandigheden die door super storm Sandy in 2012 werden veroorzaakt, concentreert alle moeilijkheden die ook in het geval een ontwrichtende cyberaanval op energie infrastructuur als gevolg kan hebben: in dat concrete geval was samenwerking vereist tussen verschillende actoren om opnieuw tot een aanvaardbare situatie te komen. In de VS heeft men zich daarom op twee bestaande documenten gebaseerd om de coördinatie van het herstel tot een goed einde te brengen:

1.Het National Response Framework (2008) ontwikkeld door het Department Homeland Security in 2008 en herzien in 2010. Dit document voorziet het doctrinaire en organisatorische gedeelte van de hulpverlening; de kritieke functies als transport communicatie en energie die zo snel mogelijk moeten worden beschikbaar gemaakt; de mandaten en de verantwoordelijkheden van ieder van de nationale en lokale betrokken actoren.

2.Het Interim National Cyber Incident Response Plan ontwikkeld door hetzelfde departement in 2010 is een plan voor het herstel na een ontwrichtende cyberaanval. Daaropvolgende oefeningen hebben echter aan het licht gebracht dat besluitvorming tijdens en na een incident te traag verliep; dat het leveren van technische middelen voor het verhelpen van een incident niet altijd mogelijk zijn; dat de rol en verantwoordelijkheden in dit gedeelte niet altijd duidelijk zijn wat verband kan houden met het gebrek aan coördinatie en de trage besluitvorming.

Voormelde documenten werden getoetst op hun tekorten tijdens de gevolgen van de superstorm. In de praktijk bleken de voor de hand liggende instrumenten en middelen niet te volstaan om een langdurende en grootschalige uitval van stroom te herstellen. Bovendien bleek ook de coördinatie tussen de betrokken actoren suboptimaal. Doel was de betere elementen uit beide teksten te weerhouden: zowel het departement energie

(Department of Energy-DoE) als het departement binnenlandse veiligheid (Department of Homeland Security-DHS), maar ook private bedrijven willen de problematiek van cyber aanvallen op het elektriciteitsnetwerk uitspitten en de kritieke middelen identificeren die noodzakelijk zijn om een dergelijke aanval op kritieke infrastructuur (waaronder energievoorziening) het hoofd te kunnen bieden: de integratie van de rampen- en noodplanning met de noodplanning in het cyberdomein vloeit voort uit de vastgestelde verschillen van verantwoordelijkheden. Nochtans stellen beide teksten voor om de coördinatie in een dergelijke gecombineerde situatie te verbeteren.

Het in kaart brengen van de bestaande instrumenten in de VS noopt ons tot enkele vaststellingen: vooreerst is het niet oninteressant vast te stellen dat het land al sinds 2010 over een specifiek noodplan beschikt voor de gevolgen van grootschalige cyberaanvallen. Verder dient te worden onderstreept dat beide voormelde instrumenten de coördinatie tussen de actoren voorzag maar ook daarnaast samen konden worden uitgebaat om een sterker raamwerk voor de respons toe te laten. Vervolgens dat vastgestelde tekorten of tegenspraken nu al worden aangepakt om in het kader van het onderwerp dat ons aanbelangt een herstel naar normale omstandigheden toe te laten. De tekorten in de VS zijn ook onze tekorten waar we rekening mee moeten houden in het dagelijks beheer van cyberincidenten: deze kunnen dus zonder enige twijfel worden opgenomen in de raadgevingen. Te weten:

1.De commandostructuren en de verantwoordelijkheden moeten in beide gevallen duidelijk worden afgebakend en in het bijzonder in het gecombineerde geval.

2.De grenzen voor federale interventie ten opzichte van lokale interventie moeten vooraf worden gedefinieerd: getransponeerd naar de Europese context dient dit ook de grens weer te geven van een interventieverantwoordelijkheid op Europese schaal (twee lidstaten of meer getroffen).

Naar Amerikaans voorbeeld dient in de Europese context de verantwoordelijkheid van lokale en nationale actoren te worden afgestemd. Daar waar de regionale benadering de verantwoordelijkheid van de gouverneur in het daglicht zet, wordt dat in sommige gevallen overgenomen door de nationale autoriteiten (en zoals eerder vermeld kan dat zelfs de supranationale respons initiëren). De casestudy van de VS leert ons dat in een Europese context zowel de nationale als de regionale afstemming van actoren noodzakelijk zijn.

Na een toelichting van de aanpak in de VS dienen we ons de vraag te stellen welke de aard van de dreiging is en of die kan gekwantificeerd worden. Hiervoor werd vermeld dat de bewustwording van de mogelijke gevolgen

voor cyberaanvallen op kritieke energie infrastructuur in de VS tot stand kwamen door grote stroomuitvallen met grensoverschrijdende en langdurende gevolgen: een voorbeeld daarvan heeft in 2003 plaatsgehad in de VS en Canada, kostte 6 miljard USD en trof 50 miljoen klanten (individuen, private bedrijven en overheid): vanuit dergelijke incidenten en de noodzaak tot connecties die nog meer interactie vergen bij de installatie van slimme netwerken, vreest men voor gevolgen in communicaties, watervoorziening en gezondheidsdiensten bij een gelijkaardig incident dat zou veroorzaakt worden door een cybernetische aanval. De impact van een dergelijk incident is sinds 2003 echter vergroot door een grotere interconnectiviteit tussen informatiesystemen met infrastructuur via controlesystemen: de standaarden die door de energieleveranciers worden gehanteerd zijn strenger dan voor andere diensten. En toch is het niet vanzelfsprekend om private investeerders te motiveren om in te zetten op veiligheid op lange termijn zonder garantie een tastbare meerwaarde te genereren voor de investeerder: een privaat bedrijf zet immers in op de maximalisatie van haar winst en daarom kan investeren in veiligheid een beperkend element zijn voor maximalisatie van de winstmarge. Het voldoen aan standaarden zal daarom eerder gericht zijn op het naleven van minimumvereisten. Nochtans zien we in de kwalificatie van de dreiging en de cijfergegevens dat het niet om onnodige investeringen gaat, hetgeen door de nucleaire industrie reeds lang is beseft: de Stuxnet-aanval op een nucleaire installatie van Iran in 2010 was de illustratie van wat men tot dan toe enkel in hypothetische denkoefeningen als mogelijk scenario voorstelde namelijk fysische vernietiging als gevolg van een cybernetische aanval in een van de traditioneel meest beveiligde installaties. Eerdere aanvallen hadden reeds zwaktes in de controlesystemen van nucleaire installaties voor dergelijke aanvallen blootgelegd (Slammer, 2003; Aurora, 2007). Als illustratie van het feit dat dit type dreiging zich niet beperkte tot nucleaire installaties, kan Night Dragon worden vermeld als voorbeeld van aanvallen op energiebedrijven (olie, gas) wereldwijd. Tot slot meldde Saoedi Aramco dat Shamoon een grootschalige campagne omvatte tot neutralisatie van hun olie- en gasproductie: 30.000 computers bleken na deze aanval onbruikbaar (Electric Grid Cybersecurity Initiative. 2014; p.21). Deze aanval op een voor de oliemarkt kritieke exploitatiefirma had zware gevolgen kunnen hebben voor de wereld olie- en gasprijs.

Zoeken we naar een evolutie van dreiging in cijfers dan vinden we in voor de jaren 2011-2014 een overzicht van de in de VS gecatalogeerde kritieke sectoren en de verdeling van het aantal incidenten over die sectoren die een dringende noodinterventie vereisten van een cyber incident emergency response team (CERT) op een site:

Tabel 1: verdeling van cyber incident-respons over sectoren (ICS-CERT, 2013 en 2014).

Sector	2011	2012	2013	2014
Chemie	0	4	0	1
Commercieel	10	2	0	2
Communicatie	1	0	2	0
Manufactuur	2	1	0	0
Dammen	0	0	0	0
Defensie industrie	0	12	1	0
Nooddiensten	2	3	0	0
Energie	11	7	18	43
Financiën	1	6	0	0
Voedsel en landbouw	5	0	0	0
Overheid	5	3	2	5
Zorg en gezondheid	6	1	5	0
Informatietechnologie	3	5	2	0
Nucleair	2	8	8	5
Transport	7	10	10	10
Water	21	25	24	38
Totaal	76	87	72	104

Vooreerst stelt men een sterke stijging van het aantal interventies vast in de tijd. De twee sectoren die daar het meeste toe bijdragen zijn water en energie: in elk van deze sectoren komt die stijging tot uiting (respectievelijk van 15-41% en 27-37% over de voormelde jaren). Te vermelden is dat de incidenten die een tussenkomst vereisten in de nucleaire sector afzonderlijk zijn vermeld en niet opgenomen zijn in de cijfers energie. Cumulatief geeft dit voor deze sector volgende cijfers van 2011 tot 2014: 17% (2011), 17% (2012), 36% (2013), 46% (2014). Men stelt vast dat niet alleen het aantal incidenten toeneemt, maar vooral dat het aantal tussenkomsten die vereist zijn ook toeneemt, wat betekent dat de aanvallen op de kritieke energie infrastructuur efficiënter blijken na verloop van jaren, ondanks de maatregelen die men ervoor in plaatst stelt. De toename die men in 2013 vaststelt ten opzichte van het jaar voordien bedraagt 157% en zet zich het jaar daarop verder met 138% stijging. Het detail van de incidenten moduleert die cijfers enigszins: alle aanvallen zijn immers niet van een vergelijkbaar type. Sommige beperken zich tot het stelen van informatie, terwijl andere de controlesystemen trachten te beïnvloeden. Nog andere trachten zich toegang te verschaffen tot het systeemnetwerk. Een toenemende frequentie van het aantal interventies toont echter een tendens die eruit bestaat dat meer impact genererende aanvallen worden vastgesteld in de loop der jaren en dat de energiesector er een bijzonder doelwit voor is: dit wordt bevestigd indien men

weet dat het totaal aantal incidenten in de energiesector gedaald is van 59% in 2013 naar 32% in 2014. Het mag echter geen geruststelling zijn dat het aantal incidenten afneemt maar dat het resterende aantal een grotere impact heeft op de sector en meer interventies vereisen. In hun rapportage maakt men bovendien gewag van een gebrek aan detectie van alle incidenten en intrusies: meer dan de helft van de gedetecteerde aanvallen zijn echter onder te brengen in een categorie die meer sofisticatie vergt[20] dan andere aanvallen die eruit bestaan servers onbruikbaar te maken door ze te overspoelen met grote aantallen requests. In het bijzonder voor kritieke infrastructuur en kritieke energie infrastructuur, gaat men ervan uit dat zich veel meer incidenten voordoen maar dat niet alle incidenten worden gedetecteerd of gemeld buiten het bedrijf omwille van de gevoeligheid van de informatie enerzijds maar ook omwille van de reactie die dat zou kunnen veroorzaken bij gebruikers of overheid: de positie van private bedrijven bestaat uit een zekere terughoudendheid in de overgrote meerderheid van de gevallen. Hoewel het belangrijkste commerciële doel van een bedrijf eruit bestaat om winst te genereren en meer veiligheid dit voor een deel in de weg zou kunnen staan, zou een te grote gevoeligheid voor incidenten een slecht commercieel beeld kunnen geven van het bedrijf, of zelfs een beeld van beleidsombekwaamheid kunnen genereren ten opzichte van de verantwoordelijke overheid.

Een van de lessen die hieruit getrokken kunnen worden bestaat eruit dat het vrijgeven en delen van informatie van de sector kritieke energie infrastructuur een bijzonder gevoelig onderwerp is en blijft: daartoe gaat men in de VS uit van het geven van geclassificeerde informatieve briefings tussen betrokken partijen en overheid (FBI, DOE). Op vraag worden ook evaluaties uitgevoerd op de robuustheid van het netwerk door Industrial Control System Cyber Emergency Response Team (ICS-CERT[21]). In het bijzonder wordt de nucleaire sector hiervoor gescreend bovenop de veiligheidsvereisten die door het internationaal atoomagentschap worden opgelegd. Drie types screenings zijn mogelijk al naargelang de mate van controle die men wil nagaan op procedures en/of netwerkstructuur (ICS-CERT, 2013):

1.Network Architecture Verification and Validation (NAVV) bestaat uit een controle van de netwerkarchitectuur en de connecties die de

[20] APT: advanced persistent threat zijn aanvallen die een permanente toegang tot netwerken toelaten en lange tijd ongedetecteerd die toegang gebruiken voor het stelen van gegevens of controle te winnen over industriële controlesystemen.

[21] ICS-CERT is afhankelijk, van het US Department of Homeland Security en staat in voor de veiligheid van industriële netwerken en controlesystemen, met in het bijzonder kritieke infrastructuur. Daartoe werkt het samen met inlichtingendiensten, politiediensten en zowel regionale als federale overheden. Internationaal wisselt deze dienst informatie uit op internationaal vlak met Computer Emergency Response Teams (CERTs) van zowel de publieke als de private sector.

controlesystemen tot stand willen brengen: onverwachte datacommunicatie wordt hiermee in kaart gebracht.

2.Cyber Security Evaluation Tool (CSET) is een soort test die eruit bestaat het industrieel controlesysteem te toetsen op de wettelijke vereisten en nationale standaarden. Bovendien worden hiermee aanbevelingen gegeven om de gebruiker beter in staat te stellen die standaarden te bereiken.

3.Design Architecture Review (DAR) is een analyse van de verschillende verdedigingslagen waaruit een controlesysteem van kritieke infrastructuur is opgebouwd: het bestaat uit een evaluatie van de moeilijkheid voor toegangsverschaffing, gebruiksregels en protocols als ook de eenvoud om gegevens te exporteren uit het systeem. Deze evaluatie laat ook toe om afhankelijkheden van andere systemen bloot te leggen.

Het volstaat echter niet om over technische middelen te beschikken om te kunnen weerstaan aan de aanvallen op KEI of de nodige veerkracht te kunnen genereren om een getroffen infrastructuur opnieuw operationeel te krijgen. Drie elementen zijn daartoe vereist: de technische capaciteiten die passen in een organisatorisch kader, de publieke en private samenwerking die een optimale technische aanwending tegoed kan komen, en tot slot het noodzakelijke juridische kader en ondersteuning om mandaten van actoren vast te leggen en verantwoordelijkheden af te bakenen.

Een stroomleverancier verwoordde onlangs de angsten van de sector als volgt (Jennifer A. Dlouhy, 2013):

> "We have to treat the cyberthreat with the same respect that we give to forces of nature that impact our grid — hurricanes, floods, ice**.** We have to put the same comprehensive approach and the same attention to cyberthreats as we do to the other threats that impact our system. We have to fund it, we have to staff it, and we have to be prepared to respond as necessary."

In de sector werd gewag gemaakt van 10000 aanvallen per maand voor één enkele stroomleverancier. De gevoeligheid van het elektriciteitsnetwerk is volgens betrokkene niet enkel te wijten aan de opwekking van energie, maar ook door de verspreiding van de transmissielijnen en distributie-infrastructuur en ook de verscheidenheid van regulatoren die het geheel dienen te beveiligen.

Laat daarom de organisatie van de VS regulatoren en toezichthouders een belangrijk element zijn dat kan bijdragen tot die veiligheid. Het voorstel

van de bipartizane commissie om de veiligheid van het energienetwerk te beveiligen zou er daarom uit bestaan om een sectorwijde organisatie in het leven te roepen naar model van wat reeds voor de kernenergie bestaat (Institute for Nuclear Power Operations – INPO). Een dergelijke organisatie zou ervoor kunnen zorgen dat de informatiestroom tussen de overheid enerzijds en de private partners anderzijds op een meer georganiseerde en doeltreffende wijze kan worden gestuurd. In Canada bestaat een dergelijke structuur, ook al is die gemandateerd om cyberdreigingen voor alle kritieke sectoren in te schatten en naar vermogen te beperken. Pas onlangs (februari 2014) werden de technische vereisten daartoe door het standaardisatie instituut (National Institute of Standards and Technology –NIST) omschreven en baseert zich op bestaande vereisten om bedrijven in staat te stellen om de huidige cyberveiligheidstoestand te verduidelijken, de te bereiken doelen te omschrijven, prioriteiten te identificeren die toelaten de huidige toestand te verbeteren, de vooruitgang te becijferen en dialoog tussen alle betrokken partijen in de hand te werken. Een duidelijk onderscheid wordt dus gemaakt tussen de fysische dreiging enerzijds en anderzijds de cybernetische dreiging. De verantwoordlijkheden voor de fysische en de cybernetische beveiliging van kritieke energie infrastructuur krijgt in de VS reeds meer aandacht dan in Europa. Toch blijkt die verantwoordelijkheid verspreid over verschillende agentschappen en departementen hetgeen niet noodzakelijk tot een optimaal plan leidt. In de VS zijn het vooral drie departementen en instituten die die bescherming moeten zien voor elkaar te krijgen en daartoe verschillende richtlijnen en plannen uitschrijven: de belangrijkste actoren zijn in deze het ministerie voor energie (Department of Energy –DoE), het departement Homeland Security (DHS) en het National Institute of Standards and Technology (NIST). In wat volgt zullen we elk van deze actoren met hun taken hieromtrent kort toelichten.

Zo is het ministerie van energie verantwoordelijk (Department of Energy –DoE) voor het National Infrastructure Protection Plan (NIPP) en het Cybersecurity for Energy Delivery Systems (CEDS) dat onderzoek wenst te steunen en de operatoren wenst aan te zetten te investeren in cyberbeveiliging. Bovendien is het federaal agentschap (Federal Energy Regulatory Commission -FERC) verantwoordelijk voor de algemene betrouwbaarheid van het netwerk en is het dus bevoegd om die na te trekken en de realisatie van verbeteringen daartoe af te dwingen: in de praktijk is het North American Electric Reliability Corporation (NERC) dat voor de praktische uitvoering ervan instaat en daartoe verplichte en afdwingbare standaarden oplegt aan de leveranciers. Daarenboven identificeert NERC de acties die te ondernemen zijn door de elektriciteitssector na de ontvangst van snelle waarschuwingen van dreigingen, of die nu worden gegenereerd in de VS (DHS; Electricity Sector Information Sharing and Analysis Centre - ES-ISAC) of daarbuiten

(Public Safety Canada). ES-ISAC is ook verantwoordelijk voor de uitwisseling van informatie tussen alle actoren van de elektrische sector voor de bescherming van kritieke infrastructuur, maar ook daarbuiten: het werkt samen met de ISAC's van de andere energiesectoren om incidentanalyse een gemeenschappelijke meerwaarde te geven. Zowel informatie als bijstand worden met die sectoren uitgewisseld om de fysische en de cybernetische beveiliging te optimaliseren. Ook de internationale samenwerking wordt door dit orgaan aangemoedigd door de organisatie van oefeningen met bijvoorbeeld Canada en Mexico.

Het staat dus vast dat het DoE, in tegenstelling van wat men zou verwachten, niet alle bevoegdheid heeft om de cyberbeveiliging van de energie infrastructuur tot een goed einde te brengen. In het bijzonder heeft het geen regulerende bevoegdheid ter zaken: de standaarden van de sector worden door andere actoren bepaald en afgedwongen. Hooguit kan het een stimulerende rol hebben voor de samenwerking met private partners maar die rol is dan ook belangrijk: door de overkoepelende positie van het departement kan het die samenwerking tot stand brengen voor alle energievormen (olie, gas en elektriciteit) en biedt het dus op termijn een meerwaarde voor de coördinatie van de aanpak van die dreiging die voor iedere sector mogelijk anders zou kunnen verlopen[22]. In die aanzet tot samenwerking wil het dan ook ver gaan en ligt het aan de basis van de coördinatie met instituten en of commissies als NIST en NERC, bijvoorbeeld voor de ontwikkeling van een aan de elektriciteitssector specifiek *Risk Management Process* richtlijn dat voor iedere leverancier gepersonaliseerd is. De optimalisatie van de samenwerking en coördinatie tussen diensten wordt nagestreefd door ook op ministerieel niveau informatie uit te wisselen, zo bijvoorbeeld tussen DoE, DHS, orde- en inlichtingendiensten en dan in het bijzonder voor de snelle waarschuwing van aan de gang zijnde aanvallen en dreigingen.

Het DHS blijkt het departement bij uitstek die de cyberbeveiliging van kritieke infrastructuur in stand moet houden in de tijd: het is wel degelijk een lange termijndoelstelling gezien de voortdurende verandering van de dreiging. Het is in dit geval niet mogelijk om de wording van een dergelijk verdedigingsplan als voltooid te beschouwen op een vergelijkbare manier als met een fysische bedreiging of een plan daaromtrent. Ook al moet de

[22] Onder het Cybersecurity for Energy Delivery Systems (CEDS) worden vijf porgramma's ondersteund die een leidraad hebben onder de vorm van een 'Roadmap to Achieve Energy Delivery Systems Cybersecurity'. De vijf motto's die dat doel moeten helpen realiseren zijn onder te brengen in volgende hoofdingen: 'build a Culture of Security', 'Assess and Monitor Risk', Develop and Implement New Protective Measures to Reduce Risk', 'Manage Incidents', 'Sustain Security Improvements'.

efficiëntie daarvan voortdurend aan het licht van mogelijke en specifieke dreigingen worden gehouden, toch vergt een cyberdreiging meer waakzaamheid en meer regelmaat in de herziening van de verdedigingssystemen. Daartoe moet een snel waarschuwingsnetwerk tot stand komen van aan de gang zijnde aanvallen en uitwisseling daaromtrent met ander departementen. Het communicatiecentrum dat DHS met dat oogmerk heeft tot stand gebracht, werkt dat in de hand: het *National Cybersecurity and Communications Integration Centre* (NCCIC) wisselt in dat verband de informatie uit tussen federale departementen, staten, lokale en internationale overheden om *situation awareness* tot stand te brengen. Daarenboven is het verantwoordelijk voor de coördinatie en verspreiding van informatie naar private entiteiten die in het bezit zijn van het elektriciteitsnetwerk met als doel dat tijdig de noodzakelijke maatregelen kunnen worden genomen om een aanval af te wenden. Door de uitwisseling van die informatie is DHS ook in staat om haar eigen ICS-CERT (*Industrial Control Systems Computer Emergency Response Team*) zo vroeg mogelijk aan te wenden om een incident op te lossen of een aanval op kritieke energie infrastructuur te ontwijken.

Het National Institute for Standards and Technology (NIST) daarentegen is verantwoordelijk voor de standaarden en hun toepassing en in die hoedanigheid is het agentschap een sleutelpartner voor het tot stand brengen van de noodzakelijke interoperabiliteit tussen departementen voor optimale reactie tegen incidenten en uitwisseling van werkbare verdedigingsmechanismen. Maar dit is geen vrijblijvend engagement: het instituut is immers bij verordening[23] verplicht om de eigenaars en operatoren bij te staan in de coördinatie van activiteiten teneinde cyber risico's op een kosten-efficiënte en flexibele manier aan te pakken. Het instituut biedt dus een zeer concrete invulling van wat men onder standaarden zou kunnen verwachten.

Het zwakste punt blijft echter ook in de VS het distributiesysteem en dit om de eenvoudige reden dat dit niet onderworpen is aan dezelfde standaarden die gehanteerd worden voor energie infrastructuur. In de VS is 63% van dergelijke distributiesystemen in private handen en toch stelt men daar nu al de vraag naar de betrouwbaarheid of eerder de kwetsbaarheid van het gehele systeem als gevolg van de enige zwakte van het distributienetwerk.

Oplossing voor de VS: ofwel nieuwe standaarden voor distributie ofwel onder bevoegdheid van een agentschap voor organisatie van cyberverdediging

[23] Executive order 13636 van 2013.

zonder de beperking te traag te zijn of onbevoegd voor de afdwingbaarheid van die standaarden. Het antwoord moet flexibel genoeg zijn om het hoofd te kunnen bieden aan de nieuwste dreiging zonder al te veel tijd te verliezen.

Ook in Canada werd een dergelijke centralisatie en coördinatie nagestreefd voor het tot stand komen van de richtlijnen: het mandaat van het departement Public Safety Canada is vergelijkbaar met dat van het Amerikaanse DHS en staat in voor de nationale en publieke veiligheid. De uitvoering en aanwending van de standaarden ligt echter volledig binnen de bevoegdheid van de regionale besturen en in het bijzonder voor de betrouwbaarheid van elektrische installaties.

3.3. De Europese Unie

Vooreerst is het kader slechts in 19 van de 28 lidstaten omschreven in een cyberstrategie. In acht landen is er die niet maar bij de overige lidstaten is die van zeer uiteenlopende samenstelling. In de minderheid van de gevallen is die strategie kracht bijgezet door de daartoe relevante wetgeving, informatiebeheersing en plannen voor bescherming van kritieke infrastructuur. In het bijzonder is die garantie van informatiebeheersing belangrijk voor de kritieke energie infrastructuur die de garantie moet kunnen geven aan private bedrijven dat hun informatie uitwisseling met de overheid en het gebruik door interventiediensten niet in het nadeel zal zijn van hun concurrerend vermogen. In ons land bestaat een strategie sinds 2012, maar de gebruikte bewoordingen zijn zeer vaag en vooralsnog zijn hiermee niet de instrumenten beschikbaar die in andere landen ter beschikking worden gesteld. De strategische objectieven van de strategie zijn als volgt te omschrijven (Cyber Security Strategy, 2012):

- streven naar een veilige en betrouwbare cyberspace met respect voor de fundamentele rechten en waarden van de moderne samenleving: evenwicht tussen nationale veiligheid en kernwaarden van de moderne samenleving;
- de optimale beveiliging en bescherming van kritieke infrastructuren van overheidssystemen tegen de cyberdreiging: kritieke infra levert waarden en diensten die te belangrijk zijn om een verstoring toe te laten. Veiligheid van de ICT systemen van die infra en van de overheid vormen dus een prioriteit;
- ontwikkelen van eigen cyber security-capaciteit voor een onafhankelijk veiligheidsbeleid en een gepaste reactie op veiligheidsincidenten.

Vervolgens zijn operationele eenheden noodzakelijk die kunnen inspringen wanneer de meest kritieke elementen van de energie infrastructuur worden bedreigd: rekening houdend met de nieuwe benadering die bij aanvang van deze studie werd gegeven aan kriticiteit, dient een inventarisatie te gebeuren van die elementen die cruciaal zijn voor de rest van het distributienetwerk en ook voor andere domeinen.

Ten slotte zijn de partnerschappen met de private sector een essentieel onderdeel van een efficiënte bescherming omdat de infrastructuur in de meerderheid van de gevallen eigendom is van private bedrijven: de landen die in de EU het verst gevorderd zijn met dergelijke overeenkomsten zijn

Oostenrijk, Nederland, Spanje en het Verenigd Koninkrijk (BSA, 2015; p.5). Tegelijk zijn dit ook de landen van wie de cyberverdediging aangepast is door sector specifieke overeenkomsten.

In een vergelijkende studie omtrent de inspanningen van alle EU lidstaten in dit domein erkennen de meeste de inspanningen die door de EU in die richting worden ondernomen: in het bijzonder is de toegenomen aandacht van de EU voor kritieke infrastructuur een prioriteit die door vele landen vertaald moet worden naar alle lidstaten. Echter de nationale verschillen zorgen voor een spanningsveld tussen de bedoeling en de realisaties wat aanleiding geeft tot mogelijke kwetsbaarheden in de Europese benadering: zowel de nationale veiligheidspolitiek, hun wettelijke toepasbaarheid en operationele verschillen dragen daartoe bij. Samenwerking tussen publieke en private entiteiten is bovendien maar in de vijf voormelde gevallen werkzaam: een grote meerderheid van het enige werkbare voor de organisatie van de bescherming van kritieke energie infrastructuur in het algemeen en cyber verdediging in het bijzonder hangt af van de positionering van private bedrijven die de dienstverlening van operationele energiedistributie in handen hebben. In de meerderheid van de gevallen is dit dus nog onbenut terrein. De lidstaten hebben dan wel alle operationele eenheden (CERTs) in werking gesteld, elk heeft zijn eigen ervaring en werkingsmiddelen en die zijn niet noodzakelijk op elkaar afgestemd. De inspanningen in dit domein zullen bovendien moeten worden onderhouden op termijn: het is geen eenmalige investering die later zou kunnen worden afgebouwd wel integendeel.

Daarnaast zijn nog een aantal wettelijke instrumenten mogelijk die de coördinatie en de efficiëntie zouden kunnen verbeteren: maar ze zijn omstreden en zouden elementen in wetteksten kunnen gieten die ook in Europa en zelfs in ons land evenzeer omstreden zijn zoals bijvoorbeeld de uitwisseling van informatie tussen private bedrijven en inlichtingendiensten. Ook al zal dit naar alle waarschijnlijkheid nu reeds occasioneel gebeuren in geval van ernstige dreiging, het bestaan van een wettekst die de systematiek ervan regelt is vanwege de gevoelige materie niet vanzelfsprekend, zelfs in de VS. In vergelijking is de VS in hun organisatie ver gevorderd in het idee dat kritieke energie infrastructuur een bijzondere bescherming moet genieten zowel voor wat de fysische als de cybernetische bescherming betreft; we weten dat in de EU deze uitwisseling van informatie en de samenwerking van private partners ook gevoelig ligt. Daar waar in de VS een instituut zich toespitst op het uitwerken van standaarden voor het realiseren van interoperabiliteit, is dit in de EU nog helemaal geen uitgemaakte zaak.

In haar cyber strategie wordt voor de EU nog veel werk voorzien: de stand van zaken lijkt te wijzen op een in 2013 niet voltooid werf (European Commission, 2013).

> "Europe will remain vulnerable without a substantial effort to enhance public and private capacities, resources and processes to prevent, detect and handle cyber security incidents. This is why the Commission has developed a policy on Network and Information Security (NIS). The European Network and Information Security Agency (ENISA) was established in 2004 and a new Regulation to strengthen ENISA and modernize its mandate is being negotiated by Council and Parliament. In addition, the Framework Directive for electronic communications requires providers of electronic communications to appropriately manage the risks to their networks and to report significant security breaches."

De vaststelling dat Europa kwetsbaar is en dat de samenwerking met de dienst voor extern optreden (EEAS) noodzakelijk blijkt, werd toen al vastgelegd in het document dat als basis zou dienen voor verder legislatief en vormingswerk enerzijds en anderzijds voor partnerschappen met de private sector. Van interoperabiliteit zoals we die in de VS hebben zien nastreven is hier echter nog geen sprake: de samenwerking met de dienst voor extern optreden is daarvoor noodzakelijk volgens de strategie[24] en dient nog werk te maken van onderzoek en ontwikkeling tijdens het laatste kaderprogramma voor het realiseren van dat doel[25]. Een belangrijk onderdeel van het interoperabiliteitsprobleem reduceert zich in de EU-visie dus tot een verantwoordelijkheid van het Europees Defensieagentschap (EDA): een bijzonder aandachtspunt blijkt in dit agentschap weggelegd voor R&D om dit aspect nader te onderzoeken. Een duidelijk verschil met de Amerikaanse visie is dat de EU in deze niet echt gericht is op het aspect cyberbeveiliging van kritieke infrastructuur in het algemeen en kritieke energie infrastructuur in het bijzonder. De benadering die er hier aan wordt gegeven kadert dus eerder in militaire activiteiten dan in het beveiligen van de netwerken voor dagelijks

[24] Assess operational EU cyberdefence requirements and promote the development of EU cyberdefence capabilities and technologies to address all aspects of capability development - including doctrine, leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability.

[25] Horizon 2020 will support security research related to emerging ICT technologies; provide solutions for end-to-end secure ICT systems, services and applications; provide the incentives for the implementation and adoption of existing solutions; and address interoperability among network and information systems. Specific attention will be drawn at EU level to optimizing and better coordinating various funding programmes (Horizon 2020, Internal Security Fund, EDA research including European Framework Cooperation)".

gebruik en de exploitatie van slimme netwerken in het kader van de optimalisatie van de distributie en de investering die hiervoor in de EU op korte termijn dienen te worden gedaan. In de VS geniet deze problematiek een bijzondere aandacht, zowel voor het inschatten van de dreigingen op die infrastructuur als voor het verbeteren van de bestaande beschermingsmaatregelen voor de bescherming van kritieke infrastructuur. De richtlijnen die het NERC hiervoor uitwerkt mogen echter geen exclusief karakter hebben: het feit dat standaarden worden uitgewerkt is een voordeel ten opzichte van wat er in de EU ter zake wordt gedaan, maar het blind vertrouwen aan dergelijke standaarden voor een zo snel veranderend milieu als het cyberdomein zou van een zekere naïviteit getuigen. Bovendien houdt het enig risico in voor een beperkte investering van private partners: deze zijn immers gesteld op hun winstmarge en kunnen zich in dat opzicht geen excessen veroorloven zonder voor een deel hun winstmarge te beperken. De goedkeuring van hun proactieve screening om cyberdreigingen van het energetische domein aan te pakken kunnen hen bovendien zwaar vallen: het gebruik van een ruimere dreigingsanalyse die potentieel meer gevoeligheden aan het licht zou kunnen brengen dan hen door die standaarden wordt opgelegd door NERC, moet de goedkeuring van het agentschap genieten. Maar de ontdekking van meer gevoeligheden en de niet beveiliging ervan kan private partners ook blootstellen aan boetes. De positie om dus slechts het vereiste minimum aan inspanningen te doen kan een logische conclusie zijn in een politiek die winst moet zien te maximaliseren. Deze discrepantie tussen de regelgeving en de te bereiken doelen is bekend bij FERC maar om die te realiseren moet een risicoanalyse de basis vormen van nieuwe vooruitgang in cyberverdediging van kritieke energie infrastructuur eerder dan standaarden die extern worden opgelegd en die slechts een minimale basis vormen voor beveiliging.

3.4. Juridische consequenties

Informatie-uitwisseling, standaarden en afdwingbaarheid, wettelijke bepalingen en coördinatie en nationaal cyber incident response planning in het domein van kritieke energie infrastructuur zijn enkele van de vele verantwoordelijkheden dat het nieuwe *cyber defense agency* van België zal moeten regelen of waarvoor een ander agentschap de verantwoordelijkheid en het mandaat zal moeten voor krijgen. Defensie kan in één of meerdere van deze verantwoordelijkheden bijdragen tot een coherente taakverdeling. Ook voor de NAVO is cyber, en in het bijzonder met betrekking tot de beveiliging van industriële controlesystemen een nog te beveiligen en op punt te zetten item. Vandaag de dag is het immers niet meer voldoende om over een eigen netwerk te beschikken dat voldoende beveiligd is, maar moeten ook alle toegangspoorten naar dat netwerk worden beveiligd. SACEUR, tijdens een toespraak bij het Koninklijk Hoger Instituut voor Defensie zegde in dit verband dat waar vroeger voldoening werd geschapen om alle toegangen te beveiligen, moet men binnen de Alliantie nu ook zekerheid hebben over het feit dat de toegang bij buren ook beveiligd is op een adequate manier of met andere woorden, daar waar de veiligheid van de buren vroeger hun eigen zorg was, is de veiligheid van buren nu vast en zeker ook een eigen probleem welk de Alliantie kopzorgen baart en in het bijzonder wanneer het over industriële controlesystemen betreft die de kritieke energie-infrastructuur van de Alliantie moet ondersteunen. Een belangrijk gevolg hiervan is in welke mate een aanval op een dergelijk systeem als dusdanig zal worden herkend (tot welke gevolgen is men bereid te wachten alvorens officieel te erkennen dat een aanval in uitvoering is), welke kwalificatie men aan die aanval wil geven (gaat het al dan niet over een aanval die men zou kunnen onderbrengen onder de definitie van een gewapende aanval), welke er de verantwoordelijken voor zijn en ten slotte welke reactie eraan moet worden gegeven. De kwalificatie van een aanval zal in zekere mate ook de reactie bepalen: hoewel er ook onder deskundigen discussie bestaat over het feit of cyberaanval al dan niet kan ondergebracht worden in de categorie van gewapende aanval[26], toch gaat men

[26] CCD CoE, 2013. p.54. Tallinn Manual on the International Law Applicable to Cyber Warfare, p.54
4. The International Group of Experts was divided as to whether the notion of armed attack, because of the term 'armed', necessarily involves the employment of 'weapons' (Rule 41). The majority took the position that it did not and that instead the critical factor was whether the effects of a cyber operation, as distinct from the means used to achieve those effects, were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack.

voor het beantwoorden van die vraag tijdens een gewapend conflict uit van de vaststelling dat de gevolgen die vergelijkbaar moeten kunnen zijn met deze die door een conventionele kinetische aanval zouden kunnen worden aangericht (schade, gewonden en/of doden) en die om die reden gelijk worden gesteld aan de aanwending van geweld. De criteria die hiermee worden in rekening gebracht, zijn belangrijk in het kader van cyberaanvallen en hun categorisatie maar ook en in het bijzonder voor het belang van kritieke energie-infrastructuur als doelwit van aanvallen die aanleiding zouden kunnen geven tot de uitoefening van het recht tot zelfverdediging. Zonder te willen pretenderen een exhaustieve lijst voor te stellen zijn te beschouwen elementen (CCD CoE, 2013; p.42 e.v. Definitie *use of force*-eigen vertaling):

-ernst van de incidenten: in de schatting zal de kans om te categoriseren onder het gebruik van geweld, overeenstemmen met de mate waarin kritieke nationale belangen worden aangevallen (omvang, duur en intensiteit van de gevolgen zullen hiervoor in aanmerking worden genomen);

-de onmiddellijke zichtbaarheid van de gevolgen: snellere gevolgen kunnen moelijker aanleiding geven tot een vreedzame regeling van een eventueel dispuut;

-causaal verband: een incident waarbij duidelijk wordt dat er een causaal en onmiddellijk gevolg is aan verbonden heeft meer kans om aanzien te worden als de aanwending van geweld;

-invasief karakter: algemeen wordt aanvaard dat hoe meer moeite er is gedaan om een systeem of een domein binnen te dringen (en zeker indien het beveiligd is), hoe invasief de aanval is;

-meetbare effecten: hoe meer effecten meetbaar zijn of weer te geven zijn in concrete getallen hoe eenvoudiger deze ondergebracht kunnen worden onder het gebruik van geweld dan subjectieve gevolgen;

-militaire karakter: het gebruik van militaire middelen vergroot de kans dat hier wel degelijk geweld wordt gebruikt;

-staatsbetrokkenheid: hoe nauwer het verband tussen de acties van een overheid en de feiten die zich in het cyberdomein afspelen, de groter de kans om als gebruik van geweld te worden aanzien;

---

5. In the view of the International Group of Experts, the term ‘armed attack’ is not to be equated with the term ‘use of force’ appearing in Rule 11. An armed attack presupposes at least a use of force in the sense of Article 2(4). However, as noted by the International Court of Justice, not every use of force rises to the level of an armed attack. The scale and effects required for an act to be characterised as an armed attack necessarily exceed those qualifying the act as a use of force. Only in the event that the use of force reaches the threshold of an armed attack is a State entitled to respond using force in self-defence.

-veronderstelde legaliteit: hetgeen niet door de wet of het gewoonterecht wordt beschouwd als zijnde illegaal is minder waarschijnlijk om beschouwd te worden als aanwending van geweld.

De aanwending van geweld zal echter niet voldoende zijn om zelf met geweld te reageren: daarom moet een aanval hebben plaatsgehad die te vergelijken valt met een gewapende aanval die de aanwending tot het recht van zelfverdediging' (art.51 van het VN handvest) verrechtvaardigt. Elementen die die inschatting mogelijk maken zijn zowel de schaal als de gevolgen van de aanval: een gewapende aanval heeft volgens het Tallinn manual een grensoverschrijdend karakter zonder dat het uitsluitend beperkt moet blijven tot statelijke interactie. Inderdaad de jurisprudentie ter zake heeft de experten in de Tallinn Manual de cyberaanval die aanleiding kan geven tot het recht op zelfverdediging uitgebreid tot proxy-groeperingen door te besluiten dat[27] een gewapende aanval niet alleen gekenmerkt wordt door reguliere troepen die een internationale grens overschrijden maar ook door irreguliere troepen die over die grens opereren en daar gewapend geweld gebruiken waarvan de gevolgen vergelijkbaar zijn met het geweld dat uit naam van een andere staat gebruikt zou worden en daardoor de betrokkenheid van die andere staat zou vastleggen (CCD CoE, 2013; p.57). Het recht op zelfverdediging dat hierdoor rechtmatig zou voorvloeien moet ook voldoen aan een aantal principes waaronder noodzakelijkheid, proportionaliteit, dreiging en dringendheid. Een element dat zou kunnen bijdragen om die principes beter in te vullen zou eruit kunnen bestaan definities te geven aan elementen als wat een vijandige actie of een vijandige intentie zou kunnen zijn die onmiddellijk aanleiding kunnen geven tot een repliek van een gelijkaardig geweldspectrum. Naast de wettelijke omschrijving van die principes die eraan moeten voldoen, kan binnen het kader van een alliantie in detail een omschrijving worden gegeven aan de toegestane reactie die automatisch zou worden gegenereerd indien een dergelijke vijandige intentie of actie wordt vastgesteld. Dit is net wat wordt bedoeld met de omschrijving van Rules of Engagement (RoE). Een sleutel, die in vele gevallen nog ontbreekt om een dergelijke methodologie toe te passen is de onomstootbare identificatie van de aanvaller. Dergelijke definities kunnen ook bijdragen tot het debat van wat als reactie is toegestaan onder de drempel van een gewapend treffen, in het bijzonder met betrekking tot attributie met andere woorden de identiteit van een schuldige in geval een aanval heeft plaatsgehad.

[27] [a]n armed attack must be understood as including not merely action by regular forces cross an international border, but also 'the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to' (*inter alia*) an actual armed attack conducted by regular forces, 'or its substantial involvement therein.

Deze attributie kan in het geval van een conventionele aanval al moeilijk blijken zoals blijkt uit het verslag van de aanval op de commerciële vlucht MH17: meer dan een jaar na het incident is er een rapport klaar voor de identificatie van de verantwoordelijke van de aanval. Echter, in het geval van een aanval op energie-infrastructuur die niet noodzakelijk zoveel slachtoffers zou genereren, zou de identificatie niet eenvoudiger zijn. Voor het geval dat een dergelijke aanval niet op een conventionele manier zou worden uitgevoerd, maar met cybernetische middelen, dan blijkt die identificatie nog moeilijker. Het feit dat een dergelijke identificatie van de verantwoordelijke *a priori* in de tijd wordt bemoeilijkt, maakt de invulling van de principes die op een rechtmatige wijze aanleiding kunnen geven tot een repliek in de praktijk onbruikbaar gezien de herkenning van een aanval moet gevolgd worden door een onomstotelijke identificatie van de verantwoordelijke *a priori* en niet *post facto*. En daarenboven is slechts een korte tijdspanne toegestaan tussen de initiële aanval en de reactie erop. Een uitstel zou een reactie kunnen laten interpreteren als een wraakactie in plaats van een uitoefening op het recht van zelfverdediging. Daarnaast is een reactie op het soeverein grondgebied van een Staat van waaruit de oorspronkelijke aanval werd georganiseerd niet vanzelfsprekend in geval de betrokken staat of de VN Veiligheidsraad geen toestemming hebben gegeven: afhankelijk van de context kan een onmiddellijke reactie nochtans vereist zijn en kan zelfs door de aangevallen staat een vraag zijn tot assistentie in het kader van collectieve verdediging (binnen het kader van een alliantie bijvoorbeeld). Onder aanval wordt immers een geweldsdaad verondersteld waarvan wordt aangenomen dat deze aanleiding kan geven tot schade, kwetsuren of zelfs dood: in die veronderstelling is het zelfs niet noodzakelijk dat een kinetische aanval wordt uitgevoerd en is die dus ook van toepassing op de gevolgen van een cybernetische aanval op kritiek energie infrastructuur. In deze benadering worden eerder de gevolgen in de plaats van de oorzaak in rekening genomen om een actie als een geweldsdaad en dus als een gewapende aanval te beschouwen: zo bijvoorbeeld de aanval op een SCADA-systeem van een elektrische centrale waardoor brand zou kunnen worden gesticht hetgeen aanleiding zou kunnen geven tot slachtoffers en/of grote schade. Zo is het ook gesteld met een SCADA aanval op een dam die benedenstrooms aanleiding zou kunnen geven tot grote schade of dit rechtstreeks dan wel onrechtstreeks zou worden aangebracht (bijvoorbeeld als gevolg van cascade-effecten of wat men in het gewoonterecht colaterale schade zou plegen te noemen). Oog hebben voor de gevolgen kan een duidelijke aanwijzing geven over het feit of een cyberintrusie al dan niet als een aanval beschouwd dient te worden: maar de analyse gaat verder dan dat. Niet alleen gevolgen vergelijkbaar aan een kinetische aanval komen voor die classificatie in aanmerking. Ook de cybernetische uitschakeling van de functionaliteit, zonder fysische schade is, volgens de meerderheid van de deskundigen ter zake, te beschouwen als een

aanval: zo is de uitschakeling van een computergestuurd controlesysteem van elektrische distributie dat ook, zelfs indien geen fysische herstelling van een van de componenten noodzakelijk zou zijn voor het herstel van de functionering van het netwerk: in dat geval is het voldoende vast te stellen dat de functionaliteit weggevallen is (CCD CoE, 2013; p.94) of zelfs dat de bedoeling bestond om die functionaliteit in het gedrang te brengen zonder evenwel een materieel tastbare schade aan te richten (Cfr. Ibid. argumentatie van regel 30 met betrekking tot cyber aanval). Het is zelfs in die omstandigheden mogelijk dat een dergelijke actie wordt op touw gezet teneinde een andere conventionele en kinetische aanval in te leiden die dan grotere schade zou kunnen aanrichten aan energetische infrastructuur door de afwezigheid van aangepaste middelen voor de verdediging en/of controle van kritieke energie infrastructuur. In dergelijke omstandigheden is het onklaar maken van een energetische infrastructuur, zelfs zonder schade, te beschouwen als een voorbereiding op de daarop volgende kinetische aanval en maakt het daardoor integraal deel uit van de aan de gang zijn de aanval en moet het dus worden gecatalogiseerd onder de noemer gewapende aanval.

In het algemeen wordt een bijzondere aandacht gevergd voor aanvallen die op installaties worden gepland die een bijzonder groot reservoir van energie betekenen, ook al zijn ze onder te brengen onder mogelijk militaire objectieven: zo moet een bevolking bescherming genieten onder het principe van proportionaliteit indien het in de nabijheid zou leven van een installatie als een kerncentrale, een dam, of dijken. Bijzondere voorzorg wordt in dat geval geboden: het feit om de productie van energie van een kerncentrale weg te nemen zou dan al niet als een aanval kunnen worden beschouwd, maar het feit om een dergelijke cyber actie in werking te stellen en als collateraal gevolg ervoor te zorgen dat het koelingssysteem van de reactorkern niet meer zou kunnen opereren wordt als een groot risico beschouwd omwille van de catastrofale gevolgen die het smelten van een nucleaire reactorkern met zich zou kunnen meebrengen. De installaties die in deze context volgens het Tallinn handboek een bijzondere aandacht vragen beperken zich tot de reeds voormelde, inclusief hun cybernetische infrastructuur. Ze hebben echter geen betrekking op chemische of petrochemische installaties.

De consequenties en de proporties van aanvallen komt nog meer tot uiting indien men weet dat de situatie van oudere geïnformatiseerde beheerssystemen tot zodanig ingewikkelde situaties leidt, dat het al de dag van vandaag tot de mogelijkheden behoort dat een industrieel proces wordt onderbroken en niet meer kan worden opgestart: reden hiervoor is eveneens de tendens om investeringen in R&D in dit domein terug te dringen. De mogelijkheid om oudere SCADA systemen te vervangen of te herstellen is immers in die mate beperkt, dat de falingen die zich vandaag voordoen niet

eens meer altijd kunnen worden verhaald op de initiële producent van het systeem: de complexiteit van het netwerk door aansluiting van meer en meer sensoren als een netwerk dat vandaag in staat moet zijn om bi-directionele communicatie mogelijk te maken, maken in sommige gevallen een SCADA systeem niet meer compatibel met de informatiestroom. De gevolgen kunnen een totale oncontroleerbaarheid van het proces als gevolg hebben. De beslissing om de laatste jaren zo veel mogelijk systemen aan een netwerk aan te sluiten, zonder daartoe noodzakelijk over de geëigende technische capaciteiten te beschikken noch van een adequate verdediging tegen aanvallen te hebben in werk gesteld, kunnen alleen maar tot de conclusie leiden dat de eventuele gevolgen van bestaande tekorten met gerichte aanvallen op gevoeligheden a priori had moeten aanleiding geven tot de uitwerking van een strategie: het onmiddellijke gevolg hiervoor is dat eventuele integratie van nieuwe systemen, weze het voor de opwekking van energie (alternatieve energievormen inbegrepen), maar ook voor de controle van industriële processen voor de aansluiting aanleiding zouden hebben moeten geven tot de nodige besluitvorming omtrent cybernetische beveiliging. Deze aanpassing zal ook voor de reeds bestaande systemen in werking moeten worden gesteld: voor systemen die deze beveiliging nog niet genieten wordt voor het ogenblik een inhaalbeweging noodzakelijk wil men in de toekomst aan dezelfde voorwaarden van veiligheid willen tegemoet komen.

3.5. Risicovolle energieopwekking

Gezien de juridische consequenties en de interconnectie van domeinen enerzijds en anderzijds na de vaststelling dat cyber ook in het gedeelte energie mee bepalend zal zijn voor de beveiliging, komt men tot de vaststelling dat in het vraagstuk ook een deel zal moeten gewijd worden aan het nucleaire: twee elementen verklaren dit. Vooreerst zal de komende jaren een belangkijk gedeelte van de energie nog steeds door het nucleaire worden geleverd. Indien al in het Westen na de ramp in Fukushima een tendens is gegroeid om in sommige gevallen snel van kernenergie af te stappen, dan is dat in de groeilanden zeker niet het geval, wel integendeel: de groei kan enkel met de beschikbaarheid van kernenergie in die landen worden gerealiseerd aangezien het 24/24 en 7/7 een stabiele output genereert. Alternatieve bronnen kunnen immers niet voldoen aan de piekvraag en fluctueren zelfs al naargelang de weersomstandigheden hetgeen niet compatibel is met een maximale rendabiliteit die noodzakelijk is voor winstmaximalisatie. De economische return van hernieuwbare bronnen is bovendien slechts haalbaar voor de producent in geval van subsidies, zoals dat ook in het begin van de nucleaire industrie werd toegepast. Vervolgens kan men er niet onderuit dat de klimaatdoelstellingen als gevolg hebben dat een lagere koolstofuitstoot moet worden nagestreefd en dat het nucleaire de facto een van de oplossingen is die daartoe kan bijdragen.

Kernenergie als een essentieel element in het beschikbare energiepallet vergt echter omwille van zijn potentieel aan catastrofale gevolgen een bijzondere aandacht in zake veiligheid. In de Angelsaksische literatuur maakt men onderscheid tussen de termen “safety en security”, daar waar dit bij ons wordt omschreven onder één verzamelnaam: veiligheid. De taken blijven: naast beveiliging van de technologie moet ook het veilig gebruik ervan worden verzekerd. De Angelsaksische term zullen we dus voor de volledigheid van dit betoog omschrijven als enerzijds veiligheid en beveiliging. Onder beveiliging moet dan worden verstaan dat men zowel de niet afwending naar militaire doeleinden zal moeten verzekeren maar ook de bescherming van de infrastructuur tegen moedwillige aanvallen en dit tegen interne en externe dreigingen. De ervaring heeft geholpen om vooruitgang te boeken voor wat de beveiliging betreft van de garantie tot energieproductie in een proliferatie-resistente benadering, de fysische beveiliging, en ten slotte de cybernetische beveiliging.

3.5.1.Proliferatie resistentie

Met betrekking tot de niet afwending van de technologie voor militaire doelen enerzijds maar ook de zorg van non-proliferatie van gevoelige technologie heeft in het dossier Iran een belangrijke rol gespeeld in de ervaring van de Westerse landen. Het meest kritische element dat in de keten van de technologie hiervoor in aanmerking zou kunnen komen is uiteraard de aanrijking van kernbrandstof en de rechtmatige vraag die landen kunnen hebben om dit gedeelte machtig te zijn. De *incentives* om de aanrijking in handen te houden van die landen die de technologie reeds bezitten heeft vanuit het standpunt van de klanten een gevoel van afhankelijkheid gecreëerd. Het is net dit gedeelte van de cyclus dat door Iran wou gecontroleerd worden. Om in de toekomst een valabel alternatief te bieden werd het idee geopperd om een internationale fuel bank op te richten om prangende noden te kunnen opvangen: de Kazakse fuel bank zou de brandstofzekerheid moeten garanderen vanaf 2017 en het is de goede werking van het mechanisme dat het nodige vertrouwen zal moeten wekken om landen in de toekomst van eigen aanrijkingsfaciliteiten te laten afzien. Nog beter ware het indien mogelijk zou zijn om een gelijkaardig statuut te kunnen genieten als het Euratom Supply Agency, waarbij wordt verondersteld dat de deelnemende landen een deel van hun soevereiniteit omwille van de veiligheid, de doelstellingen van non-proliferatie, willen opgeven en de noodzakelijke middelen daartoe in gemeen willen hebben. Een dergelijk agentschap zou voor een groot gedeelte de traceerbaarheid van de kernbrandstof kunnen documenteren en zodoende de nauwelijks haalbare verificatiedoelstellingen van het Internationaal Atoomagentschap (IAEA) verlichten. Het bestaande optierecht en exclusiviteitsrecht van het Euratomverdrag dat in de EU al sinds 1957 van kracht is, hebben binnen de landen van de EU een vorm van betrouwbaarheid gegenereerd voor wat de beschikbaarheid van die brandstof en dus onrechtstreeks de beveiliging, de beschikbaarheid van de output en traceerbaarheid van die energievorm gegarandeerd.

3.5.2.Fysische beveiliging

Naast de afscherming van de technologie voor militaire doeleinden is er in iedere nucleaire faciliteit of in landen die eraan denken om een dergelijke technologie op te starten een zorg om de fysische beveiliging ervan te kunnen verzekeren. Ook in de Europese Unie is dit een belangrijke zorg gebleken, onder meer door de mogelijke gevolgen aan een nucleair incident verbonden, vooral sinds de ramp van Fukushima en de terroristische aanslagen van 9/11. Nucleaire veiligheid, (lees beveiliging) vanuit civiel (commercieel) of militair oogpunt, wordt in de EU gebaseerd op een reeks teksten en hun implementatie

te weten: de EU Common Foreign Security Policy (1993); European Security Strategy (2003); EU Strategy Against Proliferation of Weapons of Mass Destruction (2003); EU Counter Terrorism Strategy (2005); New lines for action in combating the proliferation of WMD and their delivery systems (2008). In de onderhandelingsplannen voor toetreding door nieuwe landen wordt zelfs een instrument voorzien door de Unie: met dat instrument wil de Unie in pre-accessie fase al voorzien in de samenwerking inzake nucleaire veiligheid en uitwisseling creëren tussen kenniscentra (bijvoorbeeld de CBRN Centres of Excellence). De controle van export van materiaal voor tweeërlei gebruik (dual use items), wordt onder een speciaal regime gerealiseerd dat commerciële activiteit toelaat onder dien verstande dat niet wordt bijgedragen tot de proliferatie van materiaal dat voor wapens en/of wapensystemen zou kunnen worden gebruikt (EU dual use regulation). Verder hebben ook andere internationale fora gevolgen voor de werking van de EU: zowel het atoomagentschap, de G8, en de VN hebben grondteksten/verdragen waarop de Unie zich baseert om zijn richtlijnen en andere werkingsdocumenten te steunen. Deze kruisbestuiving van internationale en "binnenlandse" EU-documenten heeft zeer praktische samenwerkingsgevolgen: na de ramp in Japan werd bijvoorbeeld door de EU een grootschalige stress-test uitgevoerd op alle interne installaties. De voormelde documenten en verdragen hebben echter als resultaat dat ook buurlanden met nucleaire installaties, of met plannen om die te bouwen, de veiligheidscontrole van die test hebben willen ondergaan op vrijwillige basis. Maar ook intern de EU is gebleken dat aanpassingen vereist zouden kunnen zijn in installaties. We hebben al gezien dat het Euratom verdrag als referentie dient voor andere regio's en een klimaat van controle door buur- en of partnerlanden kan genereren. Meer specifieke teksten uitgebracht met betrekking tot nucleaire veiligheid werden geconcipieerd als gevolg van belangrijk gebeurtenissen of grote rampen waaruit lessen werden getrokken. Daarenboven heeft dit geleid tot de aanpassing van de Euratom-Richtlijn (2009/71/Euratom van 25 juni 2009) die voortaan de veiligheid van nucleaire installaties reguleert. In het bijzonder in het kader van landen die de technologie voor het eerst willen in gebruik nemen wordt uitgegaan van een operationele werking van om en bij de 40 jaren voor een kerncentrale (Smedts, 2015): over dit traject moet zowel een economisch als een politiek stabiel klimaat worden gegenereerd wil men private partners overhalen om die investering te doen. Maar daarboven moet men ervoor zorgen dat ook het geopolitiek kader de nodige stabiliteit verschaft die ervoor zorgt dat geen lokaal conflict de veilige exploitatie van een dergelijke installatie de weg zou kunnen staan. In Turkije is die beveiliging bijvoorbeeld een bijzonder aandachtspunt in het kader van mogelijke terroristische activiteit. De plannen die het land voorziet gaan uit van een dreiging afkomstig van buiten een kerninstallatie maar niet uitzonderlijk: evenveel kans bestaat om een samenwerking te zien met een

interne vijand die eventueel tot sabotage zou kunnen leiden. Maar ook dat vervolledigt slechts deels het dreigingslandschap: aangezien het land in een regio gelegen is die aan het Midden-Oosten grenst, wordt in dit geval ook rekening gehouden met een raketdreiging vanuit de meer onstabiele regio's van het Midden-Oosten te weten Syrië of Irak. In de plannen voor de bescherming van kritieke infrastructuur wordt daarom ook de bescherming van een rakettenschild in rekening gebracht (Center for Economics and Foreign Policy Studies, 2015; pp.18 e.v.). In een voorgaande studie werd om dergelijke redenen al vermeld dat het niet noodzakelijk raadzaam leek, of op zijn minst in vraag diende te worden gesteld of het opportuun zou zijn om in een geopolitiek onstabiele regio een dergelijke technologie in werking te stellen. Daarboven dient men zich ook af te vragen of in een dergelijke regio een private investeerder in staat kan zijn om de onvolmaakte beveiliging in bijna oorlogstoestanden kan worden aangeschreven. Op zijn minst zal in dat geval een participatie van de staat nodig zijn. In het vooropgestelde levensduur van een dergelijke installatie (+/-40 jaren) zou een zekere vorm van stabiliteit dan ook moeten kunnen worden gegarandeerd wat vandaag niet meer zo vanzelfsprekend lijkt. Als dan al een garantie kan worden bekomen die in een verdrag worden vastgelegd, dan is dat nog niet noodzakelijk toepasbaar voor proxy-groeperingen of terroristische organisaties. Tegelijk laat dit in het geval van Turkije ook toe om te genieten van de ervaring die de andere landen reeds hebben in de materie: robuustheid kan in dat geval variëren al naargelang de leverancier (hetzij privaat of publiek) en de intensiteit waarmee aan veiligheid wordt gedacht in verhouding tot de kosten die dat genereert. Bovendien is de bedreiging waartegen in dit geval moet worden beschermd gericht op de output van een centrale, maar in werkelijkheid moet de beveiliging nog beter voor de vrijwaring van eventuele gevoelige stoffen, bronnen, etc. Als afweging moet men zich de vraag stellen of zelfs in onze contreien een stabiel politiek klimaat kan worden verzekerd. Tegelijk ken men niet ontgaan aan het feit dat het nucleaire nog steeds deel uitmaakt van een strategisch koolstofarm energiepallet en bijdraagt aan de realisatie van energetische diversificatie: dat men zich nog steeds in geen politiek stabiel klimaat bevindt, bewijst de situatie in Oost-Oekraïne uitgebreid.

3.5.3.Cybernetische beveiliging

Zoals in eerder hoofdstuk aangehaald is naast de fysische veiligheid ook de cybernetische veiligheid belangrijk voor de beveiliging van nucleaire technologie. In het onderwerp dat ons in dit dossier aanbelangt concentreert het cybernetische twee gevoeligheden te weten enerzijds de beveiliging van industriële controlesystemen en anderzijds de beveiliging van nucleaire

installaties die een bijzondere bescherming moeten genieten vanwege het mogelijk catastrofale gevolg van incidenten in dit domein. Niet alleen de zekerheid van productiviteit kan op die manier worden gegarandeerd maar ook de veilige operaties: een element dat slechts sinds enkele jaren daarin aan belang heeft gewonnen is het belang van beveiliging van centrales tegen die cybernetische dreiging. Het zijn voornamelijk de incidenten in Iraanse faciliteiten na besmetting van het Stuxnet virus die hebben duidelijk gemaakt dat industriële controlesystemen wel degelijk een fysisch gevolg kunnen hebben. Twee elementen dragen hiertoe bij: vooreerst is er de groei van het besef van kwetsbaarheden door de recurrente aanvallen op commerciële industriële controlesystemen en de meerkosten of in het geval van commerciële actoren de verliespost die dit automatisch genereert, hetzij door schade hetzij door de noodzakelijke investeringen om zich te beveiligen tegen een niet noodzakelijk voorspelbare dreiging. Vervolgens is sinds 2010 ook duidelijk gebleken dat die zwakheden zich ook in de bijzonder beschermde en gemonitorde nucleaire technologie voordeden. In Iran is op een dergelijke wijze zelfs een militaire installatie zwaar beschadigd, hetgeen bij vele landen vragen heeft doen rijzen met betrekking tot de optimale manier om ook civiele installaties te beveiligen. Tijdens de conferentie omtrent computerveiligheid in een nucleaire wereld, bevestigde directeur-generaal Amano[28]:

> "Last year alone, there were cases of random malware-based attacks at nuclear power plants, and of such facilities being specifically targeted…Computers play an essential role in all aspects of the management and safe and secure operation of nuclear facilities, including maintaining physical protection, and thus it is vitally important that all such systems are properly secured against malicious intrusions".

Een initiatief van het internationaal atoomagentschap wil daarom tegen december 2016 het debat aantrekken omtrent een gedragscode voor het garanderen van cyberveiligheid in de nucleaire industrie. Die veiligheid is veel moelijker in stand te houden tegen het moedwillig beschadigen van industriële computersystemen in de nucleaire industrie door de actie van overheden of van hackers. Daarom wordt het debat in een ministeriële kring aangevat: de bedoeling is om duidelijke krijtlijnen te trekken waarbinnen de belangrijkste en de meest vermogenden actoren zouden moeten kleuren. In het verlengde daarvan heeft het gewoonterecht aangetoond in welke mate, en dit zowel tijdens als in de aanloop naar een conflict nucleaire installaties een bijkomende bescherming zouden moeten kunnen geschieden.

[28] IAEA International Conference on Computer Security in a Nuclear World, Wenen. 1 Juni 2015

Naast cyberveiligheid die moet worden gegarandeerd, zijn de kostprijs en de uitstoot van broeikasgassen elementen die mee de toekomst van die technologie zullen bepalen. De zware investeringen die het voor Westerse economieën moeilijk maakt om dergelijke investeringen te financieren over een lang traject, zorgen voor een uitstel van het opportuniteitsvenster om in de toekomst in Europa nog een leider in de markt te zijn van deze technologie. De voortdurende investeringen die groeilanden aanzetten om wel nog in deze technologie te investeren zou de Westerse landen van die nieuwe polen afhankelijk kunnen maken voor leveringen van centrales in de toekomst. Een dergelijke situatie zou ongetwijfeld leiden tot fysische en cybernetische veiligheidsimplicaties die eigen zijn aan de bouwer van de centrales, en mogelijk ook gevolgen kunnen hebben op de energiedensiteit (de verhouding tussen het reële output-vermogen en het nominale vermogen) en dus de energiezekerheid. De kosten van die technologie zullen echter voortaan ook rekening moeten houden met meer uitstoot broeikasgassen bij andere technologieën en het verlies dat daaraan gekoppeld is. Dit kan in de toekomst meer en meer een bepalend element zijn om een energie-infrastructuur al dan niet te catalogiseren onder de noemer "kritiek". Immers, de verhoogde uitstoot die een aangetoonde impact heeft op het klimaat, heeft ook securitaire aspecten die eraan verbonden zijn. Met betrekking tot dit laatste heeft men in een recente studie voor België aangetoond dat de uitstap uit kernenergie als gevolg zou kunnen hebben dat de uitstoot van broeikasgassen zou toenemen met 60% tegen 2025. Vandaag is de bijdrage van het nucleaire om en bij de 23 TWh op jaarbasis (~30% jaarbijdrage) tot aan de sluiting van de centrales van Doel 3 en Tihange 2 uit veiligheidsoverwegingen waar het nog ~15TWh (of ~20% jaarbijdrage bedroeg[29]). De volledige overstap van die hoeveelheid energie op traditionele energie zou een weerslag hebben op de uitstoot van CO_2 voor een totaal van 147% van de actuele uitstoot (of 37 miljoen ton CO_2). Ter vergelijking heeft de sluiting van Doel 3 en Tihange 2 reeds aanleiding gegeven tot de uitstoot van 3.8 miljoen ton CO_2 (Albrecht et al., 2015). Deze trend wordt bevestigd door de onvrijwillige uitstap van Japan na de ramp van Fukushima waar plots de uitstoot met 6% toenam op drie jaar tijd (2010-2013): een zoektocht naar een eengemaakte energiemarkt voor Europa blijkt dus inderdaad meer dan, een commercieel plaatje te hebben. Zowel de veiligheid als de duurzaamheid van het beschikbare pallet zal in rekening moeten worden genomen. Maar ook de beschikbaarheid en de veiligheid van de distributie: met of zonder het nucleaire verhaal zal Duitsland bijvoorbeeld tussen 27 en 45 miljard € investeren tot 2030. Dit toont aan dat de term kriticiteit niet uitsluitend meer herleidbaar is tot die infrastructuur die essentieel is om de energetische voorzieningen van een land te vrijwaren (en

[29] ENTSO-E, Country Data Packages, Belgium 2011, 2013 (geraadpleegd op 22 juli 2015).

dus moet worden beveiligd) of zelfs uitsluitend tot de catastrofale gevolgen van een incident met een dergelijke infrastructuur, maar ook moet rekening houden met de gevolgen van het gebruik (of niet) of de keuze van één of andere energievorm boven een ander en de noodzakelijke gevolgen voor de bescherming ervan, weze het cybernetisch of fysisch.

3.6. Deelbesluit

Wat we tot hier toe hebben behandeld leidt ons onvermijdelijk tot de aanpassing van onze beginstelling te weten de poging tot de omschrijving van het begrip kriticiteit en wat we in eerste instantie als definitie hebben gehanteerd. Tegen alle verwachtingen in en leidt ons dit niet naar een exhaustieve lijst kritieke energie infrastructuur, maar eerder naar een grotere samenhang in de organisatie van de samenwerking tussen domeinen. Als gevolg waarvan een zuiver departementale of zelfs nationale omschrijving van het probleem tekort schiet: elementen voor de formulering van een antwoord werden in de uiteenzetting van de voorbeelden uit de VS en de NAVO aangereikt. Zo is niet alleen het domein, nog soeverein grondgebied een maatstaf voor het omschrijven van een oplossing tot de bescherming van kritieke energie infrastructuur: elementen die deze benadering *de facto* uitbreiden werden gevonden onder de vorm van de cybernetische beveiliging (als aanvulling van de tot hier toe uitsluitend fysische beveiliging), de diversificatie in de aangewende energiebronnen (waartoe ook het nucleaire kan bijdragen), en de toename van energie efficiëntie (waaronder ook het verbruik bij krijgsmachten moet worden gerekend). Elk van deze elementen tot uitbreiding van onze probleemstelling kan en mag niet op zichzelf worden beschouwd: in elk van de gevallen dient het eerder als een aanvulling van een te restrictieve omschrijving van de problematiek van bescherming van kritieke energie infrastructuur te worden beschouwd: elk van deze elementen vullen elkaar aan.

In wat volgt willen we aandacht schenken aan aanvullende elementen die mee zullen bepalen hoe het beeld van kritieke energie infrastructuur verder kan worden vervolledigd.

Deel 4

Aanvullende structurele maatregelen

4.1. Algemeen

In dit deel wil men oog hebben voor de aanvullende structurele elementen ter bescherming van kritieke energie infrastructuur te weten diversificatie en energie-efficiëntie. We gaan in dit deel na welke de uitdagingen zijn en welke in de EU daartoe voorgesteld oplossingen in het kader van het vooropgestelde doel van reductie van uitstoot broeikasgassen kunnen bijdragen tot een garantie van beschikbaarheid en beveiliging.

Het zijn de incidenten van 2006 en 2009 die aan de basis liggen van de maatregelen en een ongewijzigde energetische politiek: tekorten in gasleveringen hebben in die jaren de leiders van de EU aan het denken gebracht over de te grote afhankelijkheid van een en dezelfde leverancier voor gas, met name Rusland. We hebben in het vorige gedeelte bovendien vermeld dat sinds de ramp van Fukushima in sommige Westerse landen de tendens is gegroeid om sneller dan voorzien van kernenergie af te stappen: in de groeilanden is dat niet het geval, wel integendeel. Economische groei kan enkel met behulp van de beschikbaarheid van kernenergie in die landen worden gerealiseerd aangezien het 24/24 en 7/7 een stabiele output genereert. Alternatieve bronnen kunnen immers nog niet voldoen aan de piekvraag en fluctueren zelfs al naargelang de weersomstandigheden wat niet compatibel is met een maximale rendabiliteit die noodzakelijk is voor winstmaximalisatie. Bovendien hebben de klimaatdoelstellingen als gevolg dat een lagere koolstofuitstoot noodzakelijk is, dat kernenergie de facto een van de oplossingen is die daartoe kan bijdragen, en om deze redenen ook deel zal blijven uitmaken van het energetische pallet. Wel is hierdoor een volledige herziening van het beschikbare energiepallet in gang gezet.

Maar welke is dan de benadering die men in de EU maar ook daarbuiten kan hebben met betrekking tot de energetische doelstellingen naast de bescherming van kritieke infrastructuur in het algemeen en energie-infrastructuur in het bijzonder. De Europese Unie houdt er een benadering op na die in de bestaande context een aanvulling zal zoeken bij diversificatie enerzijds en de daaruit voortvloeiende structurele veranderingen en hun bescherming anderzijds. Of die benadering door een beleid wordt ondersteund is wel de vraag: een gemeenschappelijk energetisch beleid ontbreekt immers in de Unie omwille van te veel verscheiden nationale belangen en verschillende accenten. Of daaruit een efficiënte strategie kan voortvloeien is de daarop aansluitende vraag. Los van het feit of men zonder gemeenschappelijk beleid wel conceptueel over een strategie kan spreken, zijn

ook in de benaming niet steeds dezelfde termen gehanteerd: wanneer men in de communicatie op de daartoe voorziene website over de "energiestrategie 2050" spreekt[30], is de benaming van de communicatie niet in overeenstemming (energy roadmap 2050) en kan dit tot verwarring leiden met andere teksten[31]. Zonder een energiebeleid van de Unie, kan men niet echt spreken over een strategie ook al hebben verschillende documenten van de EU die term in hun hoofding: hooguit zijn het doelstellingen waarnaar wordt gestreefd, maar de verschillende nationale belangen en daaruit voortvloeiende voorkeuren zorgen voor een te disparate consonantie in de uitvoering laat staan in de veiligstelling ervan. Vertrekkend van de huidige situatie waar 58% van de energiemarkt afhankelijkheid vertoont van fossiele brandstoffen (European Commission, 2011; p.5.), wil de EU in de toekomst die afhankelijkheid afbouwen en daartoe tegelijk voldoen aan de klimaatdoelstellingen: een compromis in die richting is slechts mogelijk voor het geval dat wordt gedecarboniseerd, waardoor tegelijkertijd de afhankelijkheid van import en prijsvolatiliteit zou afnemen tot een afhankelijkheid van nog slechts 35-45% (ibid.). Het verlagen van die afhankelijkheid zou als neveneffect hebben dat de totale energiekost zou verminderen (in het bijzonder door lagere investeringen voor brandstof), maar dit zou dan ook gepaard gaan met hoger kosten voor investeringen bijvoorbeeld voor infrastructuur voor het genereren van energie alsook voor de distributie ervan. Over de kost voor de bescherming van infrastructuur wordt in de meerderheid van de gevallen niet gerept: vandaag importeert de EU 53% van haar energetische behoeften waarvan voor meer dan 50% zonder koolstofuitstoot wordt gegenereerd. De European Energy Security Strategy vermeldt welke de vertreksituatie afhankelijkheid van import vertoont voor zware olie (90%), gas (66%), en in een mindere mate voor vaste brandstoffen (42%) en nucleaire brandstof (40%) (European Commission, 2014; p.2). Ook deze lagere afhankelijkheid van import voor nucleaire brandstof is een bijkomend argument om die technologie niet vervroegd af te schrijven: in een beginfase is dit immers een technologie die onze afhankelijkheid ten opzichte van externe leveranciers kan verminderen en het ons aldus mogelijk maakt om veilig te stellen.

[30] https://ec.europa.eu/energy/en/topics/energy-strategy/2050-energy-strategy
[31] European Energy Security Strategy. COM(2014)330 final.

4.2. Diversificatie

De scenario's die aanleiding zouden kunnen geven tot meer diversificatie lopen uiteen zowel in de einddoelstelling als de intensiteit waarmee die tot uitvoering kan komen maar een gemeenschappelijk doel is de vermindering van het gebruik van fossiele brandstoffen: die doelstelling is niet gemeenschappelijk aan alle lidstaten van de EU. Polen wil de komende jaren bijvoorbeeld meer gebruik maken van vaste fossiele brandstoffen voor de uitbouw van zijn economie en wil daarvoor zelfs minder tegemoet komen aan de eisen gesteld gedurende de onderhandelingen in de aanloop van de klimaatconferentie. Wat er ook van weze, mogelijke scenario's tot diversificatie beperken zich tot het diversifiëren van de energiebronnen enerzijds en het diversifiëren van externe bronnen en daaraan gekoppelde infrastructuur anderzijds.

Voor wat de diversificatie van de gebruikte bronnen betreft stelt de Europese Commissie volgende scenario's voor (European Commission, 2011; p.4 aangepast):

-hogere energie efficiëntie zal ervoor moeten zorgen dat het verbruik wordt beperkt en in 2050 nog slechts de fractie voorstelt van het verbruik dat men in de piekjaren van net voor de financiële en economische crisis van 2008 behaalde;

-gediversifieerde bronnen: zowel traditionele fossiele brandstoffen als de nieuwste technologie zullen van het beschikbare energiepallet deel blijven uitmaken maar de verdeling zal nooit statisch maar eerder dynamisch van aard zijn. De tendens om minder traditionele fossiele brandstoffen te gebruiken met als doel te decarboniseren en de klimaatdoelstellingen te behalen, zal afhangen van de marktprijs die men voor de brandstoffen wil hanteren: landen die nationale reserves hebben kunnen geneigd zijn die langer te gebruiken dan de gemeenschappelijke EU objectieven zouden willen doen aannemen. Het zal dus ook voor een deel de lokale publieke opinie zijn die mee bepaalt wat voor een lidstaat aanvaardbaar (of te verkiezen is) en wat niet. De kinetiek die een dergelijke diversificatie zal drijven zal voor een stuk door markteconomische motieven worden gedreven en die zullen waarschijnlijk meer gewicht in de schaal werpen dan technologische evolutiedrang of universele klimaatdoelstellingen die tegen individuele belangen zouden ingaan. In dit geval kunnen zowel traditionele bronnen (als steenkool) als nieuwere technologie

(kernenergie) voor een groter deel het energiepark bepalen: afhankelijk van de evolutie van het kernenergiedebat in het Westen zal dat voor die regio alleen zorgen voor een lagere bijdrage van kernenergie. In andere werelddelen is in ieder geval een groter aandeel van het energiepakket behouden voor kernenergie door een grotere vraag die enkel door toedoen van die energievorm met een constante output kan worden gegarandeerd op korte termijn;

-grote toedracht van hernieuwbare bronnen: de evolutie van het voorgaande scenario zal bepalen welke de toedracht zal zijn van hernieuwbare bronnen. Een element dat mee de dynamische verdeling tussen de verschillende bronnen zal bepalen zijn de subsidies: deze zijn nog groot in het geval van hernieuwbare bronnen. In ons land hebben die in het verleden een dermate grote proportie aangenomen dat de subsidie "groene stroomcertificaten" nog een aantal jaren door de gebruiker extra bijdrage zal vergen. Nochtans slaagt de dure nieuwe aanwending van hernieuwbare technologie voor het ogenblik slechts in haar mobilisatie in het geval van massieve ondersteuning door de overheid. De kost van nieuwe investeringen zal in de toekomst hoog blijven, in vergelijking met de goedkope opwekking van stroom door die technologie. Met andere woorden zal men in de toekomst een herhaling zien van wat tot hiertoe als argument werd gebruikt om de technologie voor kernenergie af te bouwen. Mogelijk zijn hoge kosten een reden om niet onmiddellijk oog te hebben voor bijkomende bescherming;

Geenenkel van deze voorgestelde scenario's is exclusief: eerder moet men zich verwachten aan een deel van elk van voornoemde dat zich in meer of mindere mate kan verwezenlijken en op die manier al dan niet kan bijdragen tot een prioritisatie die men ook in de tijd dynamisch moet schatten. Op die manier wordt ook de kritieke energie infrastructuur een dynamisch begrip in de tijd. Echter: het feit dat een commerciële motivatie kan worden gevonden achter de dynamiek van het beschikbare landschap van de energetische technologie, doet de vraag reizen in welke mate op een meest efficiënte manier aan beveiliging kan worden gedaan. Deze is immers niet uitsluitend de verantwoordelijkheid van de overheid maar betrekt zoals eerder vermeld de private partners welke in die inspanning een deel van hun winst verloren zien gaan: zoals het advies van het Europees en sociaal comité over de mededeling van het Europees Parlement met betrekking tot het stappenplan energie 2050 (COM(2011)885 final (punt 1.2)):

Afhankelijk van de lidstaat variëren de energiebronnen en de infrastructuur. Voor sommige landen betekent een koolstofarme

energiesector een beduidend grotere uitdaging dan voor andere. Het stappenplan is vrij flexibel van opzet, zodat elk land een adequaat actieprogramma kan uitwerken. Wel zullen de lasten in vergaande mate gedeeld moeten worden, wil men de decarbonisering daadwerkelijk verwezenlijken.

Wat het Comité niet vermeldt is dat in het licht van voorgaande het voor het ogenblik niet duidelijk is met welke andere dan financiële middelen landen als Polen kunnen worden overhaald om de commerciële en industriële voordelen van de oudere koolstof gebaseerde energieproductie op te geven en lokale subsidies voor particulieren te vervangen door subsidies voor Staten. Dit zou uitmonden op nieuwe koolstofheffingen, maar nog erger is het gesteld in andere delen van de wereld waar men de productie wil opdrijven door gebruik van koolstofrijke brandstof. In die veronderstelling is het niet mogelijk om de zuiver markteconomische motieven te laten gelden om de dynamiek van de verdeling van de verschillende beschikbare energetische technieken te bepalen, laat staan een rationele methodologie uit te bouwen voor de bescherming van kritieke energie infrastructuur: de eis voor de industrie om bij de 80% minder CO_2 uit te stoten zou als gevolg kunnen hebben dat een delokalisatie wordt veroorzaakt naar regio's in de wereld waar minder streng met uitstootnormen wordt omgesprongen met als doel een deel van de winstmarge te recupereren. Zo lang met de onzekerheid moet worden rekening gehouden over mogelijke delokalisatie, kan ook niet in strategische termen worden gedacht over de beveiliging van kritieke energie infrastructuur: de voorwaarden scheppen voor een behoud van de energieopwekking is dus een noodzakelijke voorwaarde die naast de fysische en cybernetische beveiliging, even belangrijk blijkt als de ontbrekende technische ontwikkeling voor de integratie van verspreide bronnen van hernieuwbare energie in een gemeenschappelijk netwerk: onderzoek en ontwikkeling is dus ook in deze materie een noodzakelijke voorwaarde. Het strategisch aspect kan niet ondergeschikt worden aan de commerciële motivatie dat vandaag de dag ook in deze materie meer COTS-technologie wordt in werking gesteld.

Voor de diversificatie van de externe bronnen heeft de Commissie dan weer een aantal scenario's die het energie-veiligheidsplan sturen, zoals uit volgend hoofdstuk zal blijken.

4.3. Energie efficiëntie

In de door de Europese Commissie voorgestelde scenario's is het niet duidelijk hoe deze werden uitgewerkt en welke er de basishypothesen van zijn. Tot het besluit gekomen dat geenenkele van de scenario's exclusief kan zijn of dat zelfs regionale verschillen kunnen voorkomen in de uitvoering, levert de Commissie conclusies die aantonen dat aanpassen noodzakelijk is en dat de effecten van een gewijzigde aanpak slechts merkbaar zullen zijn tegen 2020: tevens voegt ze er ook de noodzakelijke voorwaarden aan toe voor het bereiken van die doelstellingen (Europese Commissie, 2011; p.5).

-decarbonisatie is haalbaar en kan op termijn zelfs minder kosten dan de huidige energievorm;

-blijvende zware kapitaalinvesteringen maar minder kost voor brandstof;

-het aandeel van elektriciteit zal nog toenemen en daardoor wordt het belang van integratie in een slim netwerk en de bescherming van die infrastructuur a priori nog belangrijker;

-hierop aansluitend, en wetend dat Duistland in de EU reeds zware investeringen heeft gepland tegen 2020 om ook het distributienetwerk te vernieuwen, zal ook in de rest van Europa deze investeringen worden gedaan. De prijs zal hierdoor de komende jaren stijgen: de bijkomende kosten voor de bescherming van die infrastructuur zullen ook doorgerekend worden aan de gebruikers en een belangrijker deel van het budget opslorpen en dit zowel voor particuliere gebruikers als voor bedrijven;

-hierdoor zal de noodzakelijke motivatie groeien om zowel energie te besparen als meer energie efficiënte systemen in werking te stellen. Het aandeel van hernieuwbare bronnen is in theorie tot dan in een stijgende lijn, maar ook dit zal afhangen in het vooropgestelde scenario van stijgende kosten, hoe deze voor hernieuwbare bronnen relatief gezien zullen evolueren ten opzichte van de meer klassieke bronnen en de kernenergie: in de landen waar deze technologie een belangrijke toedracht heeft in het beschikbare energiepallet, zal dat in de toekomst ook waarschijnlijk zo blijven. Het verschijnen van nieuwe spelers op de markt die de endogene technologie van het nucleaire aanvullen en beconcurreren, kunnen vragen doen reizen met betrekking tot betrouwbaarheid en de beveiliging van dergelijke installaties. Enkel de toekomst zal uitwijzen in welke mate die commerciële aanwending van een gevoelige technologie op een veilige en beveiligde wijze (*safe and*

secure) kan worden uitgevoerd: de aanschaf door het Verenigd Koninkrijk van een door China gefinancierde kernreactor illustreert deze problematiek;
-indien in een scenario wordt beland dat de toedracht van hernieuwbare energie toch een groot gedeelte van het energetische landschap weet te bemachtigen, zal voor een groot gedeelte van de beveiliging van die infrastructuur te herleiden zijn tot het principe van Lovins: bij aanvang van deze studie werd in dat kader uiteengezet dat naast de diversificatie ook de geografische spreiding van infrastructuren kan bijdragen tot de beveiliging vooropgesteld dat ook de distributienetwerken op een adequate manier worden beveiligd.

In transitie zal dit soort van systemen samen moeten opereren met de gecentraliseerde en grotere types systemen: een aangepast distributienet zal reeds de flexibiliteit moeten genereren om beide systemen optimaal te kunnen bedienen. Daarnaast zal gas een essentiële rol spelen in die transitie naar meer hernieuwbare bronnen en zal de transitie pas echt van start kunnen gaan wanneer de efficiëntie van hernieuwbare bronnen wordt verhoogd en de kosten ervan worden gedrukt. De drukking van de prijs van energie zal mee worden gerealiseerd door de ervaring in traditionele technologie en in dit geval koolstofvrije productie van kernenergie. De intentie van sommige landen om vaste koolstof houdende brandstoffen te blijven gebruiken zal in dat geval moeten gepaard gaan met een efficiënte technologie voor de opvang van koolstofopslag na verbranding. Ten slotte zal het bestaan van slimme netwerken ook inhouden dat een opslagcapaciteit in werking kan worden gesteld die voor het ogenblik ontbreekt.

4.4. Gemeenschappelijk energetisch beleid

De belangrijkste structurele wijziging die te verwezenlijken is, is de politieke visie die het beleid moet ondersteunen. Tot hier toe hebben tal van documenten, plannen en vorderingsrapporten misschien op een of andere manier de naam van een strategie gekregen of het woord in de titel verwerkt, doch deze kan enkel tot stand komen indien een gemeenschappelijk energetisch beleid tot stand komt. Tot hier toe is dit omwille van markteconomische redenen en nationale belangen nog niet gerealiseerd kunnen worden: zelfs in het kader van de klimaatdoelstellingen zal dit niet mogelijk zijn zolang die individuele belangen het collectieve voordeel van de Unie overschaduwen. Echter: het realiseren ervan is in de toekomst nog meer dan vandaag van cruciaal belang. In de toekomst wordt in elk geval van de toekomstprojecties immers een stijgende afhankelijkheid van import aangetoond: onderstaande tabel geeft voor elk van de bronnen de marge van afhankelijkheid weer.

Tabel 2: vooruitzicht importafhankelijkheid van fossiele brandstoffen (European Commission, 2014; pp.101 en volgende).

		2010	2020	2030
PRIMES projectie basisscenario	Olie	84.3	87.2	90.4
	Gas	62.1	65.4	72.6
	Steenkool	39.5	40.9	49.1
PRIMES projectie 2030 strategie	Olie	84.3	87.2	90.3
	Gas	62.1	65.4	71.7
	Steenkool	39.5	40.5	48.4
World Energy Outlook projectie	Olie	82.5	84.6	89.0
	Gas	62.1	72.7	78.8
	Steenkool	39.6	43.4	48.1

De projecties duiden op de vraag en de importafhankelijkheid van de 28 EU landen. De verschillende projecties tonen een trend die vergelijkbaar is zowel in het basisscenario als in een aangepaste strategie die kadert binnen klimaatdoelstellingen enerzijds en anderzijds een toename van de energie-efficiëntie en diversificatie voor twee modellen (PRIMES en IEA model): het geeft een beeld weer van energie-afhankelijkheid. De tendens die zich aftekent is een toename van de afhankelijkheid voor import tegen 2030, zelfs in het geval van maatregelen die passen in een strategie die gericht is op een

lager verbruik intern de EU. De verklaring van een dergelijke tendens is te zoeken in een lagere productie van die bronnen binnen de 28 EU lidstaten die ondanks een grotere efficiëntie een tekort genereren: hierdoor stijgt in de toekomst de import van bronnen. De conclusie is dat een dergelijke toegenomen afhankelijkheid van import binnen de EU nog meer moet doen inzien welk een belang moet worden gehecht aan de kritieke energie infrastructuur van EU-landen. In het bijzonder de infrastructuur die intern de EU kan bijdragen tot het genereren van die bronnen welke de afhankelijkheid van import kunnen beperken moeten voorkeur genieten. Een kritieke factor in alle projecties en niet weergegeven in deze cijfers is de te laag geschatte koolstofuitstoot van China (Buckley, 2015) die, alle schattingen ten spijt, zou kunnen leiden tot versnelde maatregelen voor het reduceren van de uitstoot van broeikasgassen in de toekomst: in een dergelijk scenario wordt de bestaande nucleaire infrastructuur nog belangrijker. In sommige delen van de EU mag deze energievorm al tot een vermindering of een totale verdwijning zijn gedoemd, andere landen zullen hun nucleair erfgoed koesteren en daar hebben ze gelijk in: de vraag van de groeilanden om hun traditionele bronnen aan te vullen met kerncentrales omwille van een constante output, zorgt voor een vraag naar expertise, en technologische ontwikkeling die enkel de landen kunnen leveren die al over die technologie beschikken. De commerciële waarde van die ervaring zal indien ze niet endogeen kan worden gebruikt, alleszins een troef zijn die voor de export van kennis en kunde kan dienen.

Terwijl we merken dat de procentuele afhankelijkheid niet afneemt, merkt men dat de totale volumes van import wel afnemen. Tegelijk ziet men in die periode een toename van de hernieuwbare bronnen voor de productie van elektriciteit, verwarming en transport. Maar de belangrijkste elementen die een gemeenschappelijk energetisch beleid zullen ondersteunen zijn de diversificatie van bronnen en het verhogen van energie-efficiëntie. Maar een even, zo niet belangijker aspect, zal moeten handelen over de geografische diversificatie: naast het diversifiëren van de bronnen zelf zal men ook de afhankelijkheid van specifieke regio's moeten afbouwen waaruit elke bron wordt aangesproken. De te grote afhankelijkheid van het Russische gas en de steeds grotere eisen van dat land in Oost Europa, hebben het Westen doen inzien dat een dergelijke afhankelijkheid gevaar zou kunnen opleveren voor het economische potentieel van de EU in het algemeen en niet enkel meer de landen die een rechtstreekse afhankelijkheid van het Russische gas vertonen. Het geheel van maatregelen die men kan vinden om die afhankelijkheid te reduceren zullen echter moeten kaderen binnen de klimaatdoelstellingen die de bijdrage van fossiele brandstoffen wil beperken om de totale opwarming van de planeet af te remmen: waar men eerder van de VS en China zou verwachten koplopers te zijn in de uitstoot van broeikasgassen, stelt men vast dat de uitstoot van de Europese Unie en per inwoner, een gelijkaardig niveau

behaalt als dat van China[32]. De enige wetenschappelijke oplossing op korte termijn bestaat er dan ook uit om in de nabije toekomst gebruik te blijven maken van kernenergie indien men de uitstoot wil indijken en de opwarming van de aarde tegen 2050 beperken tot 2.7°C. De rationele invulling van die eis sterkt de commerciële positie van Rosatom erin te geloven dat een groot gedeelte van het Europees nucleair park aan vervanging toe is (en dat de firma deze markt voor een deel kan invullen) te weten 25% tegen 2020, 50% tegen 2024 en 75% tegen 2026. Dat een deel van deze redenering wordt gemotiveerd door pure commerciële overwegingen is niet te betwisten aangezien in Rusland zelf twee derden van de in gebruik zijnde kerncentrales een levensextensie wordt toegekend tot 40 jaren[33]. Toch stemmen deze cijfers tot nadenken en meer bepaald omtrent de haalbaarheid van de Europese doelstellingen door desinvestering in sommige Europese landen van het nucleaire uit politieke en/of ideologische motivering. Zowel de eisen van betaalbaarheid, decarbonisatie, als energieveiligheid vergen een voortdurende investering in het onderzoek en ontwikkeling van kernenergie wil men geen deel van de expertise en aanwendbaarheid in de tijd verloren zien gaan. Het beleid van het energiebeeld dient voor een garantie van kritieke energie infrastructuur zowel te voorzien in capaciteit, in transport als in opslag, en dit zowel voor de traditionele bronnen als voor hernieuwbare. In wat volgt gaan we voor fossiele, nucleaire en hernieuwbare bronnen na welke de kritieke elementen zijn die in rekening dienen te worden genomen.

[32] 7.5 ton/inwoner. Jos Delbeke, 2015. Energy Transition: A Multifacetted Challenge for Europe. Egmont Palace.
[33] Andrey Rozhdestvin, 2015. Energy Transition: A Multifacetted Challenge for Europe. Egmont Palace

4.5. Energiecapaciteit, -transport en -opslag

Het is duidelijk dat in elk van de gevallen die men wil beschouwen (olie, gas, kernenergie en of hernieuwbare energie) de transportcapaciteit en opslag een typische nationale aangelegenheid zijn in die zin dat een gemeenschappelijk energiebeleid niet kan verhinderen dat nationale prioriteiten en voorkeuren andere oriëntaties kennen dan de gemeenschappelijke lijn. In het bijzonder voor wat op supranationaal vlak als essentieel wordt beschouwd, kunnen lokale eisen afwijken van de meest rendabele oplossing die voor die regio kan worden gekozen. Als voorbeeld kan men het standpunt van het Verenigd Koninkrijk vinden dat prioriteiten eerder wil leggen bij de energieveiligheid voor het Verenigd Koninkrijk, de betaalbaarheid voor datzelfde land en de tegemoetkoming aan de eigen klimaatdoelstellingen[34] (niet noodzakelijk identiek aan die van de Europese Unie). Voor elk van voornoemde energiebronnen, zullen we daarom nagaan in welke mate de interne (nationale) vereisten, de externe (internationale) energie vereisten en de infrastructuur al dan niet kunnen bijdragen tot het beveiligen van die Europese energiezekerheid.

4.5.1.Olie

Voor ruwe of geraffineerde olieproducten, is de belangrijkste interne EU-argumenten de controle van de vraag: zowel de maatregelen die energie efficiëntie nastreven als de decarbonisatie horen hierbij. De bepalende externe factoren zijn de kwaliteit van de ruwe olie (die moet bruikbaar zijn voor de beschikbare raffinagecapaciteit) en de hoeveelheid. De kwaliteit van de olie is onder meer afhankelijk van de concentratie zwavel. Voor productie is 50% van de globale productie geleverd door slechts 6 landen terwijl 75% van die productie door 14 landen wordt voorzien. Het feit dat een of andere leverancier (tijdelijk) niet meer beschikbaar is, kan ernstige gevolgen hebben voor de raffinage vereisten van olie afkomstig uit andere streken. Dit is het punt waar kwantiteit en kwaliteit opnieuw samenkomen: aanpassingen van een raffinage infrastructuur om een minder kwalitatieve olie te kunnen gebruiken, kan niet op zeer korte termijn worden uitgevoerd. Voor de EU zijn Rusland en Noorwegen de belangrijkste leveranciers. Daarbij dient ook vermeld dat Rusland zowat 35% van de aan de EU externe olielevering voor

[34] Richard Folland, 2015. Energy Transition: A Multifacetted Challenge for Europe. Egmont Palace.

rekening neemt terwijl Noorwegen op de tweede plaats komt met 10% van de Europese behoeften (COM(2014)330 final).

Noodoplossingen worden in verschillende vormen nagestreefd: noodopslag, verlagen van de vraag of rantsoenering, de vervanging van brandstof in sectoren, toename van eigen productie van olie-(en/of producten), verlichting van kwalitatieve vereisten, en ten slotte het zoeken naar alternatieve routes voor de bevoorrading. Elk van deze maatregelen heeft slechts een beperkte uitwerking en is meestal niet op lange termijn houdbaar voor een optimaal resultaat. Opslag zal bijvoorbeeld moeten zorgen voor een opvang van markttekorten: deze strategische opslag zal (tijdelijk) kunnen zorgen voor een zekere stabiliteit van prijzen. Sinds de crisis van eind jaren 60 wordt voor dat doel een strategische stock voorzien van 90 dagen import of 61 dagen consumptie afhankelijk van welke waarde groter is. In 2013 bereikte de EU voor een gezamenlijke stock van ruwe olie en geraffineerde producten een equivalent van 102 dagen import. Een maatregel als het vervangen van brandstof voor sommige sectoren is niet vanzelfsprekend: industriële processen worden immers geoptimaliseerd voor een welbepaalde configuratie en het is niet een plotse aanpassing daarvan die ervoor zal zorgen dat de betrokken sector op een rendabele manier zal kunnen blijven functioneren. Dezelfde opmerking kan gelden voor een minder strenge kwaliteit van dezelfde brandstof.

Voor ons land is er een opslag van 102Mton voorzien, een centrale stock die wordt beheerd door een centraal agentschap (APETRA). De wet van 20 juli 2006 specifieert in dit geval de voorwaarden voor het aanhouden van die voorraden in artikel 3[35]:

De Koning bepaalt bij een besluit vastgesteld na overleg in de Ministerraad…

> 3°de regels voor het aanspreken van de verplichte voorraden aardolie en aardolieproducten. Dit besluit wordt genomen na overleg met de voorraad plichtige ondernemingen en met de Raad van Bestuur van de naamloze vennootschap van publiek recht APETRA, opgericht bij de wet van 26 januari 2006 betreffende de aanhouding van een verplichte voorraad aardolie en aardolieproducten en de oprichting van een agentschap voor het beheer van een deel van deze voorraad en tot wijziging van de wet van 10 juni 1997 betreffende de algemene regeling voor accijnsproducten, het voorhanden hebben, en het verkeer daarvan en de controles daarop;

[35] Wet van 20 juli 2006 wijziging van de wet van 13 juli 1976 houdende goedkeuring van de Overeenkomst inzake een internationaal energieprogramma, en van de Bijlage, opgemaakt te Parijs op 18 november 1974.

4°de lijst met de prioritaire gebruikers van aardolieproducten evenals de wijze van bekendmaking van deze lijst.

Als lid van de Europese Unie, het Internationaal Energieagentschap en de OVSE, heeft België zich ertoe verbonden om een dergelijke voorraad aan te houden. APETRA beheert die voorraad op de beschikbare reserves van de producenten: in geval van nationale of internationale tekorten, zoals erkend door de board van het Energieagentschap, de raad van Ministers of de Europese Raad zal deze organisatie op vraag van de FOD Energie deze voorraad beschikbaar maken voor de Belgische markt.

4.5.2.Gas

Intern de EU zal de gasvoorziening afhangen van de samenstelling van het brandstofverbruik, de evolutie van de productie van de Unie als ook de samenstelling van de infrastructuur, onder meer de opslag- en transportcapaciteit, zoals die reeds werden besproken voor het geval van ruwe olie. De vraag voor gas is in de Unie grotendeels afhankelijk van de temperatuur aangezien deze bron voornamelijk voor verwarmingsdoeleinden wordt gebruikt. Echter het verschil is dat er voor het gas geen minimale vereisten zijn voor de opslag van een strategische reserve. Het is dus aan iedere lidstaat om zelf uit te maken hoe het aan de vraag kan voldoen, zelfs in het geval van extreme weersomstandigheden. Tot hiertoe werd aangenomen dat tot het einde van 2014 lidstaten in staat zouden moeten zijn om in het geval van het verlies van hun grootste infrastructuur voor gasvoorziening het land met de resterende capaciteit tegemoet te komen aan de vraag. In die configuratie is het ook noodzakelijk om het transport van gas over pijpleidingen in twee richtingen mogelijk te maken teneinde de netwerking te verbeteren in de Unie. Voor het ogenblik zijn de Scandinavische landen, Duitsland, Tsjechië en België als eerste in de rij om te voldoen aan die vereisten. Maar slechts 16 lidstaten waren vorig jaar in dat geval. Natuurlijk kan men in de Unie, zoals in de VS, en vooropgesteld dat de technologie daartoe betrouwbaar blijft op lange termijn, verder de exploitatie van schaliegas voorzien als aanvulling van de bestaande beschikbare capaciteit. Deze mogelijkheid zal alleszins een aanvulling geven van de buitenlandse bronnen.

Externe leveringen gebonden aan geografische zones zullen in de toekomst gelieerd zijn aan een toegenomen aandacht voor militaire operationele betrokkenheid om die bronnen te vrijwaren. In het bijzonder zal de invoer van gas de komende jaren nog toenemen: het is dus interessant de huidige van de toekomstige interestzones te discrimineren aangezien het militair machtsapparaat van staten hoogst waarschijnlijk in die zones zal worden aangewend. Europees gas was in 2013 voor 39% afkomstig van

Rusland, voor 33% van Noorwegen en voor 22% van Noord Afrika. Voor een diversificatie van voormelde bronnen is er een uitbreiding van de infrastructuur mogelijk voor leveringen van LNG per schip onder meer vanuit de Verenigde Staten. Maar ook de interne distributie van deze vorm van energie moet op een adequate manier worden verzorgd door een verruiming van het bestaande netwerk. Daarnaast zullen de geografische zones van aandacht voor nieuwe bronnen worden uitgebreid naar Noord-Afrika, Noorwegen en het Arctisch gebied. Sommige projecten daartoe zijn omstreden: zo bijvoorbeeld het project dat in het Noord-Afrikaanse regio elektrische stroom wil opwekken met foto-voltaische cellen en die via kabels onder de Middellande zee in Europa wil leveren. De vraag rijst voor dergelijke projecten of het niet efficiënter vanuit kostenbaten analyse zou zijn om een dergelijk project te coördineren met een lokaal verbruik van een dergelijke groene stroom en de export van de fossiele reserves: dit is steeds de techniek die meer opbrengst voor het exporterende land heeft gegenereerd en ook bijvoorbeeld in Iran de voorkeur heeft genoten. Fossiele brandstoffen werden er steeds als te waardevol beschouwd om lokaal te consumeren. De transit vanuit Noord-Afrika zal dus zowel infrastructureel als een internationaal veiligheidsprobleem zijn waarvoor het buitenlands beleid van de EU een belangrijke rol zal spelen. De andere zones die op een gelijkaardige manier aan belang zullen winnen zijn het Midden-Oosten en Centraal Azië: een transit door landen als Turkije zal in de toekomst daarvoor een belangrijk plaats kunnen innemen in het energetische beleid van de EU. In het noorden van de EU zal een aanvoer vanuit Noorwegen naar de Europese markt maar ook de expertise van de Noren voor de exploitatie van mariene zones in extreme omstandigheden zoals dat in het Arctisch gebied wordt verwacht, de aandacht van de EU voor dat land opdrijven. Maar het spreekt voor zich dat de vereisten voor diversificatie zullen zorgen voor een combinatie van mogelijkheden en niet van een exclusieve keuze van de voorgestelde oplossingen. Naast de alternatieven op bestaande aanvoer, worden bijgevolg bijkomende reserves en mogelijk zelfs eigen productie, in het bijzonder in Nederland en Noorwegen als mogelijkheden voorzien.

Met betrekking tot infrastructuur, heeft men in de gassector hoofdzakelijk twee voorname posten te weten de centrales enerzijds en anderzijds de transitinfrastructuur. Het is hoofdzakelijk door deze twee elementen dat de prijs van gas op de markt wordt bepaald. Gascentrales worden echter niet systematisch ingezet voor de generatie van elektriciteit, maar het is een valabel alternatief voor de productie van energie die aan de industrie zou kunnen ontbreken als complement voor de olie-leveringen. Gedurende winterperiodes bleek de bestaande infrastructuur al meermaals een beperkende factor: opslag op het einde van september zou een indicatie geven voor de capaciteit om de wintervoorzieningen te kunnen garanderen. In wezen

is de onderbreking van de gasvoorziening uit Oekraïne voldoende om bestaande stocks terug te dringen tot niveaus lager dan de vereiste 90% om de wintermaanden zonder onderbreking door te komen. In deze gevallen zijn het voornamelijk het zuiden en zuid oosten van de EU die eerder getroffen worden door onderbreking omdat in beide gevallen weinig of beperkt transport van vloeibaar gas voorhanden is.

4.5.3.Kolen

Deze energiebron is in onze regio minder in gebruik, maar dat is niet overal in Europa het geval: veelal in Oostelijke delen van Europa is er nog steeds een grote consumptie voor het voorzien in energetische behoeften voor de industrie. Meer in het bijzonder voor ons land is de exploitatie van de reserves te duur in vergelijking met andere meer beschikbare bronnen. Maar dat hoeft niet altijd zo te zijn: in geval andere bronnen aan waarde zouden toenemen, kan de beschikbare reserve misschien nog steeds worden aangewend, zij het op tijdelijke basis: op Europees vlak is er immers geen mogelijkheid om de exploitatie van deze minder efficiënte energiebron op grote schaal en permanent uit te baten zonder in te gaan tegen de richtlijnen die moeten zorgen voor een groenere en efficiëntere energieopwekking. Maar zuiver in cijfers kan men stellen dat de beschikbare Europese reserves voor 80% uit kolen bestaan. Veelal is de eigen nationale productie of daarbij aansluitend de intra-EU markt de grote bijdrage aan de vraag die voor vaste fossiele brandstoffen nog bestaat[36]: 70% van de vraag binnen de EU zou daaraan voldoen. Het lokaal gebruik van dergelijke opgewekte energie, en zeker in het geval van prioritair gebruik van die goedkopere energievormen, maar ook het kopen van goedkopere elektriciteit van buurlanden die niet voldoet aan de vereisten van hernieuwbare energieproductie, ontstaat een markvervorming.

Extern is de EU dus niet afhankelijk van import voor de voorziening van deze grondstof maar de externe aanvoer kan nog steeds goedkoper zijn dan de eigen ontginning. Zoals eerder aangegeven voor de interne argumenten, kan in het geval van extreme prijsstijging of in geval van de schaarste van de grondstof buiten de EU, ook de aan de EU interne exploitatie opnieuw worden aangeboord.

4.5.4.Kernenergie

Om tegemoet te komen aan de stabiliteit van de markt van deze strategische en hoog gepolitiseerde energievorm, is intern de EU een *supply*

[36] COM(2014)330 final; p.159.

agentschap opgericht: niet alleen voor de brandstof maar voor alle elementen die noodzakelijk zijn voor de uitbating van de energie is, omwille van het mogelijk dubbel gebruik een toegang verzekerd via die weg die zowel controle als beschikbaarheid garandeert. De controle wordt voor kernenergie mogelijk gemaakt aangezien exclusieve rechten worden toegekend om bevoorrading te voorzien in Europa en vanuit Europa naar de rest van de wereld via de Europese samenwerking in de materie (Euratom- European Atomic Energy Community). Daartoe geeft het Euratom-verdrag aan de European Supply Agency twee instrumenten:

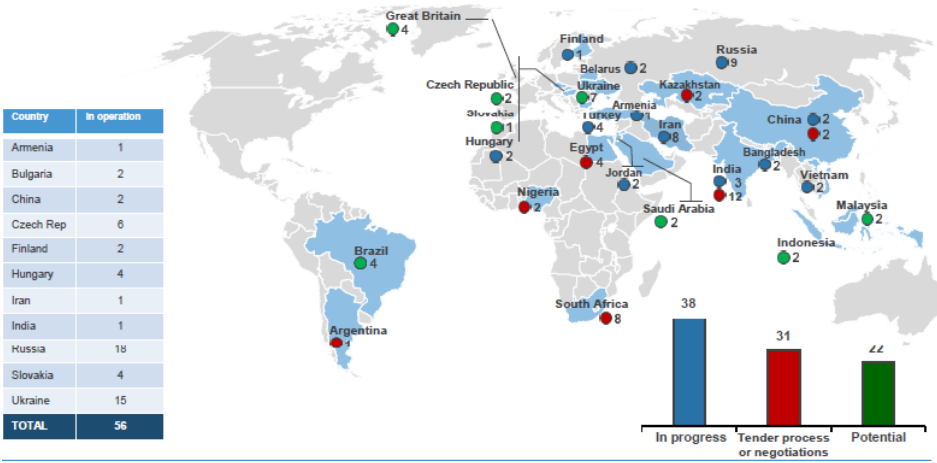
- het recht op optie voor ertsen, bronnen en splijtstoffen die geproduceerd worden op het grondgebied van de lidstaten;
- exclusieve rechten voor het afsluiten van bevoorradingscontracten voor erts, bronnen en splijtstoffen die afkomstig zijn van of uit de Euratom-gemeenschap.

Het optierecht, zoals voorzien door artikel 57 van het verdrag, vervat de eigendomsrechten van ertsen, bronnen, en splijtstoffen. De producenten van de gemeenschap worden gehouden om alle ertsen en splijtstoffen in eerste instantie aan de ESA aan te bieden voordat ze worden opgeslaan of vervoerd. Wanneer het agentschap ermee instemt, mogen materialen ter beschikking gesteld worden aan bedrijven die in de EU gelegen zijn. Dit laat controle toe door de Commissie, die moet geïnformeerd worden van eventuele afwijkingen van de algemene regel. Indien het optierecht niet wordt uitgevoerd door het agentschap, dient dit expliciet in de commerciële overeenkomst te worden vermeld, waarna de koper de volle eigendom van het materiaal verwerft: in het geval van bijzondere splijtstoffen (die in aanmerking komen voor tweeërlei gebruik) kan de koper enkel het gebruiksrecht kopen zonder over het eigendomsrecht van het materiaal te beschikken. Het tweede instrument, exclusiviteit, wordt gestoeld op artikel 52 van het verdrag. Dit geeft aan het Agentschap, als enige actor, het recht om contracten toe te staan en af te sluiten die betrekking hebben op de bevoorrading van materiaal, inclusief materiaal voor tweeërlei gebruik zoals uranium (in alle vormen), plutonium en thorium. De rol van ESA is om diversificatie van bronnen in de nucleaire sector te vergemakkelijken en wil intern de EU ook aanzetten om niet te veel afhankelijkheid van één enkele leverancier in de hand te werken: een voorbeeld van een dergelijke situatie zijn VVER reactoren die door hun constructie enkel kunnen gevoed worden door Russische brandstof. Tegelijkertijd wil het agentschap trends identificeren die mogelijk de toegang tot bronnen en brandstof zouden kunnen bedreigen en kan ook optreden indien een dergelijke afhankelijkheid zich op korte termijn zou voordoen.

De externe elementen die van belang zijn in deze energievorm zijn vaak afkomstig van een van de P5 landen (permanente leden van de VN-

veiligheidsraad, die zowel de militaire als de civiele exploitatie van kernenergie onder controle hebben en die door hun ervaring een belangrijke plaats innemen in de nucleaire markt). De vereisten van de EU om een lagere uitstoot van broeikasgassen te genereren de komende jaren, maakt van deze energievorm bovendien een bruikbaar alternatief aan de meer vervuilende fossiele brandstoffen. Hetgeen een markt garandeert voor de bestaande producenten, zoals Rosatom die voor de komende jaren zowel nationaal als internationaal een ruim klantenbestand kan genieten. Figuur één geeft hiervan een overzicht.

Figuur 1: Rosatom-markt voor kerninstallaties (Andrey Rozdesthvin, 2015. Rosatom France)

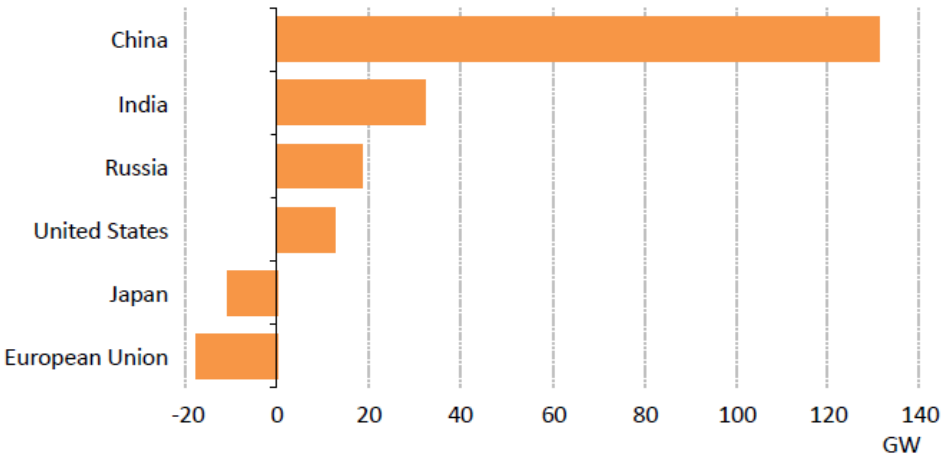


Country	In operation
Armenia	1
Bulgaria	2
China	2
Czech Rep	6
Finland	2
Hungary	4
Iran	1
India	1
Russia	18
Slovakia	4
Ukraine	15
TOTAL	56

De informatie die in dit kader wordt gegeven is commercieel en dient dus met de nodige voorzichtigheid te worden gehanteerd en dit om twee redenen. Vooreerst is de eigen capaciteit van Rusland voornamelijk gehandhaafd door de verlenging van de levensduurte van bestaande reactoren: twee derde van hun reactorenpark heeft een verlenging toegestaan gekregen tot 40 jaren. Bovendien is de informatie van lopende contracten niet altijd correct: de informatie die in de figuur wordt gegeven als zou Iran 8 kerncentrales in uitvoering hebben is niet correct: informatie van Iraanse overheden toont dat op het ogenblik van de productie van de informatie slechts twee projecten het stadium van de MoU hadden bereikt (Personal communication Ambassador Soltanieh. EU non-proliferation consortium on 11-12 november 2015). Een element dat zeker niet mag vergeten worden in de evaluatie van de beschikbare capaciteit en energie infrastructuur, is dat in de Europese Unie heel wat ervaring en capaciteit aanwezig is: bovendien zijn aanrijking en de aanmaak van brandstof eveneens door Europese technologie beheersd waarvoor onder meer Areva en het Urenco consortium. Echter, de economische en financiële crisis, de ramp van Fukushima en ideologische motivaties hebben gezorgd voor een terugloop van de nucleaire technologie in

het Westen hetgeen merkbaar werd op de orderlijst van voornoemde firma's en consortia. De ervaring van Europa in deze is echter van die aard dat ze in de toekomst nog veel meerwaarde kan brengen op eigen grondgebied of in het buitenland en dit zowel voor het realiseren van een koolstofvrije energie als voor de beveiliging van de technologie tegen proliferatierisico's, veiligheidsrisico's en voor het genereren van een stabiele baseload aan stroom die door alternatieve energievormen niet kan worden gegenereerd. De beveiliging van de energieproductie komt echter in het gedrang wanneer successieve beleidsbeslissingen onstabiliteit genereren voor de toekomst van een technologie die per definitie een lang stabiel institutioneel kader vergt voor het winnen van terugverdieneffecten: de productie van brandstofstaven is geen activiteit die onmiddellijke output genereert. Het is niet ongewoon om een dergelijke vraag zes maanden of meer voor de werkelijke noodzaak te lanceren om een stabiele en geplande transitie te kunnen realiseren. Het wegblijven van dergelijke bestellingen door commerciële exploitanten om voormelde redenen kan dus voor onderbrekingen zorgen van de energieproductie uit deze bronnen. Deze afhankelijkheid van brandstof kan in sommige gevallen nog worden aangescherpt in het geval van Oost-Europese VVER type reactoren die afhankelijk zijn van het Russische Rosatom. De mechanische eigenschappen van die brandstof zijn van die aard dat geenenkele andere leverancier in de mogelijkheid is om de oorspronkelijke brandstofstaven te vervangen tenzij ze expliciet daarvoor worden vervaardigd maar niet in de standaardproductie proces van andere producenten is voorzien. Wetende dat een deel van de markt beheersd zal worden door extra-Europese actoren in de toekomst, is het waarschijnlijk dat de landen waarin de groei het grootst is en die over de technologie beschikken ook de technologie zullen verkopen aan landen die er de aanwending van hebben teruggeschroefd en op die manier een nieuwe afhankelijkheid tot stand komt. Het is bijgevolg cruciaal voor de overblijvende installaties in West-Europa dat een pallet van leveranciers binnen en buiten de EU beschikbaar blijft voor het opereren en fuelen zodat geen artificiële afhankelijkheid tot stand komt in een sector die een alternatief biedt voor het behalen van de strikt noodzakelijke baseload capaciteit van elektriciteit.

Figuur 2: Nucleaire capaciteit in de toekomst 2013-2040 (Nobuo Tanaka, 2015; p.19).



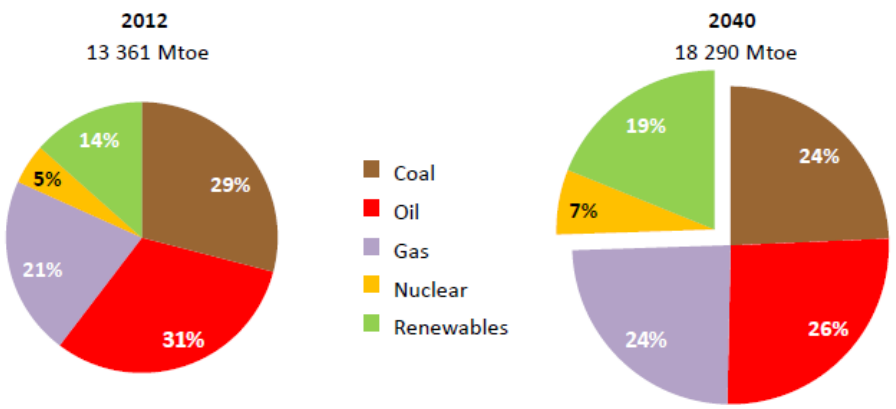
4.5.5.Hernieuwbare energie

Intern de EU is de toedracht van hernieuwbare energie toegenomen teneinde de afhankelijkheid van fossiele brandstoffen te reduceren. We hebben in vorig hoofdstuk gezien dat een dergelijke benadering voor andere technieken het gevaar inhoudt nieuwe afhankelijkheden te genereren in de productieprocessen van deze technologie. Voor wat hernieuwbare energie betreft is de EU zowel voor opwekking, verwarming als voor transport van bij aanvang van het proces een belangrijke actor geweest: de richtlijn van 2009 met betrekking tot hernieuwbare energie heeft de lidstaten van bij aanvang te behalen doelstellingen voor ogen gehouden te weten een toedracht van 20% hernieuwbare energie aandeel in het totale verbruik en 10% van de marktbezetting voor hernieuwbare bronnen voor transport. In het bijzonder werden financiële tegemoetkomingen voorzien voor het intensiever gebruik van alternatieve energiebronnen. Drie landen in de EU behaalden hun 2020 doelstellingen reeds in 2012 te weten Zweden, Estland en Bulgarije. De ontwikkelingen in de andere landen, hoewel de doelstellingen nog niet werden behaald, hebben ervoor gezorgd dat de import van traditionele bronnen naar beneden kon worden geprojecteerd: hoewel een toename in verbruik in absolute waarde kon worden vastgesteld, wordt aangenomen dat die toename nog groter was geweest zonder de toedracht van hernieuwbare bronnen.

4.5. Deelbesluit

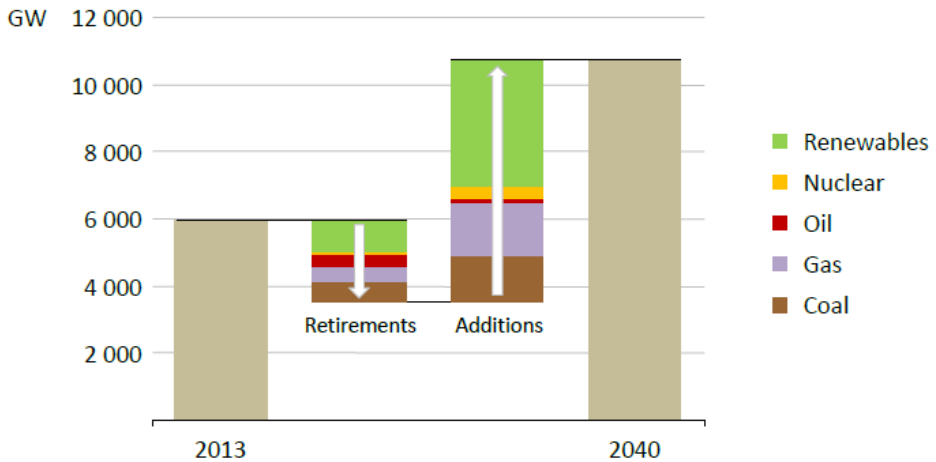
Als samenvatting van dit gedeelte met betrekking tot de verschillende energiebronnen voor Europa geldt dat in de toekomst wordt verwacht dat de afhankelijkheid van de EU zowel voor olie als gas en mogelijk ook voor nucleaire industrie zal toenemen. Tegen 2040 wordt, zoals figuur 3 het aangeeft een vermindering van de toedracht van olie en kolen verwacht; dit verloren segment wordt overgenomen door hernieuwbare bronnen, maar ook door gas en kernenergie. Een mogelijke afhankelijkheid in deze twee sectoren is daarom een verontrustende tendens

Figuur 3: Projectie van de bijdrage van verschillende energiebronnen (Nobuo Tanaka, 2015; p.4).



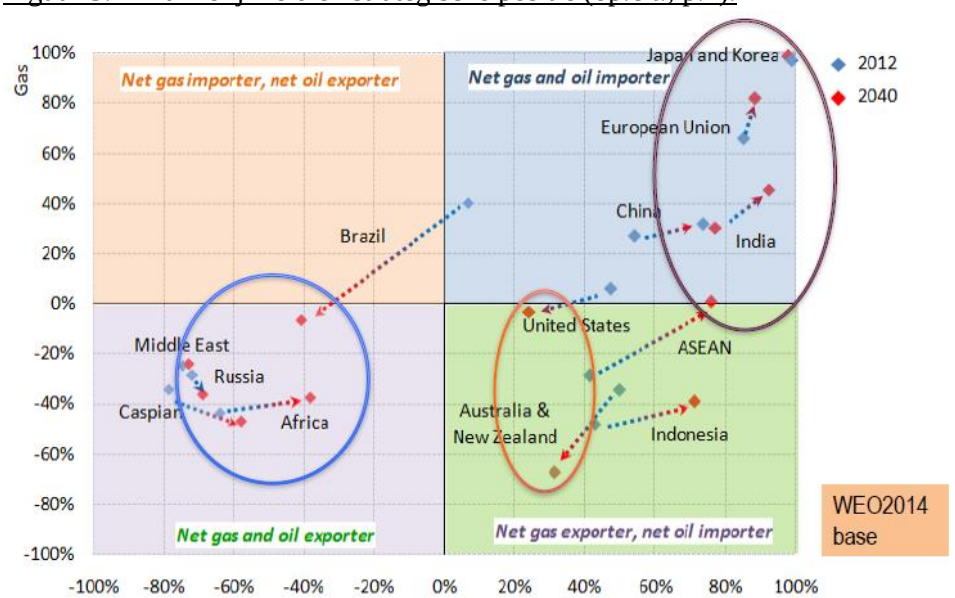
De afname van vaste koolwaterstoffen in de energiemix is een niet overeengekomen gegeven. Andere projecties laten eerder een tendens van toename van die bron uitschijnen tegen 2040. Figuur 4 geeft een idee van de absolute waarden van de veranderingen in de energiemix tegen 2040 waarin opnieuw de toename van gas, hernieuwbare bronnen en kernenergie duidelijk wordt onderlijnd.

Figuur 4: Projectie van absolute waarde van verschillende energiebronnen (Fatih Birol, 2015; p.9).



Deze aanpassing van de verdeling van bronnen gaat echter gepaard met een verschuiving (lees toename) van de vastgestelde afhankelijkheden. Voor gas blijkt die toename meer uitgesproken dan voor olie. Figuur 5 illustreert dat de EU, samen met China, India, en Japan die weinig benijdbare plaats inneemt van grootste afhankelijkheid.

Figuur 5: Afhankelijkheid en strategische positie (op.cit.; p.7).



Ook de productiecijfers van Europa in 2013 tonen aan dat de EU inderdaad achter staat op gebied van energie onafhankelijkheid en dat in het bijzonder de landen van West-Europa daar de voornaamste toedracht in

hebben. Het ontbreken van een voldoend vernieuwd en vernet distributie netwerk draagt daartoe bij. In het bijzonder was voor ons land onmiddellijk na de ramp van Fukushima in de cijfers duidelijk dat kernenergie een niet te versmaden bijdrage levert aan een koolstofarme energieproductie en deel uitmaakt van de kritieke energie infrastructuur van ons land (Tanaka, 2015; p.13). De enige oplossing die de EU in die vooruitzichten heeft bestaat eruit om decarbonisatie, betaalbaarheid en veiligheid van de voorziening te garanderen door:

- het beschikbare energiepallet zo ruim mogelijk te houden,
- kernenergie niet af te schrijven vanuit ideologische overwegingen,…
-…de expertise die het in dit domein heeft opgebouwd te exporteren,
- een stijgende vraag van energie te combineren met een stijgende energie efficiëntie,
- een gemeenschappelijk energetisch beleid aan te wenden dat de nationale voorkeuren en belangen compenseert met een gegarandeerde beschikbaarheid van energie aan een betaalbare prijs: voor het ogenblik is het nog steeds een gangbare praktijk om minder lucratieve elektriciteitsproductie vanuit gascentrales op te geven ten voordele van import van landen die hetzelfde vermogen opwekken via verouderde kolencentrales (vb. Hongarije dat importeert van de Tsjechische republiek). Commerciële overwegingen alleen gaan soms in tegen de geest van de 2020-doelstellingen en de alternatieven moeten dus gesteund worden door een gemeenschappelijk beleid ter zake,
- een betere connectiviteit van transport- en opslagcapaciteit als aanvulling van een voldoende generatiecapaciteit binnen de EU,
- mogelijk diversificatie van bronnen te verruimen, bijvoorbeeld door productie van schaliegas of meer import uit andere gebieden.

Deel 5

Hoe ver staat België?

5.1. Inleiding

In een laatste deel gaan we na hoe ons land zich positioneert in deze problematiek en tracht men te identificeren welke de uitdagingen zijn die ons op middellang tot lang termijn staan te wachten. Kritieke infrastructuren en a fortiori de bescherming ervan zijn in België al een tijd een rijpende materie. In 2010, werd reeds in een studie als aanbeveling aangestuurd op een interdisciplinaire en multi-departementale aanpak van de problematiek, inclusief de betrekking van Defensie (Smedts, 2010; 139): de aanbeveling is nog brandend actueel, nu we vertrekkend uit een omschrijving van kriticiteit tot de vaststelling zijn gekomen dat de traditionele bescherming van kritieke infrastructuur tekort schiet en dat nu ook en vooral cascade effecten moeten zien vermeden of mogelijk gecontroleerd moeten worden. In die redenering is kritieke energie infrastructuur als een prioritair element naar de voorgrond getreden. In het verder verloop van de uiteenzetting werd vervolgens ook duidelijk dat de traditionele aanpak van bescherming, een nieuw luik van cybernetische bescherming zou moeten erkennen naast het reeds bestaande luik van fysische bescherming. Verder dragen structurele elementen die overigens ook passen in een strategisch beleid naar energieveiligheid bij tot de verzekering van energiebeschikbaarheid. In wat volgt gaan we na hoe de wetgever de beveiliging en bescherming van kritieke energie heeft georganiseerd.

5.2. Wetgeving

De wet die de beveiliging en bescherming van kritieke infrastructuren regelt in ons land, dateert van 1 juli 2011 en voorziet een gedeeltelijke omzetting van de Europese richtlijn van de Raad van 8 december 2008 (2008/114/EG) inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren. Als nationaal contactpunt voor de Europese kritieke infrastructuren[37] wordt de Algemene Directie van het Crisiscentrum (ADCC) aangeduid en wordt daardoor het EPCIP (European Program for Critical Infrastructure Protection) contactpunt voor alle sectoren in België ten opzichte van de EU. In die hoedanigheid coördineert het ook de beveiliging en bescherming van de energiesector (elektriciteit, olie en gas), met uitzondering van nucleaire installaties die aangeduid worden door de wet van 15 april 1994[38] tenzij die gedeelten ervan die als bestemming hebben elektriciteit te produceren en/of te verdelen. Voor de aanduiding van de kritieke infrastructuur in de sector energie is de sectorale overheid bevoegd, waarmee men doelt op Minister bevoegd voor Energie of, bij delegatie door deze, een leidend personeelslid van zijn administratie. De aanduiding gebeurt na consultatie met de betrokken gewesten en indien nodig de vertegenwoordigers van de sector en/of exploitanten. Merkwaardig in deze wet is te merken hoe, in tegenstelling tot de benadering die in het eerst deel van dit werk werd vermeld en die de kriticiteit meet aan de hand van de gevolgen van bijvoorbeeld cascade effecten, deze opnieuw tot een sectorale aangelegenheid herleid. De maat van kriticiteit voor de nationale kritieke infrastructuur worden immers bepaald door “intersectorale criteria”(Art.6, §3)…

[37] Art.3 van de Wet van 1 Juli 2011 (6°, 5° en 4°): De nationale kritieke infrastructuur waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag in ten minste twee lidstaten van de Europese Unie zou hebben”. Waarbij de nationale kritieke infrastructuur wordt omschreven als” kritieke infrastructuur op het Belgisch grondgebied waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag in het land zou hebben” en kritieke infrastructuur wordt gedefinieerd als “installatie, systeem of een deel daarvan, van federaal belang, dat van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, en waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag zou hebben doordat die functies ontregeld zouden raken”.

[38] betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.

1° het aantal potentiële slachtoffers, met name het aantal doden of gewonden, of
2° de potentiële economische weerslag, met name de omvang van de economische verliezen en/of van de kwaliteitsvermindering van producten of diensten, met inbegrip van de weerslag op het milieu, of
3° de potentiële weerslag op de bevolking, met name de weerslag op het vertrouwen van de bevolking, het fysieke lijden en de verstoring van het dagelijkse leven, met inbegrip van het uitvallen van essentiële diensten.

…waarvan de drempelwaarden door de sectorale overheid worden bepaald (§4) in overleg met de ADCC, eventueel na raadpleging van de betrokken gewesten: deze worden gebaseerd op de ernst van de gevolgen van de verstoring van de werking of de vernietiging van een bepaalde infrastructuur. Voor Europese kritieke infrastructuur wordt de mate van kriticiteit bepaald door dezelfde criteria, maar waarvan de niveaus van weerslag of drempelwaarden geval per geval worden bepaald door de sectorale overheid in overleg met de ADCC, de betrokken lidstaten en, in voorkomend geval de betrokken gewesten. In beide gevallen wordt de potentiële aanduiding als kritieke infrastructuur gebaseerd op een geïsoleerde sectorale evaluatie die aan de overheid wordt voorgedragen. In geen van de gevallen wordt aan de basis van die aanduiding gebruik gemaakt van effecten van feedback loops of cascade effecten. Hetzelfde geldt trouwens voor de dreigingsanalyse die door de aangeduide infrastructuur exploitant moet worden opgesteld: hoewel de wettekst een analyse voorziet van de 'potentiële weerslag van de verstoring van haar werking of haar vernietiging' (Art.13, §3., 3°), wordt op geenenkel moment concreet besproken welke de daartoe voorziene externe contacten zouden kunnen zijn. Hetzelfde geldt voor de bijlage van de wettekst die de procedure detailleert voor de identificatie van de nationale en Europese kritieke infrastructuur: het enige intersectorale aspect dat in aanmerking werd genomen zijn de gevolgen voor de samenleving door de uitval van die ene infrastructuur voor dewelke beveiligingsmaatregelen werden uitgewerkt in het beveiligingsplan exploitant, zonder de penetratie naar andere sectoren te vermelden. De bijlage vermeldt in dit verband nog dat rekening dient te worden gehouden met 'het bestaan van vervangingsoplossingen, alsook met de duur van de verstoring/herneming van de activiteit (Bijlage, punt A). Mogelijk wordt dit in sommige gevallen in de individuele beveiligingsplannen voorzien, zonder evenwel op een systematische wijze te worden hernomen in de wetgeving: de complexiteit van de interacties met andere sectoren laat bovendien geen generieke oplossing toe, maar moet op een systematische wijze worden onderzocht, en de vereiste van een dergelijk onderzoek moet misschien opgenomen worden in de wetgeving. De resultaten ervan opnemen in sectorale plannen, kunnen dan in een afzonderlijke paragraaf verwijzen

naar de directe weerslag op ander sectoren en voor welke type verstoringen deze zich zouden manifesteren en welke beschermingsmaatregelen in de oorspronkelijke installatie deze overloop naar andere sectoren zou kunnen vermijden.

Het koninklijk besluit van 11 maart 2013 voorziet in de uitvoering van de artikelen 13, 24 en 25 van de wet van 1 juli 2011 met betrekking tot de beveiliging van kritieke infrastructuur en in het bijzonder voor de sector energie: hoofdstuk 2 van het K.B. geeft het toepassingsgebied (sector Energie voor nationale en Europese kritieke infrastructuren). De vitale functies die in dit verband onder de loupe worden genomen zijn elektriciteit, aardgas en aardolie. Meer bepaald wordt in elk van deze domeinen aandacht geschonken voor de productie en de verdeling. In detail[39] wil het K.B. de aandacht vragen voor:

-elektriciteit: elektriciteitsproductie en –transmissie,

-aardgas: behandeling, opslag, transmissie en terminals voor vloeibaar gas (LNG),

-aardolie: raffinage, behandeling, opslag en transport;

Informatie-uitwisseling en oefeningen enerzijds, maar ook inspecties moeten ervoor zorgen dat de maatregelen die door voornoemde worden genomen adequaat zijn en op regelmatige basis worden aangepast aan de risicoanalyses. De informatie-uitwisseling en oefeningen moeten ervoor zorgen dat een beveiligingsplan van de exploitant voorhanden is, terwijl regelmatige inspecties ook moeten zorgen voor een bevestiging dat een beveiligingsplan overeen komt met de wettelijke vereisten, maar ook dat de maatregelen erin beschreven effectief worden uitgevoerd en dat oefeningen op regelmatige tijdstippen worden georganiseerd.

[39] K.B.van 11 maart 2013, Art.4.

5.3. Fysische bescherming

Private partners hebben voor fysische bescherming een belangrijke rol te vervullen omdat verantwoordelijken voor beveiliging van grote ondernemingen, instellingen en organisaties onder meer, tot opdracht hebben om gevoelige sites, gebouwen, operaties en installaties te beveiligen tegen diverse vormen van kwaadwilligheid zoals georganiseerde misdaad, onrechtmatige informatie inwinning, terrorisme,…: kennis en kunde in zeer diverse gebieden is daartoe vereist (inschatting van de mogelijke dreigingen, inschatting van de aanvalsmiddelen en tactieken die bepaalde groepen zouden kunnen aanwenden, inschatting van de efficiëntie van diverse aanvalsmiddelen, mogelijke ontradingsmaatregelen, mogelijke detectiemaatregelen, mogelijke vertragingsmaatregelen, organisatie van de respons, etc….). Vanuit deze nood is van bij aanvang van de problematiek dan ook een vraag naar expertise en ervaring van elke publieke en private actoren die daartoe kan bijdragen. Onder de publieke actoren heeft ook Defensie een plaats omwille van expertise die niet noodzakelijk in de civiele wereld kan gevonden worden[40]: zo wordt voor organisatie en logistiek vaak op Defensie beroep gedaan omwille van de expertise op dat vlak. Het is dan ook in informele contactgroepen dat dergelijke publiek en private wisselwerking tot stand kan komen zoals het contactpunt tussen ECSA[41] en Defensie waarbij bepaalde problematiek of concrete situatie aangehaald wordt, en expertise uitgewisseld: een dergelijke ad hoc structuur kan dan wel voor concrete projecten een oplossing bieden, doch voor structurele oplossingen op nationaal niveau schiet een dergelijke vrijblijvende reflectie tekort.

Het platform kritieke infrastructuren (verder: Platform CIP) komt waarschijnlijk beter ten goede aan het geheel van noden en bestrijkt een groter aantal actoren. Het heeft als doel het verder ontwikkelen en operationaliseren van het werkingskader en de werkingsprocessen ter beveiliging en ter

[40] Effecten van explosieven op gebouwen, ballistische bescherming, eigenschappen van aanvalsmiddelen die door de georganiseerde misdaad of terroristische groeperingen zouden kunnen aangewend worden (zware bewapening, RPG's, mortieren, snijladingen, …), effecten van en bescherming tegen BCR agentia, elektromagnetische aanvallen.

[41] De Belgische vzw "European Corporate Security Association (ECSA)" is de beroepsvereniging van personen uit de publieke, private en academische sector die actief zijn in, of bijdragen tot, de beveiliging van ondernemingen, organisaties of instellingen tegen daden van kwaadwillige oorsprong. De Raad van Bestuur bestaat uit vertegenwoordigers van de publieke, private en academische sector.

bescherming van de kritieke infrastructuren op een gecoördineerde, gevalideerde wijze die uitvoerbaar is voor alle betrokken actoren. Permanente leden van het platform kritieke infrastructuren omvatten de Federale Politie, het OCAD, Defensie, VSSE (voor het wetenschappelijk en economisch potentieel-WEP), het centrum voor cyberveiligheid (Centre for Cyber Security Belgium-CCB) en NVO (voor Veiligheidsverificaties). In functie van de noden kunnen ook sectorale overheden en lokale politie en experten bij de discussie worden betrokken. Daar waar de beveiliging en de bescherming van de kritieke infrastructuren voor een deel bij de opdracht van de inlichtingendiensten past voor wat de bescherming van het wetenschappelijke en economisch potentieel (WEP) betreft, kunnen alle taken niet daartoe verbonden worden herleid: het aantal exploitanten binnen specifieke sectoren, maar anderzijds ook concrete implicaties heeft immers werking op meerdere overheidsdiensten (ADCC, Federale Politie, Lokale Politie, FANC, NVO, OCAD, Defensie, CCB, Belnet/Cert, Fedict, BIPT, Nationale Bank, FOD Financiën, FOD Mobiliteit, FOD Economie, …). Een van de taken van het platform zal eruit bestaan om de bestaande methodologie voor identificatie en beveiliging van kritieke infrastructuren te optimaliseren. Voor het ogenblik identificeren sectorale overheden (na advies van het Crisiscentrum-Algemene directie Crisiscentrum-ADCC) de kritieke infrastructuur. De exploitanten dienen beveiligingsmaatregelen te nemen, die bij verhoogde dreiging moeten worden opgeschaald en in overeenstemming moeten worden gebracht met de externe beschermingsmaatregelen beslist door ADCC en uitgevoerd door de politiediensten. Het platform zal op middellang termijn een omvattend en coherent mechanisme van beveiliging en bescherming van kritieke infrastructuren moeten tot stand brengen waarbij elke betrokken actor zijn taken in het geheel vervult volgens gecoördineerde, concrete en praktisch functionerende processen. De aandachtspunten die in dit platform aan bod zullen komen worden in wat volgt bondig besproken.

De fysische bescherming van nucleaire installaties wordt voorzien door de wet van 1994: na de ramp van Fukushima werd door de Europese Raad besloten om de veiligheid van de Europese kerncentrales te toetsen en daartoe een stresstest op te leggen. De uitvoering ervan zou onder de modaliteiten bepaald door de European Nuclear Safety Regulators' Group (ENSREG) worden uitgevoerd, vertaald door de nationale regulatoren, in casu het Federaal Agentschap voor Nucleaire Controle (FANC): de bedoeling zou zijn de gevolgen van natuurlijke of door de mens veroorzaakte rampen te ontwaren die een situatie zouden genereren die niet meer beheersbaar is omwille van ongewenste neveneffecten. In dit geval is er een bijkomende motivatie omdat ze, in tegenstelling tot andere installaties, in 'ernstige ongevalsomstandigheden aanleiding kunnen geven tot radiologische gevolgen voor de omgeving en het publiek.' (SCK.CEN, 2012; p8) als gevolg van

aardbevingen, overstromingen, extreme weersomstandigheden, branden, terroristische aanvallen, aanvallen met toxische gassen, explosieven, externe computeraanvallen en zelfs in geval van het wegvallen van stroom of on-site black-out (FANC, 2011; p.4). De aanpak van de stresstest is het enige voorbeeld dat als gevolg van een grootschalige ramp alle invloeden op de werking van nucleaire installaties in kaart wou brengen. Niet alleen de kerncentrales maar ook andere nucleaire installaties werden aan een dergelijke test onderworpen om bij vaststelling van eventuele tekorten een actieplan op touw te zetten en de vordering van de uitvoering ervan op zijn minst jaarlijks te sturen.

5.3.1.Dreigingsanalyses

In een eerdere studie (Smedts, 2010; p.120) werd reeds melding gemaakt van een te verbeteren aanpak voor de punctuele dreigingsanalyses onder de verantwoordelijkheid van het OCAD (in toepassing van de artikelen 10 en 15 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren). Deze evaluaties dienen alle dreigingen in rekening te brengen en slaan dus dan niet alleen op terroristische activiteiten maar op elk type van dreiging die onder de bevoegdheid van de ondersteunende diensten valt. Immers, de werking van kritieke infrastructuren kan ook verstoord worden door bv. problemen van openbare orde, vermogenscriminaliteit, cybercriminaliteit of –activisme, insider threat, … . Het OCAD heeft sindsdien te kennen gegeven inderdaad niet over de mogelijkheden te beschikken om deze opdracht uit te voeren voor wat de punctuele evaluaties betreft. Op het vlak van risicoanalyses en dreigingsanalyses, zouden in 2015 voornamelijk initiatieven worden genomen in de sectoren ruimtevaart, havens, elektriciteit, gas en financiën, tussen het OCAD enerzijds en anderzijds bevoegde sectorale overheden en de exploitanten. Wat dit betreft is tot hier toe steeds de aandacht gegaan naar beveiliging van infrastructuur tegen fysische dreigingen. Het zijn dus pas de meest recente initiatieven die de aandacht gaan moduleren om ook energie en energie infrastructuur in rekening te nemen. Na de aanslagen in Parijs van november 2015 is echter de aandacht vooral naar de preventie van nieuwe aanvallen op zachte doelwitten gegaan en is het zwaartepunt niet echt meer te vinden in kritieke energie infrastructuur.

5.3.2.Samenwerking tussen de eigenaars en operatoren van kritieke infrastructuren en de overheid

Het aanspreekpunt en de verantwoordelijke voor de coördinatie van de fysische veiligheid is de algemene directie van het Crisiscentrum (ADCC) dat belast is met de nationale coördinatie van de uitvoering van de nationale en de Europese reglementering inzake de beveiliging en de bescherming van de kritieke infrastructuren. De beleidsnota binnenlandse zaken vermeldt in verband met de coördinatie tussen de betrokken infrastructuren in het algemeen en energie-infrastructuren in het bijzonder het volgende (Kamer van Volksvertegenwoordigers, 2014; p.12):

> "Het Crisiscentrum zal, conform het regeerakkoord en in de schoot van de Nationale Veiligheidsraad, de categorieën van personen (met toegang tot gevoelige informatie of tot gevoelige sites) en die het voorwerp kunnen uitmaken van een veiligheidsscreening uitbreiden en objectiveren. Het Crisiscentrum fungeert tevens als nationaal contactpunt ten aanzien van de Europese instellingen en de andere Europese landen in dit verband. De betrokken sectoren waarop wordt gewerkt zijn Energie (elektriciteit, gas, olie), Transport, Elektronische Communicatie, Financiën en Ruimtevaart. Op juridisch vlak, werd de vermelde wetgeving intussen gedeeltelijk uitgevoerd (op het vlak van Energie, Havens, Financiën en Ruimtevaart), maar dienen nog bijkomende initiatieven te worden genomen op het vlak van de Nucleaire installaties, de Elektronische Communicatie en de Spoorwegen. Ook een Richtlijn van de minister van Veiligheid en Binnenlandse Zaken met betrekking tot het operationeel politioneel informatiebeheer in dit specifieke domein zal worden voorbereid, evenals een Richtlijn van de Nationale Veiligheidsoverheid voor wat Ruimtevaart betreft en een hernieuwd Protocolakkoord tussen het Crisiscentrum en de Nationale Bank van België. Op het vlak van de identificatie van de kritieke infrastructuren zullen in 2015 op nationaal niveau voornamelijk de sectoren Financiën, Elektronische Communicatie, Transport en Olie aan de orde zijn. Op Europees niveau, zal hoofdzakelijk gewerkt worden aan een Pilot Project rond Energie. Ter ondersteuning van het operationeel beheer van incidenten en dreigingen ten aanzien van kritieke infrastructuren, zullen de databases en procedures van het Crisiscentrum worden geactualiseerd. Op Europees niveau, zal het CIWIN-samenwerkingsplatform (*Critical Infrastructure Warning Information Network*) worden hervormd."

Een richtlijn van de Minister van Veiligheid en Binnenlandse Zaken zal het operationeel politioneel informatiebeheer rond de beveiliging en de bescherming van de kritieke infrastructuren concretiseren: samenwerking

tussen exploitanten/eigenaars van kritieke infrastructuren en de politiediensten dient daartoe te worden uitgewerkt. Praktische modaliteiten kunnen daarom worden uitgewerkt tussen de exploitant en de contactpersonen van de geïntegreerde politie via een "politieloket" ("front office"). Dit loket heeft zowel een lokaal als een federaal luik: dossierbeheerders bij de lokale politie worden aangeduid op initiatief van ADCC, terwijl de federale politie de federale component van het loket invult.

5.3.3.Andere betrokken overheidsactoren t.a.v. de kritieke energie infrastructuren

Het is reeds vermeld welke de belangrijkste actoren zijn die worden vermeld in de wet van 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren a fortiori energie-infrastructuren (ADCC, sectorale overheden en exploitanten, politiediensten, het OCAD). Een aantal ander actoren die ook in de problematiek zijn betrokken zonder evenwel in de wet te worden vermeld, vervolledigen onvermijdelijk het landschap. Het feit dat energie onmiddellijke impact zal hebben op het economische potentieel van het land, is het onvermijdelijk, dat ook de Veiligheid van de Staat (VSSE) in de problematiek zal moeten worden betrokken. Daar waar er bovendien een internationale dimensie bijkomt, omwille van het grensoverschrijdend karakter van de effecten dan wel voor de oorzaak die tot de verstoring van de goede werking van de infrastructuur heeft geleid, is ook de militaire inlichtingendienst (ADIV) een actor die in de problematiek dient te worden opgenomen. Gezien de mogelijk cybernetische oorzaak van de verstoring zullen ook de verantwoordelijke actoren in dat domein hun plaats hebben voor de structurele en systematische aanpak van de problematiek (CERT, CCB). Het zal dan ook waarschijnlijk een van de taken zijn van het nieuwe platform CIP om de coördinatie met deze actoren uit te werken en indien mogelijk hun bevoegdheden vast te leggen in de wetgeving.

5.3.4.Plaatsen van militair belang

Naast de aandacht die vanuit de civiele wereld naar kritieke energie-infrastructuur kan gaan, definieert de wet van 2011 de andere punten van federaal belang: « de plaatsen die niet zijn aangeduid als kritieke infrastructuur, maar die van bijzonder belang zijn voor de openbare orde, voor de bijzondere bescherming van personen en goederen, voor het beheer van noodsituaties of voor de militaire belangen en die het nemen van beschermingsmaatregelen door de ADCC zouden kunnen noodzaken » (art. 3,7°). Het is dan ook duidelijk dat deze infrastructuren die van militair belang zijn, raakpunten kunnen vertonen met een lijst kritieke energie-infrastructuur,

maar dat die lijsten niet noodzakelijk overeen zullen stemmen met de lijst die een overheidsdienst zou kunnen opstellen, die op zijn beurt weer niet noodzakelijk overeenstemt met een lijst die een private partner zou opmaken: daar waar een private partner zijn te beschermen infrastructuur zal willen opstellen op winst te maximaliseren, zal een publieke overheid die eerder opstellen om de duurzaamheid van de dienstverlening te kunnen garanderen. Een militaire instantie zal, los van de twee voornoemde motivaties eerder oog hebben voor de vrijwaring van de eigen operationele capaciteit en de te beschermen infrastructuur in functie daarvan bepalen (bijvoorbeeld de NAVO-pijpleiding vertrekkende in de haven van Gent en van belang voor de bevoorrading van de Nationale Luchthaven, of aan de Marine-basis gelegen in de haven van Zeebrugge). Daarnaast stelt zich de vraag welke kritieke infrastructuren (zoals havens, telecommunicatie-infrastructuur, gas, olie, elektriciteit, …) een bijzonder belang vertonen voor Defensie en daardoor voor Defensie een andere prioriteit zouden kunnen genieten dan deze die voorzien zijn door de civiele overheden. Als gevolg daarvan kan een nood aan prioritisatie bestaan die de samenwerking tussen civiele en militaire autoriteiten op niveau van het Platform CIP, het ADCC in uitvoeringsfase, maar eerst en vooral op niveau van de politieke prioriteiten wat dat betreft. Het is de bedoeling dat in een eerste fase een analyse zal worden gemaakt door Defensie om deze voor te leggen aan het Platform CIP. In een tweede fase zal echter naar raakpunten tussen twee lijsten moeten worden gezocht en overgegaan worden tot prioritisering: twee elementen kunnen daarvoor noodzakelijk zijn. Een eerste is een dynamische aanpassing van deze lijsten, hetgeen een permanente wisselwerking tussen civiele en militaire overheden vergt enerzijds en een dynamische evaluatie van de dreiging op de gelijste infrastructuren en hun spill-over effecten. Daar waar een dergelijke consultatie mogelijk was in de schoot van het ADCC, is die vandaag niet meer mogelijk door het ontbreken van een permanente militaire vertegenwoordiging aldaar. Het creëren van een permanent militaire liaison lijkt in dat opzicht een goede oplossing. Daarnaast zal in eerste instantie ook een politiek overleg en/of akkoord nodig zijn om het gedeelte prioritisering vast te leggen: ook die prioriteiten bepalen zal een keuze zijn die mogelijk op een dynamische wijze in de tijd moet kunnen aangepast worden. De problematiek toont ons dat het meer behelst dan een administratief dossier voor te leggen aan het platform CIP voor verder opvolging.

5.3.5.Sectoren

De sectoren waarin voor het ogenblik vanuit de ontstaansgeschiedenis van de Europese Richtlijn kritieke infrastructuren worden aangeduid behoren tot de initiële domeinen te weten Energie (elektriciteit, gas en olie), Transport (spoor, maritiem, luchtvaart), Financiën, Elektronische Communicatie en

Ruimtevaart. In dit voorbeeld komen we tot de vaststelling dat de sectoren nog steeds als afzonderlijke entiteiten worden behandeld en de infrastructuren die dienen te worden beveiligd eveneens. Los van het feit dat die sectoren niet volstaan, noch de afhankelijkheden tussen sectoren in beschouwing wordt genomen, is ook op nationaal niveau de oefening te maken. Dit is een van de taken van het platform CIP dat moet onderzoeken of deze huidige afbakening volstaat, dan wel op termijn dient te worden uitgebreid. Zo wordt de identificatie van kritieke infrastructuren in sommige deelsectoren enkel als Europese kritieke infrastructuren beschouwd en vallen domeinen als ICT, Chemie/Seveso, Water en Volksgezondheid niet onder de scope. Bovendien zal ook, in de schoot van het platform moeten worden uitgemaakt of een kritieke energie infrastructuur op Europees niveau ook niet meteen zal moeten deel uitmaken van de lijst van nationale kritieke infrastructuren. Het loutere feit dat bv. een bepaalde elektriciteitscabine cruciaal is voor de bevoorrading van de Europese instellingen, volstaat momenteel niet om deze aan te duiden als nationaal kritiek. Voorlopig blijkt eveneens de scope beperkt te zijn tot infrastructuren onder privaat beheer. De maatregelen beperken zich echter tot fysische integriteit: in een volgend hoofdstuk onderzoeken we daarom in welke mate dit voldoende is dan wel ook aandacht te worden besteed aan het cybernetische luik en in welke mate de twee elkaar aanvullen.

5.3.6.Aanpassing van de Wet van 2011?

Mogelijk zijn aanpassingen en aanvullingen van de wet van 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren vereist: de invloeden van ander sectoren dan energie en transport moeten ook in de wet worden opgenomen. Ook de intersectorale invloeden moeten mee in rekening worden gebracht en in de wet worden vermeld, zowel voor wat betreft de identificatie van de infrastructuur als voor de dreigingsanalyse die door OCAD in dat verband moet worden uitgevoerd. Verder en in het licht van voorgaande dient daarom een specifieke aandacht te worden gevestigd op energie-infrastructuur dat ook rekening houdt met distributielijnen eerder dan alleen de krachtcentrales of opslagplaatsen. De coördinatie van civiele en militaire prioriteiten kan ook bij wet worden bepaald en ondersteund door en permanent militaire liaison bij het ADCC.

5.4. Cybernetische bescherming

In België bleek in 2014 veel aan het licht te komen over gevoeligheden, cybernetische aanvallen en monitoring, onder meer van telecombedrijven, welke als gevolg van de uitbreiding van *smart grids* in de toekomst meer invloed zullen krijgen in het beheer van de energiedistributie. Ook de kanselarij en FOD buitenlandse zaken blijken in dat jaar het doelwit te zijn geweest van gerichte aanvallen[42]. De aanwezigheid van supranationale instellingen in onze hoofdstad zullen die trend niet doen afnemen. Daartoe werd besloten het Cybersecurity Centrum België (CCB) op te richten. Het Koninklijk Besluit van 10 oktober 2014 verwoordt in artikel 3° de opdracht van het CCB als volgt:

> 1.opvolgen en coördineren van en toezien op de uitvoering van het Belgisch beleid ter zake;
> 2.vanuit een geïntegreerde en gecentraliseerde aanpak de verschillende projecten op het vlak van cyberveiligheid beheren;
> 3.de coördinatie verzekeren tussen de betrokken diensten en overheden, en de publieke overheden en de private of wetenschappelijke sector;
> 4.formuleren van voorstellen tot aanpassing van het regelgevend kader op het vlak van cyberveiligheid;
> 5.in samenwerking met het Coördinatie- en Crisiscentrum van de regering, het crisisbeheer bij cyberincidenten verzekeren;
> 6.opstellen, verspreiden en toezien op de uitvoering van standaarden richtlijnen en veiligheidsnormen voor de verschillende informatiesystemen van de administraties en publieke instellingen;
> 7.coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberveiligheid, van de opvolging van internationale verplichtingen en van voorstellen van het nationale standpunt op dit vlak;
> 8.coördineren van de evaluatie en certificatie van de veiligheid van informatie- en communicatiesystemen;
> 9.informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen.

[42] Centrum voor cyberveiligheid staat in de steigers. Beschikbaar via: http://www.hln.be/hln/nl/4125/Internet/article/detail/1947092/2014/07/17/Centrum-voor-cyberveiligheid-staat-in-de-steigers.dhtml geraadpleegd op 23 jul 2015.

Deze opdracht wordt aangevuld door een beheerstaak die wordt uiteengezet in artikel 17: het CCB wordt hierin verondersteld om het beheer van de dienst Computer Emergency Response Team (CERT) over te nemen van de Federale Overheidsdienst Informatie- en Communicatietechnologie voor het opsporen, het observeren en het analyseren van online veiligheidsproblemen alsook permanent de gebruikers daarover in te lichten.

Ook het regeerakkoord 2014-15 vermeldt de strategische objectieven in het cyber domein waarin onder meer een optimale beveiliging en bescherming van kritieke infrastructuren, het wetenschappelijk en economisch potentieel en overheidssystemen tegen de cyberdreiging worden vooropgesteld. Hieronder wordt verondersteld dat ook energie-infrastructuren in de beveiligingsopdracht worden opgenomen. Het CCB zal binnen dat kader moeten zorgen voor het operationaliseren van die strategie in precieze en effectieve operationele maatregelen en zal de nationale strategie ontwikkelen in overleg met de privésector (Federaal Regeerakkoord, 2014; pp.101-102). Het zal met name gaan om de verzekering van een snelle opsporing en reactie in geval van een cyberaanval op de essentiële informatiesystemen en –netwerken van de Staat en op de kritieke infrastructuren of nog om de versterking van de informatie aan en de sensibilisering van de burgers en de ondernemingen over de bestaande bedreigingen. Ondernemingen zullen worden aangespoord om te investeren in een hoog cyberveiligheidsniveau en om informatie te delen zowel op sectoraal niveau als met de overheid.

Een noodplan zal voor de cybernetische aspecten moeten aansluiten bij de objectieven van de bestaande noodplannen waarvoor het ADCC de coördinatie verzorgt: hiervoor zal dus een samenwerking moeten tot stand komen tussen het ADCC en CCB in samenwerking met alle andere betrokken diensten (ADIV, Federale Politie, VSSE, …). Het Platform CIP, evenals het Platform Cyberveiligheid zullen hierin een coördinerende rol moeten spelen en tevens moeten bepalen welke diensten, met welke middelen en volgens welke procedures, zullen instaan voor de cyber specifieke risicoanalyses die de kritieke energie-infrastructuur aanbelangen en welke middelen kunnen worden aangewend teneinde die risico's uit te sluiten.

Een budget van 10 miljoen € zou volgens de planning moeten volstaan om het Centrum Cyber Security Belgium in staat te stellen de nationale cyberstrategie uit te voeren: het probleem is dat die bewuste strategie (Kanselarij van de Eerste Minister, 2012) wel aanhaalt dat de dreiging reëel is en dat de beveiliging en bescherming van kritieke infrastructuren en overheidssystemen tegen de cyberdreiging moet worden nagestreefd, maar dat de beveiliging van energie-infrastructuur of de distributiesystemen die net zo gevoelig blijken niet expliciet worden vermeld noch dat de middelen worden

beschreven om die tot stand te brengen. Het in het leven roepen van een dergelijk centrum zal inderdaad toelaten om de cyber beveiliging gecentraliseerd aan te pakken. Nochtans zal een wettelijk kader moeten worden uitgewerkt dat het mandaat van het centrum nauwkeurig omschrijft, onder meer voor de opvolging van de dreiging en de te trekken lessen uit incidenten, zowel in binnen als in buitenland: na de aanslagen in Brussel en het daaropvolgend onderzoek is gebleken dat ook de sector energie (onder meer de nucleaire sector) bij eventuele doelwitten hoort en in het vervolg onderwerp uitmaken van beveiligingsmaatregelen tegen moedwillige aanvallen. Een regelmatige evaluatie zou ervoor moeten zorgen dat het veiligheidsbeleid van uitbaters aangepast blijft aan de dreiging die op dat ogenblik geldt. Verder wordt in de strategie niet specifiek gesproken over de energie-infrastructuur in het gedeelte technologische ontwikkeling: de 'high tech' projecten waarvan sprake behelzen eerder defensie ruimtevaart, financiële systemen, medische sector. Daartoe wil het kwaliteitsverbeteringen doorvoeren waaronder moet worden verstaan doorgedreven beheersing van de methodologie voor het ontwerpen van software en van standaard internationale veiligheidscontroles, en het in plaats stellen van diensten voor controle en homologatie (Kanselarij van de Eerste Minister, 2012). Hiermee komt men aan stap dichter bij de standaarden die in de VS door het FERC worden opgelegd: het centrum moet inderdaad ook instaan voor het opstellen en verspreiden van standaarden, richtlijnen en veiligheidsnormen voor de verschillende soorten informatiesystemen als ook het evalueren en certificeren van de veiligheid van informatie- en communicatiesystemen van de overheid. Het centrum zou onder de bevoegdheid van de kanselarij van de eerste minister staan. De bevoegdheden zouden de nadruk leggen op de coördinatie van de verschillende actoren in zaken cyberveiligheid. Nochtans blijft de strategie te vaag met betrekking tot de betrokkenheid van de energiesector in het beveiligingsplaatje. Ook het dagelijkse toezicht en de coördinatie van de opsporing, observatie en analyse van veiligheidsincidenten door het Cyber Emergency Response Team, voordien onder toezicht van FedICT, zou bij de bevoegdheden van het Centrum horen. Nochtans blijft de bevoegdheid van iedere entiteit bestaan en is er geen organogram dat de bevoegdheden en de verantwoordelijkheden in een complexe materie als de energiesector (zoals in het Amerikaans voorbeeld heeft getoond) vastlegt.

Net de organisatie van de VS kan als voorbeeld dienen voor wat er te doen staat in ons land, net als voor wat er te doen staat op supranationaal niveau. Zo zal het Amerikaans initiatief om wetten te stemmen voor de bescherming van energie infrastructuur, buiten de klassieke beveiliging van de opwekkingsinfrastructuur, ook in ons land moeten worden gevolgd. In de VS zijn nog de Grid Reliability and Infrastructure Defense Act (2010), noch het Grid Cybersecurity Act (2011) uiteindelijk als wet gestemd. De bedoeling van

die wetten was het verantwoordelijk agentschap het mandaat te geven om de tot dan toe vrijwillige standaarden voor cyberbeveiliging van energie-netwerken dwingend te maken en het agentschap het mandaat te geven om de naleving ervan te doen respecteren. Deze standaarden werden wel hernomen in wat vervolgens als referentie is gaan gelden voor NIST, maar de private bedrijven die als operator de investering moeten doen kan enkel een vrijwillige medewerking worden gevraagd. Het is dan ook belangrijk dat in de attributies van het Belgische agentschap ook een afdwingbaar karakter van de standaarden wordt onderschreven, voor zover men over een gecoördineerde versie van dergelijke standaarden kan beschikken die zowel op het niveau voor de lokale besturen als voor de supranationale organisatie uitvoerbaar is. Bovendien zal men moeten uitmaken wie de extra kosten zal moeten dragen van dergelijke opgelegde en afdwingbare standaarden: zoals eerder vermeld zijn private bedrijven niet geneigd om extra investeringen uit te voeren die eventuele winstmarges kunnen doen slinken. De afdwingbaarheid van dergelijks standaarden zou dus een extra kost betekenen die mogelijk een prijsverhoging van de afgenomen energie tot gevolg zou hebben. Als gevolg daarvan dient dus de vraag worden gesteld welke de maatregelen zijn die een aanvaardbare kosten-efficiëntie vertonen en hoe en door wie de kost zal worden gedragen: is het een verantwoordelijkheid van de private partner, van de lokale besturen, de federale of de supranationale? Een eenvoudig antwoord is er niet meer gezien de afhankelijkheden van de netwerken en gezien lokale beperkingen van infrastructuur die niet noodzakelijk op nationaal of supranationaal niveau bestaan. Het gebruik van elk van die netwerken door elk van de voornoemde maakt het waarschijnlijk een gedeelde verantwoordelijkheid en daarom zal het antwoord liggen in een verdeling van de kosten die met die extra beveiliging gepaard gaan. Als we de vergelijking doortrekken en de controle van de uitvoering willen realiseren, is het ook aangewezen dat het nieuwe centrum een bevoegdheid krijgt die vergelijkbaar is met deze die het controleagentschap van de nucleaire industrie heeft: het niet naleven van de opgelegde minimale vereisten zou dus ook sancties als gevolg kunnen hebben voor de uitbaters. Het centrum moet daarom niet alleen de risico's op een dynamische manier kunnen evalueren, maar moet die ook kunnen vertalen in kosten-efficiënte standaarden die met technische bijstand moeten kunnen worden aangewend. Het niet naleven ervan brengt de betrouwbaarheid van het systeem in gevaar en moet dan ook met gepaste maatregelen kunnen worden afgedwongen door datzelfde agentschap: een dergelijke taak impliceert niet alleen een expertise in zake cyberveiligheid maar ook een expertise van wat die cyberveiligheid als implicaties heeft voor een kritieke energie-infrastructuur, haar distributienetwerk en de functionering ervan. In het verlengde van die bijkomende taken en de complexiteit voor de uitvoering, moet de gebruiker voortdurend worden verzekerd van de beschikbaarheid van de energie voor een haalbaar tarief. Mogelijk is een

supranationaal kader daarvoor vereist of mogelijk biedt dit en nieuwe markt voor verzekeringen die daarvoor duidelijkheid zullen willen over de uitgebreidheid van de opgelopen schade: het gebrek aan jurisprudentie in geval van fysieke schade als gevolg van een cyberaanval en de combinatie van zowel cybernetische als fysische schade, als ook de cascade effecten die ermee gepaard gaan, vergen een overzicht dat vandaag de dag nog niet is gerealiseerd. Bovendien is in dit verband ook een omschrijving noodzakelijk van de inbreng die Defensie kan geven: de ondersteuning van de netwerken van de supranationale organisaties, inclusief de NAVO, steunt immers op de nationale pijlers en daarom is inbreng van Defensie belangrijk voor zowel de ondersteuning van de cyberarchitectuur als de kritieke energie-infrastructuur op nationaal maar ook op internationaal vlak. De taakomschrijving van zowel het centrum als van aanverwante taken zal dus nog veel denkwerk vergen: definiëren van standaarden, juridische implicaties, afdwingbaarheid en statuut van het centrum, het creëren van een controleorgaan, implicaties voor tarieven en definiëren van gevolgen voor verzekeringen. Het is dus goed een strategie te hebben die algemene richtingen aangeeft, maar nog beter om de concrete invulling te geven van die algemene richting en de verantwoordelijkheden af te bakenen van eenieder die vroeg of laat in het proces zal worden betrokken.

Naast de beveiligingsplannen van de exploitanten zal ook door de overheid een meerwaarde moeten worden gegenereerd in maatregelen die door het CCB worden in werking gesteld. Ook Defensie kan hierin een rol spelen als ‘incontournable’: zowel als actor, als houder van de capaciteit en de ervaring heeft het zijn rol in de uitvoering van de cyberstrategie in het algemeen en in het bijzonder voor de bescherming van kritieke energie infrastructuur. Echter een vanzelfsprekende taak die daartoe bijdraagt zijn informatie-uitwisseling (en vermits de beveiliging van cyberinfrastructuur van kritieke energie infrastructuur een aanval van buiten het grondgebied moet kunnen weerstaan is dit een taak voor Defensie, die voor de inheemse aanvallen zal moeten samenwerken met de Staatsveiligheid), maar ook voor de uitschakeling van de dreiging die moet voldoen aan de principes van proportionaliteit en discriminatie. Voor wie de rol van Defensie in het algemeen en inlichtingendiensten in het bijzonder in deze materie nog niet overtuigend genoeg naar voren is gebracht, voor en na de aanslagen van november 2015 dient worden vermeld dat ook in de VS een voormalig CIA/NSA directeur en verantwoordelijken van FERC en DoE hebben gewezen op de gevoeligheden en de dringende nood aan een nieuwe oriëntatie die zou moeten gegeven worden aan cyberverdediging in de richting van wat hiervoor werd uiteengezet (McGuinness, 2014) waarbij zowel inlichtingendiensten als krijgsmachten meewerken.

In het voorstel tot uitwerking van een architectuur voor cyberbeveiliging van het elektrisch net, vermeldt men dat die informatie uitwisseling op verschillende niveaus dient te worden gerealiseerd tussen industrie, overheid en operatoren van kritieke energie infrastructuur (Bipartizan Policy Center, 2014):

> "This information sharing must occur along several dimensions- bilaterally between industry and government, within industry and across critical infrastructure sectors, across government agencies and different levels of government. Even with an extensive array of mandatory or voluntary standards, cyber threats will inevitably evolve faster than new standards. Close collaboration and information sharing between the government and private sectors is the primary way to identify, assess, and respond to threats in real time."

Een eerste barrière zou er bij ons uit bestaan om überhaupt informatie uitwisseling te realiseren tussen overheid (lees inlichtingendiensten) en private bedrijven in de energiesector. Een tweede zou eruit bestaan om die informatie exploiteerbaar en snel tot bij de gebruiker te krijgen en te delen met de sectoren die er baat bij hebben: de informatie moet dus zowel in de kritieke energie infrastructuur voor elektriciteit als olie en gas worden gebruikt.

Maar naast de informatievergaring en uitwisseling is er de nood aan een gepaste respons in geval van een waargenomen aanval. Naar de principes die het gewoonterecht bepalen zal een proportionele en discriminerende houding aangenomen worden: enkel de aanvaller zal worden getroffen indien men beslist terug te slaan en in diezelfde mate als hijzelf getroffen heeft. Het realiseren van deze beide objectieven is niet vanzelfsprekend. Het veronderstelt niet alleen dat de oorzaak van een dergelijke aanval op ondubbelzinnige wijze kan worden bepaald, maar bovendien veronderstelt het ook dat eventuele cascades niet zullen worden veroorzaakt door de acties die zullen worden genomen om de aanvaller uit te schakelen of de aan de gang zijnde aanval een halt toe te roepen. De te coördineren acties van alle actoren worden uiteraard gebaseerd op bestaand noodplannen in de VS: de lessen die getrokken werden uit grootschalige rampen (en de vastgestelde tekortkomingen) werden in het National Response Framework verwerkt. Maar er is nog meer: door de specificiteit van een cyberaanval of incident, werd een afzonderlijk plan uitgewerkt dat niet alleen alle betrokken actoren lijst en hun verantwoordelijkheden afbakent, maar ook de acties detailleert dat ieder van die actoren zou moeten uitvoeren om klaar te zijn in geval van een incident en er op gepaste wijze te kunnen op reageren (National Cyber Incident Response Plan). Bovendien gaat men er in de VS van uit dat er een wisselwerking moet bestaan tussen de verschillende plannen: als gevolg van een natuurlijke ramp kunnen er gevolgen zijn voor het cybernetische domein, maar ook omgekeerd

kunnen cyber incidenten fysische gevolgen hebben. Ook in ons land moet de bestaande strategie aangevuld worden door een vergelijkbaar plan dat een wisselwerking toelaat tussen bestaande noodplanning en de planning voor het beheer van cyber incidenten in het geval van faling van kritieke energie infrastructuur. Het spreekt vanzelf dat de verantwoordelijkheden van de actoren en de beslissers in beide gevallen duidelijk moeten worden bepaald en dat de gevolgen van een of andere organisatie duidelijk moeten worden afgewogen vooraleer een dergelijke planning het licht ziet. Het kan bijvoorbeeld nuttig zijn om de commandostructuur in geval van een cyberincident (tijdelijk) te hertekenen met het oog op een snellere oplossing van het incident: zowel de bedoeling, de tijdspanne als de gevolgen van die aanpassingen zullen moeten worden gecoördineerd en gemotiveerd.

In wat voorafging werd gewezen op de gevolgen voor private bedrijven en de moeilijkheid om een kosten-efficiënte investering te doen die toelaat om standaarden te implementeren die niet noodzakelijk meer vrijwillig zullen zijn maar die ervoor moeten zorgen dat een minimale betrouwbaarheid kan worden gegarandeerd van de KEI. Bovendien zal de nood om een cascade van incidenten te vermijden in andere domeinen of over uitgebreide geografische zones mogelijk een bijkomende verzekeringskost met zich meebrengen. Bovendien zal de vereiste flexibiliteit om aan punctuele dreigingen het hoofd te bieden ook een prijs gekoppeld zijn. Van de zijde van de overheid is het dan weer niet vanzelfsprekend om in te schatten in welke mate een investering die vanuit het standpunt van de overheid onontbeerlijk lijkt, ook nog vanuit het standpunt van het private bedrijf betaalbaar is. Deze standpunten zijn verdedigbaar vanuit eenieders perspectief: dat van de overheid om het algemeen goed na te streven en dat van het private bedrijf om zijn winst te maximaliseren en dus de beveiliging tot het strikte noodzakelijke te beperken. In het midden van de twee standpunten moet men zich realiseren dat de effecten van extra beveiliging niet altijd zichtbaar zijn en dat dit gebrek aan zichtbaarheid ook aanleiding kan geven tot een gebrek aan motivatie om de inspanningen in de tijd vol te houden. De argumentatie van ene en andere partij overstijgt dus de kostenbatenanalyse van één enkel bedrijf dat wel moet overhaald worden om mee te betalen voor de beveiliging van volledige energienetwerk en zijn distributie.

5.5. Structurele elementen

De plaats van ons land ten opzichte van de rest van de EU is een niet te verwaarlozen element voor de keuze van prioriteiten of richtingen die we moeten aanwenden om in alle onafhankelijkheid maatregelen te kunnen nemen/kiezen die kunnen bijdragen tot de juiste inschatting van dreiging en risico hetgeen de bescherming van energie infrastructuur in de hand kan werken, zowel fysisch als cybernetisch, maar ook kan zorgen voor een energetische keuze die, door de omstandigheden de facto zal zorgen voor een zekere garantie van veiligheid van voorziening.

Een niet te onderschatten element in de onderhandelingen naar COP21 zijn de budgettaire implicaties en verdeelsleutels die het federale en regionale niveau ertoe hebben geleid om het bestaan van een nationaal standpunt te laten afhangen van die verdeelsleutels. Ons land zou niet alleen moeten bijdragen tot het internationaal klimaatfonds, maar ook een verdeelsleutel vinden voor de subsidies die ons land kan ontvangen. Daarnaast stelde Europa het aandeel aan hernieuwbare bronnen in ons land vast op 13% in 2020: samen met een toegenomen energie efficiëntie (minder energieverbruik van 20%) ten opzichte van een onveranderde politiek die het niveau van 2020 zou bepalen wordt ook een vermindering van de broeikasgassen-uitstoot van 20% gevraagd. In concreto betekent dit een extra inspanning voor Wallonië om 12.5% van de energie met hernieuwbare bronnen op te wekken tegen 2020, terwijl Vlaanderen naar 10.4% moet evolueren. Net dit laatste element zou voor ons land moeten doen inzien dat een onberedeneerde afschrijving van de technologie die in ons land tot 6GW aan vermogen kon opleveren te weten kernenergie, niet noodzakelijk in het voordeel kan zijn van ons land. Niet alleen klimaatdoelstellingen spreken in het voordeel van kernenergie vandaag: ook de indices die onze afhankelijkheid weergeven van fossiele brandstoffen tonen aan dat België nog een redelijk grote afhankelijkheid vertoont:

- voor gas is België binnen de EU nog in een grote mate afhankelijk van de gasvoorziening die van de buurlanden komt. Van de landen extra-EU is ons land in mindere mate afhankelijk. De grootste afhankelijkheden worden in dit geval vertoond door landen als de Baltische staten, Finland, Tsjechië, Bulgarije, Oostenrijk en Ierland. Als vergelijkende orde van grootte heeft men in deze landen een *supplier*

concentration index[43] (SCI) die 80% overschrijdt, terwijl dat in ons land amper 30% is;

- voor aardolie blijken voor dezelfde landen vaak een nog grote afhankelijkheid te weten Bulgarije, de Baltische staten, Slovakije, Polen, Hongarije en Finland (80-100% daar waar België rond de 20% scoort);
- voor vaste fossiele brandstoffen als kolen zijn de indexen veel lager wat duidt op een grotere diversificatie van de markt voor dit product: de grootste indices worden bereikt voor Bulgarije, Portugal, Luxemburg, Letland, Estland en Nederland. Dit laatste geldt voor deze bron blijkbaar als doorvoerland binnen de EU (80-100%; voor België minder dan 20%).

De les die men daaruit dient te distilleren is dat in elk van voornoemde landen één of meerdere energetische bronnen kritisch en afhankelijk, zijn van extra-Europese aanvoer. Een lagere energieconsumptie en dan in het bijzonder van fossiele brandstoffen, zoals voorzien in het kader van het klimaatakkoord, kan bijdragen aan een vermindering van de afhankelijkheidsindex. Ook het aanpassen van strategische stocks kan in die richting resultaat opleveren. Maar enkel een grotere diversificatie en stocks zullen niet volstaan om ingrijpende resultaten te boeken: een groter intra-Europees distributienetwerk zowel voor de verdeling van de opgewekte stroom als ook voor de verdeling van de resthoeveelheid fossiele brandstoffen in gebruik kunnen zorgen voor het verlagen van het aantal kritieke knelpunten, en de extra-Europese afhankelijkheid waarmee meteen de vinger wordt gelegd op de infrastructuur die er betrekking op heeft.

[43] Supplier Concentration Index is een maatstaf die in getal een indicatie wil geven van de afhankelijkheid van een land ten opzichte van externe leveringen voor een energiebron. Het wordt berekend door het quotiënt van het totaal van de leveringen te delen door het verbruik in dat land, in het kwadraat: lage waarden geven een grote diversificatie aan (European Commission, 2014; p.178). Een land dat voor een bepaalde bron een SCI van 100% behaalt, is voor die bron volledig afhankelijk van externe leveranciers.

5.6. Deelbesluit

In dit deel zijn we nader ingegaan op de aanwending van voormeld instrumentarium voor het Belgische geval. We zijn vooreerst in de legale aspecten tot de vaststelling gekomen dat de aanduiding van kritieke energie infrastructuur, en kritieke infrastructuur in het algemeen niet enkel meer te reduceren is tot een sectorale aangelegenheid. Eerder zal men voor het welslagen van de wetgevende ondersteuning moeten zorgen voor het in rekening brengen van de cascade effecten en de organisatorische gevolgen ervan bepalen onder de vorm van verantwoordelijkheden en cross sectorale samenwerking. De uistluitend algemene benadering is daarvoor niet mogelijk en het niveau van de individuele beveiligingsplannen komt tekort. Het bestaan van de structuur van dit werk dat zowel de fysische als de cybernetische maar ook bijkomende veiligheidsaspecten met elkaar in verband brengt, toont de complexiteit van het probleem. Zowel voor de fysische als de cybernetische bescherming blijft het wettelijk kader de garantie voor de nodige exhaustiviteit en flexibiliteit voor de verbanden tussen alle met elkaar verbonden sectoren.

In het geval van fysische bescherming is het platform kritieke infrastructuren voornamelijk belast met het verder ontwikkelen en operationaliseren van het werkingskader en de werkingsprocessen ter beveiliging en ter bescherming van kritieke infrastructuren op een gecoördineerde wijze: met dat doel voor ogen is het platform ook bevoegd om de identificatieprocedure te optimaliseren en de wetgevende ondersteuning ervan te verfijnen. Voor het ogenblik zijn het vooral de sectorale overheden die volgens de wet van 2011 de toezichtsverantwoordelijkheid dragen maar zonder trans-sectorale coördinatievereiste. Deze coördinatietaak ligt voor het ogenblik uitsluitend bij het ADCC, terwijl de analyse van de dreiging het OCAD toekomt. Bovendien heeft het bestaan van civiele en militaire kritieke infrastructuurvereisten tot gevolg dat een verschillende prioriteit zou kunnen worden gegeven aan energie infrastructuur, wanneer die door louter civiele, dan wel door militaire instanties zou worden opgesteld. Een permante en dynamische inschatting van prioriteiten en coördinatie vereisen daarom de herinvoering van een permanente militaire vertegenwoordiger in de schoot van het ADCC. Bovendien is een zekere overeenkomst vereist tussen de Europese en de nationale kritieke infrastructuren, welke zich niet mogen beperken tot krachtcentrales alleen, maar in de toekomst meer en meer ook de distributielijnen en de grondstofbronnen in rekening zullen moeten nemen.

Voor de cybernetische bescherming is vooral het cyber veiligheidscentrum het platform waarnaar wordt gekeken om de coördinatie

op zich te nemen. Echter de wetenschap dat zowel de fysische als de cybernetische veiligheid reeds versmolten zijn, heeft als gevolg dat de directeur van het CCB ook zetelt in het platform CIP. Naast een coördinatie tussen en civiele en militaire prioriteiten, zien we in dit geval een bijkomende coördinatienoodzaak tussen de private en de publieke actoren. Een noodplan voor cybernetische aspecten zal daarom nauw moeten aansluiten bij de objectieven van bestaande noodplannen, waarvoor het ADCC de coördinatie uitvoert: het mandaat van het CCB kan daartoe worden uitgebreid, maar het wetgevend kader moet dat toelaten, wat voorlopig niet het geval is. De bevoegdheid van het centrum in zaken energiesector blijft echter te vaag in de strategie voor cyber veiligheid: in het verlengde van de Amerikaanse historiek zou daarom een *energy cyber security* wetgeving de bevoegdheden van het CCB moeten versterken waarbij opgelegde standaarden afdwingbaar worden, ook voor private actoren. De afdwingbaarheid zou vergelijkbaar moeten zijn met de bevoegdheid van een controleorganisme in de nucleaire industrie. In het verlengde van een dergelijk cyber incident response plan voor exploitanten kan worden gesteld dat ook op nationaal vlak een dergelijk plan tot stand zou moeten komen.

Ten slotte is men tot de vaststelling gekomen dat naast de fysische en de cybernetische veiligheid ook in België een derde dimensie bestaat die ervoor kan zorgen dat de gevoeligheden in die twee eerste domeinen naar beneden wordt herzien waaronder een gereduceerde afhankelijkheid van bronnen: een toegenomen diversificatie van technologie en geografische oorsprong van bronnen enerzijds maar ook een grotere energie-efficiëntie dragen daartoe bij. Hoewel ons land voor gas bijvoorbeeld niet de grootste afhankelijkheid vertoont binnen de EU, kan men er niet onderuit dat we voor een constante gasvoorziening toch nog afhankelijk zijn van de bevoorrading in buurlanden. Voor vaste en vloeibare fossiele brandstof, ligt die bij ons ongeveer op gelijk niveau (uitgedrukt in supplier concentration index). Lagere energieconsumptie op nationaal vlak, passend in een globaal klimaatakkoord, grotere strategische stocks en een dichter distributienetwerk (zowel voor gegenereerd vermogen als voor voormelde grondstoffen) kunnen daartoe bijdragen.

Aanbevelingen en besluit

Aanbevelingen

Internationaal

1. We zijn tot de vaststelling gekomen dat in de VS specifieke noodplannen bestaan voor de grootschalige gevolgen van cyberincidenten en onder meer voor het geval kritieke energie infrastructuur zou worden getroffen bestaan standaarden waaraan energieleveranciers moeten voldoen. In de EU is pas een akkoord bereikt voor de vastlegging van vereisten voor operatoren van essentiële diensten (waaronder energie, transport en financiën). De lidstaten zullen wellicht een oplijsting moeten maken van de betrokken operatoren in elke sector. Echter een richtlijn zal in de komende maanden nog een dergelijk akkoord moeten concretiseren, welk in de daaropvolgende maanden in nationaal wetgeving zal moeten worden vertaald waarbij rekening moeten worden gehouden dat zowel op nationaal als op supranationaal vlak commandostructuren en verantwoordelijkheden duidelijk worden afgebakend tussen de departementen energie en interne veiligheid. Tegelijk moet een supranationale coördinatie tot stand komen met het nationale beleid in zaken definitie en afbakening van grenzen tussen regionale, nationale en supranationale verantwoordelijken.

2. Een geïntegreerde benadering van fysieke en cybernetische beveiliging van kritieke energie infrastructuren heeft weliswaar in de VS geleid tot het vastleggen van standaarden, doch een wettekst om de uitwisseling van informatie tussen veiligheidsdiensten en private partners te verbeteren voor deze specifieke gevallen kon niet worden gerealiseerd: de gevoelige materie enerzijds en de niet altijd samenvloeiende belangen van private en publieke partners anderzijds zullen voor een deel van de verklaring uitmaken. Daar waar in de VS een geïntegreerde aanpak van bescherming van kritieke energie infrastructuur al wordt nagestreefd, is dat in de EU nog verre van bereikt: naast een domein specifieke en geïsoleerde definitie van wat onder kritieke infrastructuur wordt verstaan, is een organisme aan te duiden dat de bevoegdheid zal hebben om standaarden te definiëren en af te dwingen voor het realiseren van interoperabiliteit tussen domeinen en operatoren die een geïntegreerde fysische en cybernetische beschermingspolitiek mogelijk maken.

3. Als gevolg van de mogelijke implicaties van een cyberaanval op kritieke energie infrastructuur, moet in een juridisch aanvaard en gemeenschappelijk forum worden bepaald wat precies op internationaal vlak

als een vijandige aanval of een vijandige intentie zou worden beschouwd in het cybernetische domein in het algemeen en met gevolgen in de sector energie in het bijzonder. Derhalve zal binnen een militaire alliantie in voorkomend geval ook moeten worden uitgemaakt welke de automatisch voortvloeiende gevolgen zullen zijn na de vaststelling van een dergelijk incident voor de eigen infrastructuur zowel voor wat betreft concomitante gevolgen in aanpalende domeinen, als voor de afbakening van de gevolgen van maatregelen die als respons zullen moeten worden aangewend.

4. In de grootschalige integratie van nieuwe objecten en generatoren voor alternatieve energie opwekking is tot hier toe uitsluitend uitgegaan van een markteconomisch standpunt van bedrijven zonder de noodzakelijke maatregelen te willen voorzien in een beveiligd distributienet. Los van het feit of de diversificatie van de verschillende bronnen voldoende is verzekerd, dient de nagestreefde netwerking a priori van een voldoende grote beveiliging te zijn voorzien wat vandaag nog zeker niet het geval is. Daartoe kan in het uitsluitend cybernetische domein, maar ook in het aansluitende domein van energie een voortdurende inspanning van onderzoek en ontwikkeling gepereniseerd te worden in de plaats van COTS aankopen de voorkeur te laten genieten.

5. Het wegblijven op Europees niveau van een geïntegreerd energetisch beleid en dito eengemaakte markt, of een nationaal fluctuerend standpunt in de tijd kan er in de toekomst voor zorgen dat operatoren en/of investeerders markteconomische motieven laten primeren en binnen of buiten de Unie minder strenge uitstootnormen of beveiligingsstandaarden opzoeken: delokalisatie kan er uiteindelijk het gevolg van zijn indien supranationaal en regionale stabiliserende voorwaarden wegblijven. In dat geval zal de EU en a fortiori sommige lidstaten meer dan andere de speelbal zijn van aan de Unie externe leveranciers. Het wegblijven van een dergelijk beleid en dito markt is voornamelijk door nationale prioriteiten gemotiveerd: een gemeenschappelijk lijn zal de nationale of regionale specificiteit niet uit het oog mogen verliezen.

6. Wetende dat een groot gedeelte van de beveiliging van een nieuw distributienet moet worden beveiligd, en dat Duitsland tegen 2030 daartoe zware investeringen heeft gepland, zal men ook, in de rest van de Unie werk moeten maken van een vernieuwing van het distributienet dat energetische eilanden doet verdwijnen (onafhankelijk van de bron die men beschouwt). Zowel de kosten daarvan als de kosten voor de reeds vermelde beveiliging zullen worden doorgerekend naar de consument. Het zal dus in de komende jaren essentieel zijn om een rationale keuze te maken van het beschikbare pallet eerder dan een dogmatische acceptatie of verwerping te willen opleggen die na jaren onbetaalbaar blijkt te zijn of die nefastere gevolgen blijkt te

hebben voor het milieu door een onverrekende uitstoot van broeikasgassen voor de geproduceerde materialen. De keuze van ene of gene technologie moet daarom een werkelijke productiekost van de energie weergeven zonder die zoals vandaag te koppelen aan fossiele brandstoffen of een artificiële subsidiëring van alternatieve bronnen in concurrentie te zetten met andere technologie: een competitieve marktprijs nastreven veronderstelt ook dat de werkelijke output van een energiebron wordt verrekend eerder dan de nominale output en dat rekening wordt gehouden met de totale vraagtijd (rekening houdend met de onbeschikbaarheid van een energiebron in de tijd).

7. In het verlengde van deze redenering, is het afzweren van nucleaire technologie op ideologische of politiek gemotiveerde basis niet aanvaardbaar: in een voor de EU-leidend land is de energierevolutie geen succes gebleken daar het nog steeds afhankelijk is van externe actoren, sinds de afwijzing van kernenergie veel meer broeikasgassen uitstoot dan voordien, het land voor 50% consument is geworden van bruinkool, dat energie wordt ingevoerd van landen die minder strengere uitstootnormen hebben of energie dat in andere landen toch door kenenergie wordt geproduceerd, dat zeker dit land nog jaren zware investeringen wacht voor de vervanging van zijn distributienetwerken.
Om voormelde redenen moet men zich afvragen of kernenergie niet op een meer rationale manier moet worden benaderd en dat andere vormen van energieopwekking ook moeten rekening houden met energieconservatie in de tijd enerzijds en effectief vermogen in de plaats van nominaal vermogen anderzijds. Los van het feit of die criteria al dan niet een behoud van kernenergie zullen voorschrijven, is voor de verzilvering van de kennis in ons land belangrijk dat die wordt behouden en beschikbaar gesteld in binnen of buitenland, waar de vraag zich zal voordoen. In de toekomst blijft de vraag bestaan en wordt betaald voor dergelijke kennis: indien we ze zelf nodig zouden hebben zullen we in geval van afschrijving elders moeten kopen. De vraag rijst niet alleen te weten of het vermogen beschikbaar zal zijn om koper te zijn indien nodig maar ook of het aangeboden product zal voldoen aan de kwaliteitsvereisten van veiligheid en beveiliging zoals die in Europese Unie worden nagestreefd.

8. De keuze van een rendabele energiebron zal moeten aansluiten aan een diversificatie van de bronnen die extern de EU worden aangeleverd. Naast een kwalitatieve verscheidenheid zal ook een geografische spreiding moeten worden gezocht van de beschikbare bronnen. De te grote afhankelijkheid die de Unie tot hier toe heeft vertoond van Russisch gas, heeft na de Oekraïense crisis zorgen gebaard: alternatieven hebben zich sindsdien aangeboden doch met nieuwe bedenkingen. Turkije zou in elk van de Midden-Oosten- of Oostelijke opties een belangrijk doorvoerland zijn, doch gezien de moeilijke positie van dat land met betrekking tot de Syrië en Irak-crisissen enerzijds en

Rusland anderzijds, voert in die doorvoercapaciteit misschien een onvoorspelbaar element waaraan de bestaande infrastructuur nog geen alternatief te bieden heeft. Een alternatief op dit gebied zal dus van de Noordelijke of Westelijke regio moeten komen: in het Noorden is Noorwegen een goede optie voor aanvoer voor de Unie, in het Westen kan dat zowel voor gas uit het kanaal of van over de Atlantische oceaan. In beide van deze opties zal men er echter voor moeten zorgen dat de noodzakelijke infrastructuur kan worden onderhouden die de transit van die gas-en oliereserves kan worden verzekeren.

Voor België

1. In de wettekst van 1 juli 2011 ter beveiliging en bescherming van kritieke infrastructuur wordt voor de aanduiding van kritieke infrastructuur en a fortiori kritieke energie infrastructuur een geïsoleerde sectorale benadering gevolgd: de invloed van feedback loops of cascade-effecten worden niet in beschouwing genomen. Hetzelfde geldt voor de dreigingsanalyses die door de exploitant van een aangeduide infrastructuur moet worden opgesteld: hoewel Art.13, §3.,3 vermeldt dat de potentiële weerslag van de verstoring in de analyse moet worden opgenomen, wordt op geenenkel moment gesproken over de contacten die hiervoor zouden moeten worden geraadpleegd. Zowel voor de identificatie van kritieke infrastructuur als voor de dreigingsanalyses en de beveiligingsplannen van de exploitant dient systematisch een trans sectorale benadering te worden onderschreven: hiervoor kan worden verwezen naar welke verstoringen welke gevolgen zouden hebben in welke andere sectoren en welke beveiligingsmaatregelen een dergelijke overloop zou kunnen doen vermijden.

2. Het veiligheids- en beveiligingsprobleem van kritieke energie infrastructuur heeft aangetoond dat de oplossing niet te herleiden valt tot een fysisch, maar ook een cybernetisch luik inhoudt. Verantwoordelijke actoren in dit cybernetisch aspect, waaronder ADIV, VSSE, CCB en het FCCU zullen dus ook hun plaats hebben in de structurele en systematische oplossing van het probleem. Het zal dan ook een van de taken zijn van het nieuwe platform CIP om de coördinatie met deze actoren concreet uit te werken en waar mogelijk hun bevoegdheden af te bakenen vast te leggen en voor te stellen tot wijziging van de wetgeving ter beveiliging van kritieke energie infrastructuur.

3. In het verlengde van voorgaande voorziet dezelfde wet van 2011 een definitie van andere punten van federaal en militair belang. Art 3,7° beschrijft deze als plaatsen, niet aangeduid als kritieke (energie) infrastructuur maar die voor het beheer van noodsituaties of militair belang beschermingsmaatregelen vereisen die door het ADCC zouden beheerd worden. Het is echter duidelijk

uit de formulering dat de kritieke energie infrastructuur mogelijk maar niet noodzakelijk zal samenvallen met de punten van militair belang en zeker niet met de volgorde van de prioriteiten die eraan zullen worden verleend. Het volgt hieruit dat een vorm van coördinatie tussen de civiele en de militaire lijst zal moeten tot stand komen en dus een consultatie van civiele en militaire overheden zal vergen op niveau van het platform CIP voor de prioritisatie, op niveau ADCC voor de uitvoeringsfase van de bescherming en beveiliging, maar in eerste plaats op politiek niveau voor de bepaling van de prioriteiten en verantwoordelijkheden hetgeen tussen de overheid en private partners ook een interactie zal vergen. Daarnaast zal een aan Defensie eigen analyse moeten worden geïntegreerd met een vergelijkbare civiele oefening. Het is in de schoot van het platform CIP dat raakpunten van ene en andere lijst kunnen worden geïdentificeerd. De prioritisering die hieruit moet voortvloeien zal het resultaat zijn van een dynamische evaluatie van de dreiging en mogelijke invloed van spill-over effecten: een dergelijke dynamische en recurrente interactie vraag in de schoot van het ADCC een permanente vertegenwoordiging van Defensie, hetgeen voor het ogenblik niet mogelijk is: een dergelijke permanentie is een meerwaarde in de schoot van het crisiscentrum. Een aanpassing van de wet van 2011 zou in die zin kunnen worden aangepast met als verantwoordelijkheid om een permanente en dynamische aanpassing van de civiel-militaire prioriteitenlijst te toetsen aan de actuele dreigingsanalyse aan het OCAD ontsproten.

4. In het kader van dit werk werd de vaststelling van de vereiste voor fysische beveiliging van kritieke energie infrastructuur aangevuld door een cybernetisch luik. In ons land zal de verantwoordelijkheid voor de realisatie daarvan automatisch bij het CCB gelegen zijn. Hierdoor veronderstellen we dat automatisch ook de beveiliging van kritieke energie infrastructuren in de beveiligingsopdracht van het centrum wordt opgenomen: het centrum zal daarom zorgen voor het operationaliseren van de cyberstrategie van België in overleg met de privésector: meer in het bijzonder zal een noodplan voor cybernetische incidenten moeten aansluiten bij de objectieven van bestaande noodplannen (die onder de coördinatieopdracht van het ADCC vallen). Voor dit specifieke voorbeeld zal dus een vorm van samenwerking moeten tot stand komen tussen het ADCC en het CCB in de uitvoeringsfase. Eerder zal een overleg, lees coördinatie en bepaling van verantwoordelijkheden, moeten worden vastgelegd tussen het Platform CIP enerzijds en het Platform Cyberveiligheid anderzijds: hierdoor zal men moeten vastleggen welke middelen volgens welke procedures zullen instaan voor cyber specifieke risico's die kritieke energie infrastructuur aanbelangen. Het wettelijk kader dat de werking van het CCB bepaalt zal moeten worden aangevuld met een duidelijk mandaat om de vereisten voor bescherming van kritieke energie infrastructuur en distributiesystemen te evalueren en op te leggen.

5. Bevoegdheden in zaken energie zijn zoals we hebben gezien verspreid over verschillende agentschappen in de VS. De optimale organisatie van de beveiliging van kritieke energie infrastructuur vereist echter een korte afstand tussen de betrokken actoren. Indien een gemeenschappelijk energetisch forum de fysische en de cybernetische veiligheidsvereisten kan doen samensmelten, moet er ook een zekere afdwingbaarheid mogelijk worden die vandaag nog niet in de wet is ingeschreven: het uitvoerbaar maken van standaarden zal voor private partners een extra kost met zich meebrengen die als een drempel kan fungeren voor het aanwenden van die standaarden omdat een deel van de winstmarge verloren gaat voor bedrijven. Men zal dus ook de denkoefening moeten doen wie de kosten van een dergelijke standaard-bescherming gaat betalen en welke de kostenbaten efficiëntie is: het is meer dan waarschijnlijk dat in de toekomst de prijs van energie, los van de grondstofprijzen, omwille van deze problematiek alleen een prijsstijging zal verwerken naar de consument. Na het schrijven van de cyberstrategie van België blijft het werkblad nog nodig: definiëren van standaarden, kosten baten analyse, juridische implicaties, afdwingbaarheid van standaarden, creëren van een controleorgaan, implicaties voor tarieven zijn slechts enkele elementen die op korte termijn nog een antwoord moeten krijgen.

6. In de VS ging men uit van de wisselwerking tussen verschillende noodplannen. Ook in ons land moet een soort van wisselwerking bestaan: als gevolg van een natuurlijke ramp kunnen er immers gevolgen zijn op cybernetisch domeinen en omgekeerd. Naar voorbeeld van het Amerikaanse Cyber Incident Response Plan, dient een vergelijkbaar plan wisselwerking toe te laten tussen bestaande noodplanning en de planning voor het beheer van cyber incidenten in geval van faling van kritieke energie infrastructuur.

7. Een beter vertakt distributienet en gediversifieerde bronnen die een rationele voorstelling geven van het beschikbare pallet kunnen de gevoeligheden voor incidenten beperken. Voor België houdt dit ook in dat maximaal gebruik wordt gemaakt van de kennis die bestaat in de nucleaire sector en die, in geval de nationale exploitatie wordt opgegeven, nog steeds zijn internationale meerwaarde moet zien te verzilveren door te blijven investeren in R&D en die te exporteren naar de nieuwe groeilanden.

Besluit

Vanuit het oogpunt een omschrijving te vinden van kritieke energie infrastructuur, zijn we tot de vaststelling gekomen dat een exhaustieve definitie tot hier toe ontbrak: als invulling zijn we tot de modulatie van een eerste voorstel tot een definitie gekomen die zowel rekening houdt met afhankelijkheden van verschillende domeinen als gevolg van toegenomen connectiviteit. De mate van kriticiteit overstijgt dus de identificatie van individuele essentiële energetische infrastructurele elementen maar moet eerder omschreven worden als de mate waarin een incident een cascade aan effecten kan veroorzaken in andere domeinen. Het belang van distributienetwerken treedt hierdoor in de toekomst nog meer naar de voorgrond dan vroeger. We zijn in het vervolg van deze redenering ook tot de vaststelling gekomen dat de organisatie van de bescherming van kritieke energie infrastructuur vandaag niet meer herleid kan worden tot een fysische bescherming alleen. Een cybernetisch aspect zal de complexiteit van de problematiek verhogen. Daarnaast zijn structurele maatregelen mogelijk die zullen bijdragen tot een verspreiding van het risico op disruptie.

Een analyse van de maatregelen die gelden in de VS, de EU en de NAVO heeft reeds de complexiteit van het fysisch aspect aan het licht gebracht. Het belang van veiligheidsactoren kan vandaag niet meer worden ontkend: na de aanslagen van 13 november 2015 in Parijs en 22 maart 2016 in Brussel werd duidelijk waarom Defensie vandaag van de ene dag op de andere en in alle lagen van de bevolking plots meer relevantie geniet. We zijn ook tot de vaststelling gekomen dat dit zowel intern als extern een aantal uitdagingen zal genereren. Intern zal een fysische bescherming slechts mogelijk zijn op een dynamische manier door een evolutief beeld te schetsen van de dreiging enerzijds en door private partners een klimaat te bieden dat hen toelaat om ook in fysische veiligheid te investeren anderzijds. Vandaag is dit niet altijd mogelijk omdat een stabiel klimaat op lange termijn daartoe ontbreekt. Extern zal men voor een connectie met distributienetwerken moeten zorgen die overeenstemming van standaarden en voldoende connectiepunten en capaciteit vergen. De geostrategische belangen zullen hierin eveneens een rol spelen daar op Europees vlak een te grote afhankelijkheid van een unieke energie leverancier zal moeten kunnen worden gemoduleerd: het belang van landen als Turkije, het Midden-Oosten in het algemeen maar ook Noorwegen zullen daarom een belangrijke rol spelen in de energetische problematiek van Europa.

De analyse van de veiligheidsoplossingen in landen en organisaties heeft tot de vaststelling geleid dat het cybernetische aspect in de toekomst ook voor deze specifieke problematiek enkel aan belang kan winnen: een onderzoek van incidenten heeft de penetratie in de sector energie duidelijk als de belangrijkste aangewezen. De VS als model gebruiken is geen allesomvattende oplossing: we hebben gemerkt dat ook daar een tekort bestaat doordat een afdwingbaarheid van standaarden nog niet bij wet kon worden vastgelegd. Echter, er is wel in de VS een geïnstitutionaliseerde aanvaarde standaardiseringsprocedure ter bescherming van kritieke infrastructuren. Bij ons zijn we nog niet zo ver gevorderd, laat staan dat een dergelijk erkend instituut ook afdwingbare standaarden kan genereren op Europees niveau. Zowel voor operationele militaire cybernetische operaties en meer in het bijzonder voor kerninstallaties heeft dit zoals in dit werk duidelijk gemaakt welke juridische en operationele consequenties de beveiliging kan inhouden.

De vaststelling dat naast het fysische luik ook een cybernetisch luik bestaat, heeft de uitgebreidheid van de problematiek aangeduid: de zoektocht naar een afdoende bescherming, met het concomitant fenomeen om de uitstoot van broeikasgassen te reduceren leidt onherroepelijk naar de oplossing van diversificatie en energie-efficiëntie. Diversificatie van bronnen betrekt uiteraard ook hernieuwbare bronnen zonder te vergeten dat deze de connectiviteitsvereisten van het distributienetwerk verhogen alsook de verifieerbaarheid van beschermingsstandaarden bemoeilijken. De overmatige subsidiëring in alternatieve bronnen, het wegblijven van een stabiel investeringsklimaat, en de irrationele voorstelling van maximale outputvermogens ten opzichte van werkelijke energiebeschikbaarheid laten geen rationele kosten baten analyse van de beschikbare bronnen toe: een gemeenschappelijk energetisch beleid op Europees vlak zou een stabiel investeringsklimaat kunnen faciliteren. De nood aan een rationele besluitvorming wordt zowel nationaal als internationaal geïllustreerd: nationaal heeft de Duitse politieke keuze voor kernuitstap tot een verhoogde afhankelijkheid, gevoeligheid en uitstoot van broeikasgassen geleid. Internationaal duwt dezelfde beslissing op Europees niveau tot een grotere afhankelijkheid en dito kwetsbaarheid.

Wat dit voor België betekent werd in een afzonderlijk deel behandeld. Vooreerst werden de implicaties van de wet op de bescherming van kritieke infrastructuren in het algemeen, en het K.B. ter uitvoering ervan in de sector energie bestudeerd: de rol die Defensie kan innemen is te vinden ofwel in de informatie uitwisseling als in de coördinatie van de civiele en de militaire lijst kritieke infrastructuur. De nood om een aanvulling van de wettekst van 11 juli 2011 uit te breiden naar andere sectoren dan alleen energie en transport wordt geïllustreerd door het belang van het cybernetisch domein. Ook dit specifieke

domein vergt een rol voor Defensie maar een meer afgelijnde rol van de actoren dringt zich op: in het bijzonder het CCB zal een duidelijk mandaat moeten krijgen voor de organisatie van het complexe energie-netwerk. Daarnaast zal ons land, naar Amerikaans voorbeeld moeten beschikken over een cyber incident response plan dat een wisselwerking toelaat tussen bestaande noodplannen enerzijds en de planning voor het beheer van cyber incidenten in het geval van faling van kritieke energie infrastructuur in het bijzonder. Meer a-dogmatische diversificatie en opslagcapaciteit zullen ook in ons land niet volstaan om kwetsbaarheden weg te werken: aansluiten bij het grensoverschrijdend distributienetwerk hoort bij de noden, maar verhoogt tegelijk de complexiteit van de bescherming van die infrastructuur.

Tot de vaststelling gekomen dat zowel met betrekking tot definiëring van de problematiek als de zoektocht naar oplossingen, de bescherming van kritieke energie infrastructuur een multi departementaal, multidisciplinair en multilateraal probleem is waarvan de complexiteit enkel toeneemt, daagt het besluit dat de tendens om te desinvesteren in onderzoek en ontwikkeling indruist tegen de rationele genese van de oplossing ervan: het samenwerkingsverband tussen Defensie, industrie en wetenschap, moet daarom worden gesteund. Enkel die benadering zal ervoor zorgen dat op een rationele manier de optimale bescherming van deze complexe problematiek tot een goed einde wordt gebracht en dit op alle vereiste niveaus: regionaal, nationaal en supranationaal.

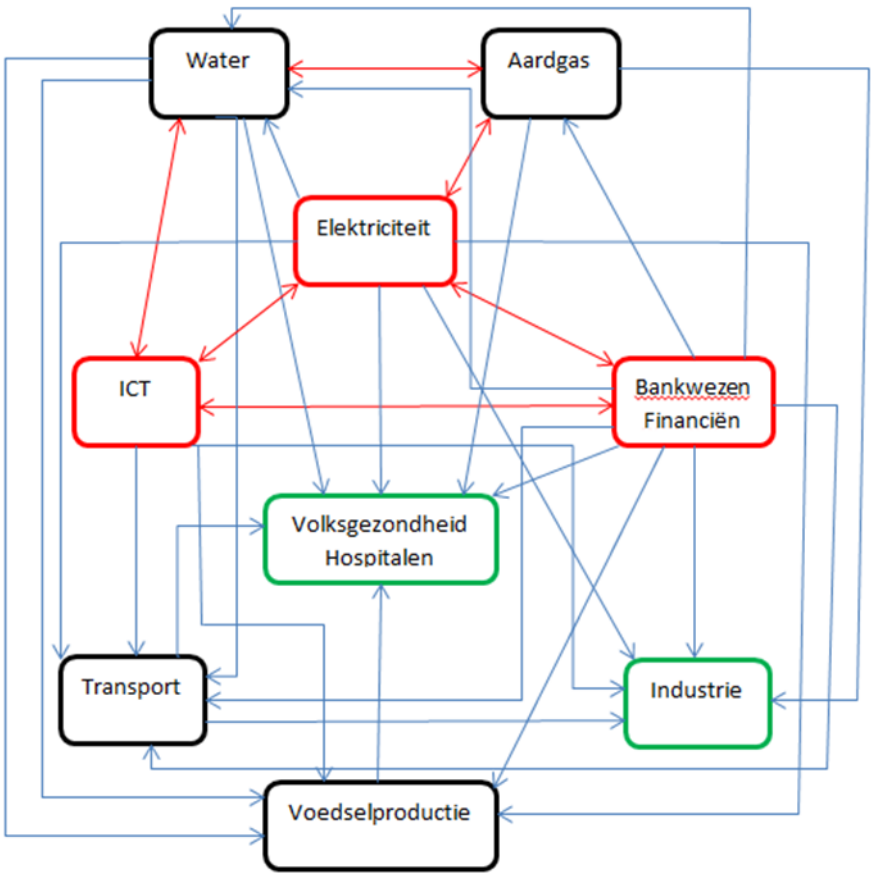
Bijlagen

Bijlage 1: Sites en toedracht van domeinen

Aantal sites, relatieve toedracht van de domeinen en lokalisatie (Clemente, 2013; p.22)

Telecommunicatie:	29%
Energie:	17%
Farmacie:	14%
Grenzen:	9%
Mineralen:	8%
Havens:	6%
Militaire installaties:	4%
Industrie:	4%
Zeevaart (doorvaart):	5%
Dammen:	4%

Bijlage 2: Terugkoppeling hogere orde cascade



Bron: naar OECD, 2011; p.62.

Bijlage 3: Corridors van energie infrastructuur

PRIORITAIRE CORRIDORS EN GEBIEDEN VOOR ENERGIE-INFRASTRUCTUUR

Deze verordening is van toepassing op de volgende prioritaire corridors en gebieden van de trans-Europese energie-infrastructuur:

1. PRIORITAIRE ELEKTRICITEITSCORRIDORS

1. Offshore-elektriciteitsnetwerk in de noordelijke zeeën („NSOG"): ontwikkeling van een geïntegreerd offshore-elektriciteitsnetwerk en de daaraan gekoppelde interconnectoren in de Noordzee, de Ierse Zee, het Kanaal, de Oostzee en de naburige wateren om elektriciteit uit hernieuwbare offshore-energiebronnen te transporteren naar centra van verbruik en opslag en om de grensoverschrijdende uitwisseling van elektriciteit te bevorderen.

   Betrokken lidstaten: België, Denemarken, Frankrijk, Duitsland, Ierland, Luxemburg, Nederland, Zweden, het Verenigd Koninkrijk.

2. Noord-zuid elektriciteitsinterconnecties in West-Europa („NSI-West Electricity"): interconnecties tussen lidstaten van de regio onderling en met de mediterrane regio, met inbegrip van het Iberisch schiereiland, met name met het oog op de integratie van elektriciteit uit hernieuwbare energiebronnen en de versterking van de interne netwerkinfrastructuren om de marktintegratie in de regio te bevorderen.

   Betrokken lidstaten: Oostenrijk, België, Frankrijk, Duitsland, Ierland, Italië, Luxemburg, Nederland, Malta, Oostenrijk, Portugal, Spanje, het Verenigd Koninkrijk.

3. Noord-zuid elektriciteitsinterconnecties in middenoostelijk en zuidoostelijk Europa („NSI–East Electricity"): interconnecties en interne lijnen in noord-zuidelijke en oost-westelijke richting met het oog op de voltooiing van de interne markt en de integratie van uit hernieuwbare bronnen opgewekte elektriciteit.

   Betrokken lidstaten: Oostenrijk, Bulgarije, Kroatië [1], Tsjechië, Cyprus, Duitsland, Griekenland, Hongarije, Italië, Polen, Roemenië, Slowakije, Slovenië.

4. Interconnectieplan voor de energiemarkt in het Oostzeegebied voor elektriciteit („BEMIP Electricity"): interconnecties tussen lidstaten in de Oostzeeregio en dienovereenkomstige versterking van de interne netwerkinfrastructuur teneinde het isolement van de Oostzeelanden te beëindigen en de marktintegratie te bevorderen, onder andere door aan te sturen op de integratie van uit hernieuwbare bronnen opgewekte energie in de regio.

   Betrokken lidstaten: Denemarken, Estland, Finland, Duitsland, Letland, Litouwen, Polen, Zweden.

2. PRIORITAIRE GASCORRIDORS

5. Noord-zuid-gasinterconnecties in West-Europa („NSI-West Gas"): gasinfrastructuur voor noord-zuid-gasstromen in West-Europa met het oog op een verdere diversificatie van voorzieningsroutes en de uitbreiding van de leverbaarheid van gas op korte termijn.

   Betrokken lidstaten: België, Denemarken, Frankrijk, Duitsland, Ierland, Italië, Luxemburg, Malta, Nederland, Portugal, Spanje, het Verenigd Koninkrijk.

6. Noord-zuid-gasinterconnecties in middenoostelijk en zuidoostelijk Europa („NSI-East Gas"): gasinfrastructuur voor regionale verbindingen tussen en in de Oostzeeregio, de Adriatische en Egeïsche Zee, de oostelijke Middellandse Zee en de Zwarte Zee, en om de diversificatie en de zekerheid van de gasvoorziening te versterken.

   Betrokken lidstaten: Oostenrijk, Bulgarije, Kroatië [1], Cyprus, Tsjechië, Duitsland, Griekenland, Hongarije, Italië, Polen, Roemenië, Slowakije, Slovenië.

7. Zuidelijke gascorridor („SGC"): infrastructuur voor de transmissie van gas van het Kaspische Zeebekken, Centraal-Azië, het Midden-Oosten en het bekken van de oostelijke Middellandse Zee naar de Unie teneinde de diversificatie van de gasvoorziening te versterken.

[1] Onder voorbehoud van toetreding en vanaf de toetredingsdatum van Kroatië.

Betrokken lidstaten: Oostenrijk, Bulgarije, Kroatië (1), Tsjechië, Cyprus, Frankrijk, Duitsland, Hongarije, Griekenland, Italië, Polen, Roemenië, Slowakije, Slovenië;

8. Interconnectieplan voor de energiemarkt in het Oostzeegebied voor gas („BEMIP Gas"): gasinfrastructuur teneinde het isolement van de drie Oostzeelanden en Finland, alsook hun afhankelijkheid van één leverancier te beëindigen, om de interne netwerkinfrastructuur dienovereenkomstig te versterken en om de diversificatie en de zekerheid van de voorziening in de Oostzeeregio te vergroten.

   Betrokken lidstaten: Denemarken, Estland, Finland, Duitsland, Letland, Litouwen, Polen, Zweden.

3. PRIORITAIRE OLIECORRIDOR

9. Olievoorzieningsverbindingen in middenoostelijk Europa („OSC"): interoperabiliteit van het oliepijpleidingsnetwerk in middenoostelijk Europa teneinde de voorzieningszekerheid te versterken en de milieurisico's te verminderen.

   Betrokken lidstaten: Oostenrijk, Kroatië (1), Tsjechië, Duitsland, Hongarije, Polen, Slowakije.

4. PRIORITAIRE THEMATISCHE GEBIEDEN

10. Uitrol van slimme netwerken: invoering van technologieën voor slimme netwerken in het geheel van de Unie teneinde het gedrag en de acties van alle met het netwerk verbonden gebruikers op efficiënte wijze te integreren, met name de opwekking van grote hoeveelheden elektriciteit uit hernieuwbare of gedecentraliseerde energiebronnen en vraagrespons van klanten.

    Betrokken lidstaten: alle.

11. Elektriciteitssnelwegen: eerste elektriciteitssnelwegen in 2020 met het oogmerk een elektriciteitssnelwegsysteem in het geheel van de Unie uit te bouwen dat in staat is om:

    a) het aanzwellende surplus aan windenergie in en rond de noordelijke zeeën en de Oostzee en de toenemende hernieuwbare elektriciteitsproductie in Oost- en Zuid-Europa alsmede Noord-Afrika op te vangen;

    b) deze nieuwe productiehubs te verbinden met de grote opslagfaciliteiten in de noordelijke landen en de Alpen en andere regio's met grote verbruikscentra, en

    c) een steeds variabeler en gedecentraliseerder elektriciteitsaanbod en een flexibele elektriciteitsvraag te ondervangen.

    Betrokken lidstaten: alle.

12. Grensoverschrijdend koolstofdioxidenetwerk: ontwikkeling van een infrastructuur voor het transport van koolstofdioxide tussen lidstaten onderling en met naburige derde landen met het oog op de tenuitvoerlegging van koolstofdioxideafvang en -opslag.

    Betrokken lidstaten: alle.

(1) Onder voorbehoud van toetreding en vanaf de toetredingsdatum van Kroatië.

Bron: Verordening (EU) Nr.437/2013 van het Europees parlement en de Raad van 17 april 2013; Bijlage I p.115/62

Bijlage 4: Categorieën energie infrastructuur

CATEGORIEËN ENERGIE-INFRASTRUCTUUR

De energie-infrastructuurcategorieën die moet worden ontwikkeld om de in bijlage I genoemde prioriteiten qua energie-infrastructuur ten uitvoer te leggen, zijn de volgende:

1. Elektriciteit:
   a) bovengrondse hoogspanningstransmissielijnen, mits zij zijn ontworpen voor een spanning van 220 kV of meer, en ondergrondse of onder de zee lopende transmissiekabels, mits zij zijn ontworpen voor een spanning van 150 kV of meer;
   b) wat met name elektriciteitssnelwegen betreft, alle fysieke uitrusting die is ontworpen om het transport van elektriciteit over het hoogspannings- of ultrahoogspanningsnetwerk mogelijk te maken met het oog op de verbinding van grote hoeveelheden elektriciteit, opgewekt of opgeslagen in verscheidene lidstaten of derde landen, met grootschalig elektriciteitsverbruik in één of meer andere lidstaten;
   c) elektriciteitsopslagfaciliteiten gebruikt voor de permanente of tijdelijke opslag van elektriciteit in boven- of ondergrondse infrastructuur of geologische locaties, mits zij direct zijn verbonden met hoogspanningstransmissielijnen ontworpen voor een spanning van 110 kV of meer;
   d) elke uitrusting of installatie die essentieel is om ervoor te zorgen dat de in a) t/m c) omschreven systemen op een veilige, beveiligde en efficiënte wijze kunnen functioneren, met inbegrip van beschermings-, monitorings- en toezichtssystemen op alle spanningsniveaus en onderstations;
   e) elke uitrusting of installatie, zowel op transmissie- als op middenspanningsdistributieniveau, waarmee digitale tweewegscommunicatie, realtime of bijna realtime, interactieve en intelligente monitoring en sturing van elektriciteitsproductie, -transmissie, -distributie en -verbruik binnen een elektriciteitsnetwerk wordt beoogd met het oog op de ontwikkeling van een netwerk dat op een efficiënte wijze het gedrag en de acties van alle met het netwerk verbonden gebruikers — producenten, consumenten en die welke beide doen — integreert om zo een economisch efficiënt en duurzaam elektriciteitssysteem tot stand te brengen met slechts beperkte verliezen, van hoge kwaliteit, met grote voorzieningszekerheid en goed beveiligd.
2. Gas:
   a) transmissiepijpleidingen voor het transport van aardgas en biogas die deel uitmaken van een netwerk dat grotendeels bestaat uit hogedrukpijpleidingen, exclusief hogedrukpijpleidingen die worden gebruikt voor de upstream- of lokale distributie van aardgas;
   b) met de hierboven bedoelde hogedrukgaspijpleidingen verbonden ondergrondse opslagfaciliteiten;
   c) faciliteiten voor de ontvangst, opslag en hervergassing of decompressie van vloeibaar gemaakt aardgas (lng) of gecomprimeerd aardgas (CNG);
   d) elke uitrusting of installatie die essentieel is voor een veilige, beveiligde en efficiënte uitbating van het systeem of om een bidirectionele capaciteit mogelijk te maken, met inbegrip van compressorstations;
3. Olie:
   a) pijpleidingen gebruikt voor het transport van ruwe aardolie;
   b) pompstations en opslagfaciliteiten die vereist zijn voor de werking van pijpleidingen voor ruwe aardolie;
   c) elke uitrusting of installatie die essentieel is om het mogelijk te maken dat het systeem in kwestie op een behoorlijke, veilige en efficiënte wijze functioneert, met inbegrip van beschermings-, monitorings- en toezichtssystemen en reverse-flow-apparatuur.
4. Koolstofdioxide:
   a) specifieke pijpleidingen, die niet tot het upstream-pijpleidingsnetwerk behoren, gebruikt voor het transport van koolstofdioxide van menselijke oorsprong uit meer dan één bron, d.w.z. industriële installaties (inclusief elektriciteitscentrales) die koolstofdioxidegas produceren ten gevolge van verbranding of andere chemische reacties waarbij verbindingen betrokken zijn die koolstof van al dan niet fossiele aard bevatten, met het oog op de permanente geologische opslag van die koolstofdioxide overeenkomstig Richtlijn 2009/31/EG van het Europees Parlement en de Raad [1];
   b) faciliteiten voor het vloeibaar maken en voor de bufferopslag van koolstofdioxide met het oog op het verdere transport ervan. Dit omvat niet de infrastructuur binnen een geologische formatie die wordt gebruikt voor de permanente geologische opslag van koolstofdioxide overeenkomstig Richtlijn 2009/31/EG en de daarmee verband houdende injectiefaciliteiten en andere faciliteiten aan de oppervlakte;
   c) elke uitrusting of installatie die essentieel is om het mogelijk te maken dat het systeem in kwestie op een behoorlijke, veilige en efficiënte wijze functioneert, met inbegrip van beschermings-, monitorings- en toezichtssystemen.

[1] PB L 140 van 5.6.2009, blz. 114.

Bron: Verordening (EU) Nr.437/2013 van het Europees parlement en de Raad van 17 april 2013; Bijlage II p.115/64

Bibliografie

Bibliografie

Albrecht, Johan en Ruben Laleman. *Hoe sterk stijgt de –uitstoot na de kernuitstap?* 25 juni 2015. Universiteit Gent.

Bipartizan Policy Center. 2014. Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat. A report from the Co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative. Beschikbaar via http://bipartisanpolicy.org/ geraadpleegd 22 juni 2015.

Birol, Fatih. World Energy Outlook 2014. International Energy Agency. Brussels, 2015. Geraadpleegd op 25 november 2015. Beschikbaar via http://www.iea.org/textbase/npsum/weo2014sum.pdf

Buckley, Chris. *China Burns Much More Coal Than Reported, Complicating Climate Talks In:* The New York Times. 03 November 2015. Geraadpleegd op 04 November 2015 beschikbaar via http://www.nytimes.com.

Butrimas Vytautas and Audrius Bruzga. *The Cyber Security Dimension of Critical Energy Infrastructure*. Concordiam. Energy Security. Vol 3, issue 4; 2012.

BSA. 2015. The EU Cyber security dashboard. A path to secure European Cyberspace. Washington DC. 2015.

CCD CoE. 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. Centre for Cyber Defence Centre for Excellence. Cambridge University Press. 2013

Clemente, Dave. 2006. Cyber Security and Global Interdependence: What Is Critical? Chatham House. February 2013.

Cogan, Kevin. 2011. In The Dark: Military Planning for a Catastrophic Critical Infrastructure Event. US Army War College. Carlisle Pennsylvania. Study 2-11. May 2011.

Cornell, Philip. *NATO and energy security*. In: Understanding NATO in the 21st century. Edited by Graeme P.Herd and John Kriendler. Routlegde 2013. p.192.

Cyber security strategy. Securing cyberspace 2012. Beschikbaar via https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_BE_NCSS.pdf. Geraadpleegd op 22 juli 2015.

Department of Homeland Security (DHS), Office of Inspections and General Reviews. 2006. Progress in Developing the National Asset Database. Beschikbaar via http://www.nytimes.com/packages/pdf/politics/20060711_DHS.pdf. Geraadpleegd op 8 oktober 2015.

Dlouhy, Jennifer A. 2013. In *Utility executives: Major cyberattack on power grid is inevitable.* Beschikbaar via http://fuelfix.com/blog/2013/08/06/utility-executives-major-cyberattack-on-power-grid-is-inevitable/. Geraadpleegd op 22 juli 2015.

Donnelly, Marie. Director. DG Energy of the European Commission. A new departure for the EU. Brussels Think Tank dialogue-State of the Union 2015. Conference co-organised by Egmont Institute on 28 January 2015.

EDAM. Nuclear Security: a Turkish Perspective. Center for Economics and Foreign Policy Studies, 2015.

Egmont conference. Energy transition: A Multifaceted Challenge for Europe. Securing Europe's electricity supply. 05 Mai 2015.

Electric Grid Cybersecurity Initiative. 2014. *Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat*. Bipartizan Policy Centre. February 2014.

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.

Energy Sector Control Systems Working Group (ESCSWG). September 2011. Roadmap to achieve energy delivery systems cybersecurity. Beschikbaar via http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf. Geraadpleegd op 01 april 2015.

European Commission. Communication form the commission tot the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2011) 885 final. Energy Roadmap 2050. Brussels, December 2011.

European Commission. Commission Staff Working Document. SWD(2013) 318 final. On a new approach to the European Programme for Critical

Infrastructure Protection Making European Critical Infrastructures more secure. Brussels, August 2013.

European Commission. 2013. Joint communication to the European Parliament, the Council, the European economic and social committee and the committee of the regions. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Geraapleegd op 27 juli 2015. Beschikbaar via http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission. 2014. European Energy Security Strategy. COM(2014)330 final. Geraadpleegd op 21 oktober 2015. Beschikbaar via https://ec.europa.eu/energy/en/topics/energy-strategy/2050-energy-strategy.

Europees Economisch en Sociaal Comité over de mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's-Stappenplan Energie 2050. 2012. (2012/C 229/25). Geraadpleegd op 29 oktober 2015. Beschikbaar via http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52012AE1315

Federaal Agentschap voor Nucleaire Controle, 2011. "Belgian Stress tests" specifications applicable to power reactors. Beschikbaar via http://www.fanc.fgov.be/GED/00000000/2800/2847.pdf. Geraadpleegd op 14 oktober 2015.

Federaal Regeerakkoord. 2014. Beschikbaar via http://www.demorgen.be/bijlagen/2723.pdf. Geraadpleegd op 15 oktober 2015.

Hohlmeyer, Monika. 2015. Intervention at the Conference "Trends in Combatting Cybercrime-Key considerations for the European Parliament". Representation of the State of Hessen to the European Union. 2 June 2015.

Homeland Security. Department of Energy. 2007. Energy; Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan. Beschikbaar via http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Energy_SSP_Public.pdf geraadpleegd op 10 april 2015.

ICS-CERT Monitor, 2013. ICS-CERT Monitor October, November, December 2013. Industrial Control System Cyber Emergency Response Team. Department of Homeland Security. National Cyber Security and Communication Integration Centre. Geraadpleegd op 17 juni 2015. Beschikbaar via https://ics-cert.us-cert.gov/monitors.

ICS-CERT, 2013. ICS-CERT Year in review. Industrial Control System Cyber Emergency Response Team. Department of Homeland Security. National Cyber Security and Communication Integration Centre. Geraadpleegd op 17 juni 2015. Beschikbaar via https://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf

ICS-CERT, 2014. ICS-CERT Year in review. Industrial Control System Cyber Emergency Response Team. Department of Homeland Security. National Cyber Security and Communication Integration Centre. Geraadpleegd op 17 juni 2015. Beschikbaar via https://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2014_Final.pdf

Kanselarij van de Eerste Minister. 2012. Cyber Security Strategy. Erkennen van de cyber dreiging; verbeteren van de veiligheid; kunnen reageren op incidenten. Beschikbaar via https://ccdcoe.org/strategies/BEL-CyberStrat%202012.PDF. Geraadpleegd op 28 juli 2015.

Kamer van Volksvertegenwoordigers. 2014. Algemene Beleidsnota Veiligheid en Binnenlandse Zaken. 4 december 2014. Beschikbaar via http://jambon.belgium.be/sites/default/files/articles/54K0588016.pdf. Geraadpleegd op 12 oktober 2015.

Lovins, 1982. *Brittle Power. Energy Strategy for National Security*. Brick House Publishing, Massachussets.

Macguinness, Meghan. 2014. *A new organization for cybersecurity across the electric grid*. Bulletin of the Atomic Scientists. Beschikbaar via https://www.google.be/?gws_rd=ssl#q=bulletin+of+atomic+scientists Geraadpleegd op 9 juni 2015.

Matheu, Michel. 2015. EDF statement during the Symposium co-organised by Egmont and Development group on Energy transition: A multifaceted Challenge for Europe. Securing Europe's electricity supply-Making the switch towards an integrated and long-term approach. May 2015.

NATO, 2010. Active engagement, Modern Defence. Strategic Concept, 19 November 2010. Beschikbaar via http://www.nato.int/cps/en/natolive/official_texts_68580.htm. Geraadpleegd op 26 augustus 2015.

NATO, 2014. Wales Summit declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. Beschikbaar via http://www.nato.int/cps/en/natohq/official_texts_112964.htm. Geraadpleegd op 11 augustus 2015.

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

Petkevicius, Romualdas. 2012. Critical Energy Infrastructure Protection. Advanced Research Workshop. 13-14 November 2012, Ankara, Turkey.

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.

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.

Rühle, Michael. 2011. NATO and energy security. Beschikbaar via http://www.nato.int/docu/review/2011/climate-action/energy_security/EN/index.htm. Geraadpleegd op 26 augustus 2015.

Salmon, Doug and Mark Zeller, Armando Guzmán, Venkat Mynam, and Marcos Donolo. *Mitigating the Aurora Vulnerability With Existing Technology*. Presented at the 64th Annual Georgia Tech Protective Relaying Conference Atlanta, Georgia.

SCK.CEN. Studiecentrum voor kernenenergie. *Stress Test*. SCK.CEN. Juni 2012.

Senate Armed Services Committee (SASC). Clapper, James R., 2015. Worldwide Threat Assessment of the US Intelligence Community. February, 2015.

Smedts, Bart. 2010. Bescherming van de nationale kritische infrastructuur tegen een dreiging tot asymmetrische proliferatie. Koninklijk Hoger Instituut voor Defensie, april 2010.

Smedts, Bart. 2015. Civiel gebruik van kernenergie en militaire proliferatie: actoren en belangen. Koninklijk Hoger Instituut voor Defensie, juni 2015.

Symantec. How to protect critical infrastructure, mitigate fraud and guarantee privacy. New threats in the energy sector. Geraadpleegd op 19 juni 2015. Beschikbaar via https://www.google.be/?gws_rd=ssl#q=Symantec.

Symantec. Security Response. Targetted Attacks Against the Energy Sector. 2014. Version 1.0, January 2013. Geraadpleegd op 30 april 2015. Beschikbaar via http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf

Tanaka, Nobuo. 2015. Energy Security and sustainable nuclear power. Sasakawa Peace Foundation. 7 oktober 2015. Geraapleegd op 24 november 2015. Beschikbaar via https://www.icef-

forum.org/annual_2015/speakers/october7/cs1/ne/pdf/cs-1_20050-1_nobuo_tanaka.pdf

Kritieke energie infrastructuur: kadrering en afhankelijkheden.

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

Het belang van distributiesystemen als onderdeel van kritieke energie infrastructuur, hun fysische en cybernetische bescherming, maar ook andere structurele maatregelen zoals diversificatie en energie efficiëntie winnen aan belang in een beschermingsstrategie. Met de VS als model en aanzetten in elk van de domeinen op EU-niveau, gaan we in deze studie na welke de stand van zaken in België is en welke de toedracht van Belgische Defensie met betrekking tot het onderwerp zou kunnen zijn. A-dogmatische diversificatie van bronnen en capaciteit is noodzakelijk om de kwetsbaarheid te verlichten, maar zal tegelijkertijd de complexiteit van het veiligheidsbeleid doen toenemen. Deze complexiteitsdynamiek onderstreept de nood om de desinvesteringstendens in onderzoek en ontwikkeling in dit kader te herzien.

Voor deze en andere publicaties:
www.khid.be